

Celestix WSA SSL VPN Appliance
with SecurEnvoy server installed on the same appliance

Contact information		
SecurEnvoy	www.securenvoy.com	0845 2600010
	1210 Parkview Arlington Business Park Theale Reading RG7 4TY	
Andy Kemshall	akemshall@securenvoy.com	
Version	1.0	
Date	20 th Aug 2007	

This guide is based on a Celestix WSA 3000 appliance which has Microsoft IAG and ISA server pre-Install.

Software Pre-Installed:

Microsoft IAG (Whale) Version 3.7.0.0.14
Microsoft ISA Server Version 5.0.5720.100

SecurEnvoy Software to be Install

SecurAccess Version v4.1.501

Overview

This integration guide shows how to install the SecurEnvoy server on the Celestix Appliance and 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 should be already configured to authenticate a Microsoft (or other) *password* (in this example the authentication server is called *dev.com*)

A Microsoft or Novell Domain must be available with an administration account that can write to the users Telex Number fields, see Install and Administration Guide Section 15.4 for more information.

A method for sending SMS texts

Option 1 Use a SMS Modem, supported devices include the Wavecom fasttrack or Siemens T35 modem. You will also need a mobile phone SIM card.

Option 2 Use a Web SMS Service with a SecurEnvoy Trial License (Build in SecurEnvoy HSL gateway account for testing) or setup an account with HSL www.hslsms.com

2. Installing SecurEnvoy

Install the SecurEnvoy server

This can be downloaded from www.securenvoy.com/trial.aspx

After the advanced conf program starts enter the following:

Web Server **http://localhost:6001**

Supports https (**un-check this**)

Domain Name: enter the name of your Microsoft Domain in this example dev.com
Search for DN: If you have joined the Celestix box to a domain and logged in with a domain admin account, use this tool to lookup the distinguished name of your SecurEnvoy admin account. If not ignore this tool.

Admin UserID: If you have not used the Search for DN tool and wish to use the default "Administrator" account press "Example".
If you wish to use a different administrator account, enter the distinguished name of this user.
Password: Enter the password for the Admin Account
Re-Enter Password: Re-enter this password

Server1: Enter the IP address of one of your domain controllers and press "Test Server1" you should get the message "OK"

Server2: Optional for resilience, enter the IP address of a second domain controller and press "Test Server2" you should get the message "OK"

If you wish to manage additional domain press "Add/Edit Next Domain" and repeat the above for the next domain. If not press "Continue"



The screenshot shows the "Secure Server Configuration" window in SecurEnvoy. The window title is "SecurEnvoy Secure Server". The main heading is "Secure Server Configuration". Below the heading, there is a text field for "Enter This Hosts Webserver's Name (Example: www.mycompany.com)". The "Web Server" section has a text field for "http://" containing "localhost:6001" and a checkbox for "Supports https" which is unchecked. The "Select Directory Type" section has two radio buttons: "Microsoft Active Directory" (selected) and "Novell eDirectory". The "Primary Domain Name (Example mycompany.com)" section has a text field for "Domain Name" containing "dev.com". The "Search for DN" section has a text field for "Enter UserID Below" containing "Administrator" and a "Get DN of UserID" button. The "Directory Administrator Account Distinguished Name (DN)" section has a text field for "Admin UserID" containing "CN=Administrator,CN=Users,DC=dev,DC=com" and an "Example" button. The "Password" and "Re-Enter Password" fields are masked with asterisks. The "Directory Server Details" section has two text fields for "Server1 Name" (containing "192.168.99.10") and "Server2 Name" (empty), each with a "Use SSL" checkbox. Below the "Server2 Name" field is the text "Leave Blank for only one Server". On the right side, there is a "Test" section with a text area containing "OK" and two buttons: "Test Server1" and "Test Server2". At the bottom, there are three buttons: "Skip", "Add/Edit Next Domain", and "Continue".

Setup the SMS Gateway:

Option 1 (SMS Modem)

Country Dial Code: Enter the country dial code for this servers location for example in the US enter 1 or for the UK enter 44.

If you wish to use a SMS Modem, setup the following or press "Continue" and skip to Option 2 Web Gateway.

Plug the modem into serial port located an the back of the Celestrix Appliance
Make sure you have an active SIM card with no SIM PIN set.

Check "Enable Phone Gateway1 Server

If you have a Vodafone SIM card check "Vodafone Sim:"

Enter Serial Port: **2** (the real of the Celestix appliance is com2)

Press the "Test Modem" button

You some get a +CSQ: and a number from 0 to 31 that defines the signal strength then OK



The screenshot shows the 'SecurEnvoy Phone Gateway1 Configuration' window. At the top, there is a blue header with the SecurEnvoy logo. Below the header, the title 'Phone Gateway1 Configuration' is centered. A checkbox labeled 'Enable Phone Gateway1 Service' is checked. Below this, a note says 'Connect The Mobile Phone Modem To a Serial Port and Power On'. There are four configuration fields: 'Vodafone Sim:' with an unchecked checkbox, 'Enter Serial Port:' with a text box containing '2', 'Enter Baud Rate:' with a dropdown menu set to '115200', and 'Country Dial Code:' with a text box containing '44'. A small text box next to the Country Dial Code field provides an example: 'International Contry Dial Code for this server's location Example UK=44, USA=1, Sweden=46'. Below these fields is a 'Text Modem' section containing a 'Test Modem' button and a text area showing the output: 'Modem Returned: (signal strength from 0 to 31) AT+CSQ +CSQ: 20,5 OK'. At the bottom of the window are 'Skip' and 'Continue' buttons.

Option 2 (Web Gateway or trial with no modem)

If you have not installed a modem and wish to use a trial license or live web SMS gateway account setup the following, else un-check "Enable Web SMS Gateway Service", press "Continue" and "Continue" again after Radius Server Configuration is displayed then skip to section 3 SecurEnvoy Post Install Settings.

Add the web gateway URL as a trusted site to the Microsoft ISA server as follows:

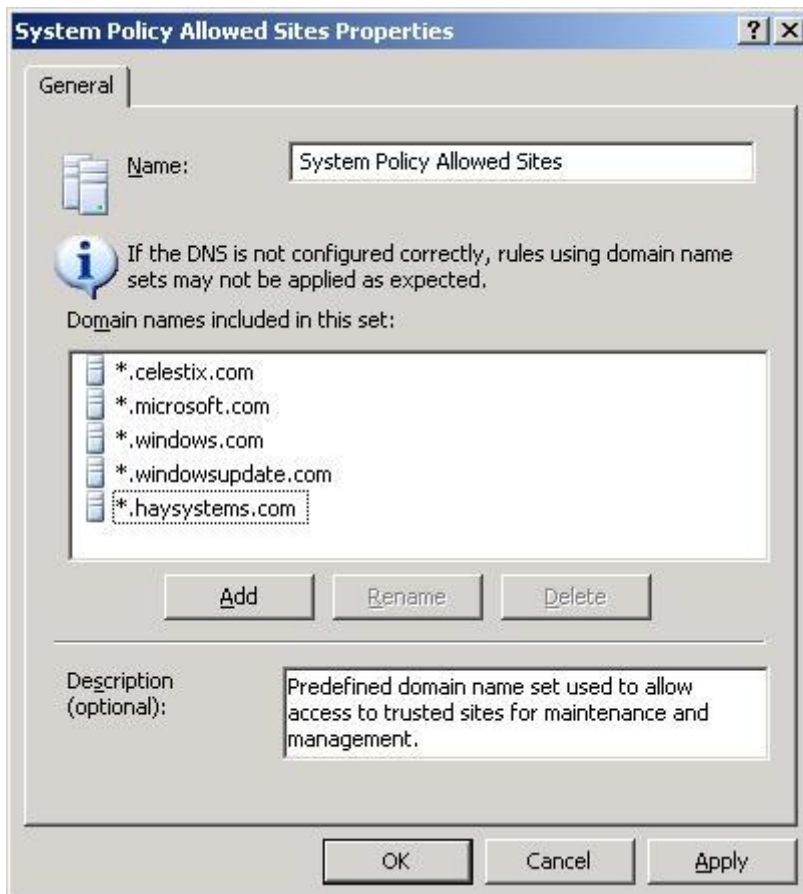
Start ISA Server Management

On the Right under System Policy Tasks select "Edit System Policy"

Select the Configuration Group "Various" at the bottom and select "Allowed Sites"

Select the tab "To" and Edit "System Policy Allowed Sites"

Press Add and enter *.haysystems.com to trust the HSL SMS Gateway servers.



Press "Apply" to save changes and update the ISA server configuration.

Switch back to the SecurEnvoy Advanced Conf Window

Check "Enable Web SMS Gateway Service"

If this is a Live SecurEnvoy License, enter the UserID and Password of your SMS web provider in this example, an HSLSMS account.

Level the Web Proxy Address setting blank as the Celestix Appliance has a direct connection to the internet.

Press the "Test Gateway" button, you should see the message "Web Gateway Responded OK"

Press "Continue" and "Continue" again after Radius Server Configuration is displayed.



The screenshot shows the SecurEnvoy WEB SMS Gateway Configuration window. At the top, the SecurEnvoy logo is displayed. Below the logo, the title "WEB SMS Gateway Configuration" is centered. Underneath the title, there is a checkbox labeled "Enable Web SMS Gateway Service" which is checked. A red warning message states: "This is a Trial License and is limited to 50 SMS Messages".

The configuration section includes:

- Country Dial Code:** A text box containing "44". To its right, a note reads: "International Contry Dial Code for this server's location Example UK=44, USA=1, Sweden=46".
- Web Proxy Address:** An empty text box.
- Port:** An empty text box.
- To the right of the proxy fields, a note says: "Leave Both Blank If Proxy Isn't Required".

Below the configuration fields is a "Text Web Gateway" section. It contains a "Test Gateway" button. Below the button is a text area showing the output of the test: "Connecting To Web Gateway, Please Wait" followed by "Web Gateway Responded OK".

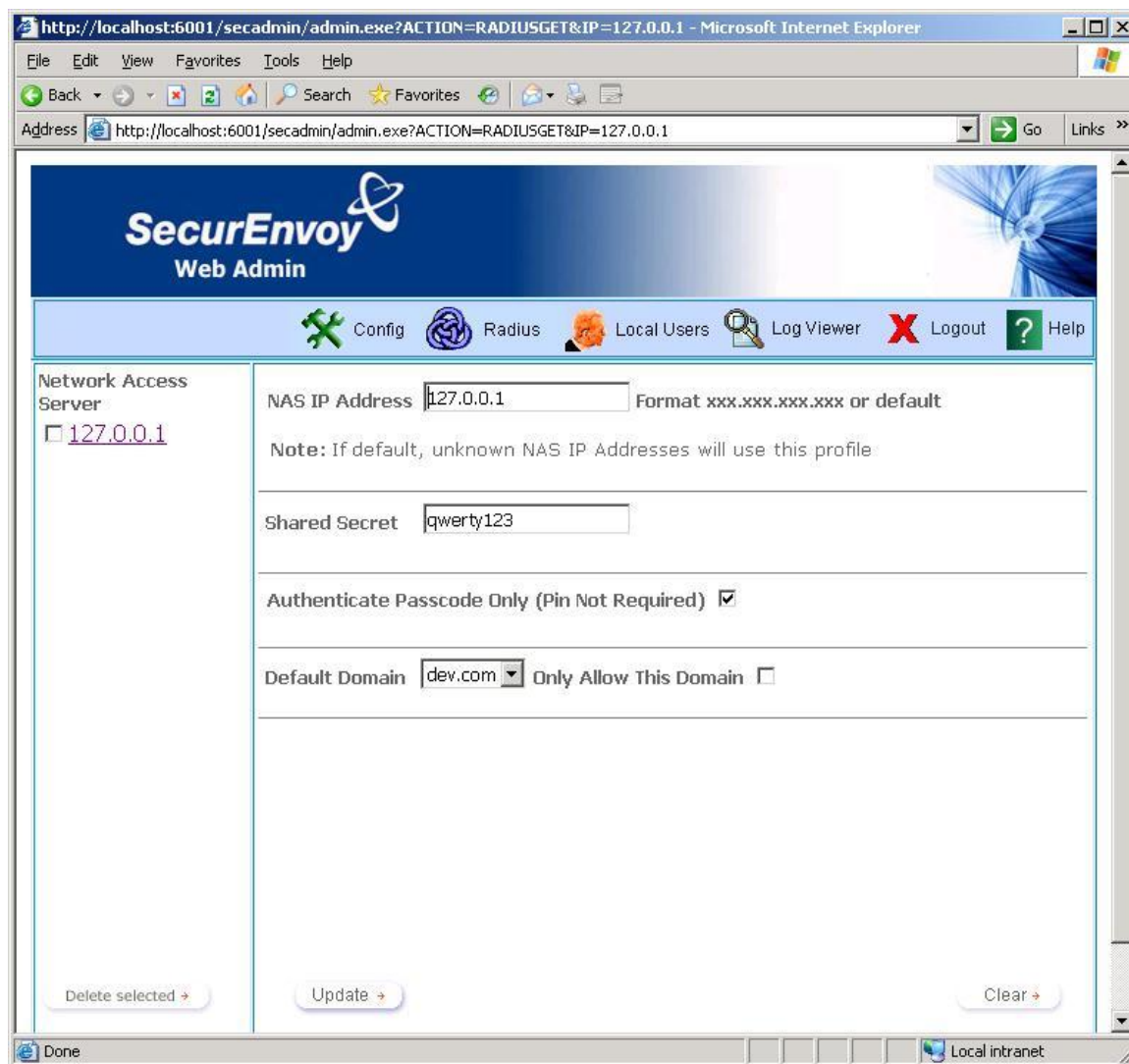
At the bottom of the "Text Web Gateway" section, there is a blue hyperlink: "[Open Browser To WEB Gateway Server One](#)" and a note: "Should Return 'FAIL AUTH'".

At the very bottom of the window, there are two buttons: "Skip" on the left and "Continue" on the right.

3. SecurEnvoy Post Install Settings

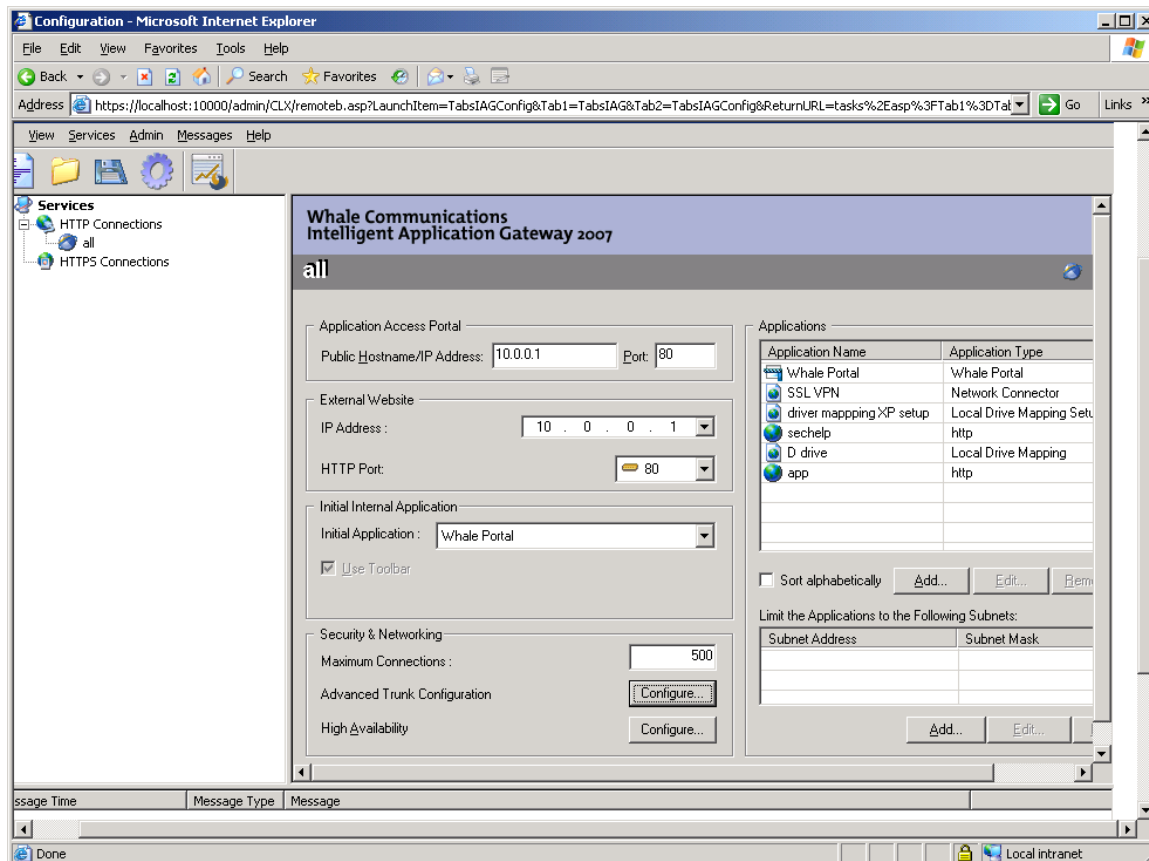
Setup a user for one time authentication.

Select the "Radius" menu option and enter 127.0.0.1 as the IP Address. Enter a shared secret (this can be any password you like) and select "Authenticate Passcode Only" option.



4. 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 **127.0.0.1**

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).

Edit Server

Type: RADIUS

Name: SecurEnvoy SMS

IP/Host: 127.0.0.1

Port: 1812

Alternate IP/Host:

Alternate Port: 1812

Secret Key: *****

Support Challenge Response

Use a Different Server for User/Group Authorization

Select Server: Built-In Users/Groups

Extract User's Groups from RADIUS Attribute

Attribute Type: 25

Attribute Format: ou=<group>;

Application Access Portal | URL Insp

General | Authentication

Authenticate User on Session Login

Select Authentication Servers:

dev.com	
SecurEnvoy SMS	

Add..

Remove

↑ ↓

User Selects From a List of Servers

Show Server Names

User Must Provide Credentials for Each Selected Server

Use the Same User Name

Enable Users to Add Credentials On-the-Fly

Enable Users to Change Their Passwords

Notify User 7 Days Prior to Expiration

Enable Users to Manage Their Credentials

Enable Users to Select Language

Login Page: Login.asp

On-the-Fly Login Page: Login.asp

Permitted Authentication Attempts: 3

Block Period: 0 Minutes

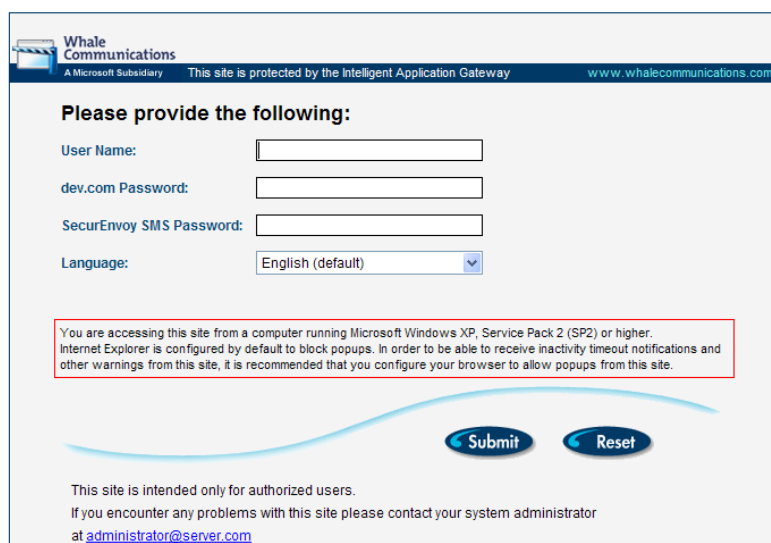
5. Testing Authentication

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 page for Whale Communications. At the top, it says "Whale Communications" and "A Microsoft Subsidiary". Below that, it says "This site is protected by the Intelligent Application Gateway" and "www.whalecommunications.com". The main heading is "Please provide the following:". There are four input fields: "User Name:", "dev.com Password:", "SecurEnvoy SMS Password:", and "Language:" (with a dropdown menu set to "English (default)"). Below the fields is a red-bordered box with a warning: "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 inactivity timeout notifications and other warnings from this site, it is recommended that you configure your browser to allow popups from this site." At the bottom of the form are two buttons: "Submit" and "Reset". Below the buttons, it says "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".

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