

External Authentication with Array Networks SPX SSL/VPN Appliance

Authenticating Users Using SecurAccess Server by SecurEnvoy

Contact information		
SecurEnvoy	www.securenvoy.com	0845 2600010
	1210 Parkview Arlington Business Park Theale Reading RG7 4TY	
Phil Underwood	Punderwood@securenvoy.com	
ArrayNetworks INC	www.arraynetworks.net	001-866-692-7729
	Array Networks, Inc. 1371 McCarthy Blvd. Milpitas, CA 95035 U.S.A.	
Simon McNally	Smcnally@arraynetworks.net	

Array Networks SPX Integration Guide

This document describes how to integrate an Array Networks SPX SSL/VPN appliance with SecurEnvoy two-factor Authentication solution called 'SecurAccess'.

Array Networks SPX SSL/VPN appliance provides Secure Remote Access to the internal corporate network for all Client/Server applications.

SecurAccess provides two-factor, strong authentication for remote Access solutions (such as Array SSL/VPN), 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.

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. As SecurEnvoy can integrate well with the Active Directory the PIN can be the user's Microsoft password.

The equipment used for the integration process is listed below:

Array Networks

Array Network SPX SSL/VPN appliance

Software release version 8.4.4.2

SecurEnvoy

Windows 2003 server SP1

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

Active Directory installed or connection to Active Directory via LDAP protocol.

SecurAccess software release v5.3.502

Index

1.0 Pre Requisites.....	3
2.0 Configuration Overview-Array Networks SPX appliance	3
3.0 Configuration of SecurEnvoy Radius	8
4.0 Test Login	9
5.0 Appendix.....	10
5.1 Using Real Time Passcodes	10

1.0 Pre Requisites

Assumptions:

- Basic SPX system configuration has already been performed i.e. networking, name resolution, default gateway etc.
- The SPX Advanced console will be used for this configuration. For assistance contact Array Networks Support (support@arraynetworks.net)
- The SecurEnvoy server component and Microsoft Active Directory have already been configured.
- Authorisation [through LDAP] to Active Directory will be performed, using standard AD/LDAP configuration parameters.

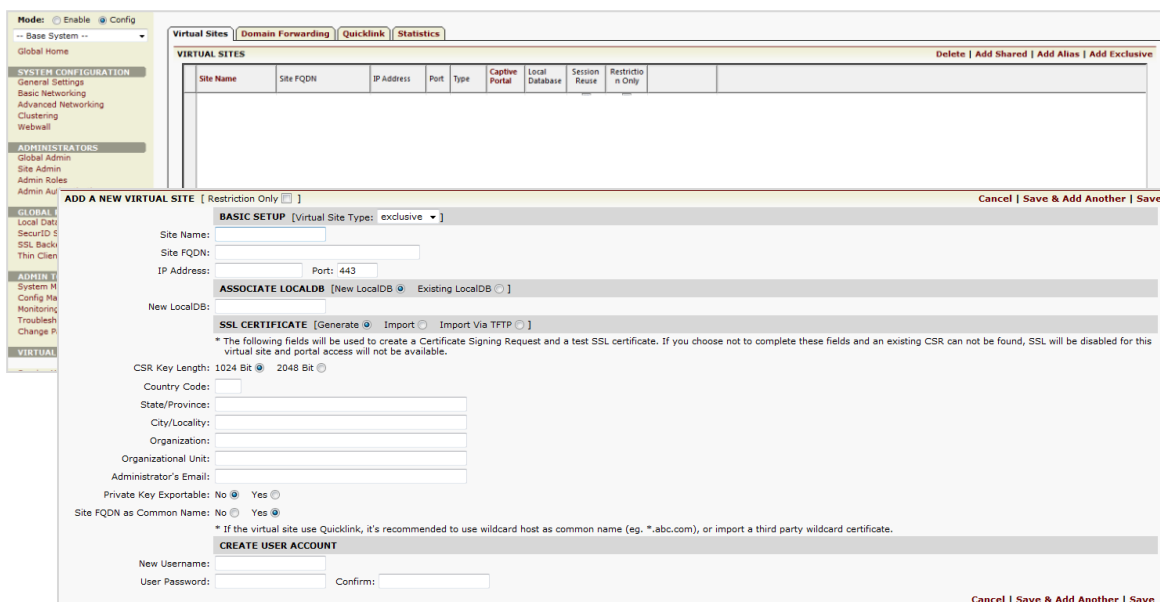
2.0 Configuration Overview-Array Networks SPX appliance

2.1 Create the virtual site (portal) for which SecurEnvoy authentication will be used. Go to the WebUI 'Virtual Sites' branch in the left hand navigation tree and in the right hand config window enter the details for the new virtual site then click the 'Add' button.

If an existing virtual site is being used, the steps for creating the virtual site and SSL configuration can be skipped - go to step 2.6.

Notes:

- Global config privilege is required to create the virtual site, and you need to be in CONFIG mode as shown in the top right of the screen shot.
- The Site FQDN may be the same as the site's IP Address. If using a FQDN then the client must be able to resolve it through DNS to the site's IP Address.
- The site IP Address cannot be the same as an assigned physical interface IP address, but must be on the same subnet.



2.2 When creating a new Virtual Site, you will be prompted to generate an SSL Certificate Signing Request (CSR) In the CSR form complete the relevant site details.

When you click the 'Save' button, the PEM format CSR will be created. You can copy this text and forward it to your Certificate Authority for signing and then import the signed certificate under the SSL->Import Cert/Key branch.

Notes:

- a) The SPX will automatically create a self signed certificate for testing purposes. Do not use this in a production environment.
- b) Before selecting the "Save" button, ensure the right CSR Key Length is chosen for your Certificate Signing Authority.
- b) CREATE USER ACCOUNT is optional. Any accounts created are stored in the local database for the Virtual Site.
- c) The 2 character country code identifier for United Kingdom is GB, not UK. Some browsers may not display content correctly if UK is entered in the SSL CSR.



CSR Key Length: 1024 Bit 2048 Bit

Country Code: GB

State/Province: Berkshire

City/Locality: Theale

Organization: SecurEnvoy

Organizational Unit: Sales

Administrator's Email: info@secureenvoy.com

Private Key Exportable: No Yes

Site FQDN as Common Name: No Yes

* If the virtual site use Quicklink, it's recommended to use wildcard host as common name (eg. *.abc.com), or import a third party wildcard certificate.

Tip: wherever applicable in the WebUI, remember to click the appropriate 'Save Changes' or 'Apply' button, else changes will be lost when changing context also click the "Save Config" to commit the changes to the Startup config.

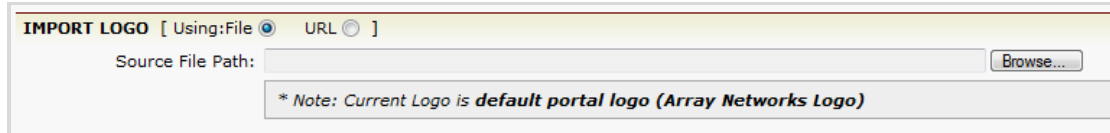
2.4 Customise the portal page by navigating to the Portal branch and enter details for Standard Portal Page Settings and Web Links (these are the Web App links users will see after logging into the virtual site).

Notes:

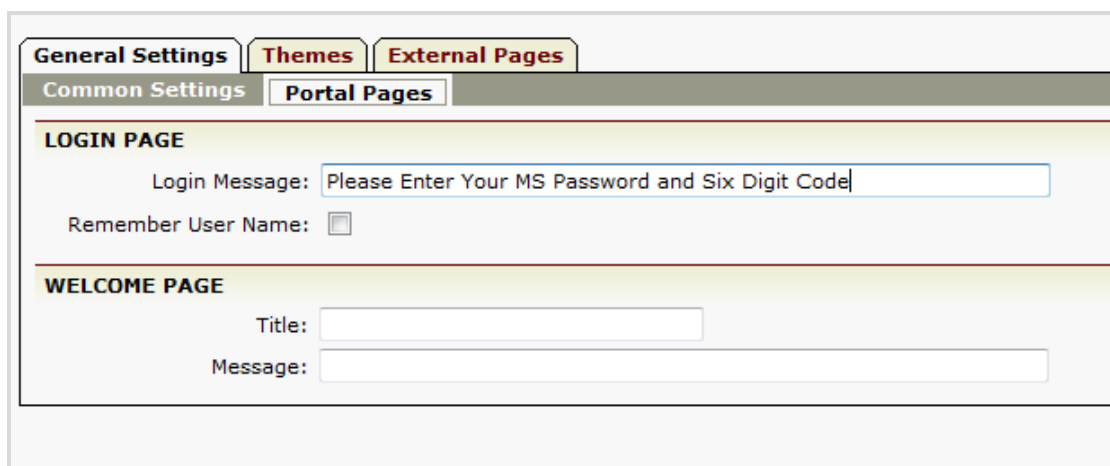
- a). The Web Links URL must be in the format '<scheme>://<host>/<content path>' where:
 <scheme> = http or https
 <host> = web server IP address or host name (if host name then the SPX must be able to resolve it)
 <content path> = optional path to content i.e. for MS Exchange running OWA it will be /exchange

WEB LINKS			Delete Web Link Add Web Link
URL	Description	Web Link Position	
http://exchsrn/exchange	Outlook Web Access	1	

b) A custom logo can be imported for display at the top of the Login/Portal page instead of the standard Array Networks logo using the 'Custom Logo' setting at the bottom of the config page. This requires the logo .GIF or .JPG image file be retrieved from an external server using the format 'http://<host>/<file path>/<file name>' or by browsing for the image'.

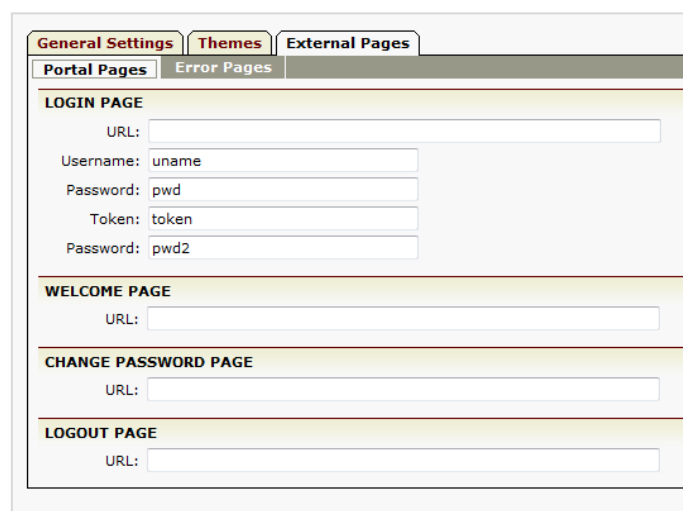


2.5 If desired, custom login page text can be added. Navigate to the Portal->Portal Pages tab then in the right hand config window navigate to the Login Page configuration area.



Alternatively a customised login, logout or welcome page can be referenced from an external web server.

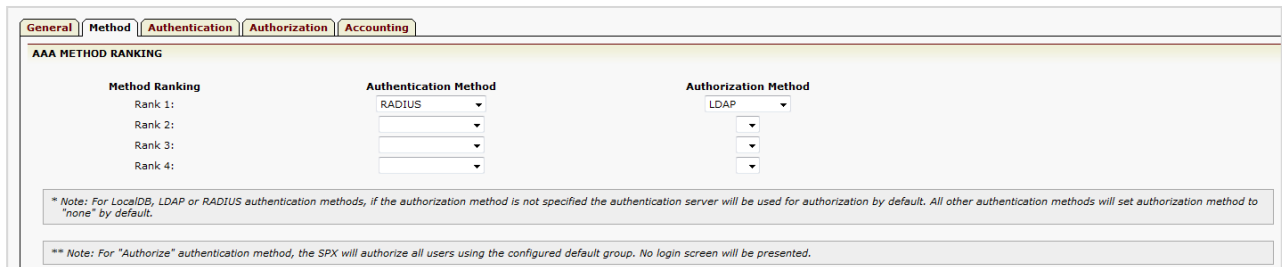
Tip: Contact your local Array Support department should assistance be required.



Notes:

When using an external login page, ensure the variables *uname*, *pwd* and *pwd2* are used. *PWD* should always be used for the pincode.

2.6 Configure the AAA method to be Radius Authentication and LDAP Authorisation. Navigate to the AAA branch and in the Method tab for Rank 1 Authentication select Radius then in Authorization select LDAP.



The screenshot shows the 'AAA METHOD RANKING' configuration page. It has tabs for 'General', 'Method', 'Authentication', 'Authorization', and 'Accounting'. Under 'Method Ranking', there are four rows for Rank 1 through Rank 4. Rank 1 has 'RADIUS' selected for the Authentication Method and 'LDAP' selected for the Authorization Method. Below the form, there are two notes:

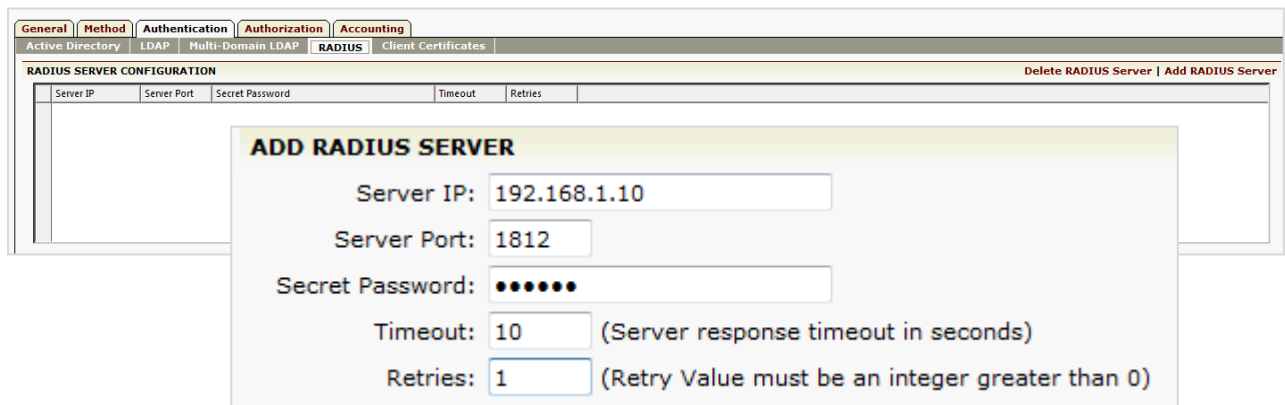
* Note: For LocalDB, LDAP or RADIUS authentication methods, if the authorization method is not specified the authentication server will be used for authorization by default. All other authentication methods will set authorization method to "none" by default.

** Note: For "Authorize" authentication method, the SPX will authorize all users using the configured default group. No login screen will be presented.

2.7 Configure the Radius authentication server parameters. Navigate to the AAA->Authentication->RADIUS branch and add details relating to the SecurEnvoy radius server instance as provided by the SecurEnvoy administrator. Up to 3 Radius instances can be added.

Note:

At this point, if the requirement is only for Authentication with no Authorisation, the configuration is complete and the configuration can be saved/tested. If the retry is set to Zero (0) no Radius authentication is attempted.



The screenshot shows the 'RADIUS SERVER CONFIGURATION' page with tabs for 'Active Directory', 'LDAP', 'Multi-Domain LDAP', 'RADIUS', and 'Client Certificates'. An 'ADD RADIUS SERVER' dialog box is open, containing the following fields:

Server IP: 192.168.1.10

Server Port: 1812

Secret Password: [masked]

Timeout: 10 (Server response timeout in seconds)

Retries: 1 (Retry Value must be an integer greater than 0)

SecurEnvoy Note:

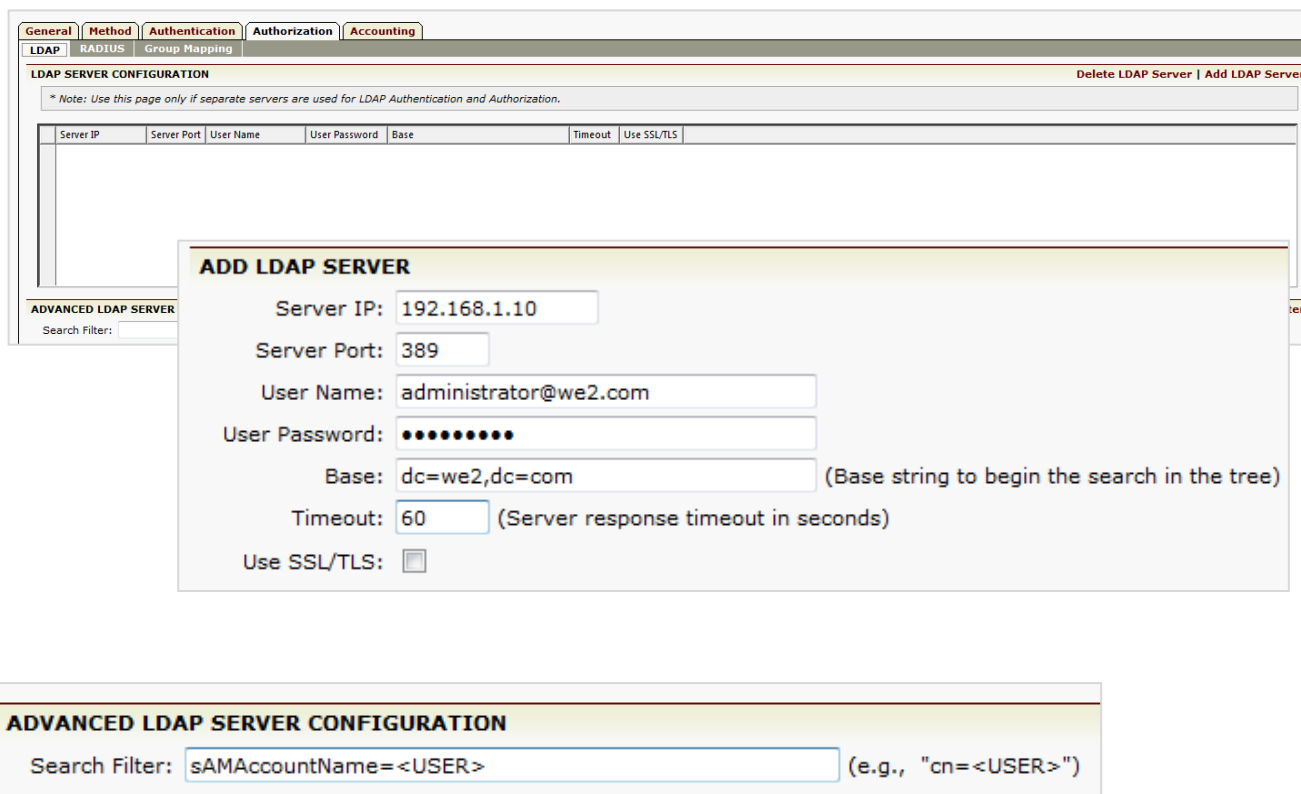
It is recommended that the retry is set to 1 and the timeout set to 10 seconds, if the timeout is too short there is a chance that the authentication reply has not responded before the authentication request has timed out.

2.8 Configure the LDAP Authorisation server parameters. Navigate back to the virtual site and then to the AAA->Authorization->LDAP branch. Add details for the Basic Configuration parameters as provided by the LDAP/AD administrator. Up to 3 Authorization servers can be configured.

Also, remember to enter the correct Search Filter under Additional configuration.

Note:

In terms of configuration the Base, User Name and Search Filter are the most common entered incorrectly. If during testing login fails, some debugging may need to take place on the LDAP/AD server to determine which is incorrectly configured.



The screenshot shows the SecurEnvoy configuration interface. At the top, there are tabs for General, Method, Authentication, Authorization, and Accounting. Under the Authorization tab, there are sub-tabs for LDAP, RADIUS, and Group Mapping. The main area is titled 'LDAP SERVER CONFIGURATION' and contains a table with columns for Server IP, Server Port, User Name, User Password, Base, Timeout, and Use SSL/TLS. Below this is an 'ADD LDAP SERVER' dialog box with the following fields:

- Server IP: 192.168.1.10
- Server Port: 389
- User Name: administrator@we2.com
- User Password: [masked]
- Base: dc=we2,dc=com (Base string to begin the search in the tree)
- Timeout: 60 (Server response timeout in seconds)
- Use SSL/TLS:

Below the dialog box is an 'ADVANCED LDAP SERVER CONFIGURATION' section with a 'Search Filter' field containing 'sAMAccountName=<USER>' and a note '(e.g., "cn=<USER>")'.

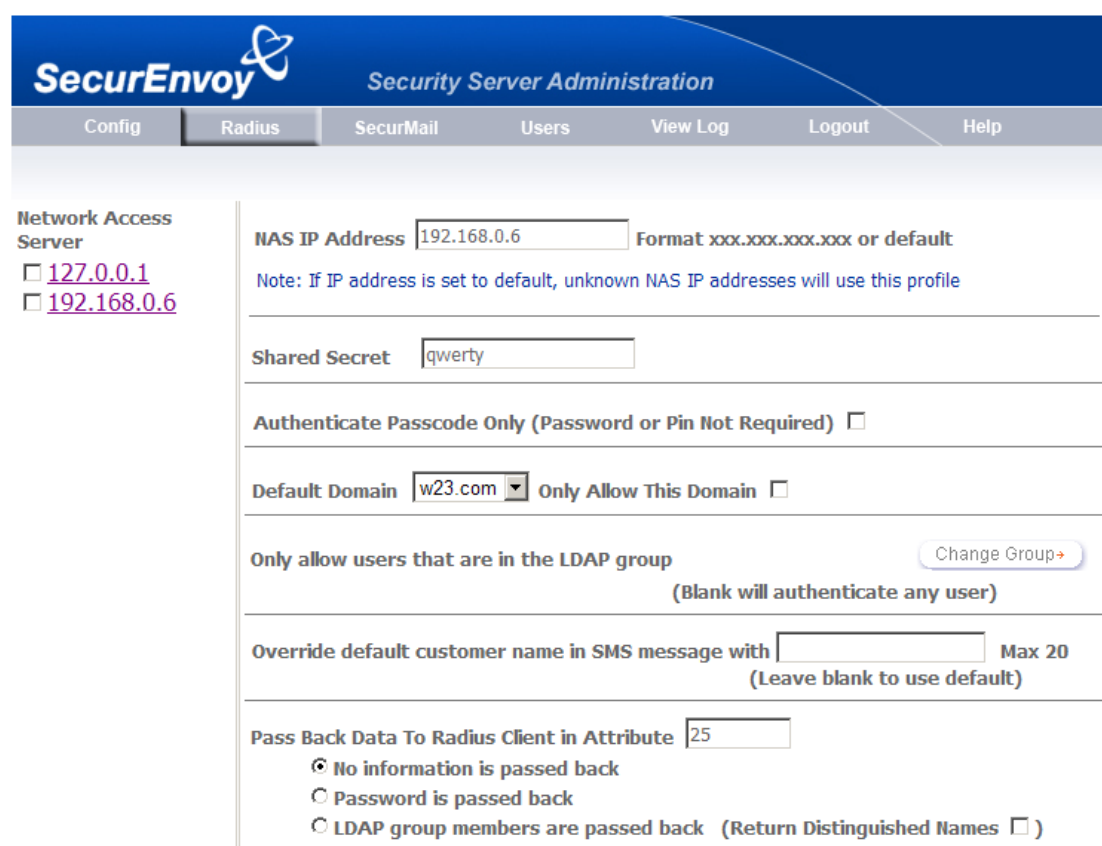
This completes the basic setup of the SPX, Save the config.

3.0 Configuration of SecurEnvoy Radius

To set up Radius on SecurEnvoy SecurAccess, launch local Security Server Administration
Select Radius

Enter NAS IP address
(This is the respective IP interface address of the Array Networks SPX appliance)

By default the Radius port is 1812 UDP
Enter "Radius Shared Secret"
Click Update to save configuration



The screenshot shows the SecurEnvoy Security Server Administration interface. The top navigation bar includes 'Config', 'Radius', 'SecurMail', 'Users', 'View Log', 'Logout', and 'Help'. The 'Radius' tab is selected. On the left, under 'Network Access Server', there are two radio button options: 127.0.0.1 and 192.168.0.6. The main configuration area contains the following fields and options:

- NAS IP Address:** A text box containing '192.168.0.6' with a note: 'Format xxx.xxx.xxx.xxx or default'. Below it is a note: 'Note: If IP address is set to default, unknown NAS IP addresses will use this profile'.
- Shared Secret:** A text box containing 'qwerty'.
- Authenticate Passcode Only (Password or Pin Not Required):** An unchecked checkbox.
- Default Domain:** A dropdown menu showing 'w23.com' and an unchecked checkbox for 'Only Allow This Domain'.
- Only allow users that are in the LDAP group:** A section with a 'Change Group' button and a note: '(Blank will authenticate any user)'.
- Override default customer name in SMS message with:** A text box with 'Max 20' and a note: '(Leave blank to use default)'.
- Pass Back Data To Radius Client in Attribute:** A text box containing '25'.
- Radio button options for data passing back:**
 - No information is passed back
 - Password is passed back
 - LDAP group members are passed back (Return Distinguished Names)

Once the configuration is completed, all Radius settings are stored within a NAS file which is located at:

C:\Program Files\SecurEnvoy\Security Server\Data\RADIUS\NAS

except for the port settings which are stored within the registry under:

HKLM\SOFTWARE\SecurEnvoy\Radius Server.

4.0 Test Login

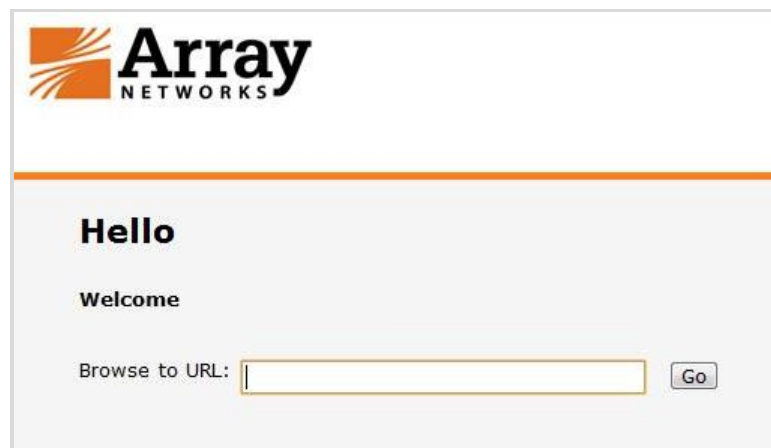
Test the login process by pointing your browser at the virtual site FQDN e.g. <https://securenvoy.corp.com> (your client machine must be able to resolve the hostname to the site IP Address).

You should be presented with a login page similar to the following. Enter your username in the 'Username' field and your password+6 digit code into the 'Password' field then click the 'Sign In' button.



The screenshot shows a login page with the Array Networks logo at the top. Below the logo, the word "Login" is displayed in a bold font. Underneath, there is a prompt: "Please enter your MS password and 6 digit code". This is followed by two input fields: "Username:" and "Password:". Below the "Password:" field is a "Sign In" button.

You should now be presented with the home portal as illustrated below.



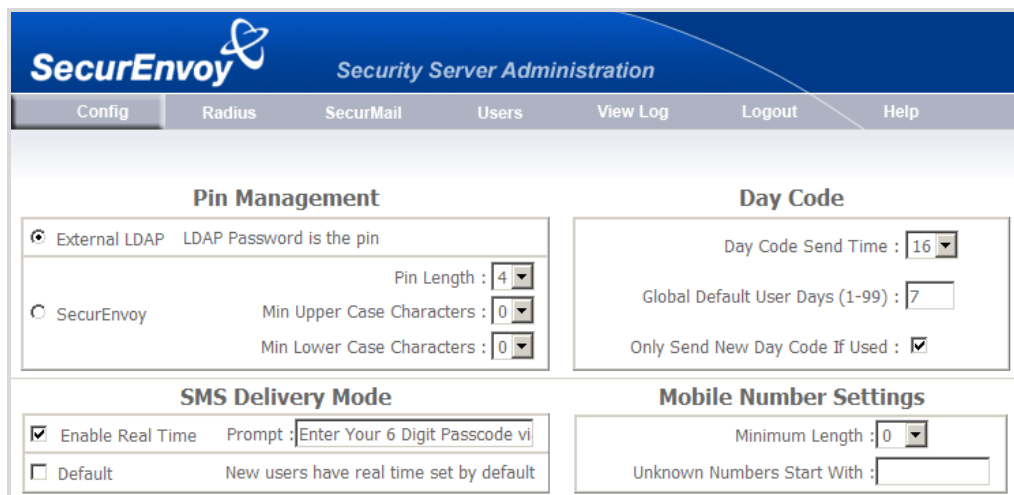
The screenshot shows the home portal of Array Networks. At the top is the Array Networks logo. Below the logo, the word "Hello" is displayed in a bold font, followed by "Welcome". At the bottom, there is a "Browse to URL:" label followed by an input field and a "Go" button.

5.0 Appendix

5.1 Using Real Time Passcodes

Array Networks SPX also has the ability to support real time passcodes. To enable this feature upon, first setup SecurEnvoy to enable "real time passcode" delivery.

Launch to the SecurEnvoy admin console, and then navigate to the "config" page. Locate the section "SMS Delivery Mode" and checkbox to enable real time delivery. Enter the prompt you wished returned to the user at time of logon.

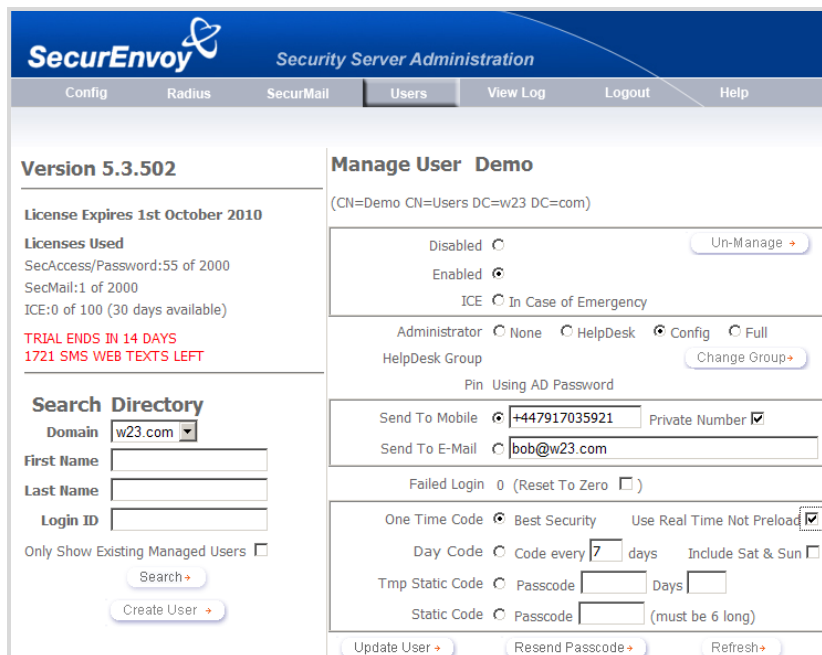


The screenshot shows the SecurEnvoy Security Server Administration interface. The top navigation bar includes 'Config', 'Radius', 'SecurMail', 'Users', 'View Log', 'Logout', and 'Help'. The 'Config' page is divided into several sections:

- Pin Management:**
 - External LDAP: LDAP Password is the pin
 - SecurEnvoy:
 - Pin Length: 4
 - Min Upper Case Characters: 0
 - Min Lower Case Characters: 0
- Day Code:**
 - Day Code Send Time: 16
 - Global Default User Days (1-99): 7
 - Only Send New Day Code If Used:
- SMS Delivery Mode:**
 - Enable Real Time: Prompt: Enter Your 6 Digit Passcode vi
 - Default: New users have real time set by default
- Mobile Number Settings:**
 - Minimum Length: 0
 - Unknown Numbers Start With:

Real time passcodes can be set on a per user basis. Navigate to the "Users" page and locate the desired user, select the "Use Real Time Not Preload" checkbox. Click Update User.

Any previous passcodes associated with this user have now been deleted.



The screenshot shows the SecurEnvoy Security Server Administration interface, specifically the 'Users' page. The top navigation bar includes 'Config', 'Radius', 'SecurMail', 'Users', 'View Log', 'Logout', and 'Help'. The 'Users' page is divided into several sections:

- Version 5.3.502**
- License Expires 1st October 2010**
- Licenses Used:**
 - SecAccess/Password: 55 of 2000
 - SecMail: 1 of 2000
 - ICE: 0 of 100 (30 days available)
 - TRIAL ENDS IN 14 DAYS
 - 1721 SMS WEB TEXTS LEFT
- Search Directory:**
 - Domain: w23.com
 - First Name:
 - Last Name:
 - Login ID:
 - Only Show Existing Managed Users:
 - Search:
 - Create User:
- Manage User Demo** (CN=Demo CN=Users DC=w23 DC=com)
 - Disabled: Un-Manage:
 - Enabled:
 - ICE: In Case of Emergency
 - Administrator: None HelpDesk Config Full
 - HelpDesk Group: Change Group:
 - Pin: Using AD Password
 - Send To Mobile: +447917035921 Private Number:
 - Send To E-Mail: bob@w23.com
 - Failed Login: 0 (Reset To Zero:)
 - One Time Code: Best Security Use Real Time Not Preload:
 - Day Code: Code every 7 days Include Sat & Sun:
 - Tmp Static Code: Passcode: Days:
 - Static Code: Passcode: (must be 6 long)
 - Update User: Resend Passcode: Refresh:

Browse to the web URL address of the Array Networks® SSL appliance
Enter a UserID Enter your Windows Password



The screenshot shows the Array Networks login interface. At the top left is the Array Networks logo. Below it, the word "Login" is displayed in a bold, black font. Underneath, the instruction "Please enter your MS password" is shown. There are two input fields: "Username:" followed by a text box, and "Password:" followed by a text box. At the bottom of the form is a "Sign In" button.

You will be sent a real time passcode to your phone, enter this 6 digit code at the Response: prompt.



The screenshot shows the Array Networks Radius Challenge screen. At the top left is the Array Networks logo. Below it, the text "Radius Challenge" is displayed in a bold, black font. Underneath, the instruction "Enter Your 6 Digit Passcode via SMS" is shown. There is one input field labeled "Password:" followed by a text box. At the bottom of the form are two buttons: "Sign In" and "Cancel".