

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	

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 integrates 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 7.3.3

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 v2.9 0011

Index

1.0 Pre Requisites.....	3
2.0 Configuration Overview-Array Networks SPX appliance	3
3.0 Array Network SPX configuration file	10
4.0 Configuration of SecurEnvoy Radius.....	11
5.0 Test Login	12
6.0 Appendix.....	13

1.0 Pre Requisites

Assumptions:

- Basic SPX system configuration has already been performed i.e. networking, name resolution etc.
- The SecurEnvoy server component and Microsoft Active Directory have already been configured.
- Authorisation [through LDAP group mapping] to Active Directory will be performed, using standard AD/LDAP configuration parameters.

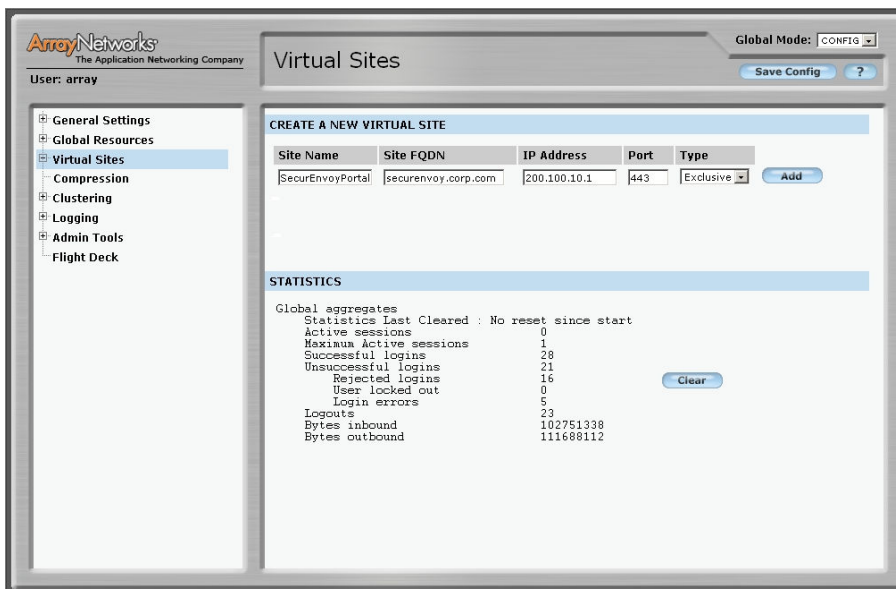
2.0 Configuration Overview-Array Networks SPX appliance

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 sites IP Address. If using a FQDN then the client must be able to resolve it through DNS to the sites IP Address.
- The site IP Address cannot be the same as an assigned physical interface IP address, but must be on the same subnet.



Array Networks
The Application Networking Company

User: array

Global Mode: CONFIG

Save Config ?

Virtual Sites

CREATE A NEW VIRTUAL SITE

Site Name	Site FQDN	IP Address	Port	Type	
SecurEnvoyPortal	securenvoy.corp.com	200.100.10.1	443	Exclusive	Add

STATISTICS

Global aggregates

Statistics Last Cleared : No reset since start

Active sessions	0
Maximum Active sessions	1
Successful logins	28
Unsuccessful logins	21
Rejected logins	16
User locked out	0
Login errors	5
Logouts	23
Bytes inbound	102751338
Bytes outbound	111688112

Clear

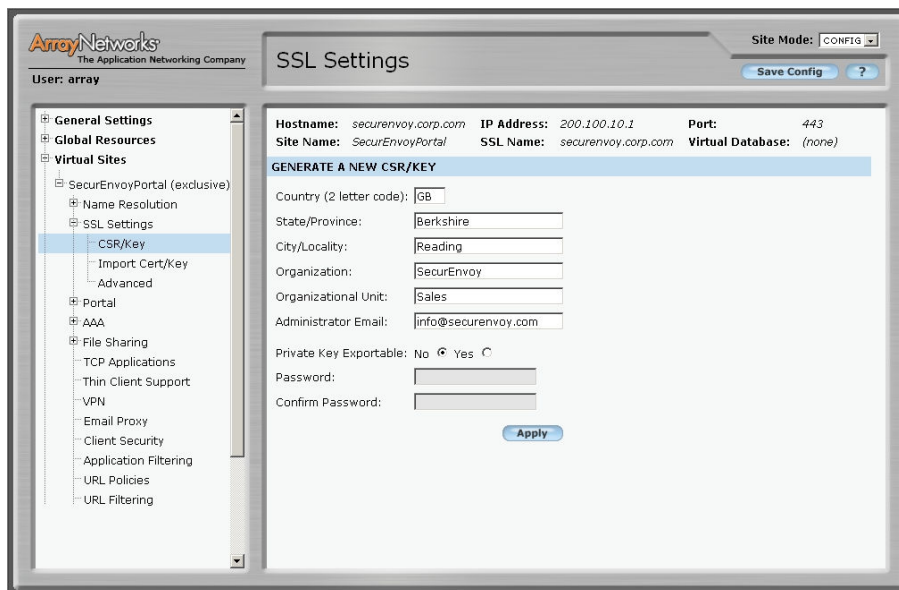
2.2 You will notice that under Virtual Sites in the navigation tree a new branch has been created for the virtual site. Create an SSL Certificate Signing Request (CSR) by clicking on the new virtual site and then navigating the tree to SSL->CSR/Key. In the CSR form complete the relevant site details.

When you click the 'Apply' 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:

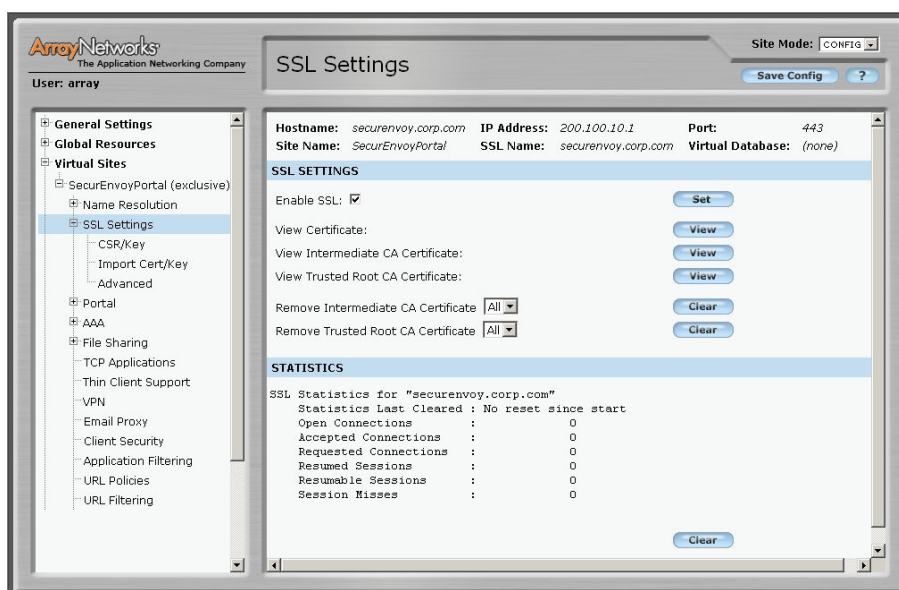
a) The SPX will automatically create a self signed certificate for testing purposes. Do not use this in a production environment.

b) 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.



2.3 Enable SSL by navigating back to the SSL Settings branch, tick the 'Enable SSL' checkbox then click the respective 'Set' button.

Tip: wherever applicable in the WebUI, remember to click the appropriate 'Set' or 'Apply' button, else changes will be lost when changing context.



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:

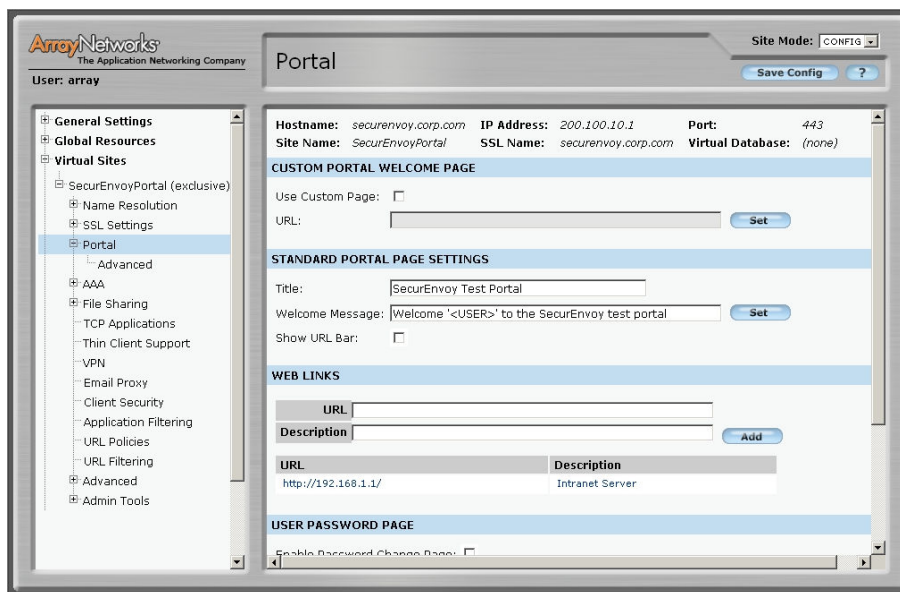
1. The Web Links URL must be in the format '<scheme>://<host>/<content path>' where:

<scheme> = http or https

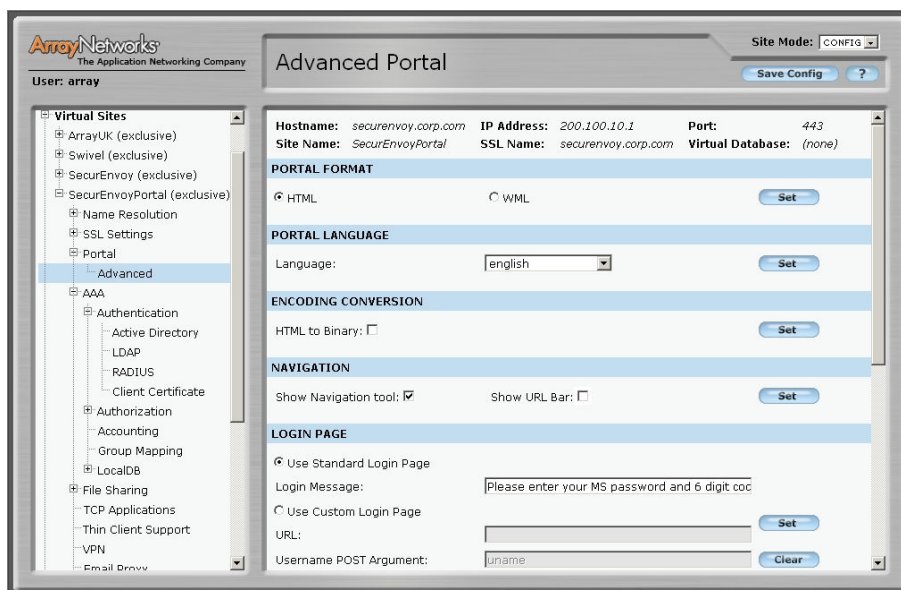
<host> = web server IP address or host name (if host name then the SPX must be able to resolve it)

<content path> = optional path to content i.e. for MS Exchange running OWA it will be /exchange

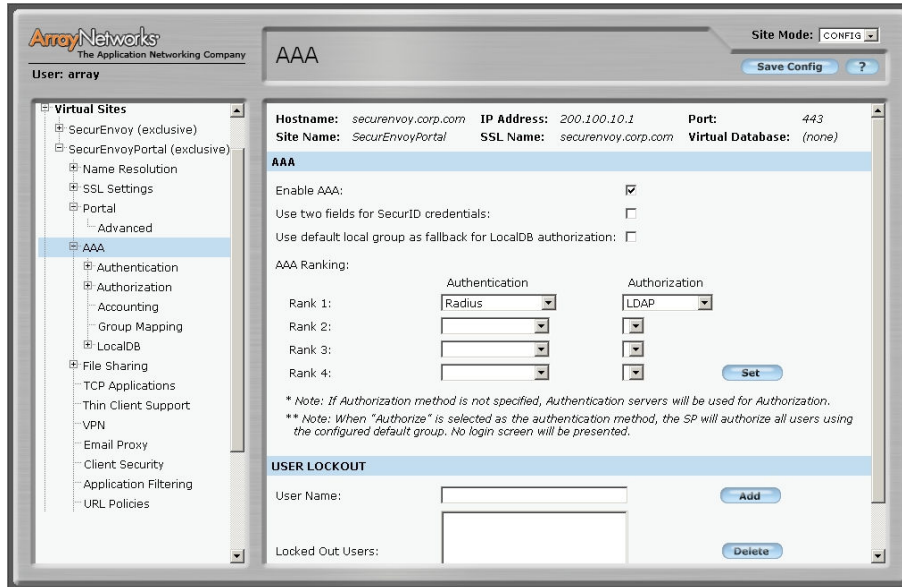
2. A custom logo can be imported for display at the top of the Login/Portal page instead of the standard Array Networks logo using the 'Custom Logo' setting at the bottom of the config page. This requires the logo .GIF or .JPG image file be retrieved from an external server using the format 'http!ftp://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



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



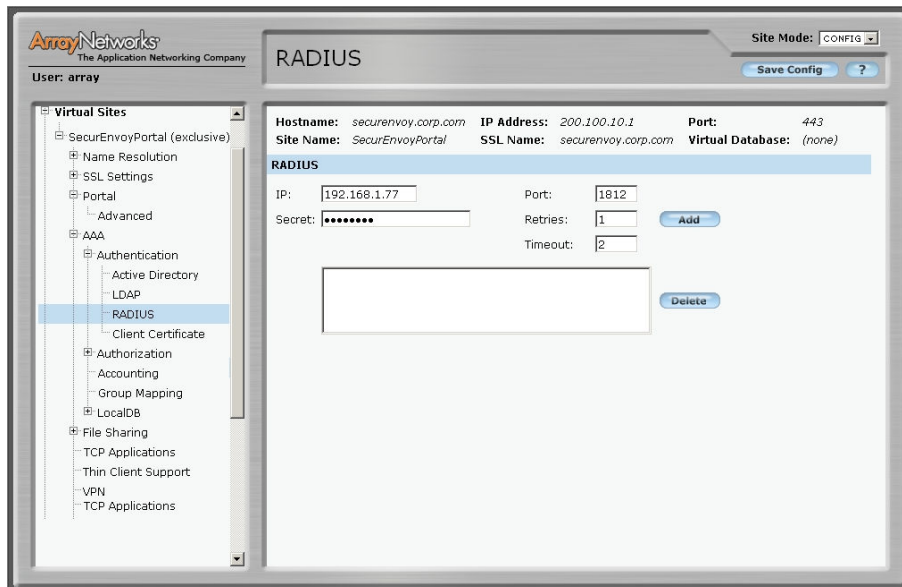
2.6 Configure the AAA method to be Radius Authentication and LDAP Authorisation. Navigate to the AAA branch and in the config window for Rank 1 Authentication select Radius then in Authorization select LDAP.



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:

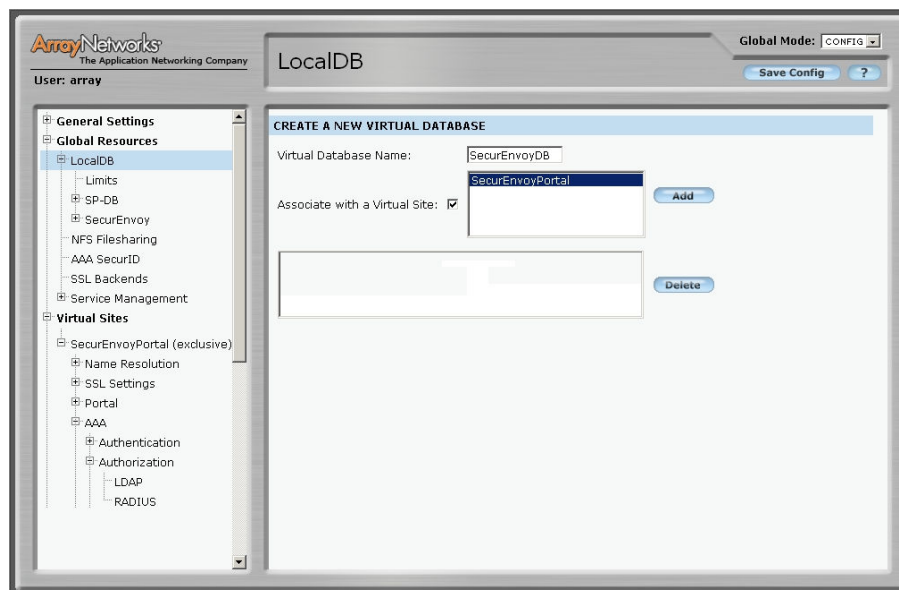
At this point, if the requirement is only for Authentication with no Authorisation, the configuration is complete and the configuration can be saved/tested. If the retry is set to Zero (0) no Radius authentication is attempted.



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.

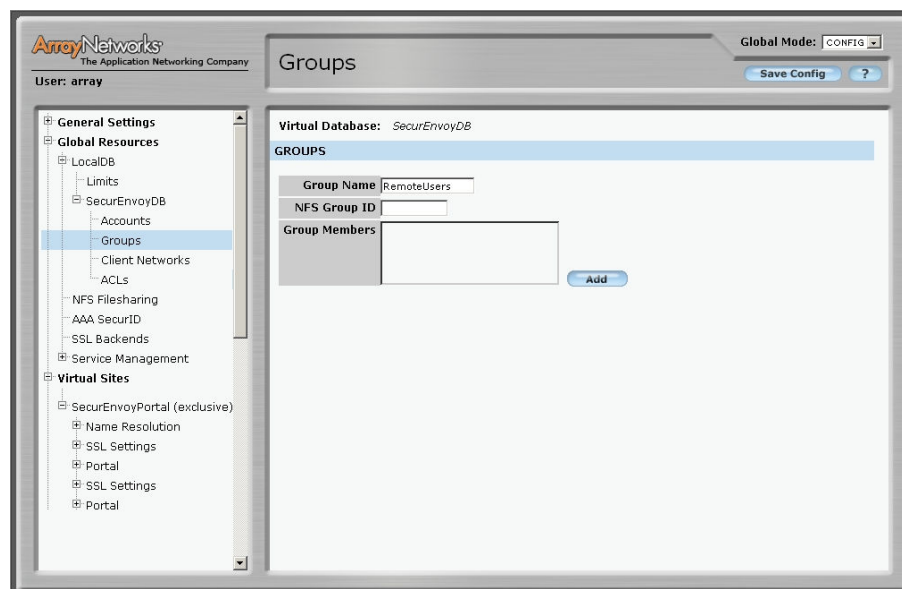
2.8 Create a local database and associate it with the virtual site to be used in group mapping for authorisation. Navigate to the Global Resource->LocalDB branch, enter a new Virtual Database name (or select an existing virtual database), check the Associate tick box and select the virtual site to associate it with.



2.9 Create a LocalDB group to be used in group mapping. Under the Global Resources->LocalDB branch, navigate to your new LocalDB->Groups branch and add a Group.

Note:

The LocalDB group can also be added in the virtual site once the database has been associated with the virtual site under the virtual site AAA->LocalDB branch.

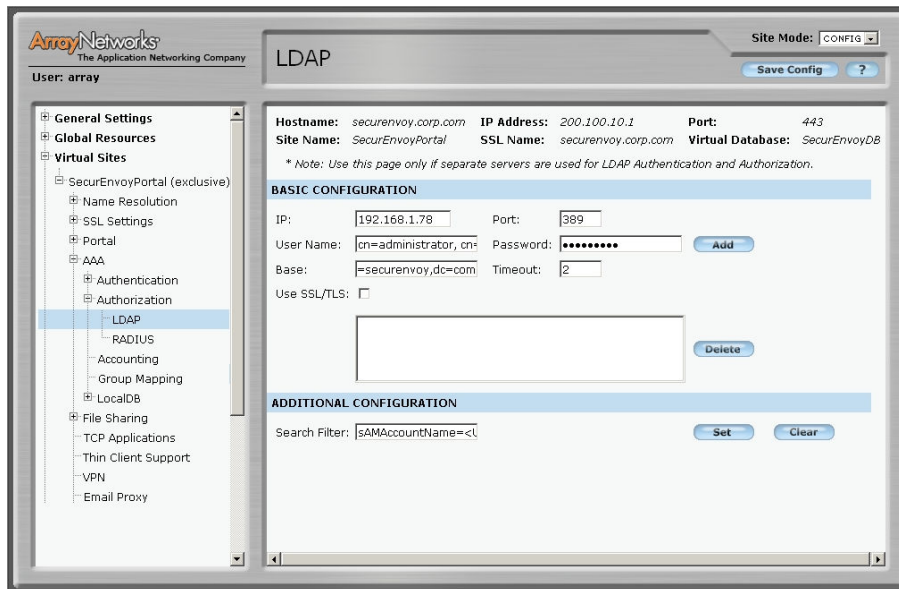


2.10 Configure the LDAP Authorisation server parameters. Navigate back to the virtual site and then to the AAA->Authorization->LDAP branch. Add details for the Basic Configuration parameters as provided by the LDAP/AD administrator. Up to 3 Authorization servers can be configured.

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

Note:

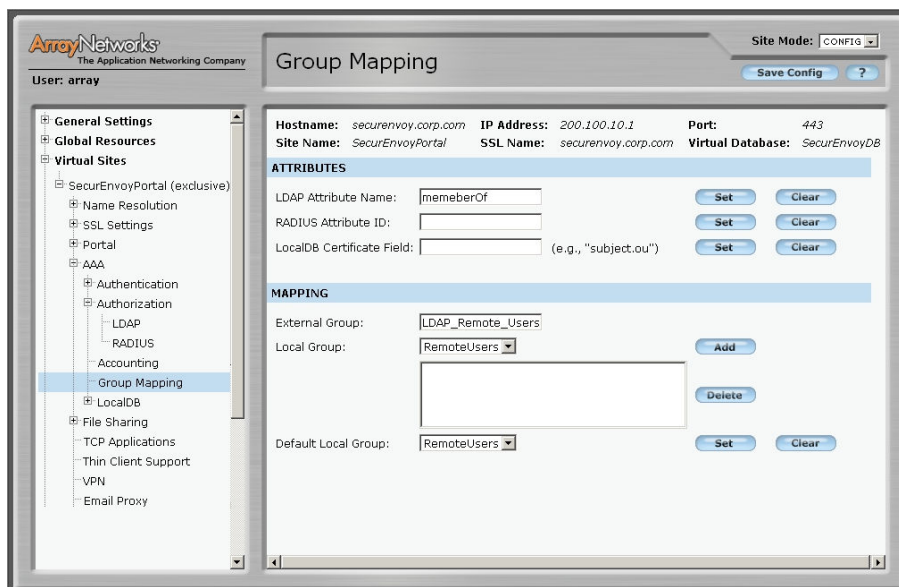
In terms of configuration the Base, User Name and Search Filter are the most common entered incorrectly. If during testing login fails, some debugging may need to take place on the LDAP/AD server to determine which is incorrectly configured.



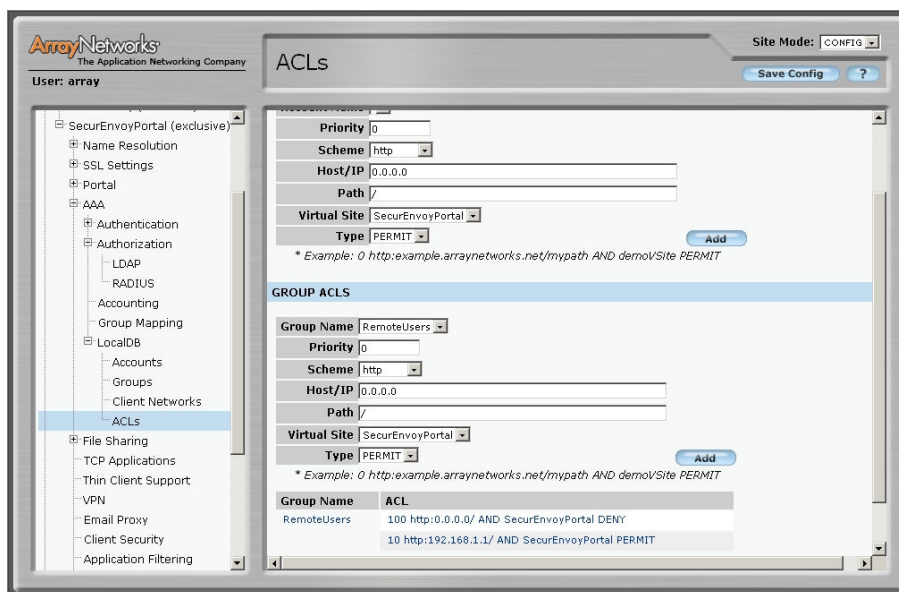
2.11 Create the LDAP to Local Group mapping. The SPX will perform a look up in the LDAP/AD directory to see if the user attempting authentication is a member of a corresponding LDAP/AD group. If they are then they will be mapped to a Local DB group to which local ACLs (Access Control Lists) can be applied.

Navigate to the Authorization->Group mapping branch in the virtual site. The important configuration fields are the LDAP Attribute Name, External Group name and Local Group name to map to.

Note: *If no Default Local Group is configured and the user does not belong to any configured External Group(s) then authentication will fail.*



2.12 If LocalDB Group Authorisation ACLs are to be used, these can be configured under the AAA->LocalDB->ACLs branch in the virtual site.



NOTE: Save your configuration. You must save both the virtual site and global context configurations.

3.0 Array Network SPX configuration file

The following is an extract of the relevant configuration parameters from the CLI config file.

#Global Configuration

```
#virtual service configuration
virtual site host "SecurEnvoyPortal" "securenvoy.corp.com" 200.100.10.1 443 "exclusive"
virtual site session reuse on "SecurEnvoyPortal"
```

```
#ssl configuration
ssl host virtual "securenvoy.corp.com" "SecurEnvoyPortal"
```

```
#localdb virtual database configuration
localdb database "SecurEnvoyDB"
localdb associate "SecurEnvoyPortal" "SecurEnvoyDB"
```

#Virtual Site SecurEnvoyPortal Configuration

```
#Portal interface configuration
portal title "SecurEnvoy Test Portal"
portal message welcome "Welcome '<USER>' to the SecurEnvoy test login portal"
portal message login "Please enter your MS password and 6 digit code from Mobile phone"
no portal urlbar
portal navtool
portal language "english"
portal link "http://192.168.1.1/" "Intranet Server" 1
```

```
#aaa configuration
aaa on
aaa radius accounting off
aaa method radius 1 ldap
aaa radius host 192.168.1.77 1812 "XXXXXcXdlcnR5" 5 1
aaa ldap authorize host 192.168.1.78 389
"cn=administrator,cn=users,dc=securenvoy,dc=com" "XXXXXcDBzdGNvZGU="
"dc=securenvoy,dc=com" 5
aaa ldap authorize search filter "sAMAccountName=<USER>"
aaa ldap group "memberOf"
aaa localdb group default "Remoteusers"
aaa map group "Remoteusers" "Remoteusers"
```

```
#Filter settings
localdb group "Remoteusers"
localdb acl group "Remoteusers" "10 http:192.168.1.1/ AND SecurEnvoyPortal PERMIT"
localdb acl group "Remoteusers" "100 http:0.0.0.0/ AND SecurEnvoyPortal DENY"
```

4.0 Configuration of SecurEnvoy Radius

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

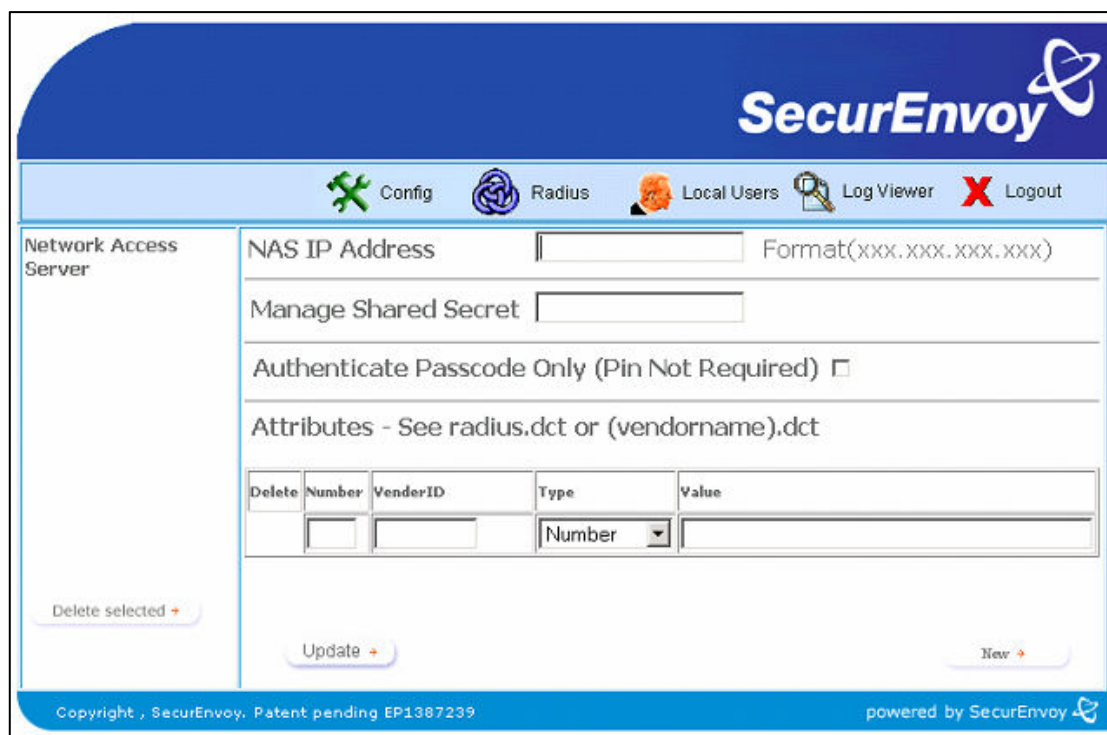
Enter NAS IP address

(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



SecurEnvoy

Config Radius Local Users Log Viewer Logout

Network Access Server

NAS IP Address Format(XXX.XXX.XXX.XXX)

Manage Shared Secret

Authenticate Passcode Only (Pin Not Required)

Attributes - See radius.dct or (vendorname).dct

Delete	Number	VendorID	Type	Value
<input type="checkbox"/>	<input type="text"/>	<input type="text"/>	Number	<input type="text"/>

Delete selected + Update + New +

Copyright , SecurEnvoy. Patent pending EP1387239 powered by SecurEnvoy

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

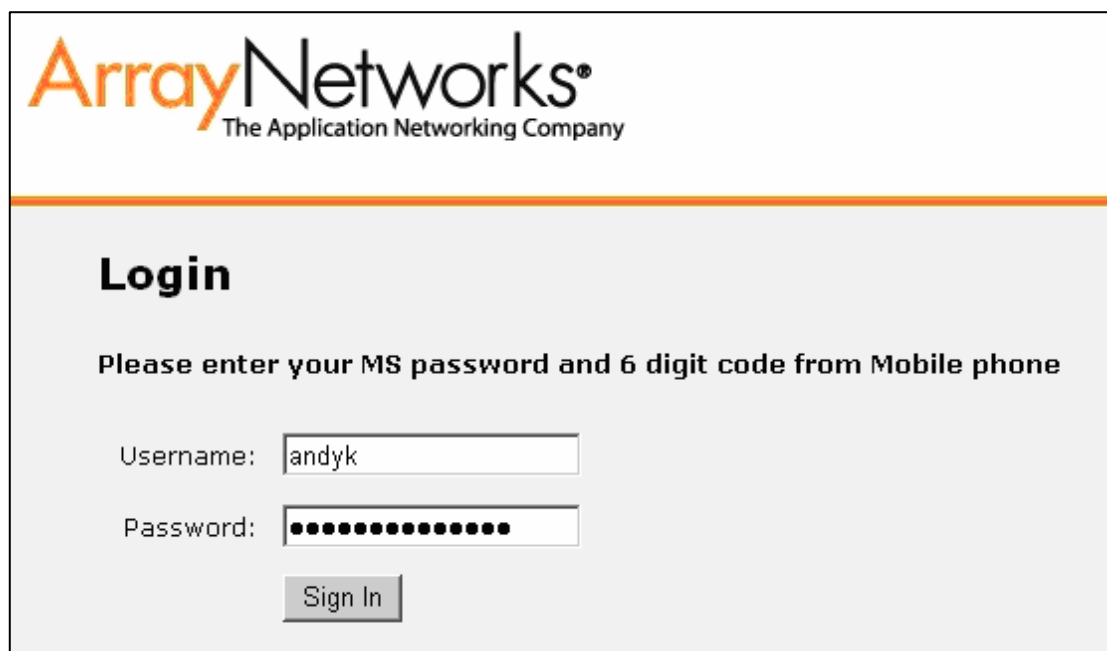
except for the port settings which are stored within the registry under:

HKLM\SOFTWARE\SecurEnvoy\Radius Server.

5.0 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.



Array Networks®
The Application Networking Company

Login

Please enter your MS password and 6 digit code from Mobile phone

Username:

Password:

You should now be presented with the home portal page showing any configured Web Links as illustrated below.

Intranet Server'." data-bbox="195 619 790 892"/>

Array Networks®
The Application Networking Company

SecurEnvoy Test Portal

Welcome 'andyk' to the SecurEnvoy test login portal

Web Links:

- [Intranet Server](#)

6.0 Appendix