

**iPad or iPhone with Junos Pulse and Juniper<sup>®</sup> SSL  
VPN appliance**

**Authenticating Users Using SecurAccess Server by  
SecurEnvoy**

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

## **Juniper® SSL VPN appliance Integration Guide**

This document describes how to setup an iPad or iPhone with the Junos Pulse application connecting to a Juniper® SSL VPN appliance with SecurEnvoy two-factor Authentication solution called 'SecurAccess'.

Junos Pulse and Juniper® SSL VPN appliance provides - Secure Remote Access to the internal corporate network for iPad's or iPhones.

SecurAccess provides two-factor, strong authentication for remote Access solutions (such as Juniper®), 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.

SecurEnvoy Security Server can be configured in such a way that it can use the existing Microsoft password. Utilising the Windows password as the PIN, allows the User to enter their UserID, Windows password and One Time Passcode received upon their mobile phone. This authentication request is passed via the Radius protocol to the SecurEnvoy Radius server where it carries out a Two-Factor authentication. SecurEnvoy utilises a web GUI for configuration, as does the Juniper® SSL VPN appliance. All notes within this integration guide refer to this type of approach.

Note that two configuration options exists, one for Pre-loaded Passcodes including Day Codes, Tmp Codes and Static Codes ( Section 1.1 to 3), the other for Real Time Codes (Appendix A to C)

### **The equipment used for the integration process is listed below:**

#### **Juniper**

Juniper® SSL VPN appliance version 7.0R1

#### **SecurEnvoy**

Windows 2003 server SP1

IIS installed with SSL certificate (required for remote administration)

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

SecurAccess software release v5.4.501

iPad with Junos Pulse

## Index

1.0	Pre Requisites.....	3
1.1	Configuration of Juniper® for Pre-Loaded Passcodes .....	4
2.0	Configuration of SecurEnvoy for Pre-Loaded Passcodes .....	7
3.0	Test Pre-Loaded Codes Logon.....	8
Appendix A	Configuration of Juniper® for Real Time Authentication .....	12
Appendix B	Configuration of SecurEnvoy for Real Time Passcodes .....	15
Appendix C	Test Real Time Codes Logon.....	17

### 1.0 Pre Requisites

*It is assumed that the Juniper® SSL VPN appliance has been installed and basic configuration carried out. A user can connect by authenticating with their Microsoft AD Domain username and password. (This could be configured for any username and password authentication server)*

*Securenvoy Security Server has been installed with the Radius service and has a suitable account that has read and write privileges to the Active Directory, if firewalls are between the SecurEnvoy Security server, Active Directory servers, and the Juniper® SSL VPN appliance(s), additional open ports will be required.*

**NOTE:** Add radius profiles for each Juniper® SSL VPN appliance that requires Two-Factor Authentication.

## 1.1 Configuration of Juniper® for Pre-Loaded Passcodes

Login to the Juniper® SSL VPN appliance with administrative permissions.

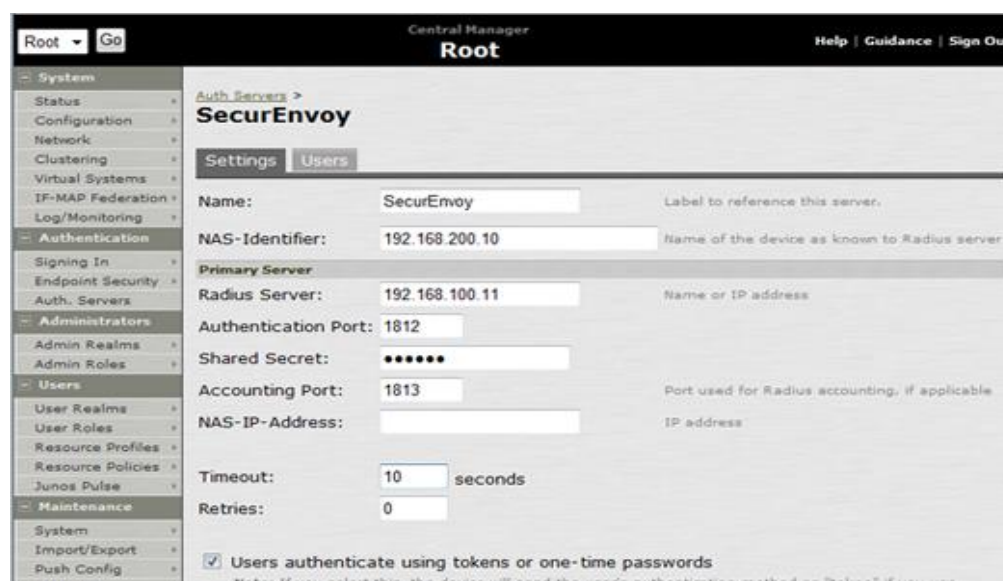
Navigate to "Authentication" "Auth. Servers" select new "Radius Server" and press "New Server"



Populate information for the new Radius server (SecurEnvoy)  
Enter Name, IP address, authentication port and shared secret.

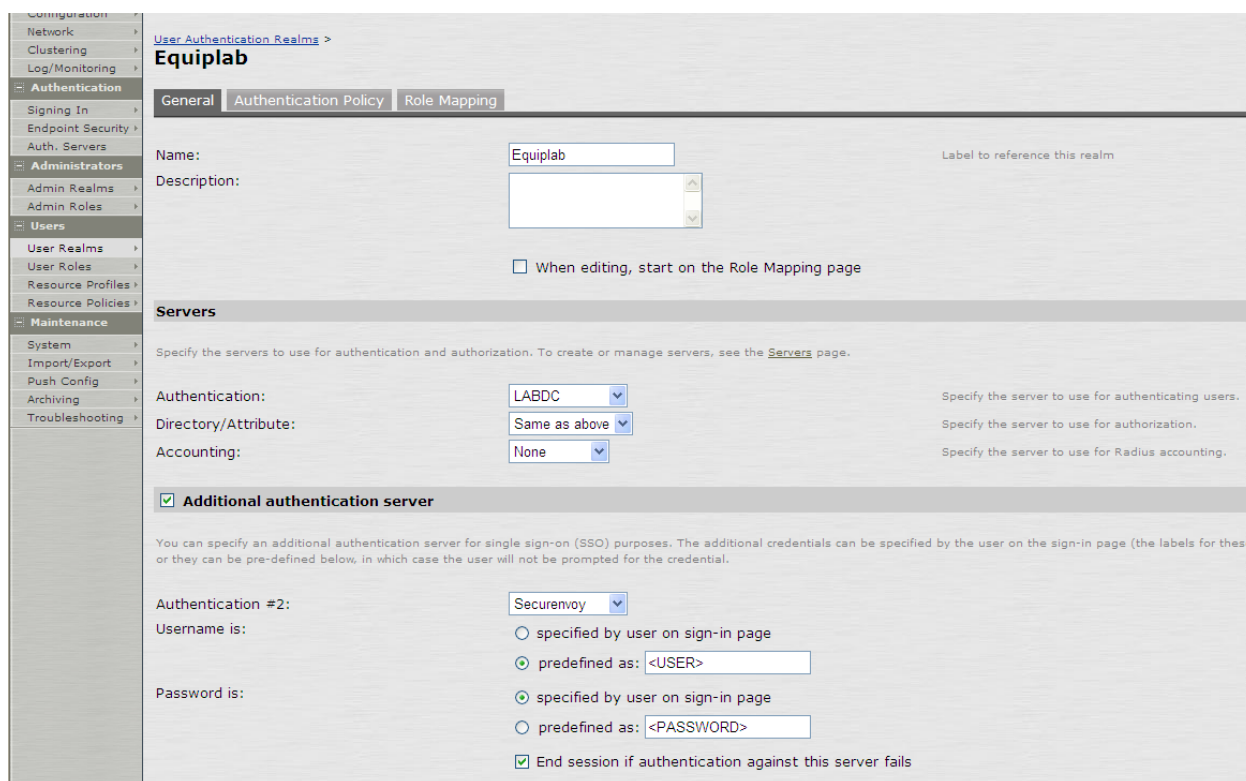
SecurEnvoy recommend to set the timeout settings to at least 10 seconds or greater with a retry of 0.

If redundancy is required, enter details for a second SecurEnvoy Radius server.



Click "Save changes" to submit all configuration parameters

Navigate to "Users", "User Realms" and select the user realm for Microsoft AD Domain authentication.



**Equiplab**

General | Authentication Policy | Role Mapping

Name: Equiplab Label to reference this realm

Description:

When editing, start on the Role Mapping page

**Servers**

Specify the servers to use for authentication and authorization. To create or manage servers, see the [Servers](#) page.

Authentication: LABDC Specify the server to use for authenticating users.

Directory/Attribute: Same as above Specify the server to use for authorization.

Accounting: None Specify the server to use for Radius accounting.

**Additional authentication server**

You can specify an additional authentication server for single sign-on (SSO) purposes. The additional credentials can be specified by the user on the sign-in page (the labels for these or they can be pre-defined below, in which case the user will not be prompted for the credential).

Authentication #2: Securenvoy

Username is:  specified by user on sign-in page  
 predefined as: <USER>

Password is:  specified by user on sign-in page  
 predefined as: <PASSWORD>

End session if authentication against this server fails

Click the checkbox "Additional authentication server"

Populate information for "Authentication #2" select "Securenvoy" (this is the previously setup Radius authentication server)

Set "Username is" to radial button "predefined as <USER>"

Set "Password is" to radial button "specified by user on sign-in page"

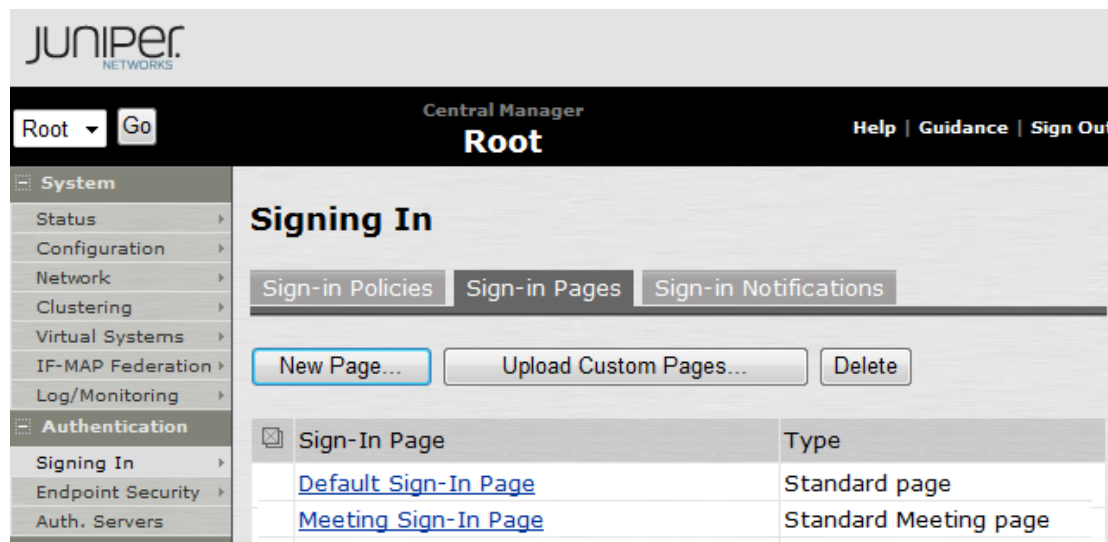
Click checkbox "End session if authentication this server fails"

Click "Save changes" to submit all configuration parameters

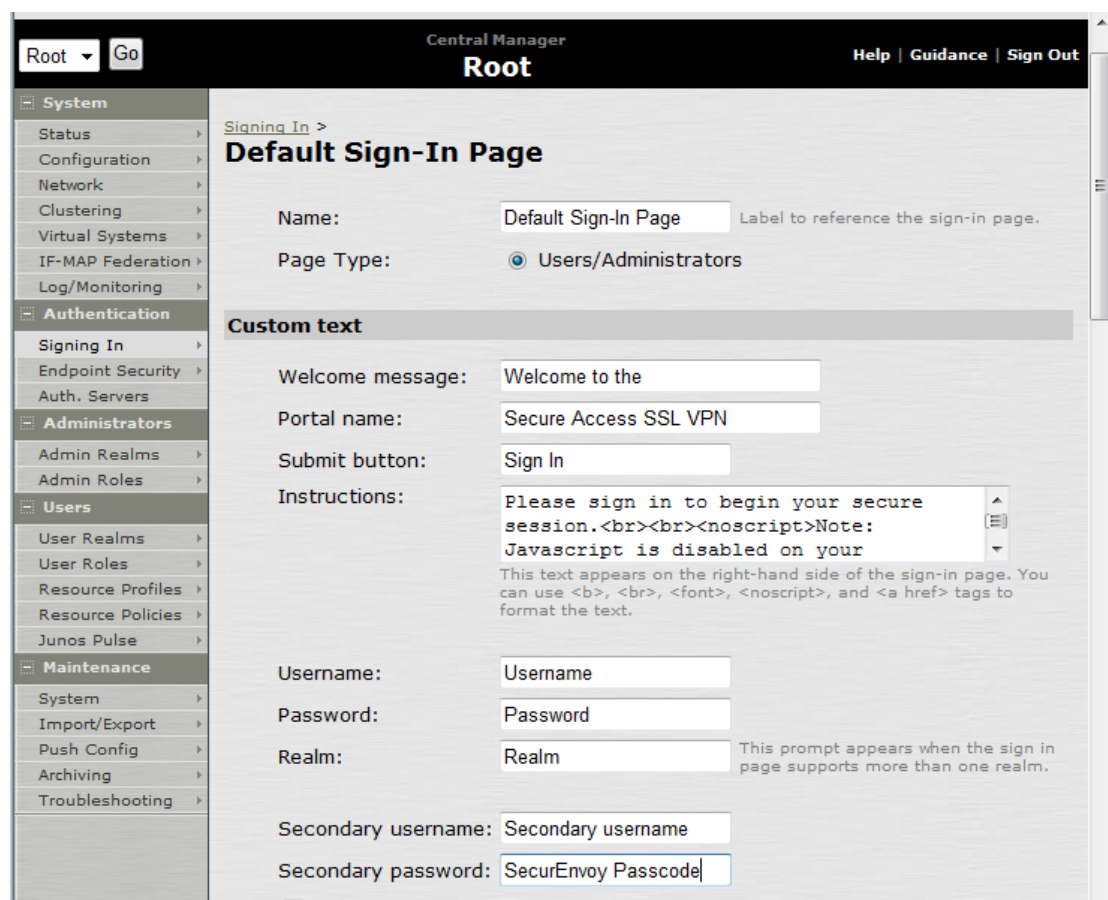
Navigate to "Authentication" "Signing In" "Sign-in Pages"

Select the sign in page associated with the Microsoft AD Domain authentication, in this example this is the "Default Sign-In Page"

Click the link for "Default Sign-In Page"



Enter details for secondary password prompt, in this example "SMS Pass Code" was used



Click "Save changes" to submit all configuration parameters

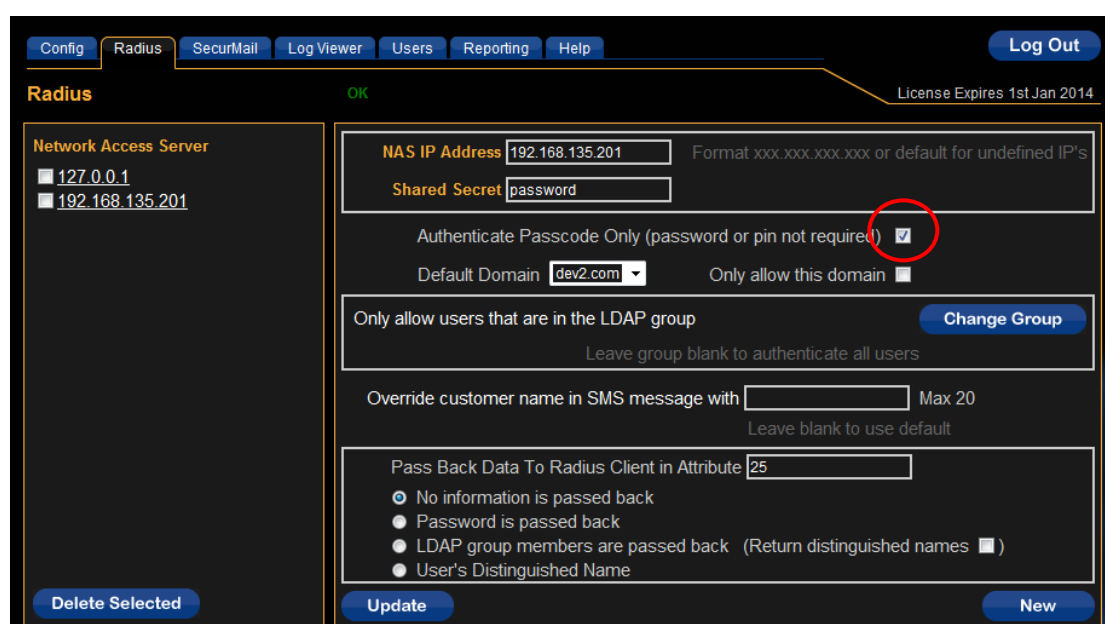
## 2.0 Configuration of SecurEnvoy for Pre-Loaded Passcodes

To help facilitate an easy to use environment, SecurEnvoy can be set up to use the existing Windows password as the PIN component. SecurEnvoy supplies the second factor of authentication, which is the dynamic one time passcode (OTP) which is sent to the user's mobile phone.

Launch the SecurEnvoy admin interface, by executing the Local Security Server Administration link on the SecurEnvoy Security Server.

Click the **"Radius"** Button

Enter IP address and Shared secret for each Juniper® SSL VPN appliance that wishes to use **SecurEnvoy** Two-Factor authentication.



The screenshot shows the SecurEnvoy administration interface for configuring a Radius server. The top navigation bar includes 'Config', 'Radius', 'SecurMail', 'Log Viewer', 'Users', 'Reporting', 'Help', and 'Log Out'. The 'Radius' section is active, showing a list of Network Access Servers (NAS) on the left: 127.0.0.1 and 192.168.135.201. The main configuration area for the selected NAS (192.168.135.201) includes the following fields and options:

- NAS IP Address:** 192.168.135.201 (Format xxx.xxx.xxx.xxx or default for undefined IP's)
- Shared Secret:** password
- Authenticate Passcode Only (password or pin not required):**  (This checkbox is circled in red in the image)
- Default Domain:** dev2.com (Only allow this domain )
- Only allow users that are in the LDAP group:** (Change Group button)
- Override customer name in SMS message with:** (Max 20, Leave blank to use default)
- Pass Back Data To Radius Client in Attribute:** 25
- Pass Back Options:**
  - No information is passed back
  - Password is passed back
  - LDAP group members are passed back (Return distinguished names )
  - User's Distinguished Name

Buttons for 'Delete Selected', 'Update', and 'New' are located at the bottom of the configuration area.

Click checkbox "Authenticate Passcode Only (password or pin not required)"

Click **"Update"** to confirm settings.

Click **"Logout"** when finished. This will log out of the Administrative session.

## 2.0 Setup iPad with Junos Pulse

On the iPad, download Junos Pulse from the App Store



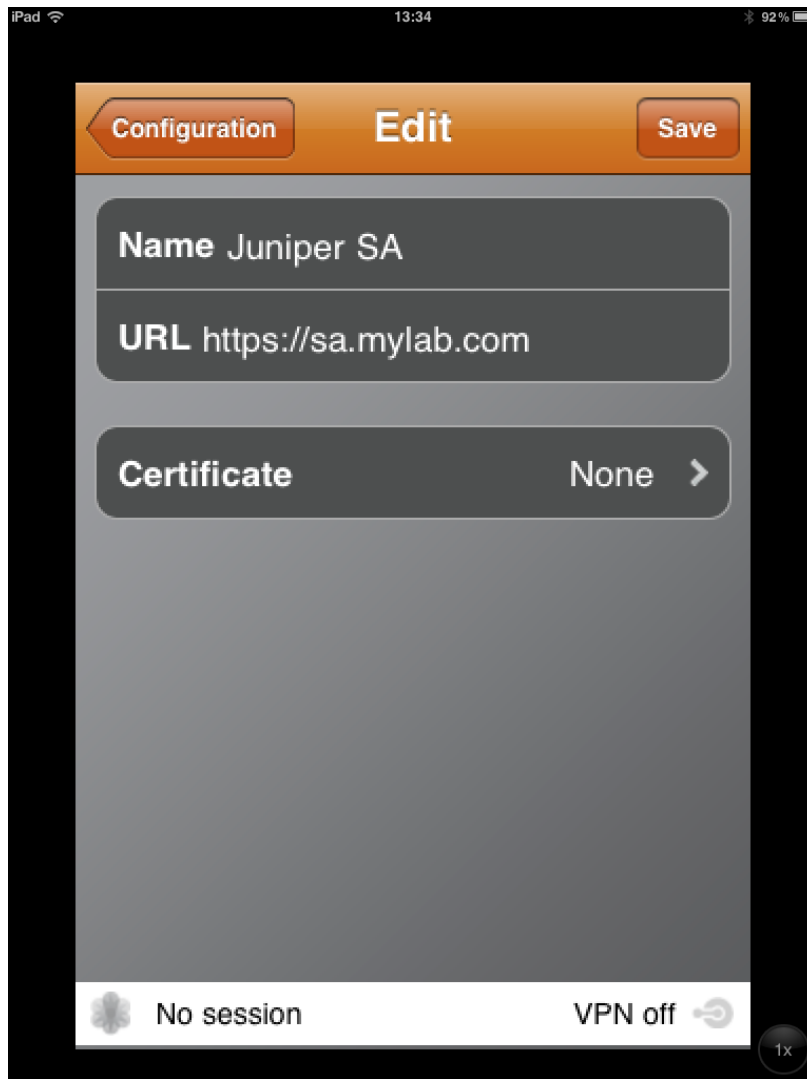
Start Junos Pulse and select "Configuration" and "Add new configuration"

Enter Name details

Enter the URL to your Juniper SA Box

Add Certificate details

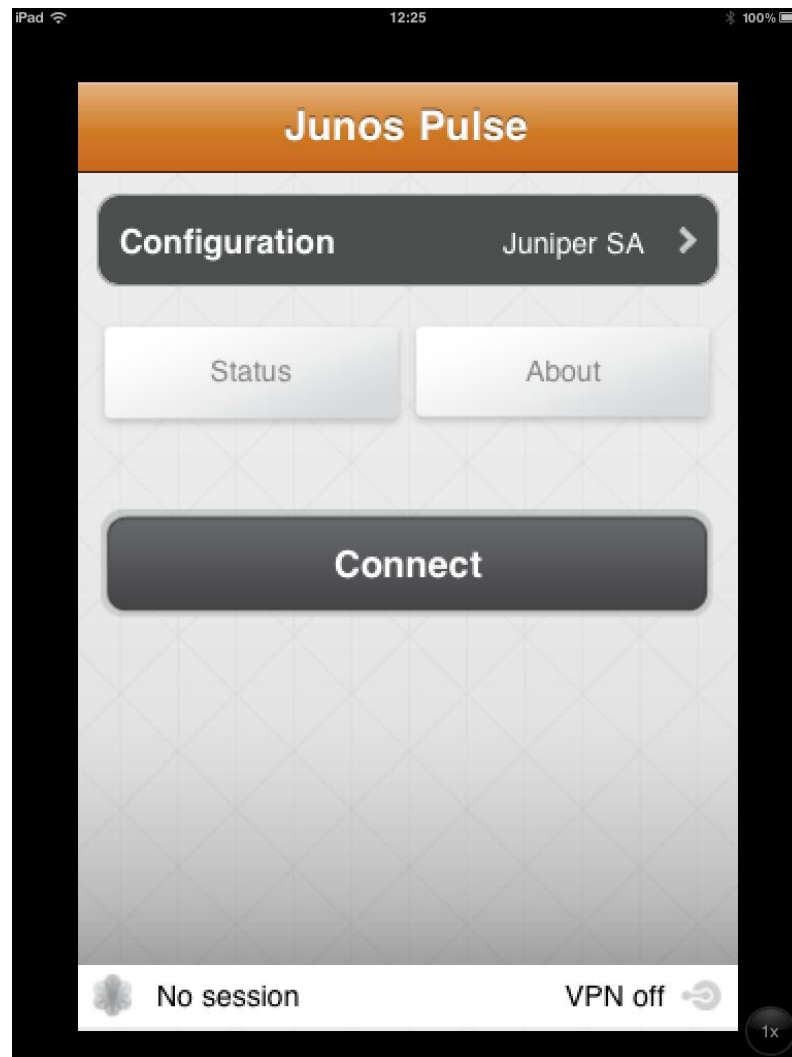
Press "Save" Button



### 3.0 Test iPad Junos Pulse Pre-Loaded Codes Logon

On the iPad, Start Junos Pulse Application

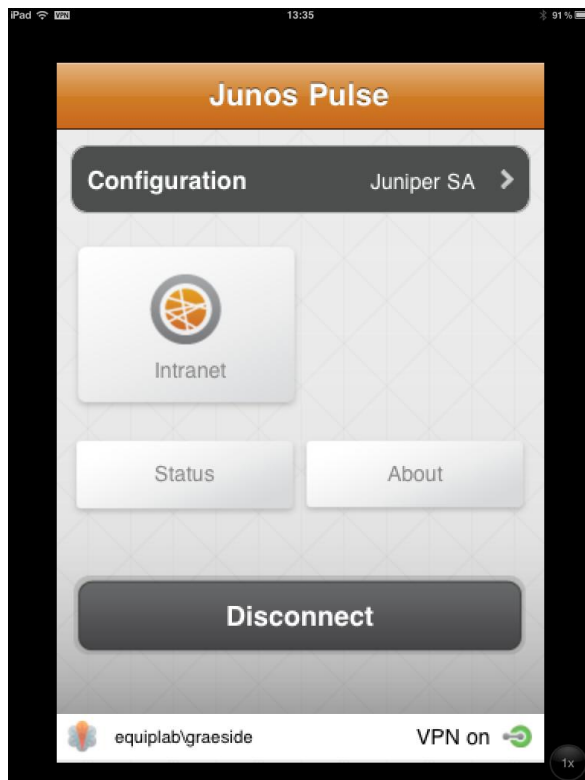
Select Connect Button



User will enter: UserID in the Username box  
Microsoft AD Domain password in password box  
SMS Passcode in the SecurEnvoy Passcode box (received via SMS upon your mobile phone)



Once authenticated a new SMS passcode will be sent to the user's mobile phone, ready for the next authentication. The following screen should then be seen.



## Appendix A Configuration of Juniper® for Real Time Authentication

Login to the Juniper® SSL VPN appliance with administrative permissions.

Navigate to "Authentication" "Auth Servers" select new "Radius Server"



Populate information for the new Radius server (SecurEnvoy)

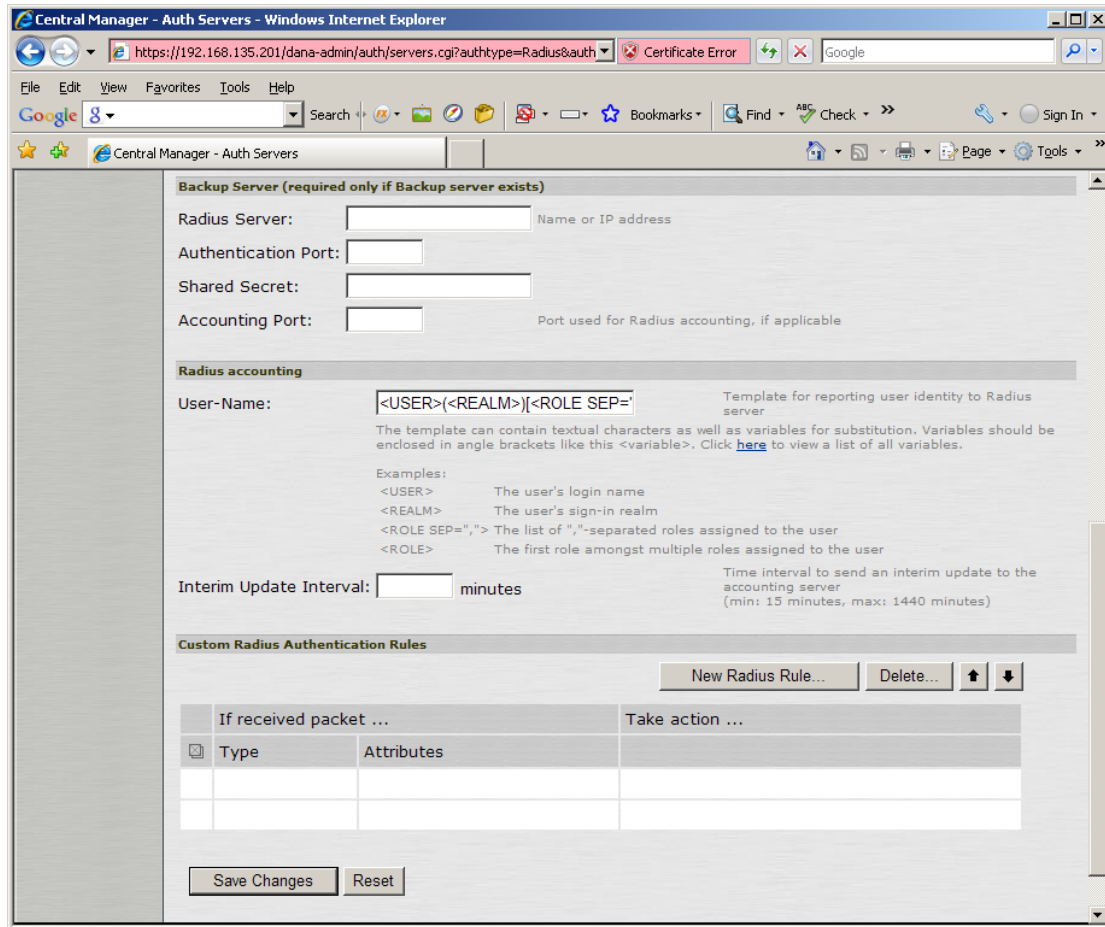
Enter Name, IP address, authentication port and shared secret.

SecurEnvoy recommend you set the timeout settings to at least 10 seconds or greater with a retry of 0.

If redundancy is required, enter details for a second SecurEnvoy Radius server.

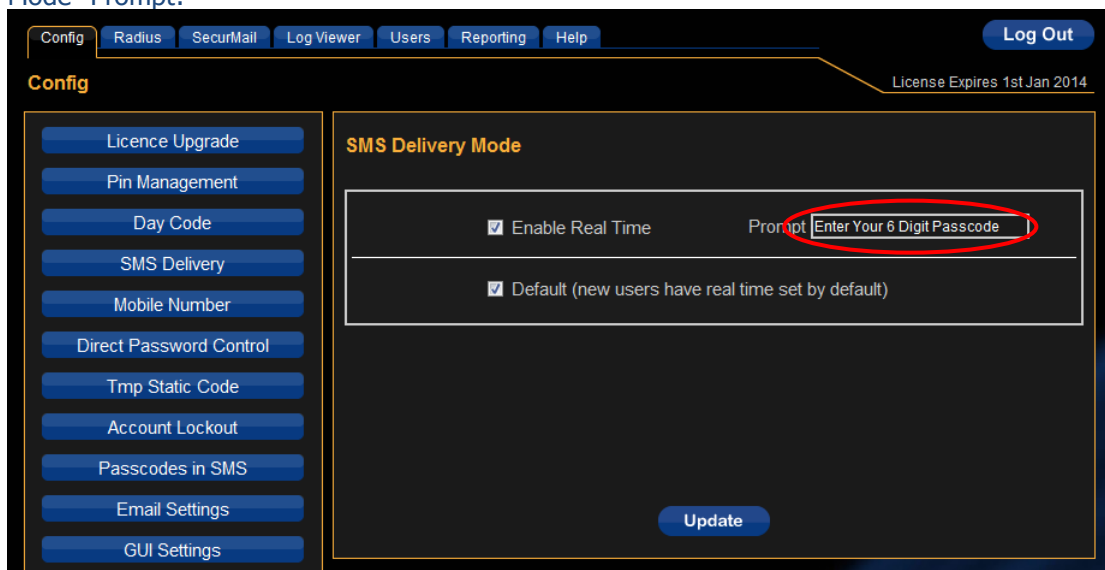


Scroll to bottom and select "New Radius Rule" button as shown below.



Select Radius Attribute "Reply-Message(18)"  
 Select Operand "matches the expression"  
 Set Value to "Enter Your 6 Digit Passcode"

Note this value MUST match the setting in the SecurEnvoy GUI Config setting "SMS Delivery Mode" Prompt:

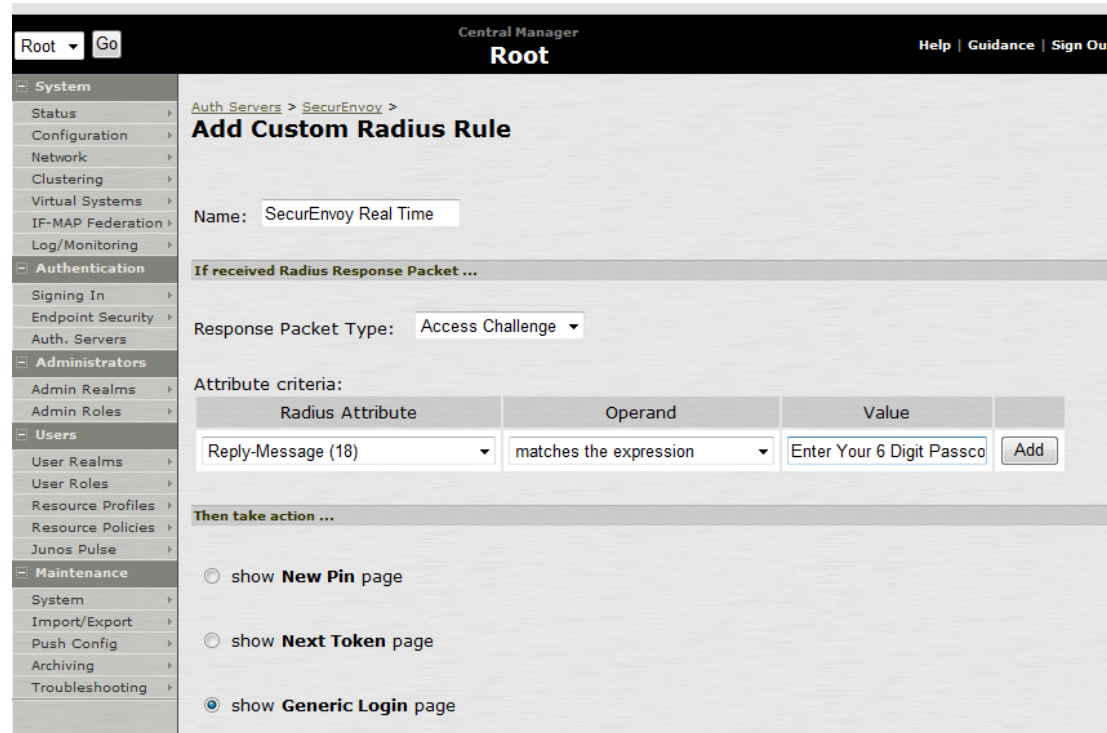


Press the "ADD" button to add this rule

Select Show GENERIC LOGIC Page

Press "Save Changes"

Press "Close"



The screenshot shows the 'Add Custom Radius Rule' configuration page in the SecurEnvoy Central Manager. The breadcrumb trail is 'Auth Servers > SecurEnvoy > Add Custom Radius Rule'. The page title is 'Add Custom Radius Rule'. The 'Name' field is set to 'SecurEnvoy Real Time'. The condition is 'If received Radius Response Packet ...' with 'Response Packet Type' set to 'Access Challenge'. The 'Attribute criteria' table is as follows:

Radius Attribute	Operand	Value	
Reply-Message (18)	matches the expression	Enter Your 6 Digit Passco	Add

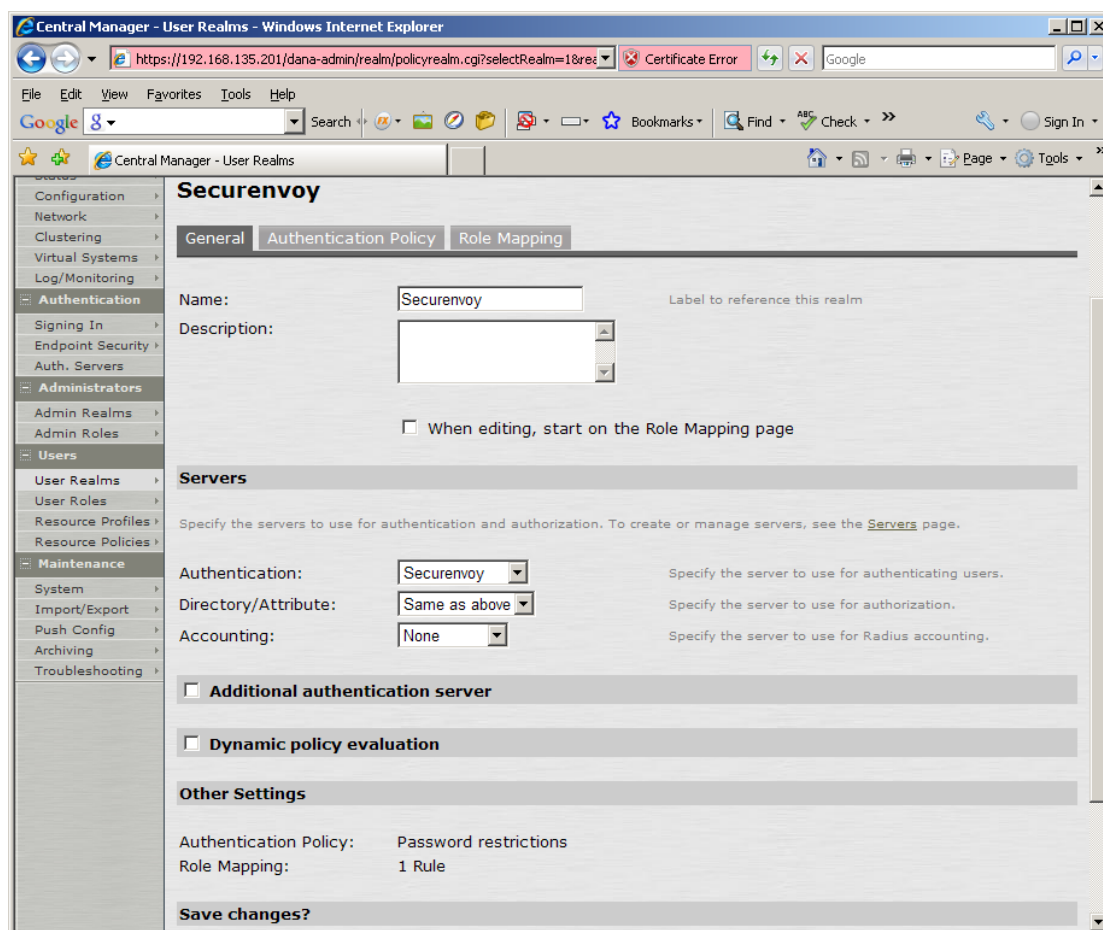
The 'Then take action ...' section has three radio button options: 'show New Pin page', 'show Next Token page', and 'show Generic Login page'. The 'show Generic Login page' option is selected.

Click "Save changes" to submit all configuration parameters

Navigate to "Users", "User Realms" and select the realm configured for SecurEnvoy  
Populate information for "Servers" (this is the previously setup Radius authentication server)

Additional authentication server is not required.

Click "Save changes" to submit all configuration parameters



Save Changes

## Appendix B Configuration of SecurEnvoy for Real Time Passcodes

To help facilitate an easy to use environment, SecurEnvoy can be set up to use the existing Windows password as the PIN component. SecurEnvoy supplies the second factor of authentication, which is the dynamic one time passcode (OTP) which is sent to the user's mobile phone.

Launch the SecurEnvoy admin interface, by executing the Local Security Server Administration link on the SecurEnvoy Security Server.

Click the **"Radius"** Button

Enter IP address and Shared secret for each Juniper® SSL VPN appliance that wishes to use **SecurEnvoy** Two-Factor authentication.

Config **Radius** SecurMail Log Viewer Users Reporting Help Log Out

Radius OK License Expires 1st Jan 2014

**Network Access Server**

- 127.0.0.1
- 192.168.135.201

**NAS IP Address**  Format xxx.xxx.xxx.xxx or default for undefined IP's

**Shared Secret**

Authenticate Passcode Only (password or pin not required)

Default Domain  Only allow this domain

Only allow users that are in the LDAP group Change Group  
Leave group blank to authenticate all users

Override customer name in SMS message with  Max 20  
Leave blank to use default

Pass Back Data To Radius Client in Attribute

- No information is passed back
- Password is passed back
- LDAP group members are passed back (Return distinguished names )
- User's Distinguished Name

Delete Selected Update New

Do **NOT** click the checkbox "Authenticate Passcode Only"

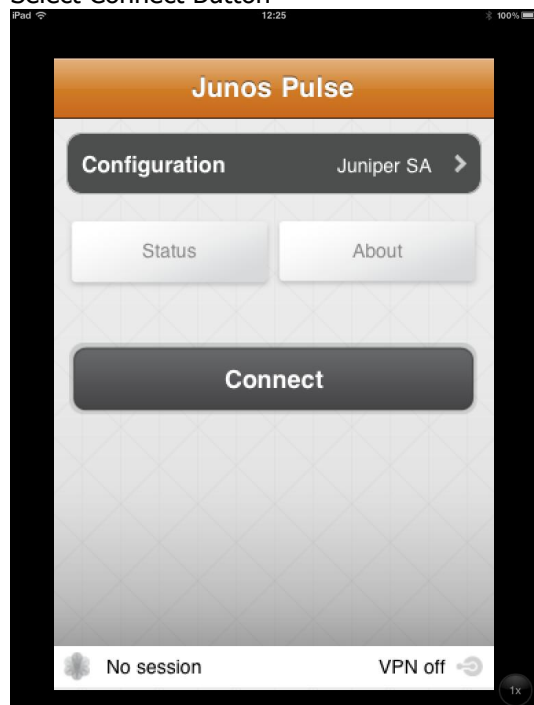
Click **"Update"** to confirm settings.

Click **"Logout"** when finished. This will log out of the Administrative session.

### Appendix C Test iPad Junos Pulse Real Time Codes Logon

On the iPad, Start Junos Pulse Application

Select Connect Button

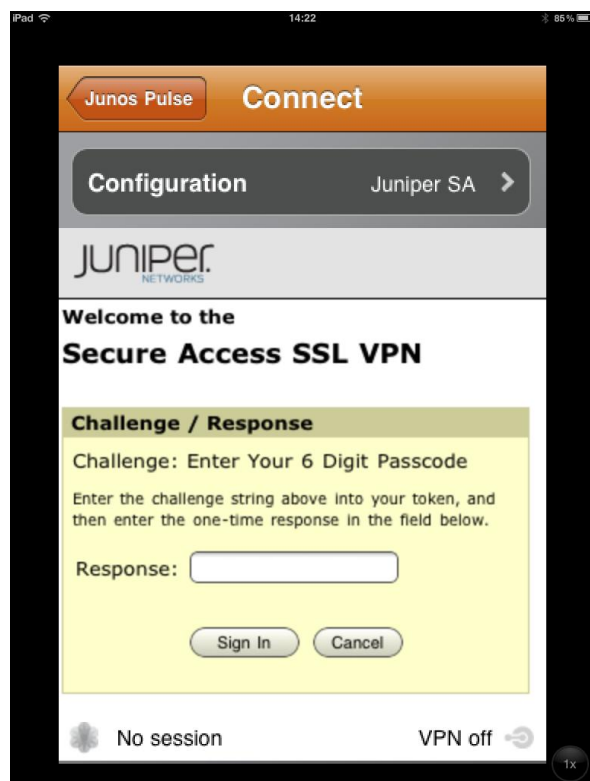


User will enter: UserID in the Username box  
Microsoft AD Domain password in password box



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

Note: the Juniper Generic Login page can be customised to change this pages text and prompt, see Juniper's guide on customising web templates.



After authentication you should see the following

