

External Authentication with Juniper® 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	

Juniper® SSL VPN appliance Integration Guide

This document describes how to integrate a Juniper® SSL VPN appliance with SecurEnvoy two-factor Authentication solution called 'SecurAccess'.

Juniper® SSL VPN appliance provides - Secure Remote Access to the internal corporate network.

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 6.0R2

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 v5.1.500

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	9
Appendix B	Configuration of SecurEnvoy for Real Time Passcodes	12
Appendix C	Test Real Time Codes Logon.....	14

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)

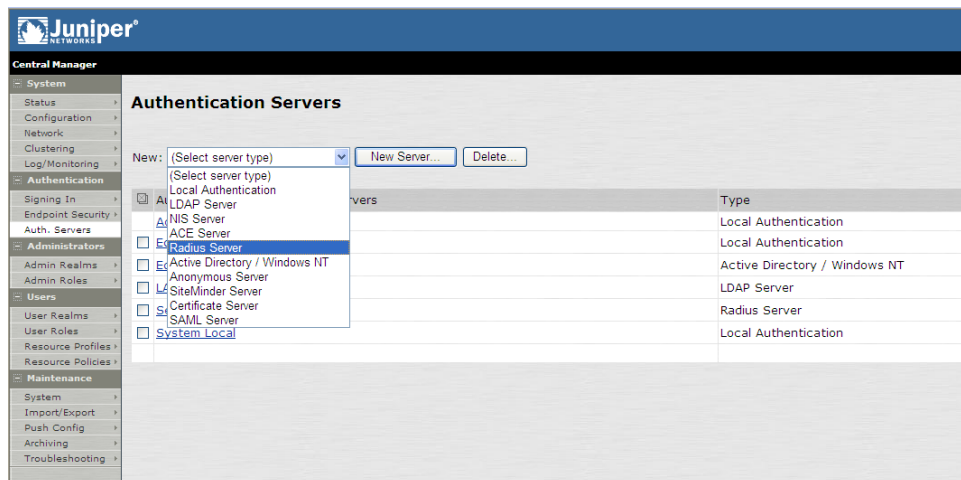
Securenvoy Security Server has been installed with the Radius service and has a suitable account that has read and write privileges to the Active Directory, if firewalls are between the SecurEnvoy Security server, Active Directory servers, and the Juniper® SSL VPN appliance(s), additional open ports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

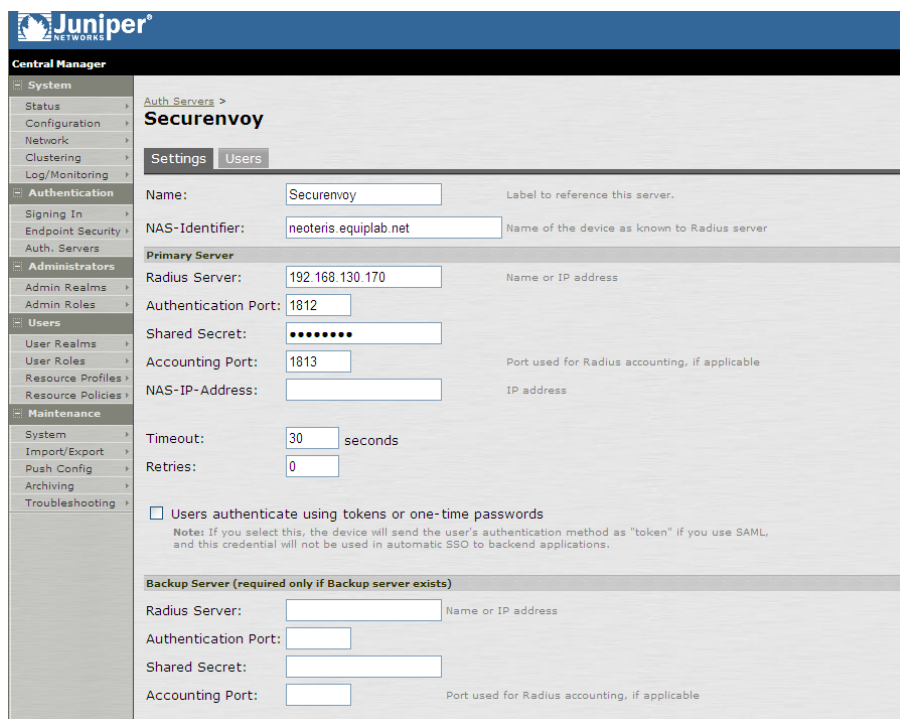


Populate information for the new Radius server (SecurEnvoy)

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

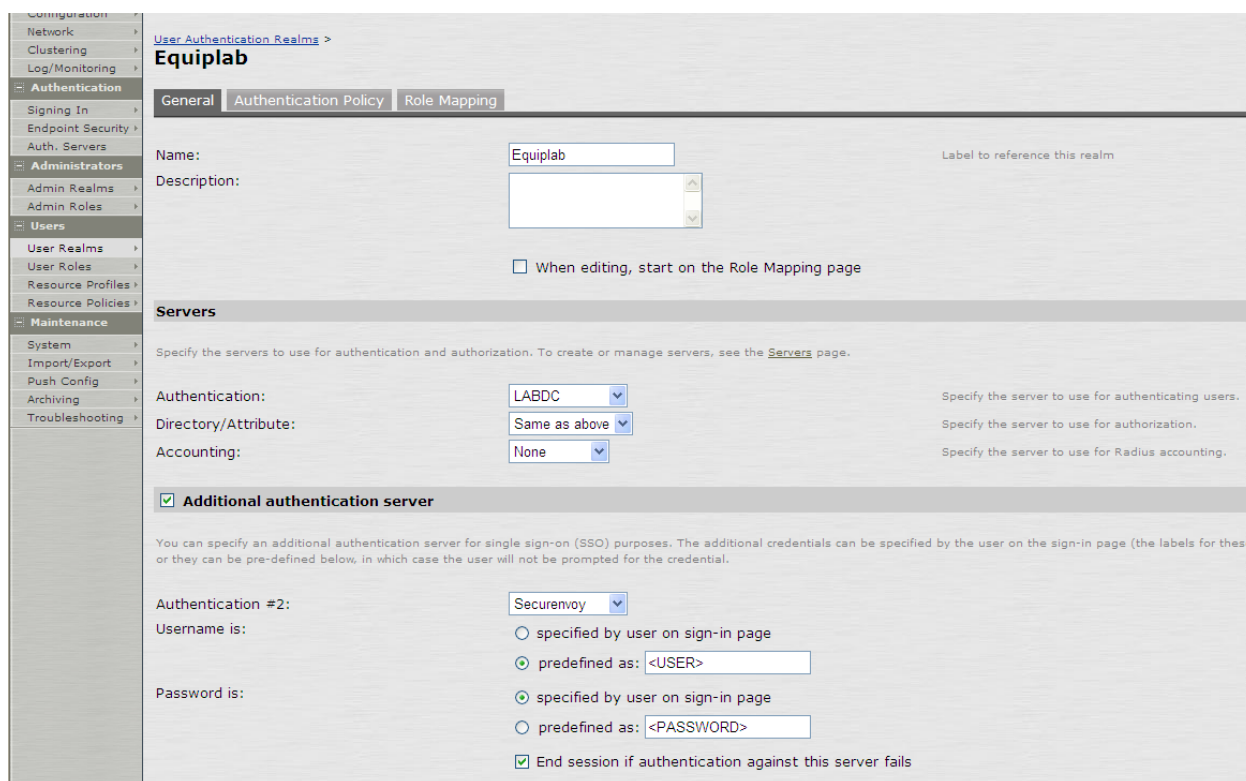
SecurEnvoy recommend to set the timeout settings to at least 10 seconds or greater with a retry of 0.

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.



The screenshot shows the configuration page for a user realm named "Equiplab". The left sidebar contains a navigation menu with categories like Configuration, Network, Clustering, Log/Monitoring, Authentication, Signing In, Endpoint Security, Administrators, Users, and Maintenance. The "Users" section is expanded to show "User Realms".

The main content area has three tabs: "General", "Authentication Policy", and "Role Mapping". The "General" tab is active. It contains the following fields:

- Name:** Equiplab (Text input)
- Description:** (Text area)
- When editing, start on the Role Mapping page
- Servers:**
 - Authentication: LABDC (Dropdown)
 - Directory/Attribute: Same as above (Dropdown)
 - Accounting: None (Dropdown)
- Additional authentication server**
 - Authentication #2: Securenvoy (Dropdown)
 - Username is:
 - specified by user on sign-in page
 - predefined as: <USER> (Text input)
 - Password is:
 - specified by user on sign-in page
 - predefined as: <PASSWORD> (Text input)
 - 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"

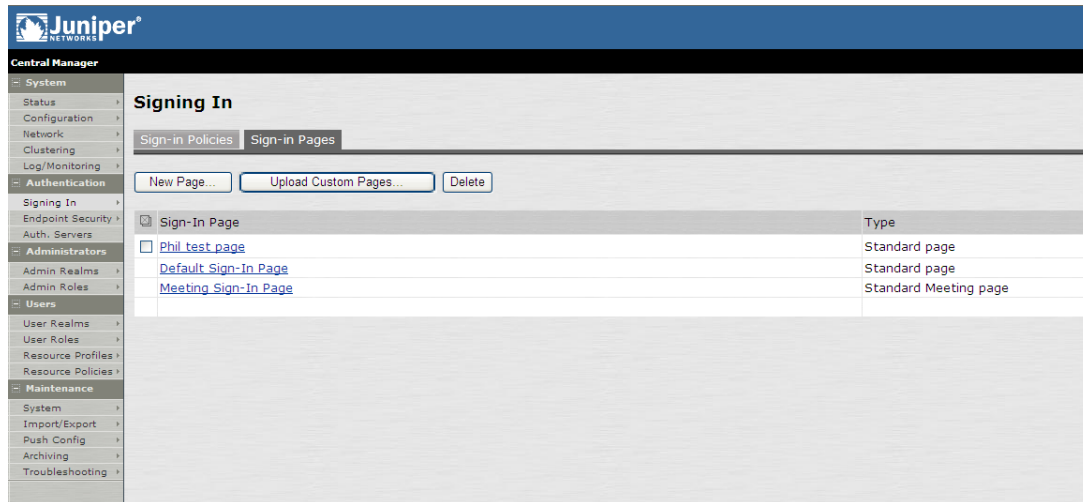
Click checkbox "End session if authentication this server fails"

Click "Save changes" to submit all configuration parameters

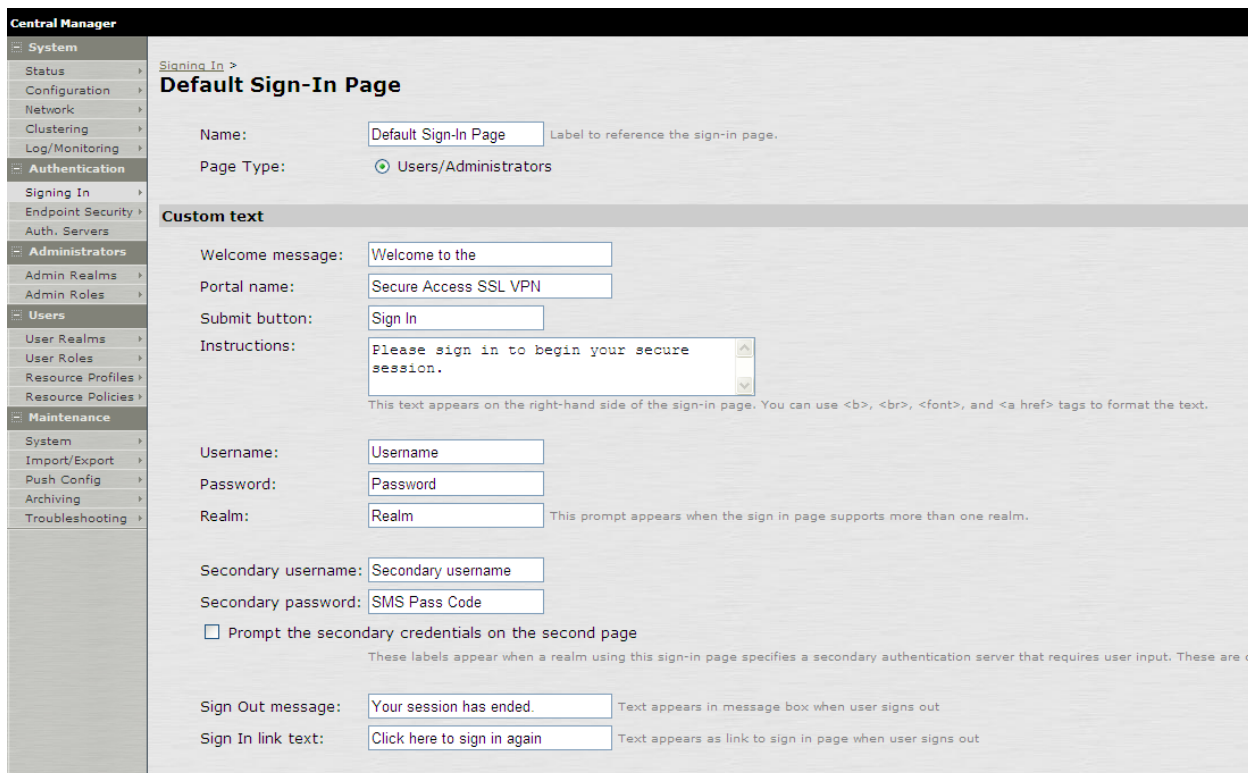
Navigate to "Authentication" "Signing In" "Sign-in Pages"

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

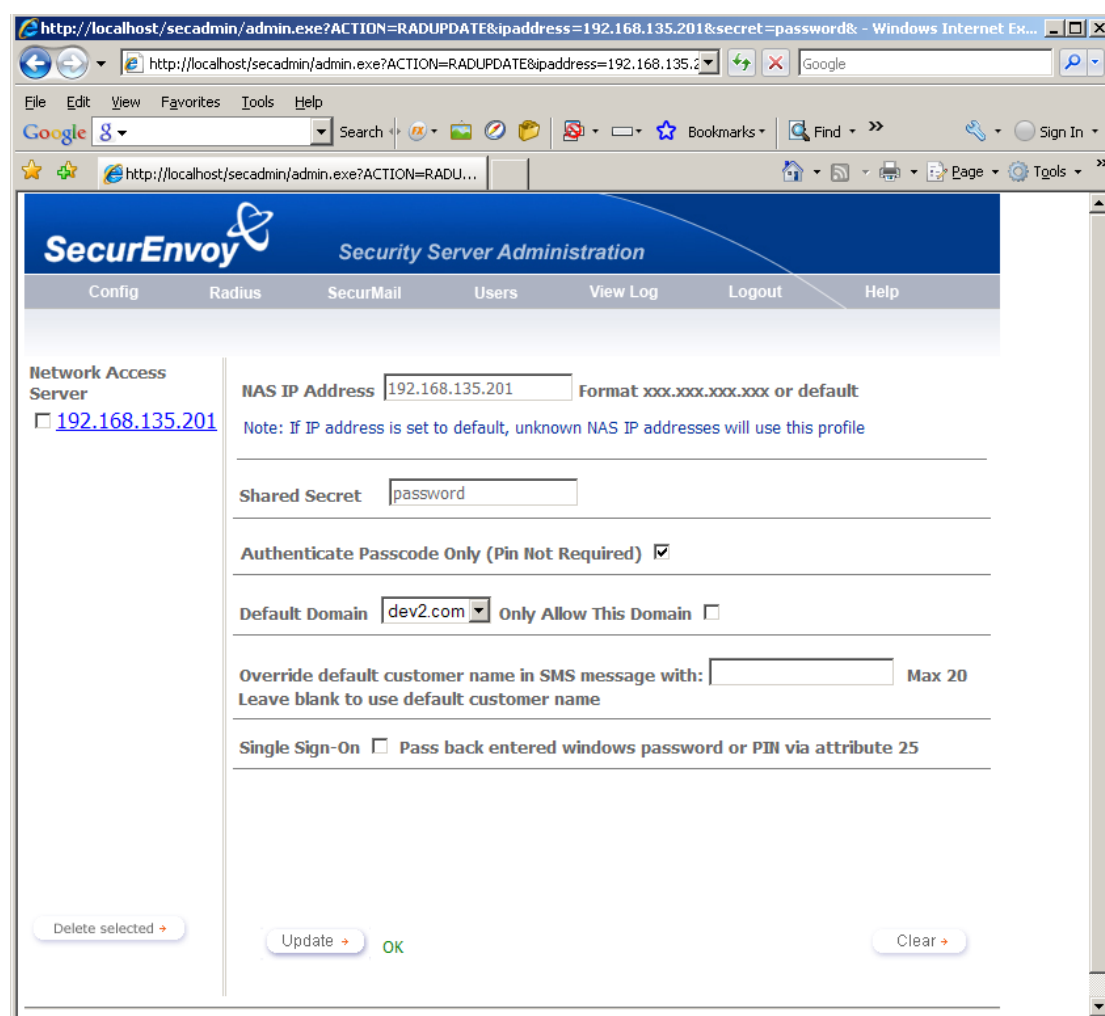
2.0 Configuration of SecurEnvoy for Pre-Loaded Passcodes

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 Security Server Administration interface. The browser address bar displays the URL: `http://localhost/secadmin/admin.exe?ACTION=RADUPDATE&ipaddress=192.168.135.201&secret=password&`. The page title is "SecurEnvoy Security Server Administration". The navigation menu includes "Config", "Radius", "SecurMail", "Users", "View Log", "Logout", and "Help". The "Radius" tab is selected. The "Network Access Server" section shows a list of servers with a checkbox next to "192.168.135.201". The configuration form for this server includes the following fields and options:

- NAS IP Address:** Format xxx.xxx.xxx.xxx or default
- Shared Secret:**
- Authenticate Passcode Only (Pin Not Required):**
- Default Domain:** Only Allow This Domain
- Override default customer name in SMS message with:** Max 20
Leave blank to use default customer name
- Single Sign-On:** Pass back entered windows password or PIN via attribute 25

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

Click checkbox "Authenticate Passcode Only (PIN Not Required)"

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

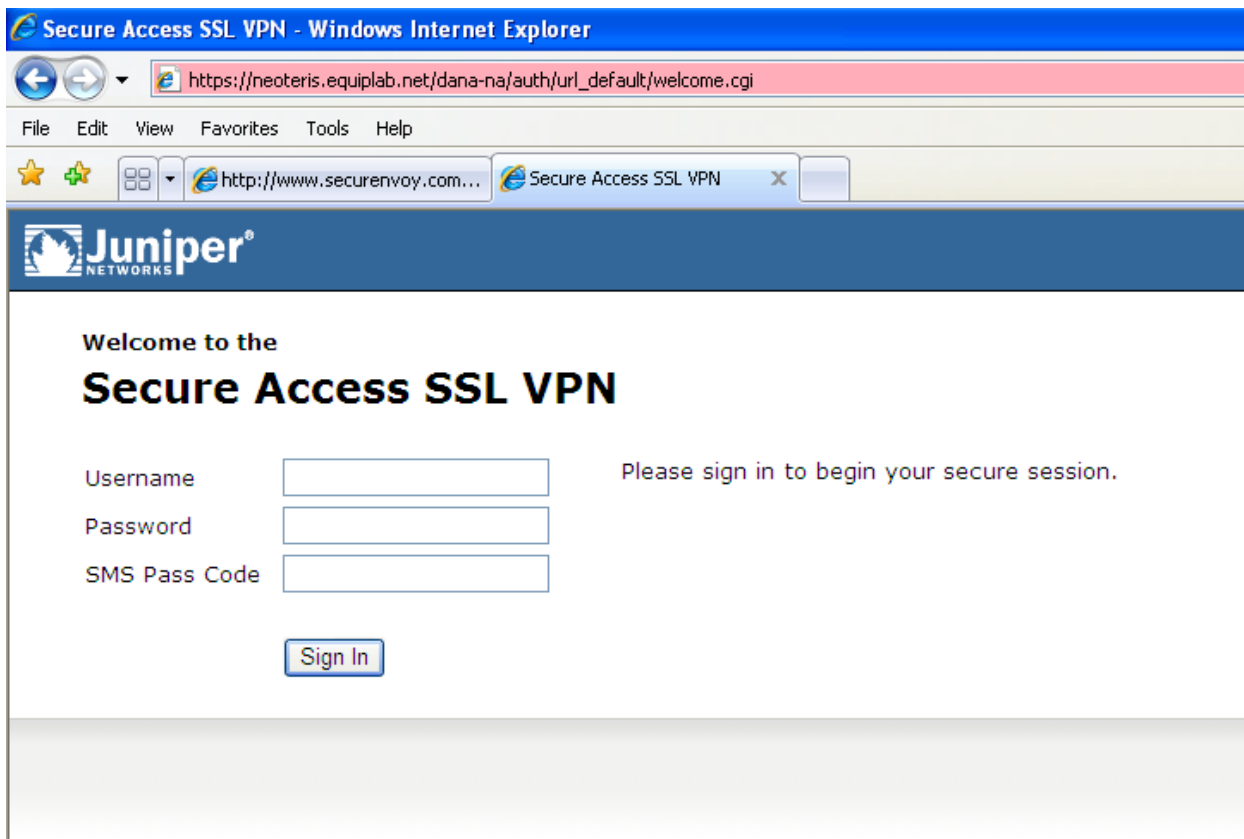
Click **"Logout"** when finished. This will log out of the Administrative session.

3.0 Test Pre-Loaded Codes Logon

Browse to the web URL address of the Juniper® SSL appliance

Three input dialogue boxes will be displayed.

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



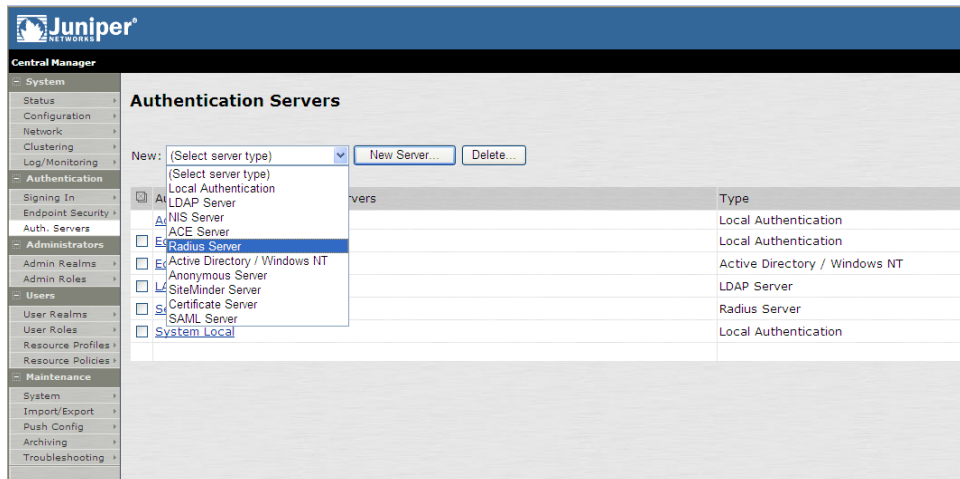
Click "Sign In" to complete the process.

Once authenticated a new SMS passcode will be sent to the user's mobile phone, ready for the next authentication.

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"

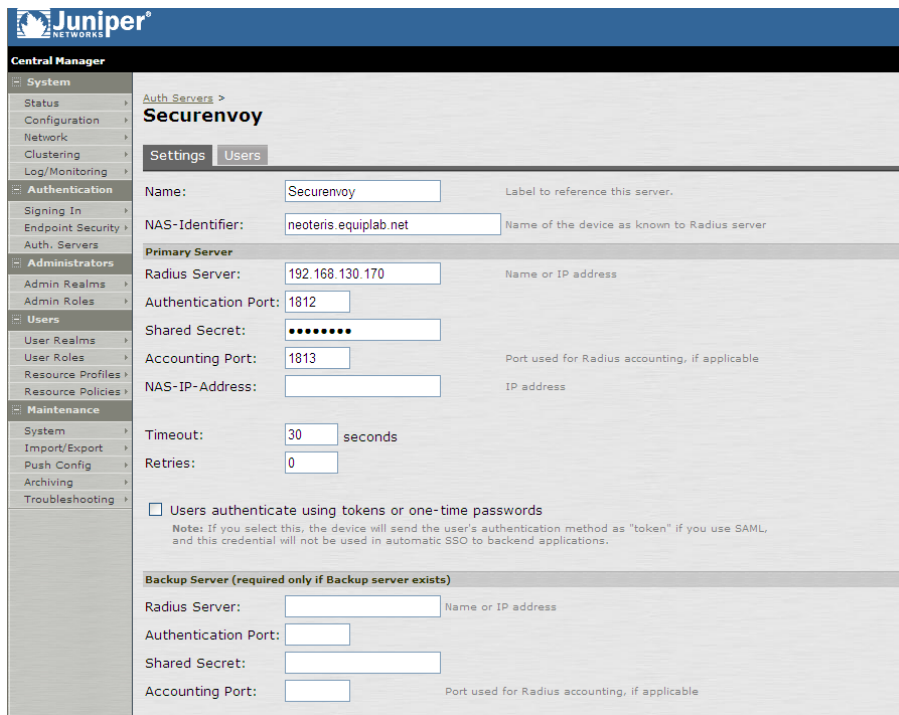


Populate information for the new Radius server (SecurEnvoy)

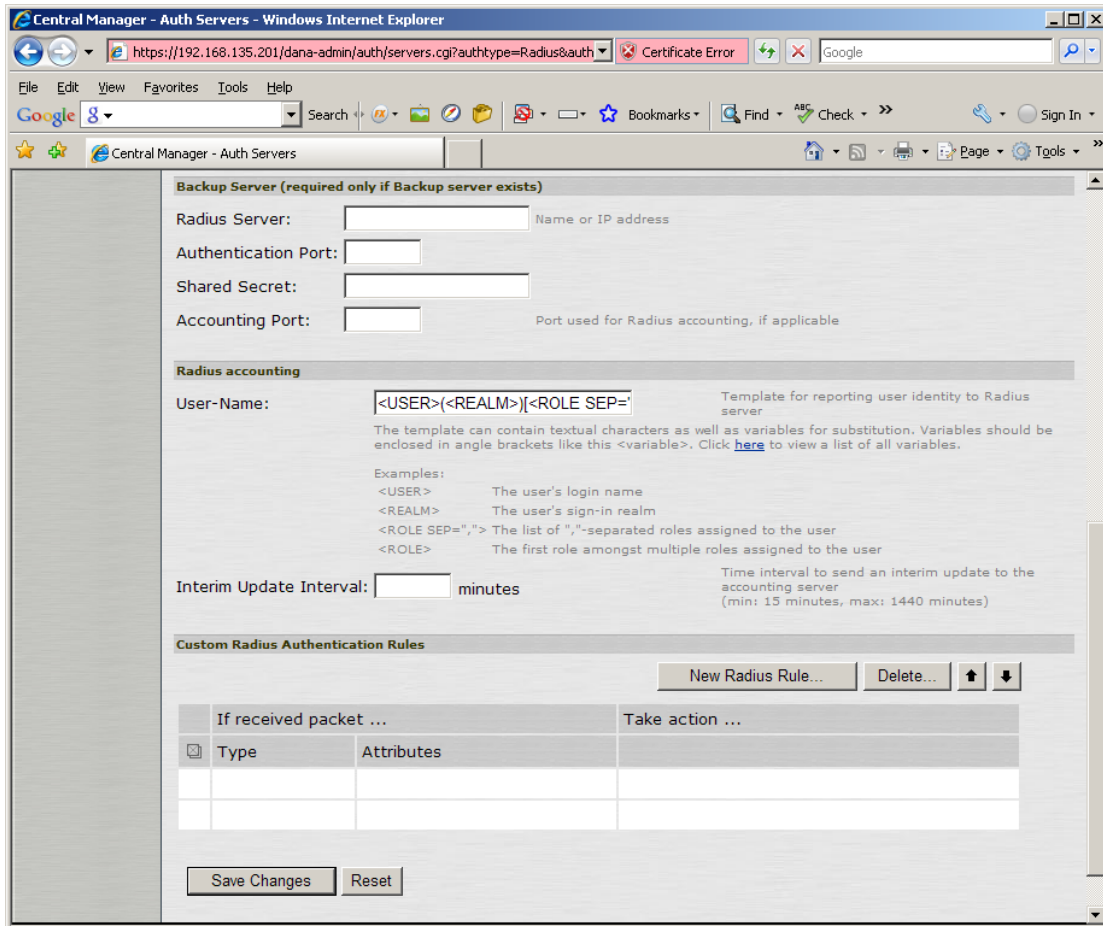
Enter Name, IP address, authentication port and shared secret.

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.

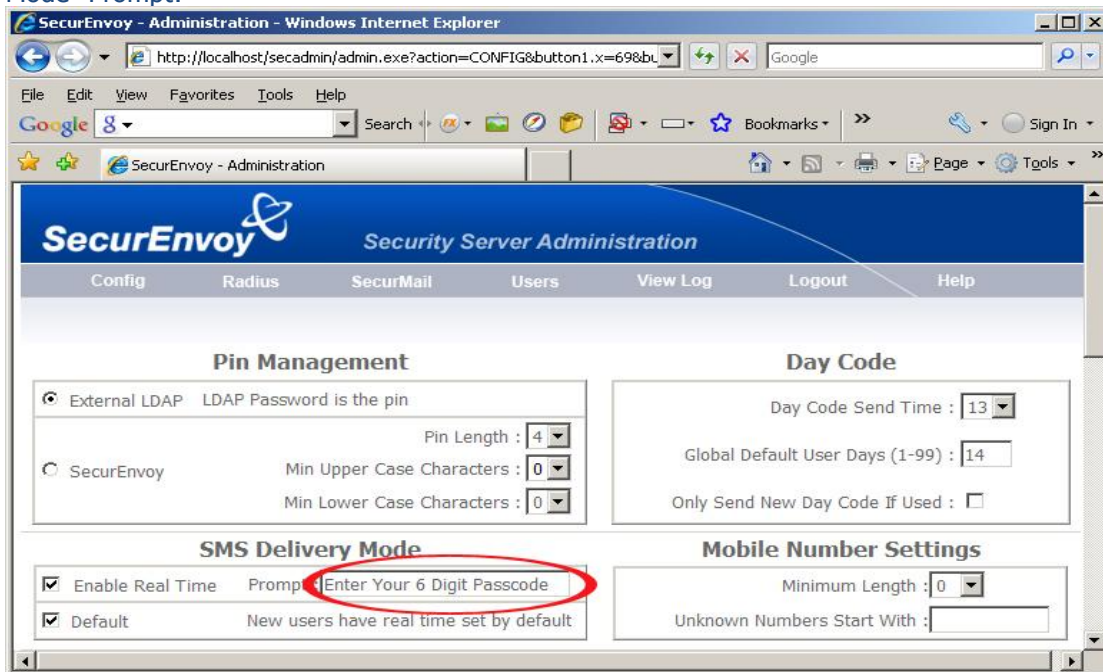


Scroll to bottom and select "New Radius Rule" button as shown below.



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:

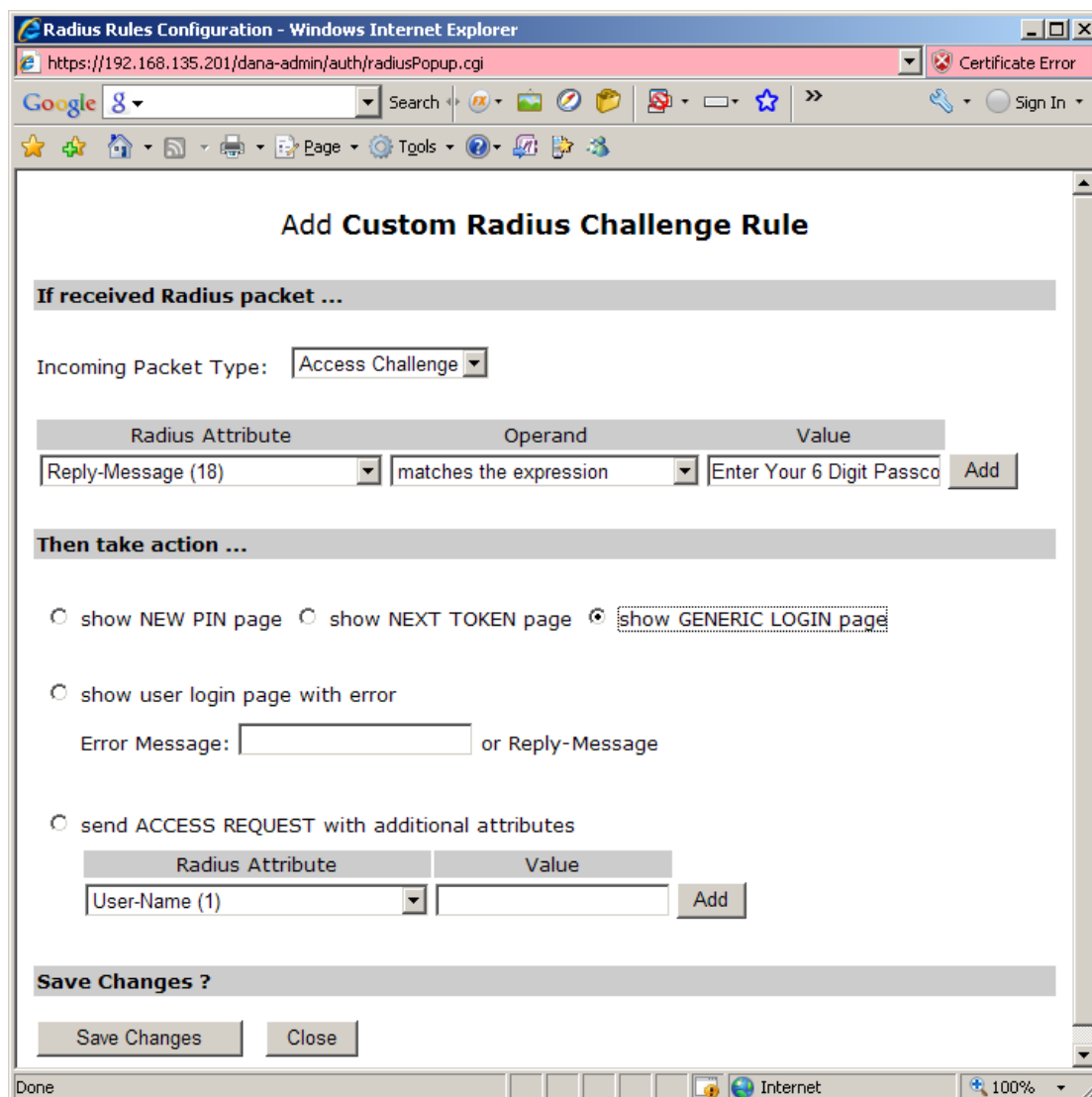


Press the "ADD" button to add this rule

Select Show GENERIC LOGIC Page

Press "Save Changes"

Press "Close"



Add Custom Radius Challenge Rule

If received Radius packet ...

Incoming Packet Type:

Radius Attribute	Operand	Value
<input type="text" value="Reply-Message (18)"/>	<input type="text" value="matches the expression"/>	<input type="text" value="Enter Your 6 Digit Passco"/> <input type="button" value="Add"/>

Then take action ...

show NEW PIN page
 show NEXT TOKEN page
 show GENERIC LOGIN page

show user login page with error
 Error Message: or Reply-Message

send ACCESS REQUEST with additional attributes

Radius Attribute	Value
<input type="text" value="User-Name (1)"/>	<input type="text"/> <input type="button" value="Add"/>

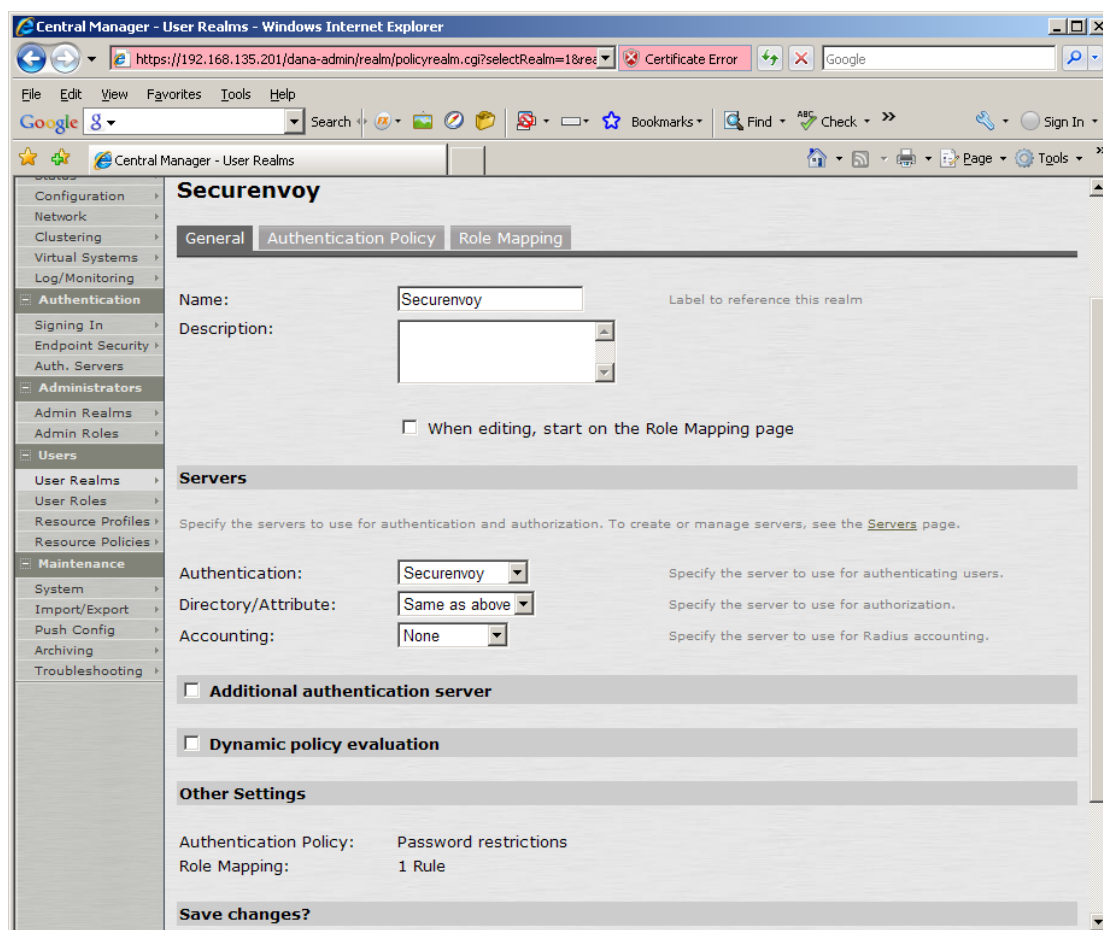
Save Changes ?

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.

http://localhost/secadmin/admin.exe?ACTION=RADUPDATE&ipaddress=192.168.135.201&secret=password& - Windows Internet Ex...

http://localhost/secadmin/admin.exe?ACTION=RADUPDATE&ipaddress=192.168.135.201

File Edit View Favorites Tools Help

Google 8 Search

http://localhost/secadmin/admin.exe?ACTION=RADU...

SecurEnvoy Security Server Administration

Config Radius SecurMail Users View Log Logout Help

Network Access Server

[192.168.135.201](#)

NAS IP Address Format xxx.xxx.xxx.xxx or default

Note: If IP address is set to default, unknown NAS IP addresses will use this profile

Shared Secret

Authenticate Passcode Only (Pin Not Required)

Default Domain Only Allow This Domain

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

Single Sign-On Pass back entered windows password or PIN via attribute 25

Delete selected → Update → OK Clear →

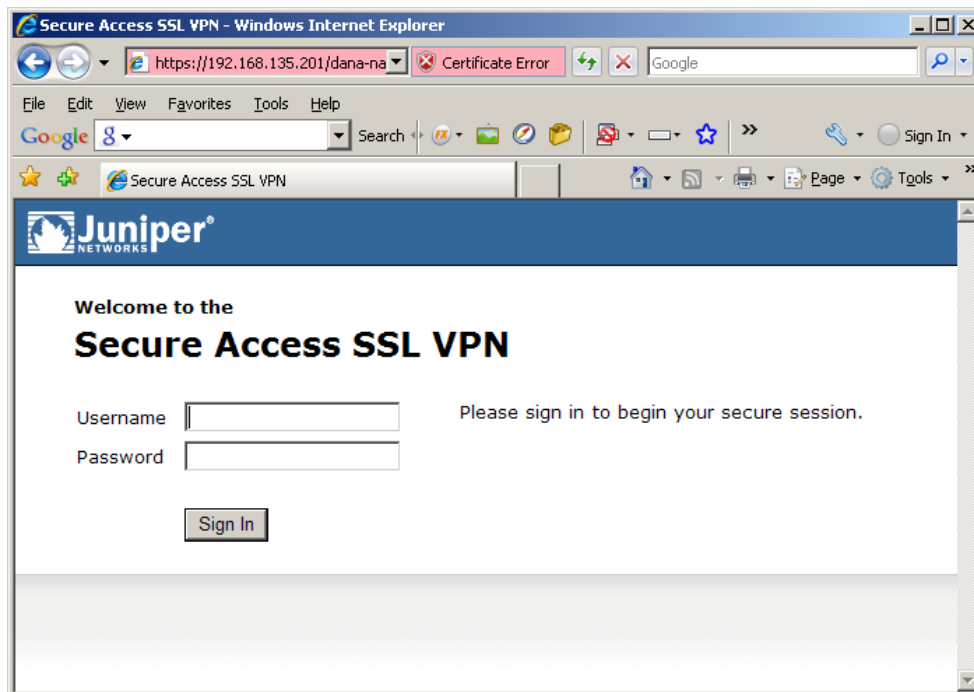
Do **NOT** click the checkbox "Authenticate Passcode Only"

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

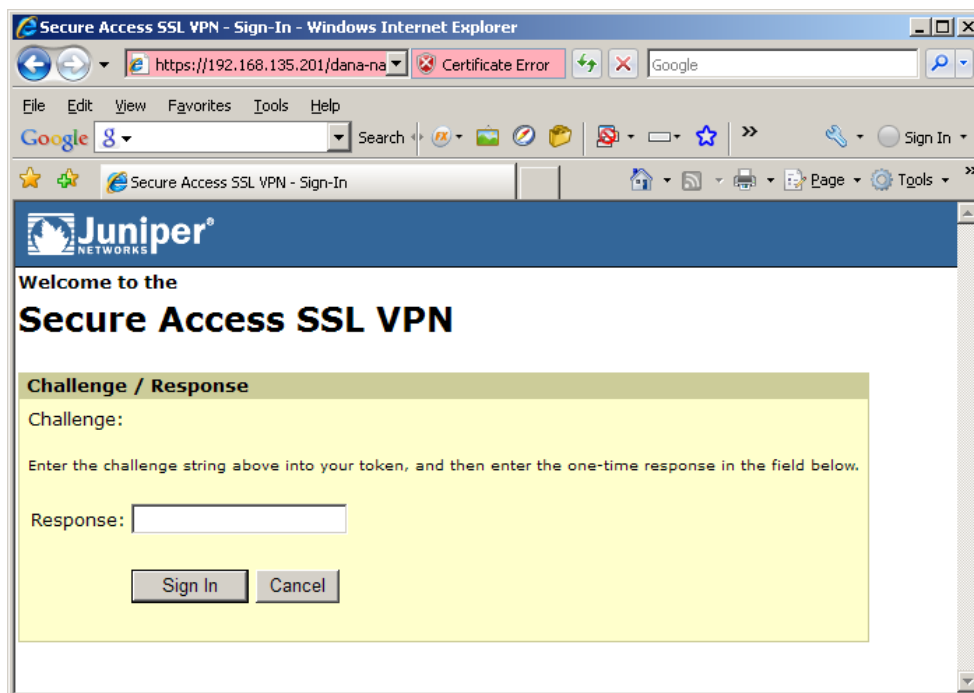
Click "**Logout**" when finished. This will log out of the Administrative session.

Appendix C Test Real Time Codes Logon

Browse to the web URL address of the Juniper® SSL appliance
Enter a valid SecurEnvoy UserID
Enter your Windows Password (or PIN) at the password prompt



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.