# External Authentication with Juniper® SSL VPN appliance

# Authenticating Users Using SecurAccess Server by SecurEnvoy

| **Contact information** | | |
|---|---|---|
| SecurEnvoy | www.securenvoy.com | 0845 2600010 |
| | 1210 Parkview<br>Arlington Business Park<br>Theale<br>Reading<br>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 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

**Index**

## 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)*

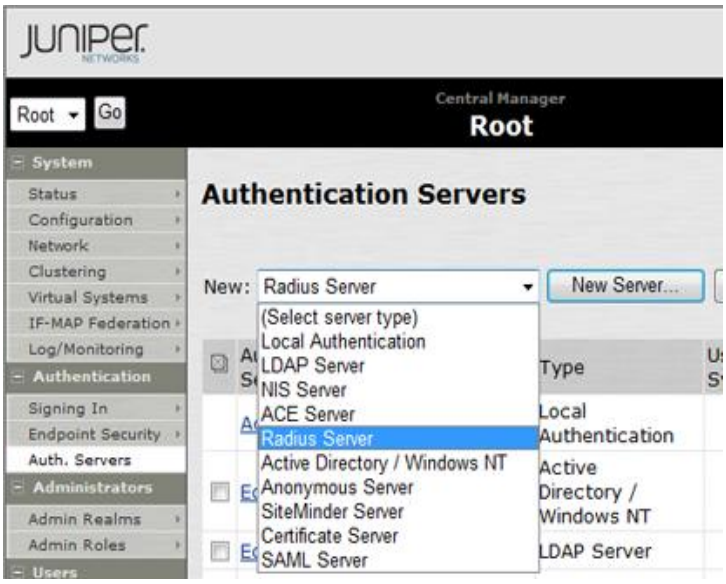
*Securenvoy Security Server has been installed with the Radius service and has a suitable account that has read and write privileges to the Active Directory, if firewalls are between the SecurEnvoy Security server, Active Directory servers, and the Juniper® SSL VPN appliance(s), additional open ports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



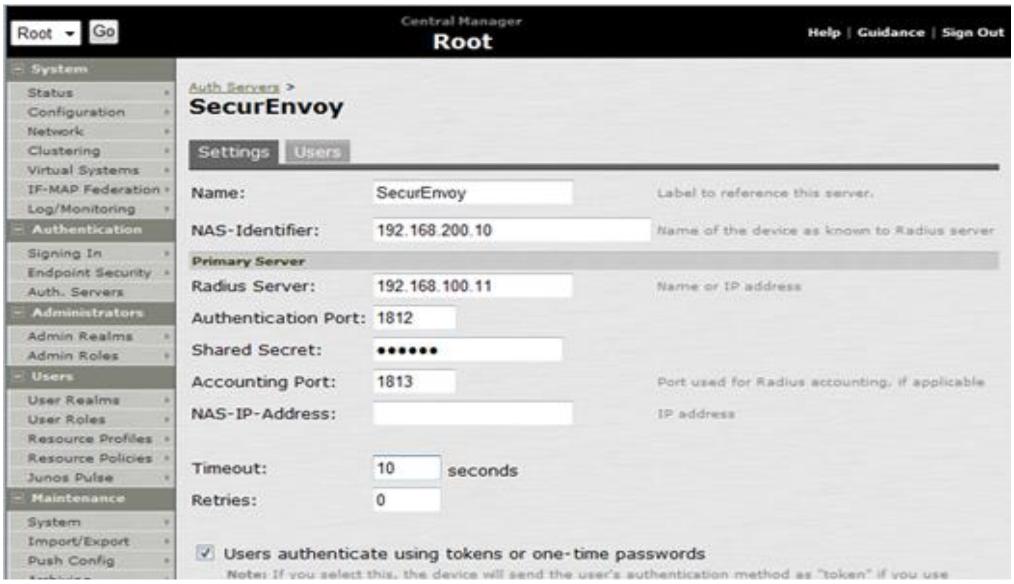
Authentication Servers

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.



Auth Servers >

SecurEnvoy

Name: SecurEnvoy — Label to reference this server.

NAS-Identifier: 192.168.200.10 — Name of the device as known to Radius server

Primary Server

Radius Server: 192.168.100.11 — Name or IP address

Authentication Port: 1812

Shared Secret: ••••••

Accounting Port: 1813 — Port used for Radius accounting, if applicable

NAS-IP-Address: — IP address

Timeout: 10 seconds

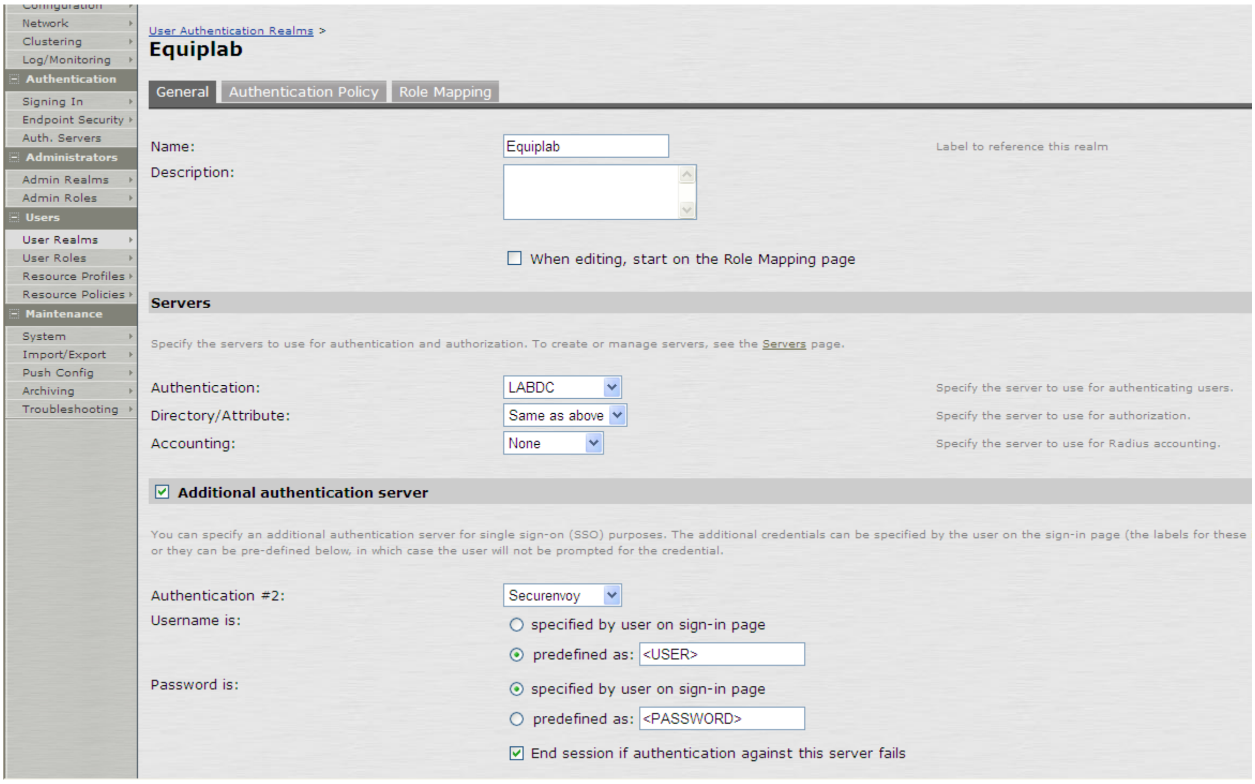
Retries: 0

☑ Users authenticate using tokens or one-time passwords

Note: If you select this, the device will send the user's authentication method as "token" if you use

Click "Save changes" to submit all configuration parameters

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



User Authentication Realms >

**Equiplab**

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”

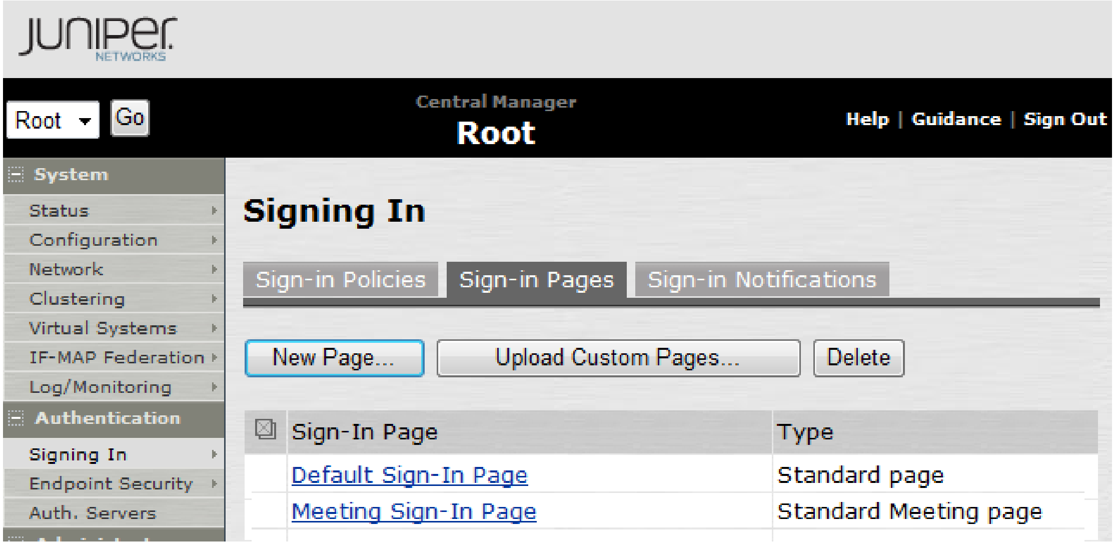
Click checkbox “End session if authentication this server fails”

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"

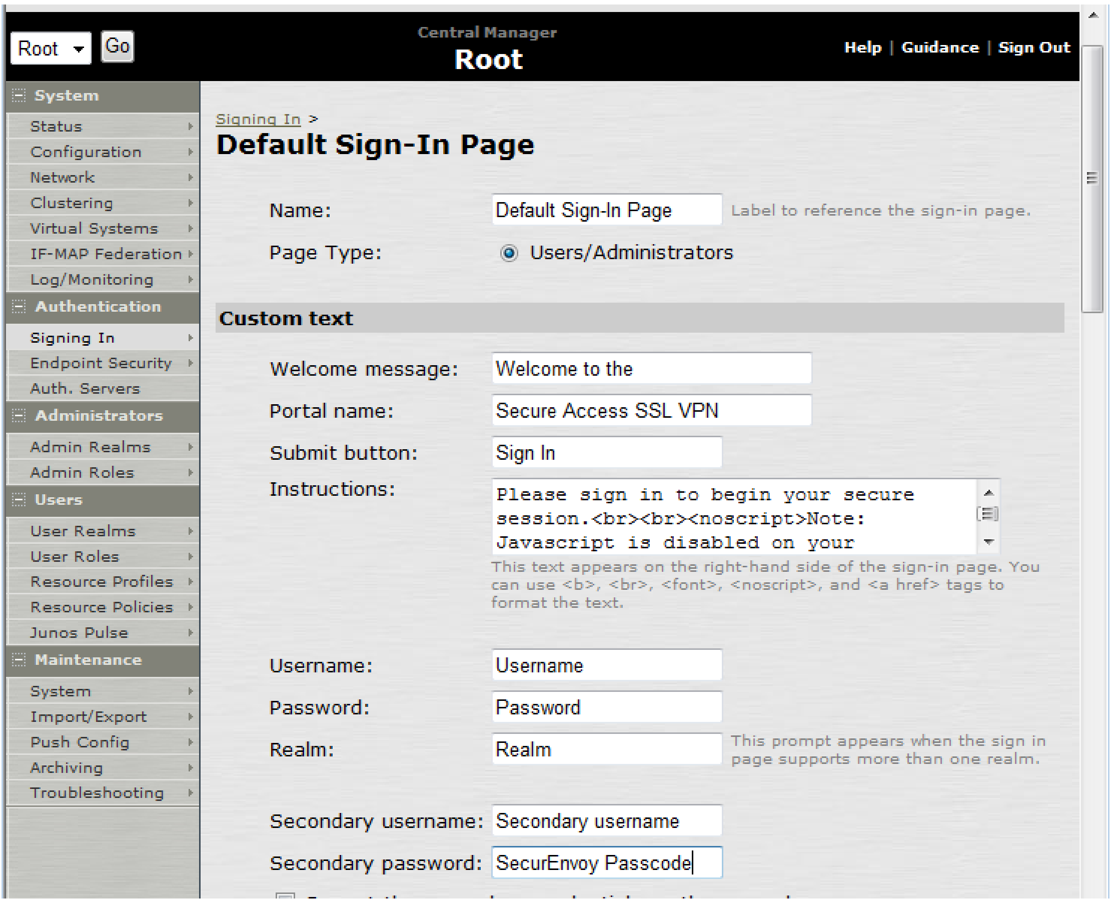
Click the link for "Default Sign-In Page"



Signing In

| ☒ | Sign-In Page | Type |
|---|---|---|
| | Default Sign-In Page | Standard page |
| | Meeting Sign-In Page | Standard Meeting page |

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



Signing In >

Default Sign-In Page

Name: Default Sign-In Page — Label to reference the sign-in page.

Page Type: ● Users/Administrators

Custom text

Welcome message: Welcome to the

Portal name: Secure Access SSL VPN

Submit button: Sign In

Instructions:
```
Please sign in to begin your secure
session.<br><br><noscript>Note:
Javascript is disabled on your
```
This text appears on the right-hand side of the sign-in page. You can use <b>, <br>, <font>, <noscript>, and <a href> tags to format the text.

Username: Username

Password: Password

Realm: Realm — This prompt appears when the sign in page supports more than one realm.

Secondary username: Secondary username

Secondary password: SecurEnvoy Passcode

Click "Save changes" to submit all configuration parameters

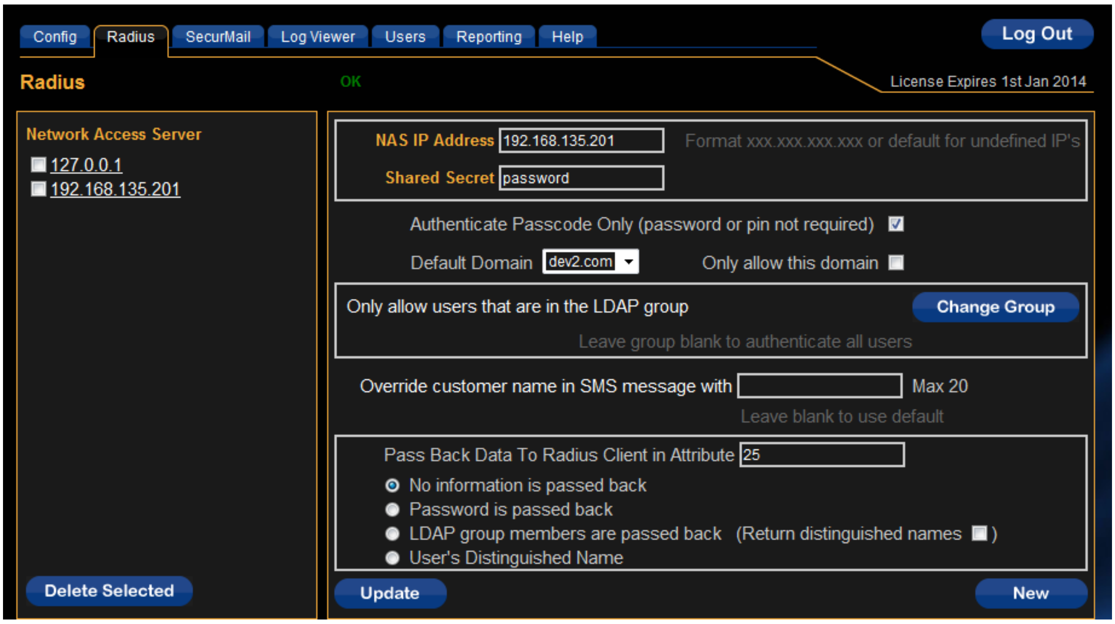
## 2.0 Configuration of SecurEnvoy for Pre-Loaded Passcodes

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.



Radius

OK

License Expires 1st Jan 2014

Network Access Server

☐ 127.0.0.1

☐ 192.168.135.201

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) ☑

Default Domain: dev2.com — Only allow this domain ☐

Only allow users that are in the LDAP 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: 25

● No information is passed back

○ Password is passed back

○ LDAP group members are passed back (Return distinguished names ☐ )

○ User's Distinguished Name

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

Click **“Update”** to confirm settings.

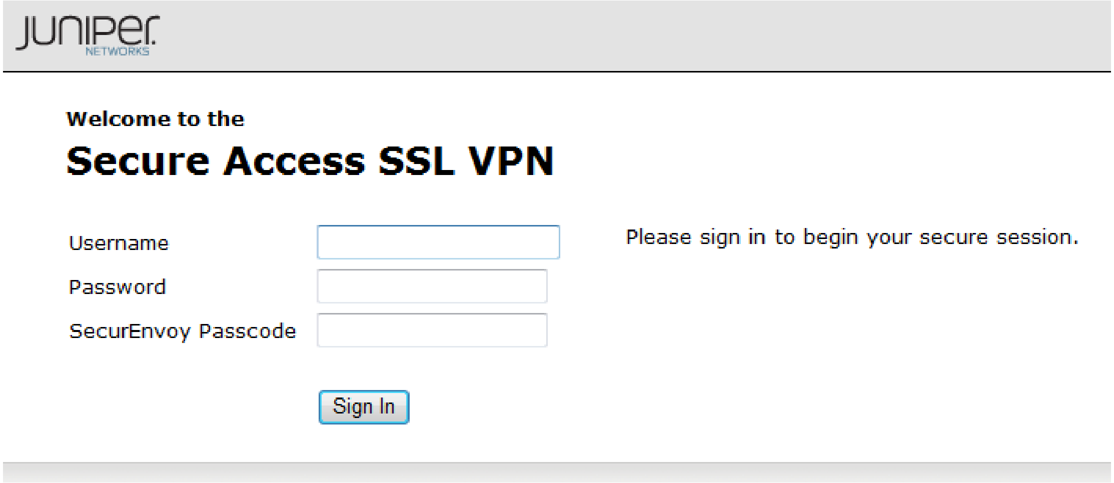
Click **“Logout”** when finished. This will log out of the Administrative session.

## 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 SecurEnvoy Passcode box (received via SMS upon your mobile phone)



Welcome to the

Secure Access SSL VPN

Please sign in to begin your secure session.

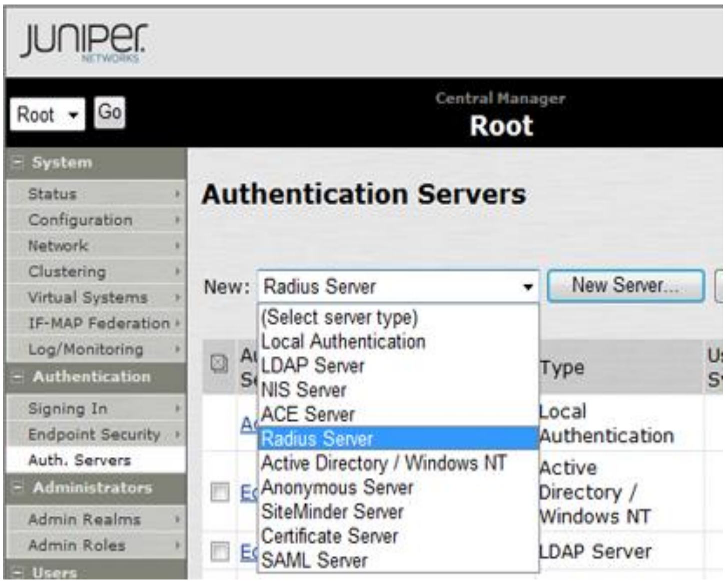
Click "Sign In" to complete the process.

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”



Central Manager
Root

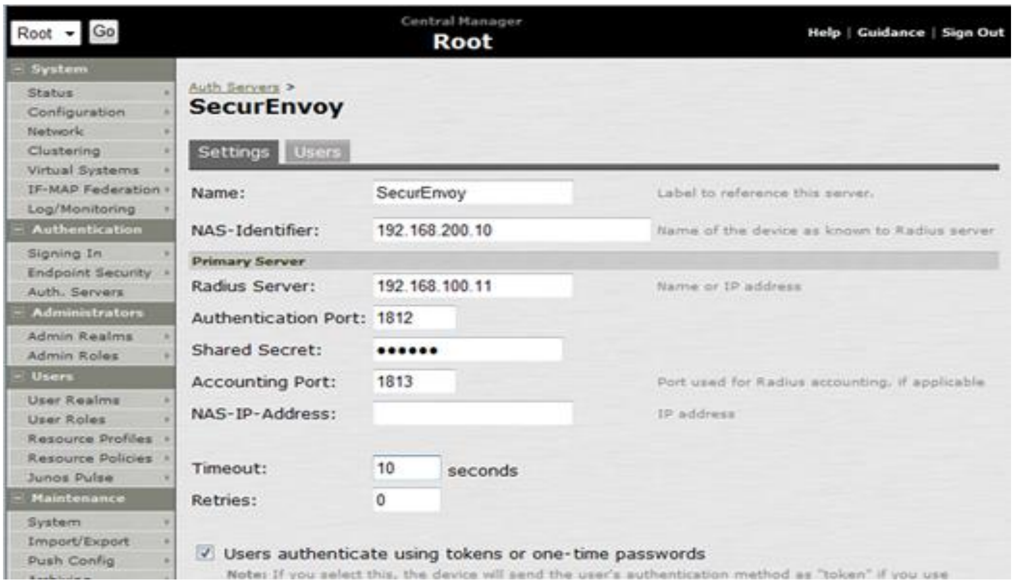
Authentication Servers

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.



Central Manager
Root

Auth Servers >
SecurEnvoy

Settings | Users

Name: SecurEnvoy — Label to reference this server.

NAS-Identifier: 192.168.200.10 — Name of the device as known to Radius server

Primary Server

Radius Server: 192.168.100.11 — Name or IP address

Authentication Port: 1812

Shared Secret: ••••••

Accounting Port: 1813 — Port used for Radius accounting, if applicable

NAS-IP-Address: — IP address

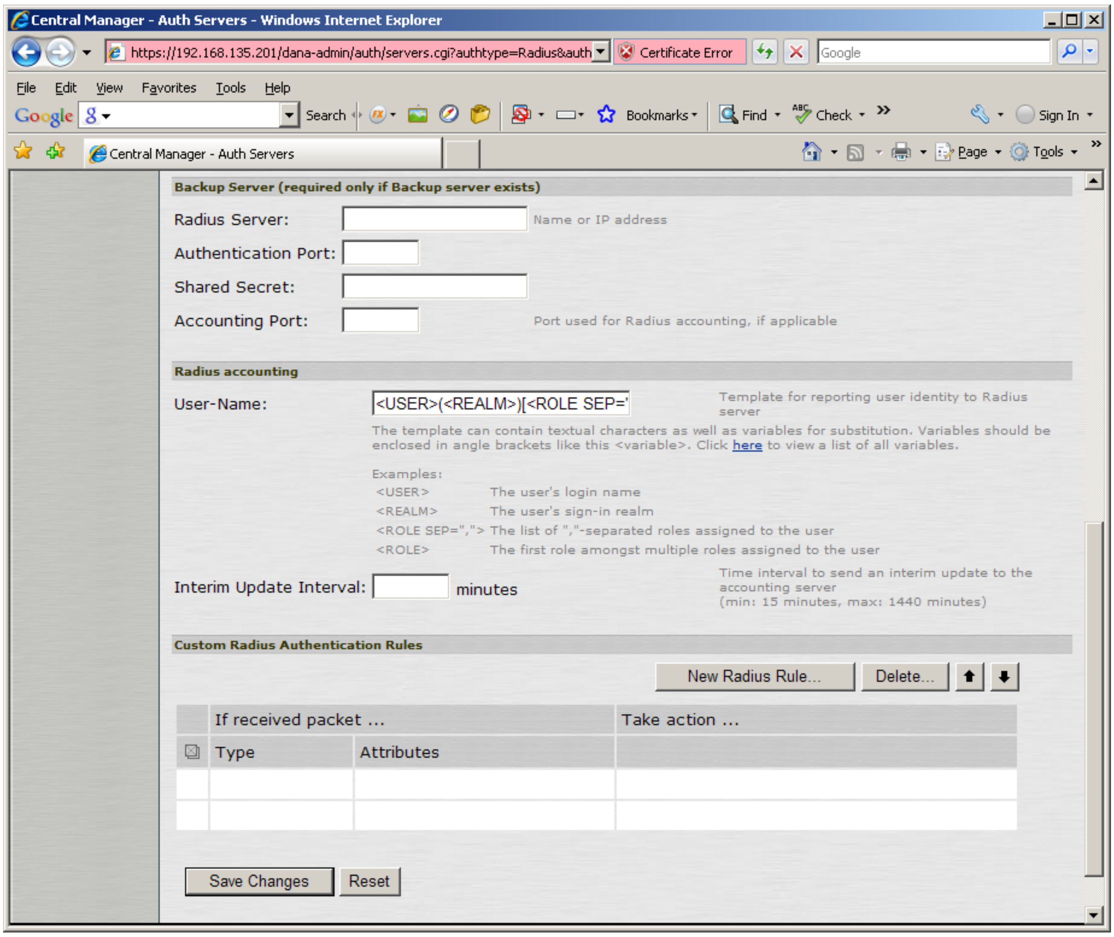
Timeout: 10 seconds

Retries: 0

☑ Users authenticate using tokens or one-time passwords

Note: If you select this, the device will send the user's authentication method as "token" if you use

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



Central Manager - Auth Servers - Windows Internet Explorer
https://192.168.135.201/dana-admin/auth/servers.cgi?authtype=Radius&auth
Certificate Error
File Edit View Favorites Tools Help
Central Manager - Auth Servers

**Backup Server (required only if Backup server exists)**

Radius Server: ____ Name or IP address

Authentication Port: ____

Shared Secret: ____

Accounting Port: ____ Port used for Radius accounting, if applicable

**Radius accounting**

User-Name: <USER>(<REALM>)[<ROLE SEP=' — Template for reporting user identity to Radius server

The template can contain textual characters as well as variables for substitution. Variables should be enclosed in angle brackets like this <variable>. Click here to view a list of all variables.

Examples:

| | |
|---|---|
| <USER> | The user's login name |
| <REALM> | The user's sign-in realm |
| <ROLE SEP=","> | The list of ","-separated roles assigned to the user |
| <ROLE> | The first role amongst multiple roles assigned to the user |

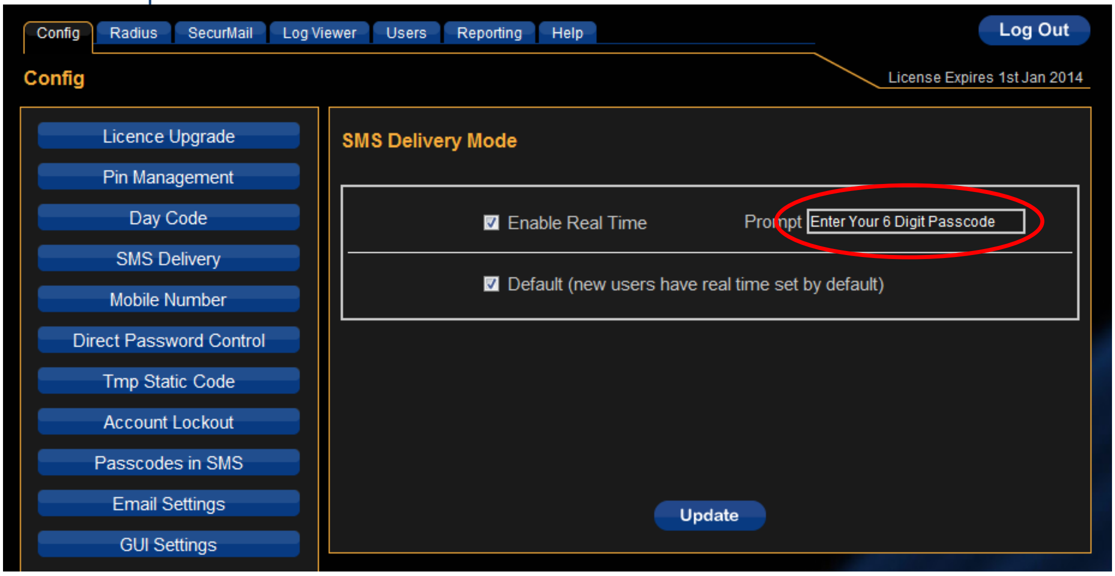
Interim Update Interval: ____ minutes — Time interval to send an interim update to the accounting server (min: 15 minutes, max: 1440 minutes)

**Custom Radius Authentication Rules**

| If received packet ... | | Take action ... |
|---|---|---|
| Type | Attributes | |
| | | |
| | | |

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:



**SMS Delivery Mode**

☑ Enable Real Time — Prompt: Enter Your 6 Digit Passcode

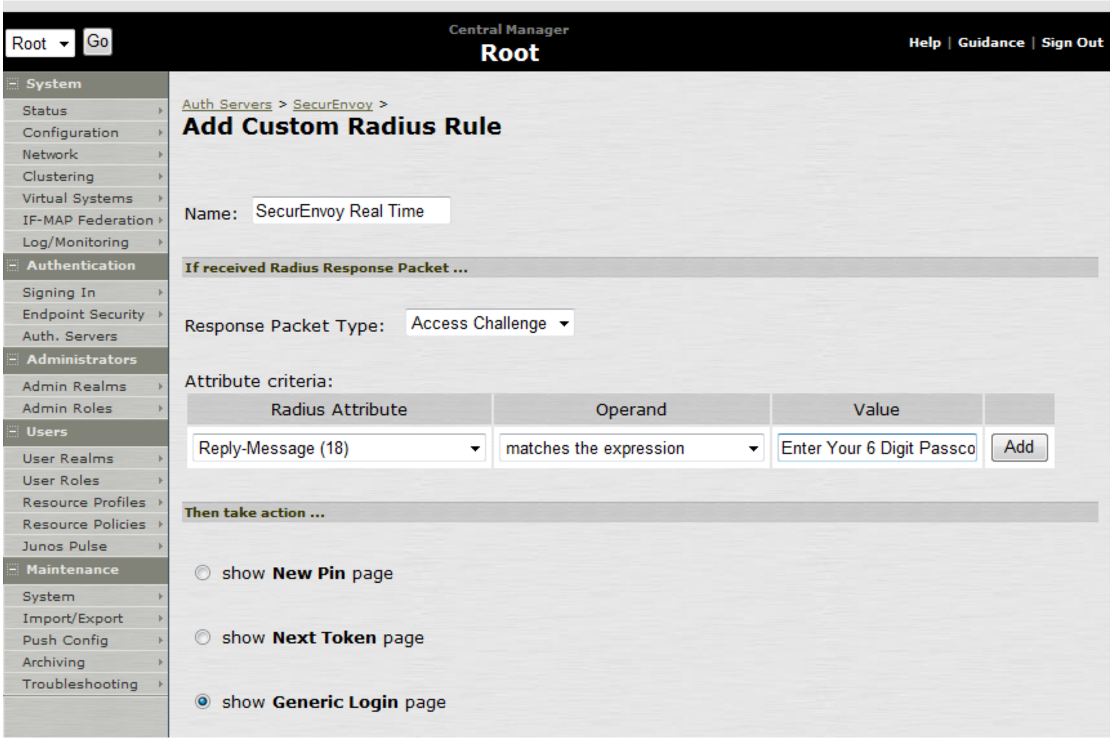
☑ Default (new users have real time set by default)

Press the "ADD" button to add this rule

Select Show GENERIC LOGIC Page

Press "Save Changes"

Press "Close"



Auth Servers > SecurEnvoy >

Add Custom Radius Rule

Name: SecurEnvoy Real Time

If received Radius Response Packet ...

Response Packet Type: Access Challenge

Attribute criteria:

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

Then take action ...

○ show **New Pin** page

○ show **Next Token** page

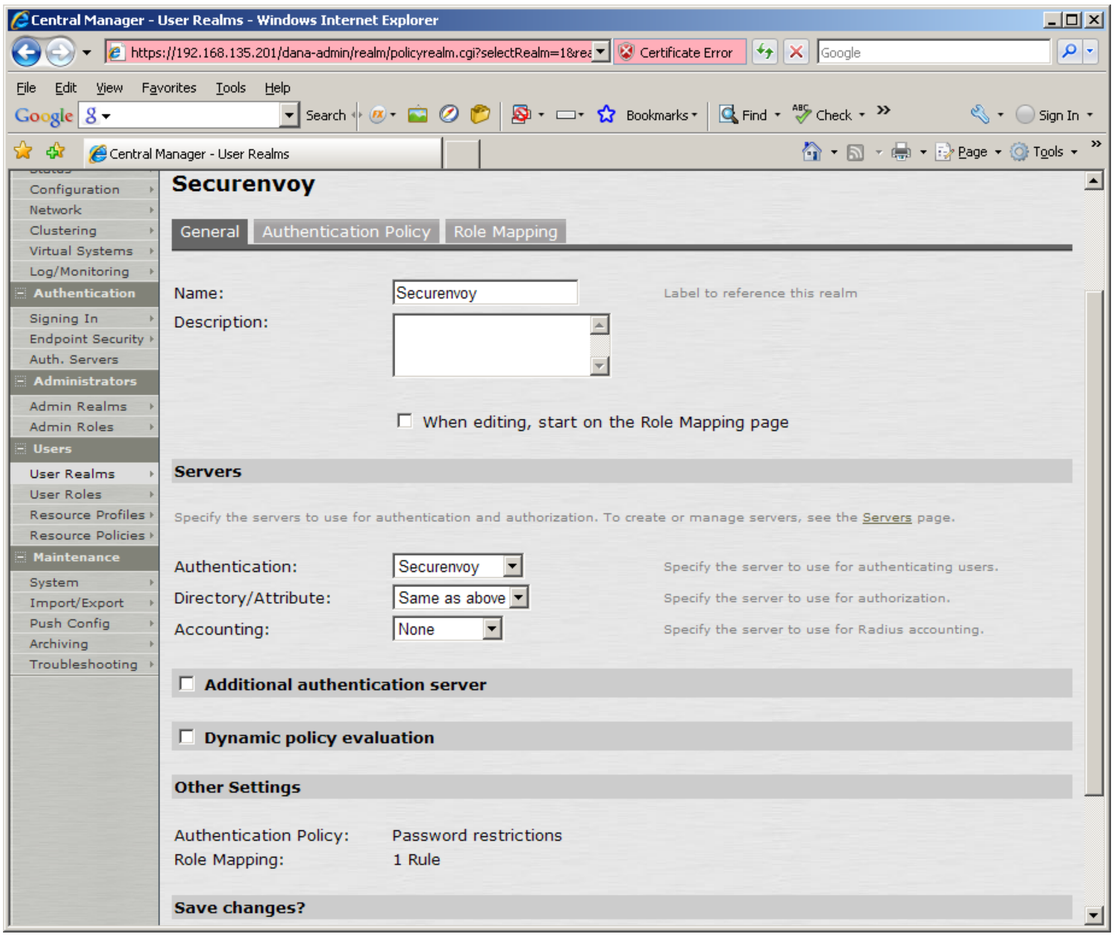
● show **Generic Login** page

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



**Securenvoy**

Name: Securenvoy — 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: Securenvoy — 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**

□ **Dynamic policy evaluation**

**Other Settings**

Authentication Policy: Password restrictions

Role Mapping: 1 Rule

**Save changes?**

Save Changes

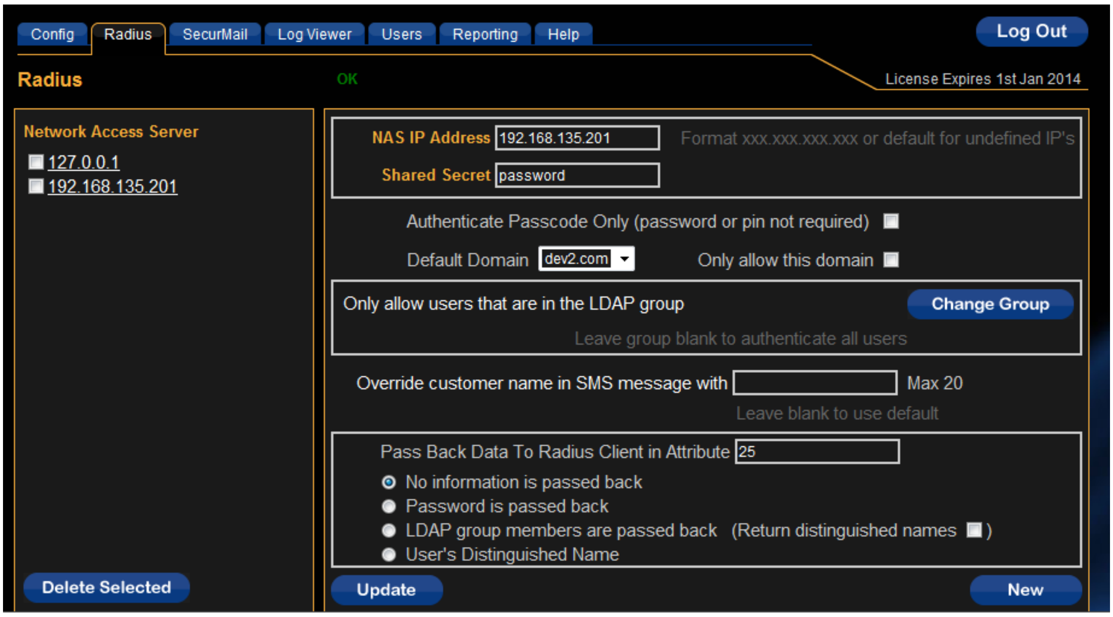
## Appendix B Configuration of SecurEnvoy for Real Time Passcodes

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.



Radius OK

License Expires 1st Jan 2014

Network Access Server

- □ 127.0.0.1
- □ 192.168.135.201

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) □

Default Domain: dev2.com Only allow this domain □

Only allow users that are in the LDAP 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: 25

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

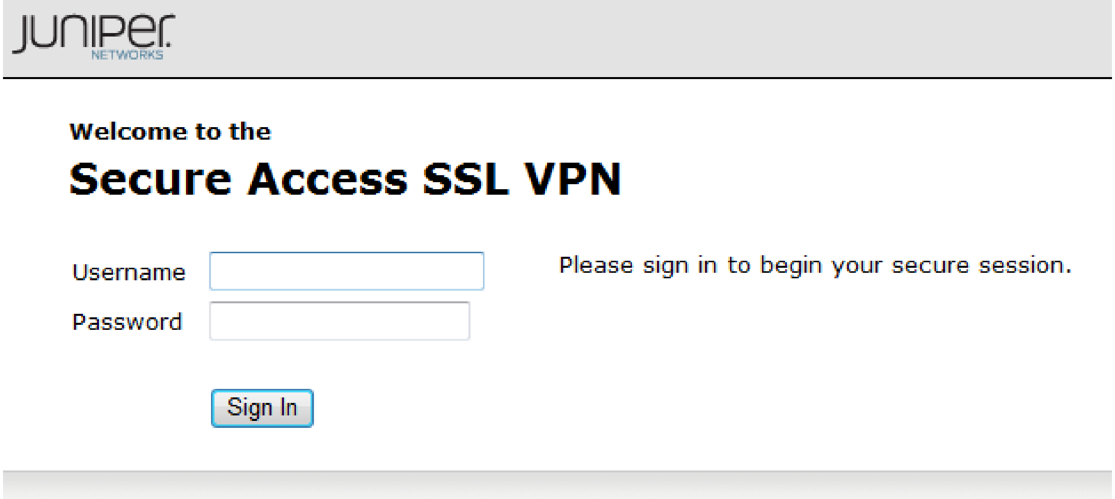
Do **NOT** click the checkbox “Authenticate Passcode Only”

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



Welcome to the

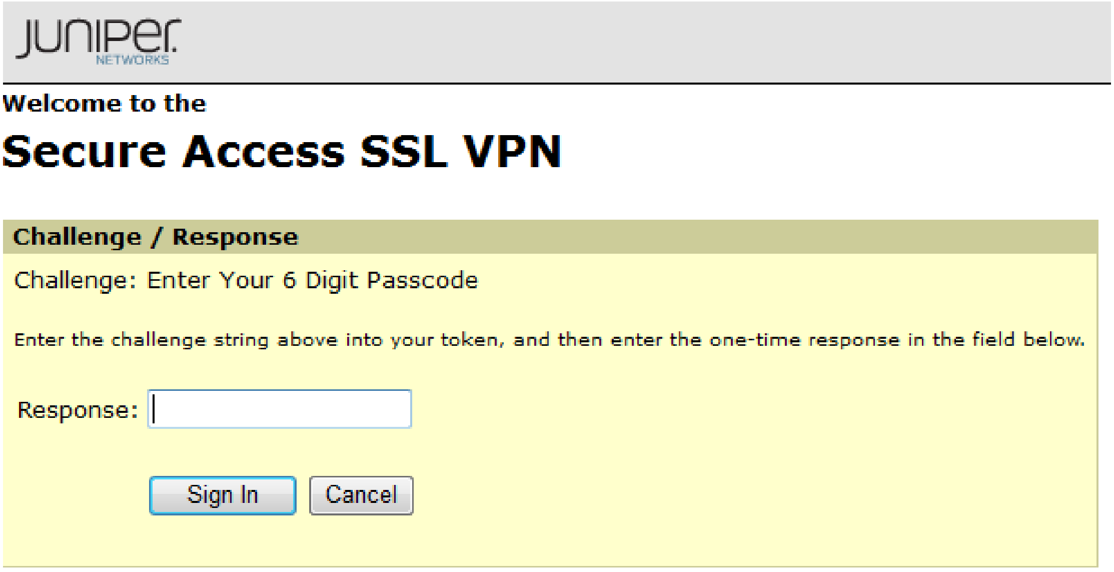
Secure Access SSL VPN

Username:

Password:

Please sign in to begin your secure session.

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



Welcome to the

Secure Access SSL VPN

Challenge / Response

Challenge: Enter Your 6 Digit Passcode

Enter the challenge string above into your token, and then enter the one-time response in the field below.

Response:

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