External Authentication with Juniper SSL VPN

Authenticating Users Using SecurAccess Server by SecurEnvoy

Contact information		
SecurEnvoy	www.securenvoy.com	0845 2600010
	Merlin House Brunel Road Theale Reading RG7 4AB	
Tony Davis	tdavis@securenvoy.com	

Juniper® SSL VPN Access Service Integration Guide

This document describes how to integrate a Juniper® SSL VPN Access Service (Juniper SA) with SecurEnvoy two-factor Authentication solution called 'SecurAccess'.

Juniper SA provides Secure Remote Access and Firewalling 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 any LDAP server 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 in real time.

SecurEnvoy Security Server can be configured in such a way that it can use the existing LDAP password. Utilising the LDAP password as the PIN, allows the User to enter their UserID, Domain 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. It provides a seemless login into the Windows Server environment by entering three pieces of information. SecurEnvoy utilises a web GUI for configuration, as does the Juniper SA. All notes within this integration guide refer to this type of approach.

The equipment used for the integration process is listed below:

Juniper® SSL VPN Secure Access Service
Juniper® SSL VPN Secure Access Service Release 8(27973)

SecurEnvoy

Windows 2012 R2 Server
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 v7.2.503

© 2014 SecurEnvoy Ltd. All rights reserved

Index

1.0 Prerequisites 3
1.1 Configuration of Juniper® SA 4
1.2 Configuration of SecurEnvoy 9
2.0 Test OneSwipe Logon 10
3.0 Notes 12

1.0 Prerequisites

It is assumed that the Juniper SA has been installed and is authenticating users with a username and password.

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 Routing and Remote Access server(s), additional open ports will be required.

***NOTE:** Add radius profiles for each Juniper SA that requires Two-Factor Authentication.*

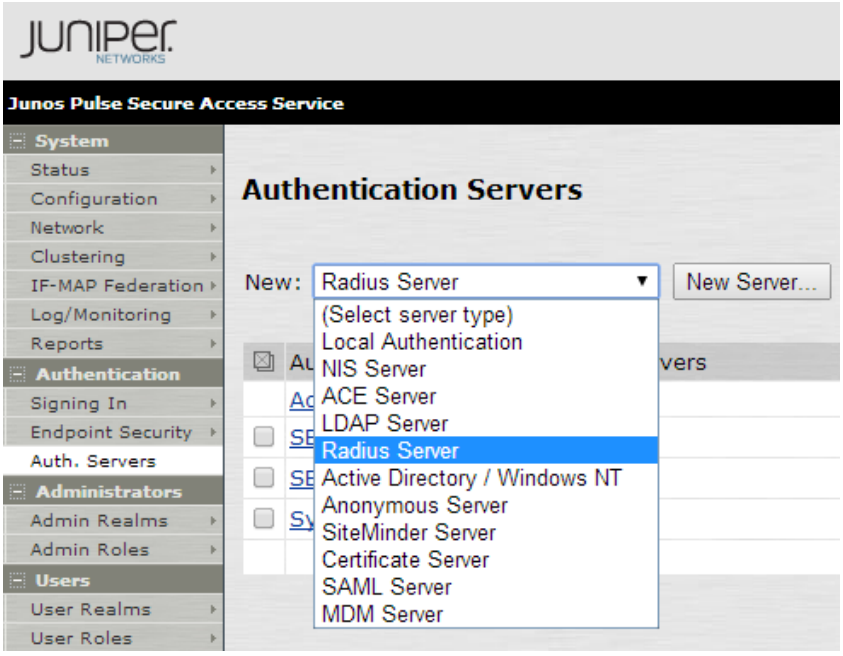
The following table shows what token types are supported.

Token Type Supported	
Real Time SMS or Email	✓
Preload SMS or Email	✓
Soft Token Code	✓
Soft Token Next Code	✓
Voice Call	✗
One Swipe	✓

© 2014 SecurEnvoy Ltd. All rights reserved

1.1 Configuration of Juniper® SA

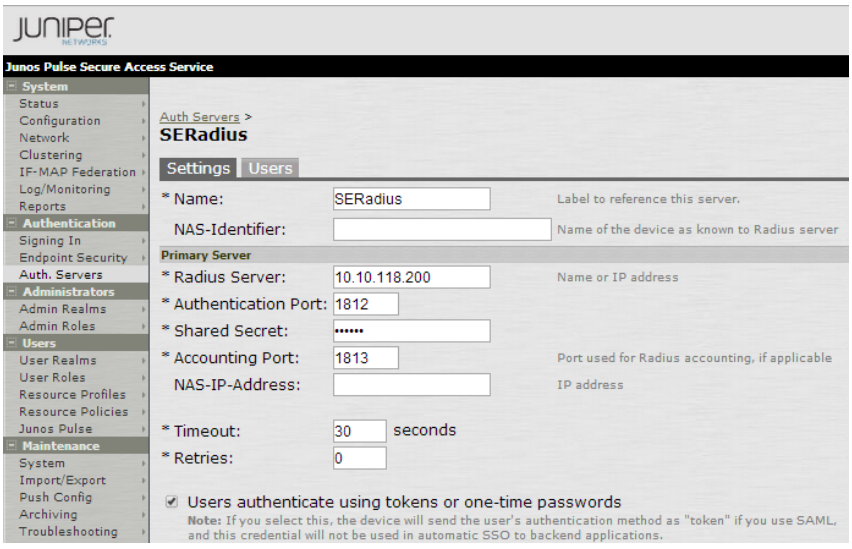
Launch the Junos Pulse Secure Access Service, select Auth Servers from Authentication, Navigate to "Authentication" "Auth. Servers" select new "Radius Server" and press "New Server"



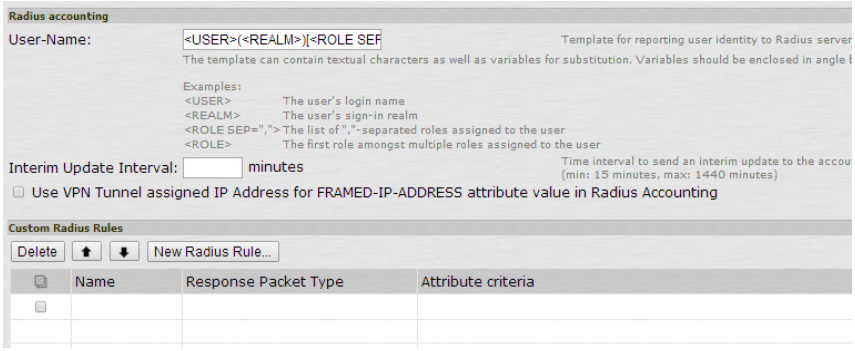
Populate information for the new Radius server (SecurEnvoy)
Enter Name, IP address, authentication port and shared secret.

SecurEnvoy recommends 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.



Scroll to bottom and select "New Radius Rule" button



© 2014 SecurEnvoy Ltd. All rights reserved

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

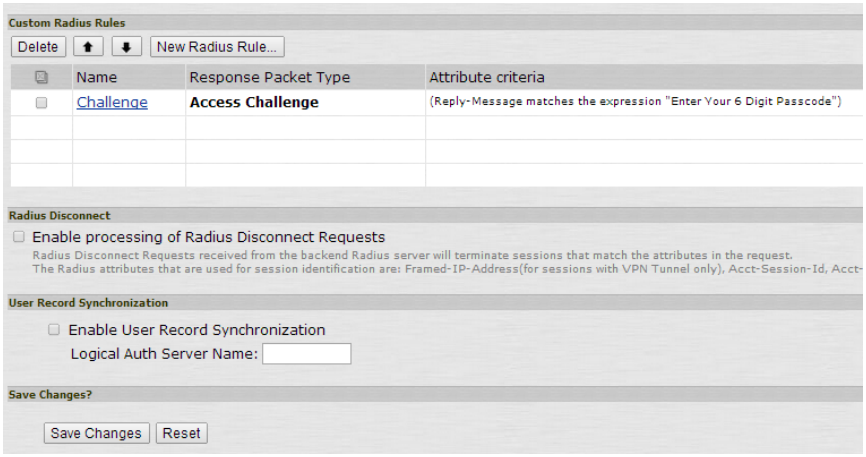
Press the "ADD" button to add this rule

Select Show GENERIC LOGIC Page

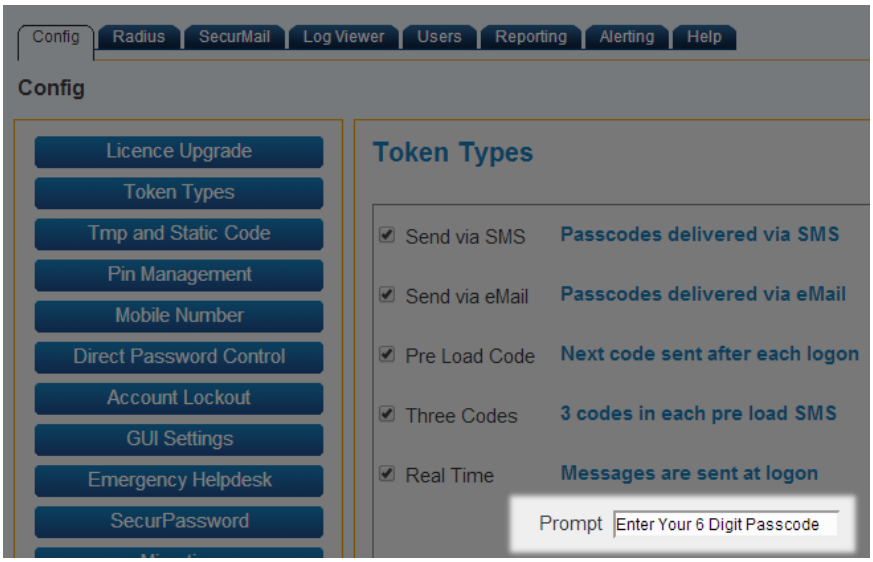


Press "Save Changes"

Press "Close"



Note this value MUST match the setting in the SecurEnvoy GUI Config setting "Token Types" Prompt:



Click "Save changes" to submit all configuration parameters

© 2014 SecurEnvoy Ltd. All rights reserved

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

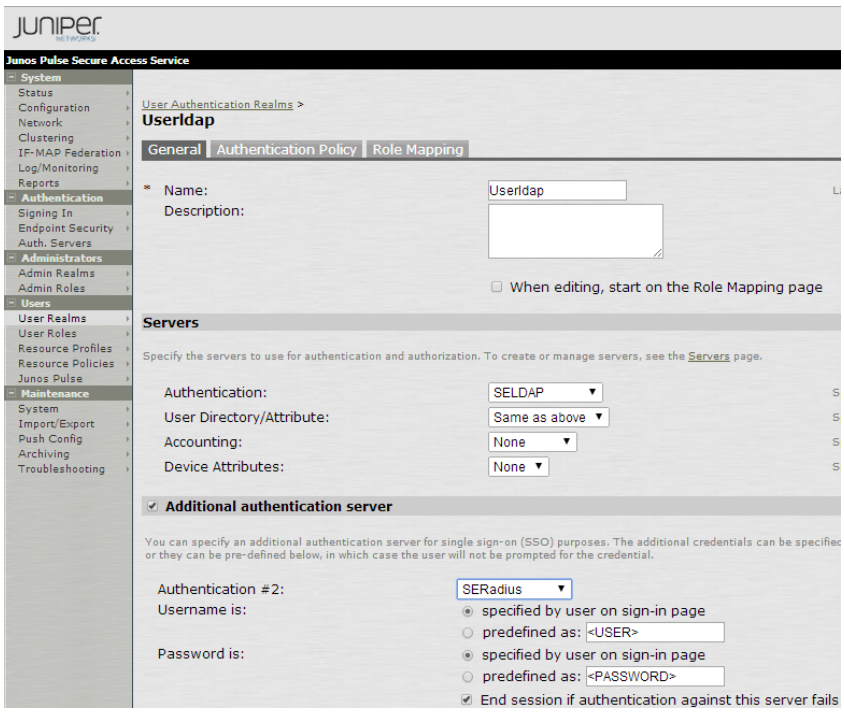
Click the checkbox "Additional authentication server"

Populate information for "Authentication #2" select "SERadius" (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 "Upload Custom Pages



© 2014 SecurEnvoy Ltd. All rights reserved

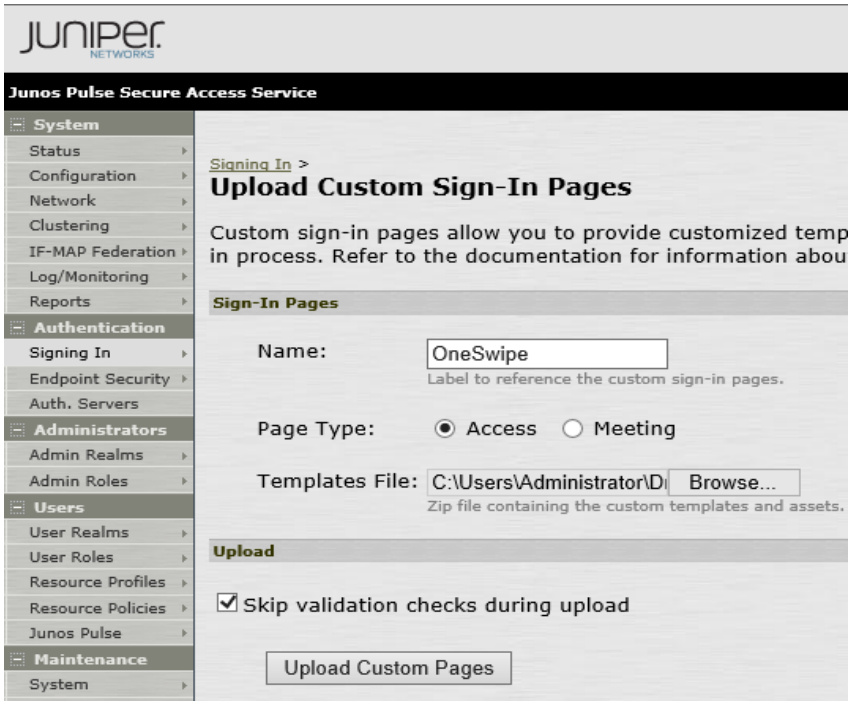
Enter a Name, in this example "OneSwipe"

From the Templates File, click "Choose File", browse and Select the oneswipe.zip (available here)

Check "Skip validation checks during upload"

Click "Upload Custom Pages"

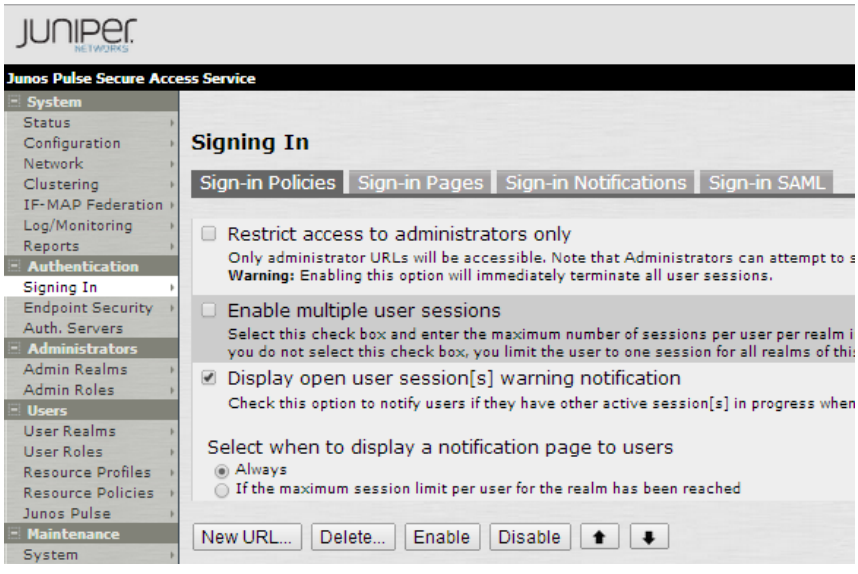
Once uploaded, click "Save Changes"



Back at the "Sign-in Pages", you should see the "oneswipe" sign-in page



Select "Sign-in Policies" then click "New URL



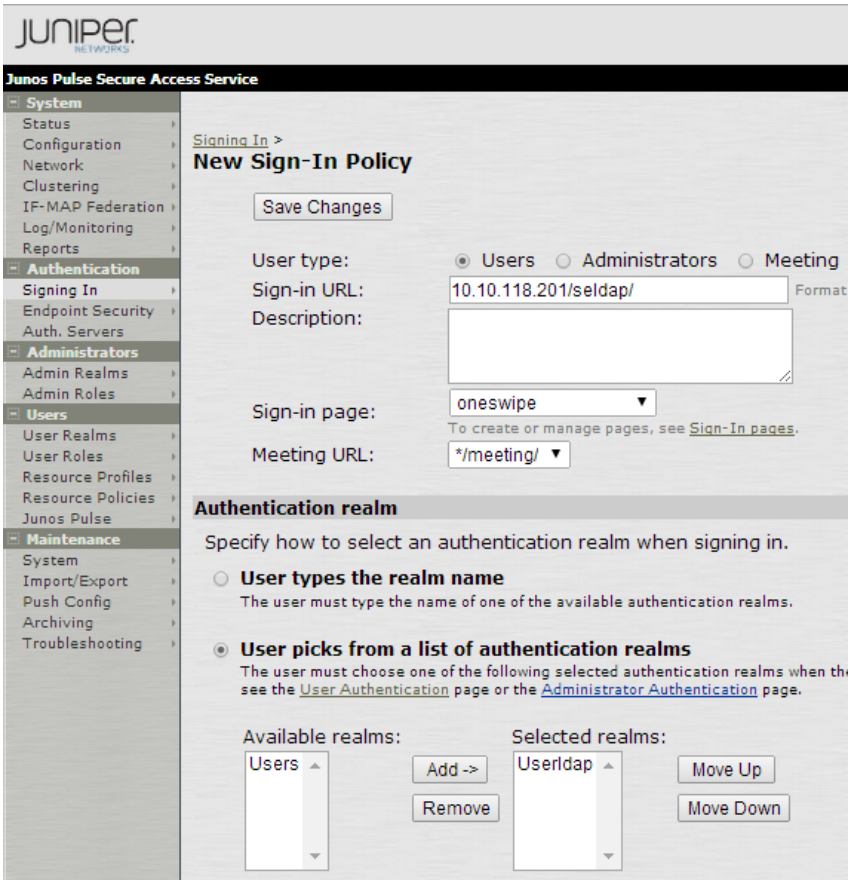
© 2014 SecurEnvoy Ltd. All rights reserved

Populate information for "Sign-in URL" and Sign-in page.

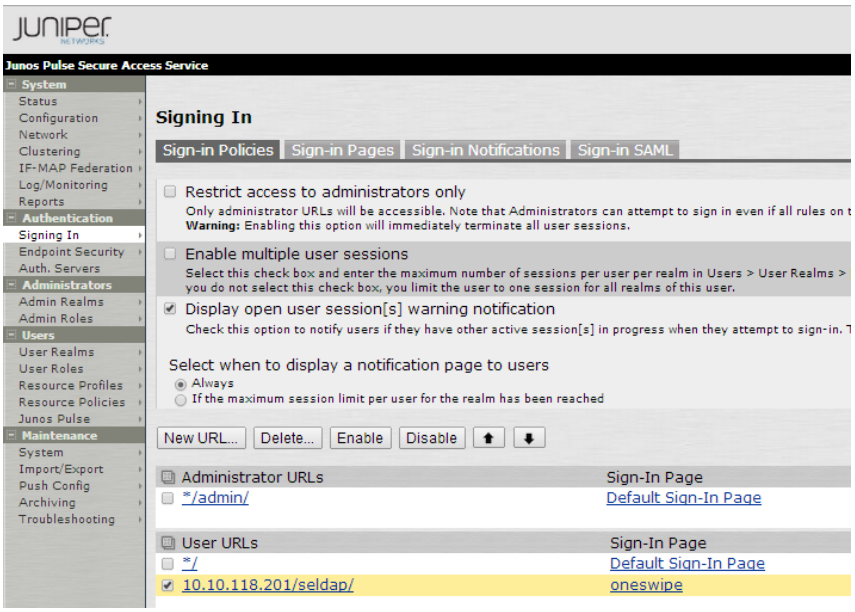
Select "user picks from a list of authentication realms.

Add "Userldap" to "Selected realms"

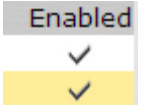
Click "Save Changes"



Select the newly created policy from the list and click "Enable".



Policy will show "Enabled"



© 2014 SecurEnvoy Ltd. All rights reserved

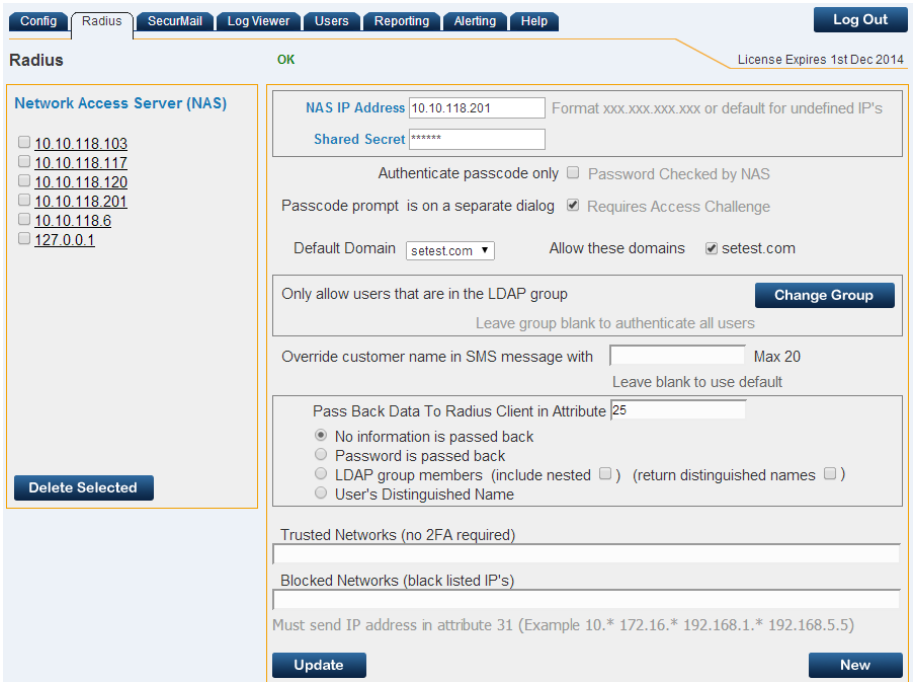
1.2 Configuration of SecurEnvoy

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"** tab

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



Click checkbox "Passcode prompt is on a separate dialog".

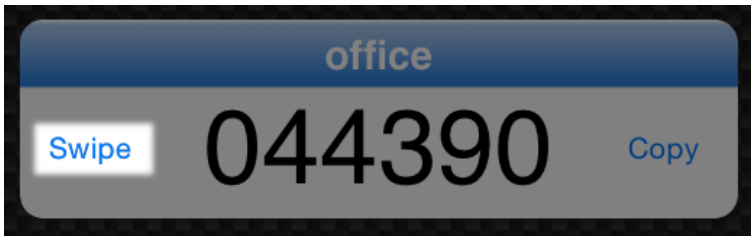
Click **"Update"** to confirm settings.

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

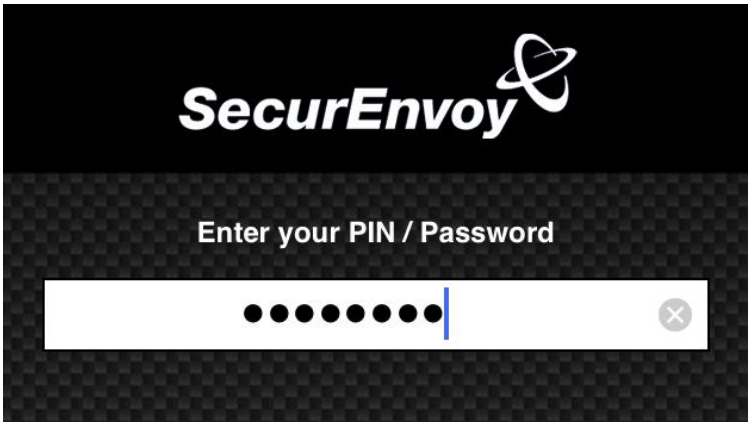
© 2014 SecurEnvoy Ltd. All rights reserved

2.0 Test OneSwipe Logon

Select 'Swipe' from the phone Soft Token

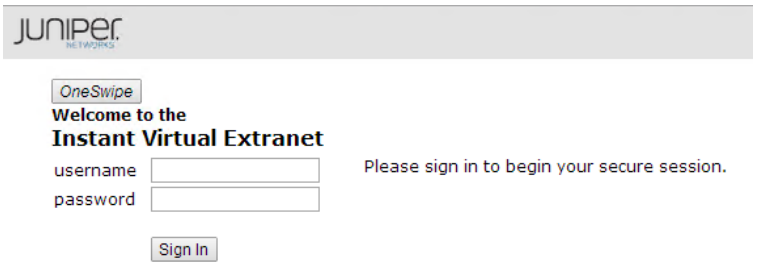


Enter your PIN /Password into the PIN / Password field and click 'Done'.



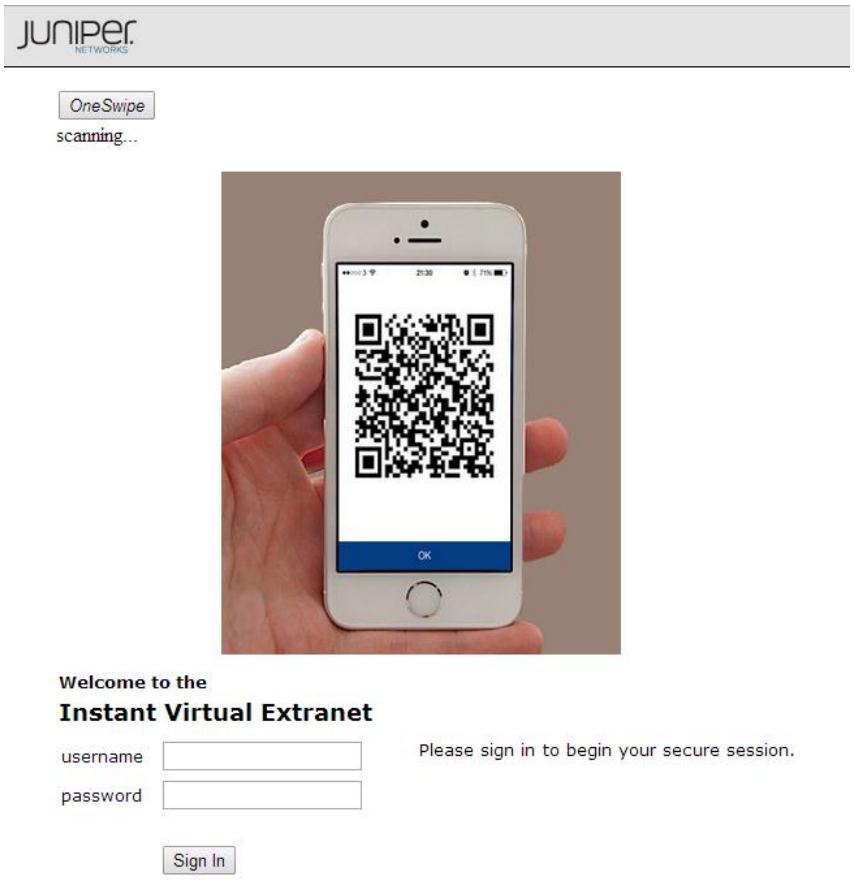
Browse to the web URL address of the Juniper® SSL appliance.

Click the OneSwipe button

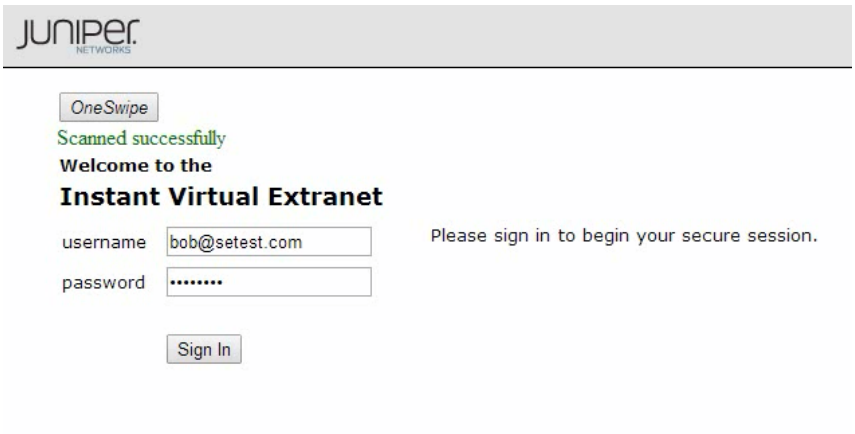


© 2014 SecurEnvoy Ltd. All rights reserved

Your webcam is now activated & you will be able to present the QRCode on your phone.



UserID, password and passcode are passed to the Juniper authentication page and user successfully logs in.



© 2014 SecurEnvoy Ltd. All rights reserved

3.0 Notes

© 2014 SecurEnvoy Ltd. All rights reserved