PINsafe®

SWIVEL®
AUTHENTICATION YOU CAN IDENTIFY WITH

Juniper SSL Clientless Installation Notes

Created October 2008 Graham Field
Amended April 2011 Graham Field and Rob Allen

Table of Contents

1. Introduction

This document outlines the steps required to integrate the Juniper SSL Clientless VPNs with Swivel PINsafe. Juniper SA servers are able to use external RADIUS servers for providing authentication, and PINsafe servers are able to provide RADIUS authentication, so this forms the basis for the integration approach.

PINsafe users can use either PINsafe's Single Channel (Turing, Pattern) or Dual Channel (SMS, J2ME) methods to retrieve Security Strings, which are applied against the user's PIN to extract a One-Time Code (OTC) which represents the password for an authentication request.

With Dual Channel methods, the user already holds one or more Security Strings on their mobile device (and can request more at any time) so with the Juniper configured to use the matching PINsafe server for RADIUS authentication, no further integration is required.

(The Authentication Realm configuration section below describes how to achieve the RADIUS configuration).

However with Single Channel methods, the user must be presented with a Turing or Pattern image at sign-in time (representing a single time-limited Security String), so they can extract their OTC. (The Single Channel Sign-in Page section below describes how to achieve this).

2. Overview

2.1. Prerequisites

Juniper VPN server with correct licenses installed to modify and upload the login page.
PINsafe server
A DNS entry pointing to the PINsafe server is required for the Turing image to be displayed

2.2. Baseline

The Juniper server used was NetScreen-SA-2000 Advanced - 100 Simultaneous Users, with System Version 6.2 R1.
The PINsafe server used was PINsafe 3.x – 100 User License.
The primary web browser used for testing was Internet Explorer 7

2.3. Architecture

The user connects to the Juniper VPN using a web browser, pointing to the appropriate sign-in URL for the VPN in question. The Juniper VPN is configured to use a PINsafe server for radius authentication. Users are stored and maintained in the PINsafe server. A proxy rewriting rule rewrites requests on a specific DNS to the PINsafe server to deliver Turing images.

3. Installation

3.1. DNS entry for Turing

If using the Turing single channel, an external DNS entry is required that points to the Juniper SSL VPN.

Example:

Juniper SSL VPN	vpn.mycompany.com
Turing Image	turing.mycompany.com

Swivel Example:

Juniper SSL VPN	vpn1.swivelsecure.com
Turing Image	turing.swivelsecure.com

3.2. Downloading Sample Login Pages

From the Signing-In menu select the Sign-in-Pages then Upload Custom Pages, then from the Upload Custom Sign-In Pages select sample, download the zip file.

Figure 1 – Selecting Upload Custom Pages

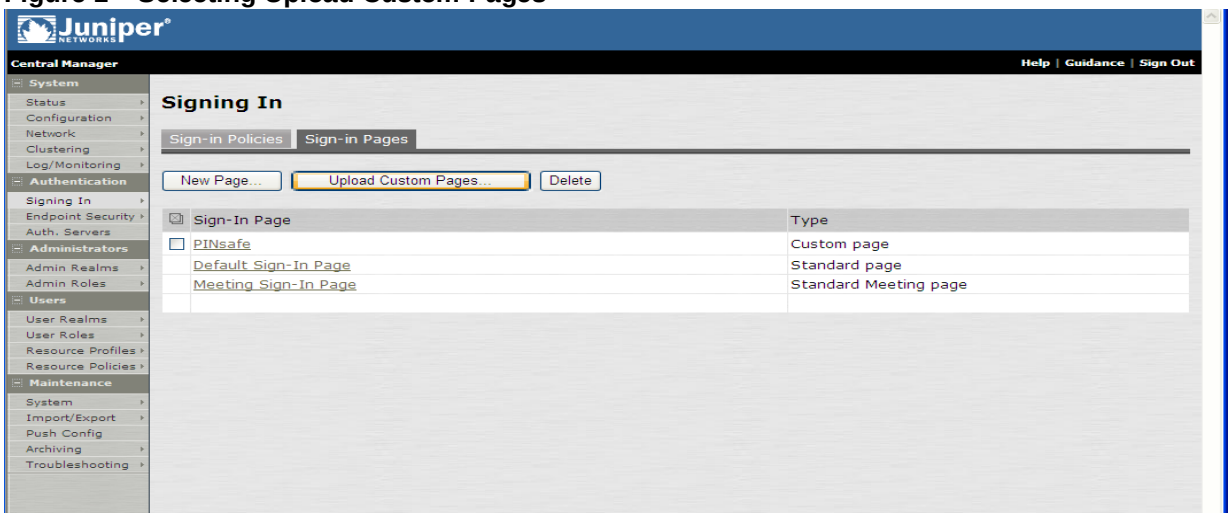
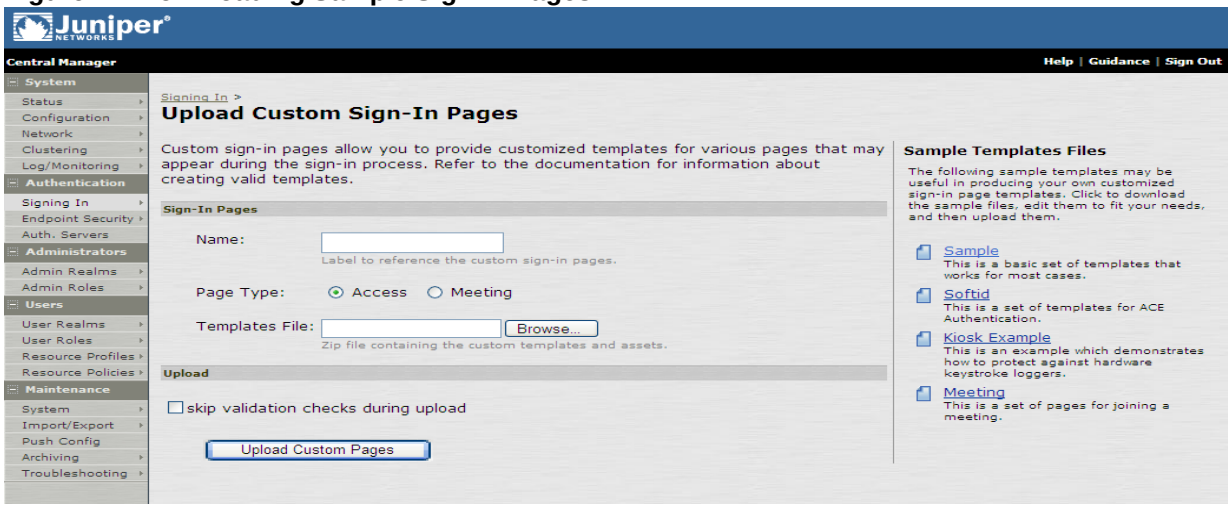
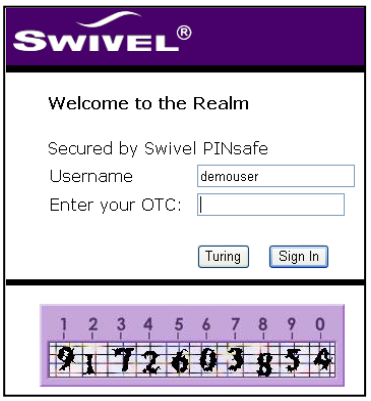


Figure 2 – Downloading Sample Sign-In Pages



3.3. Creating A Custom Login Page

3.3.1. Adding the single channel authentication script



Using Dual Channel a user can enter their OTC and login. Using Single Channel, a TURing image must be presented to the user. The user makes the request for the TURing image in their web browser. The TURing image is requested using an html request using a pass-through proxy request. The Juniper VPN rewrites the request using its proxy and hides the internal IP address and port.

Example:

https://turing.swivelsecure.com/proxy/SCImage?username=

which the proxy rewrites as:

https://192.168.0.35:8443/proxy/SCImage?username=

Use the PINsafe LoginPage.thtml or modify the original LoginPage.thtml, using the Swivel page a guide for the required changes.

3.3.2. Modifying the login page script

The configuration section within LoginPage.thtml should be edited to suit your environment:

OTC_OPTION: Controls how the TURing image will be displayed to the user:

Value	Description	Single	Dual
image	When the user tabs down from the username field, the TURing will automatically show.	Y	N
button	The login page will present a TURing button. Click the button to display the TURing.	Y	Y
disable	The TURing image will not be shown.	Y	Y

OTC_RANDOM: Displays a button on screen to refresh the TURing image:

Value	Description	Single	Dual
true	Button will be displayed	Y	Y
false	Button will not be displayed	Y	Y

TURingImage: URL for generating a TURing image:

Value	Description	Single	Dual
https://192.168.0.35:8443/proxy/SCImage?username=";		Y	Y

Change the TURingImage value to reflect the IP address of the PINsafe appliance.

3.4. Uploading the modified login page

Zip the files and uploaded to the newly created “Swivel” sign-in page:

Figure 3 – Selecting Upload Custom Pages

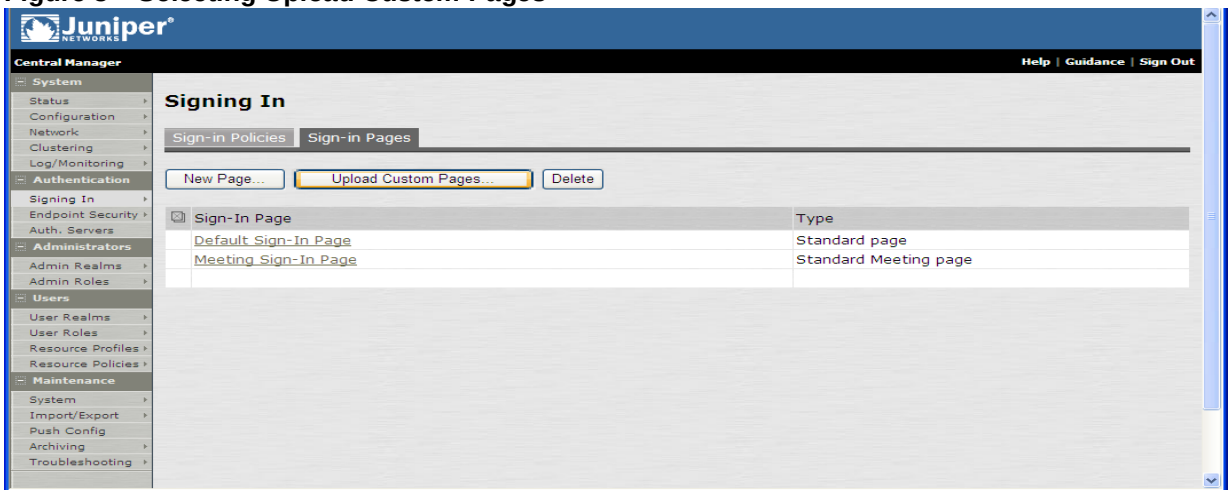
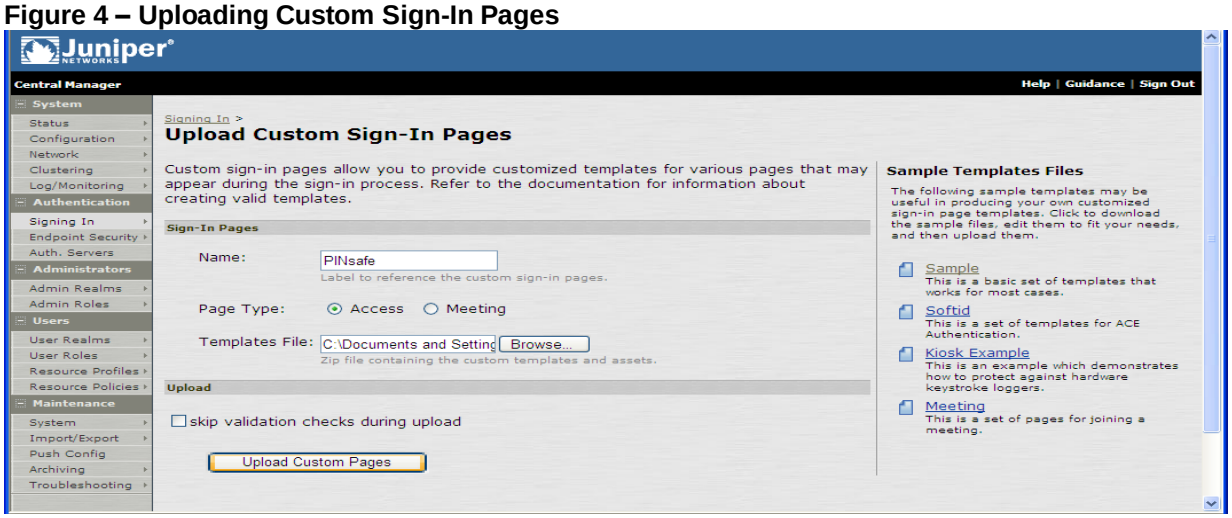
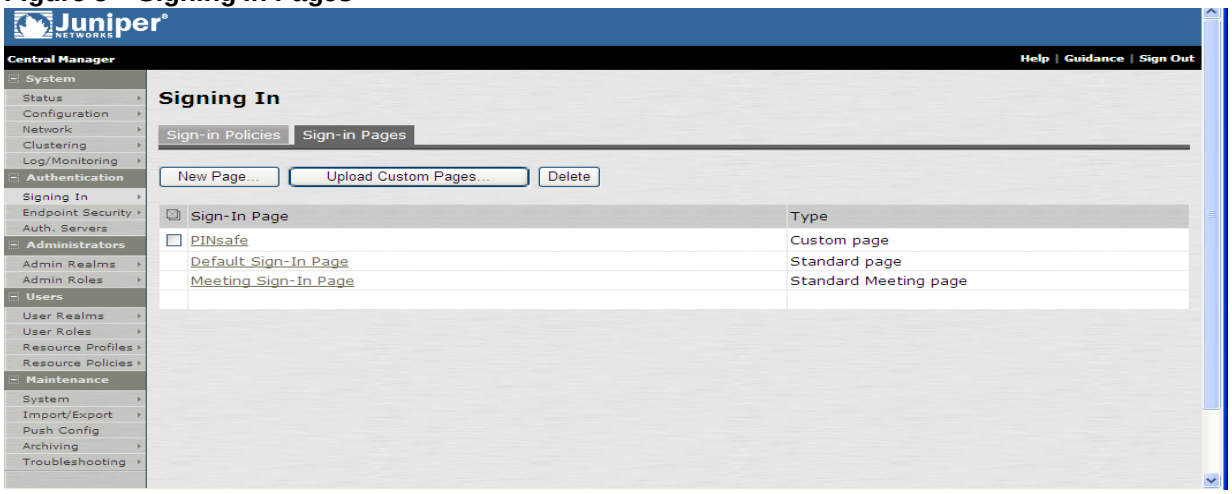


Figure 4 – Uploading Custom Sign-In Pages



A signing in page should now be listed

Figure 5 – Signing In Pages



3.5. Creating a Virtual Hostname

Select the Authentication/Signing In/Sign-In Policies and then select New Page. Select the Authorization Only Access radio button for User type. Complete the following information:

Virtual Hostname: enter the DNS name that will point to the PINsafe appliance for the TURing image

Example: turing.swivelsecure.com/

Backend URL: enter the protocol, IP address and port of the PINsafe appliance

Example: http://192.168.0.35:8443/*

Authorization Server: select No Authorization
Role Option: Select a Role

Save the Changes

Note: you can verify the TURing image path by using a web browser:

Internally	http://<PINsafe appliance URL>:8443/proxy/SCImage?username=demouser
Externally	https://<turing.mycompany.com>/proxy/SCImage?username=demouser

Figure 6 – Virtual Hostname Configuration

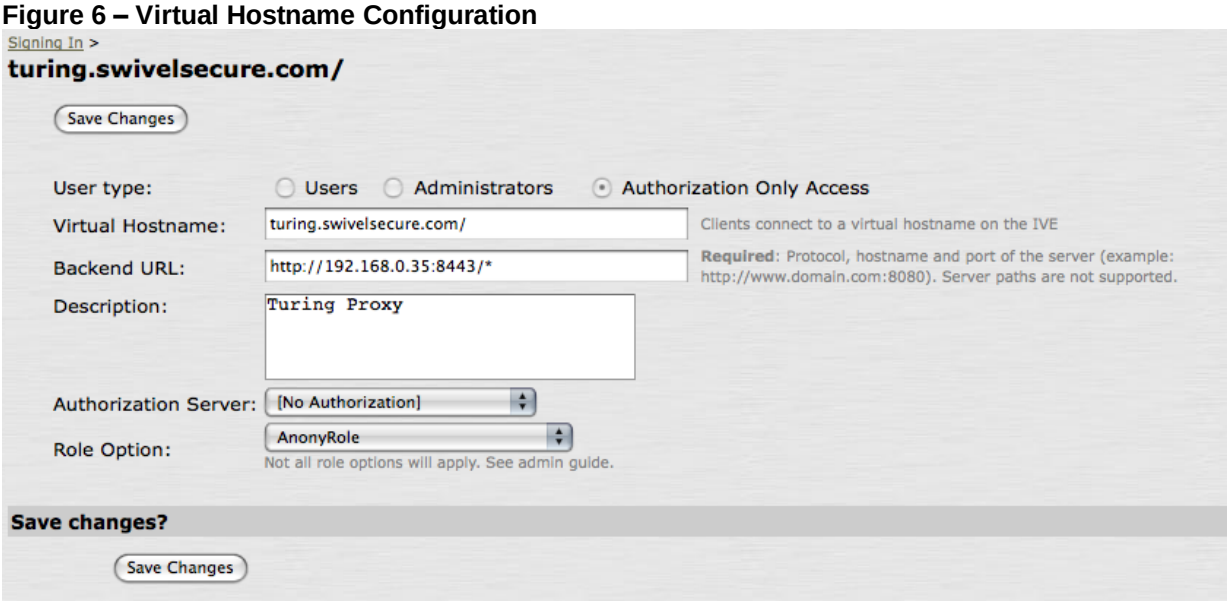


Figure 7 – Virtual Hostname

3.6. Authentication Server Configuration

A new authentication server was created by selecting Authentication servers, with the IP address of the PINsafe server being used for the integration and the shared secret key. (A corresponding NAS entry was created on the PINsafe server.) The NAS-IP-Address can be used to define an IP address of the Juniper SSL to be used for RADIUS authentication, leaving it blank will use the default internal address. Tick the box to select Users authenticate using tokens or one time passwords.

Figure 8 – Selecting Authentication Server Type

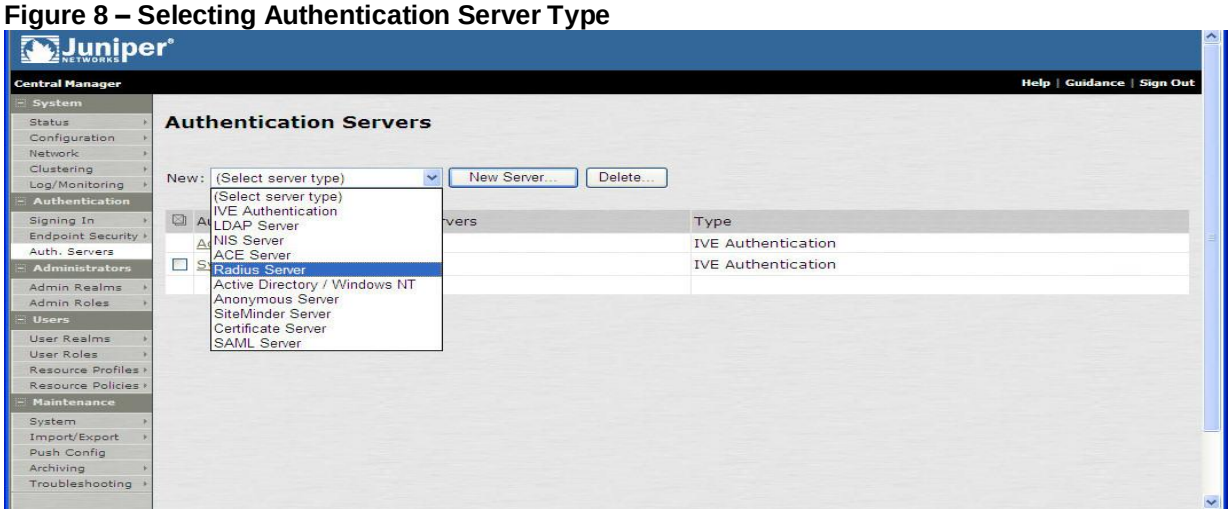
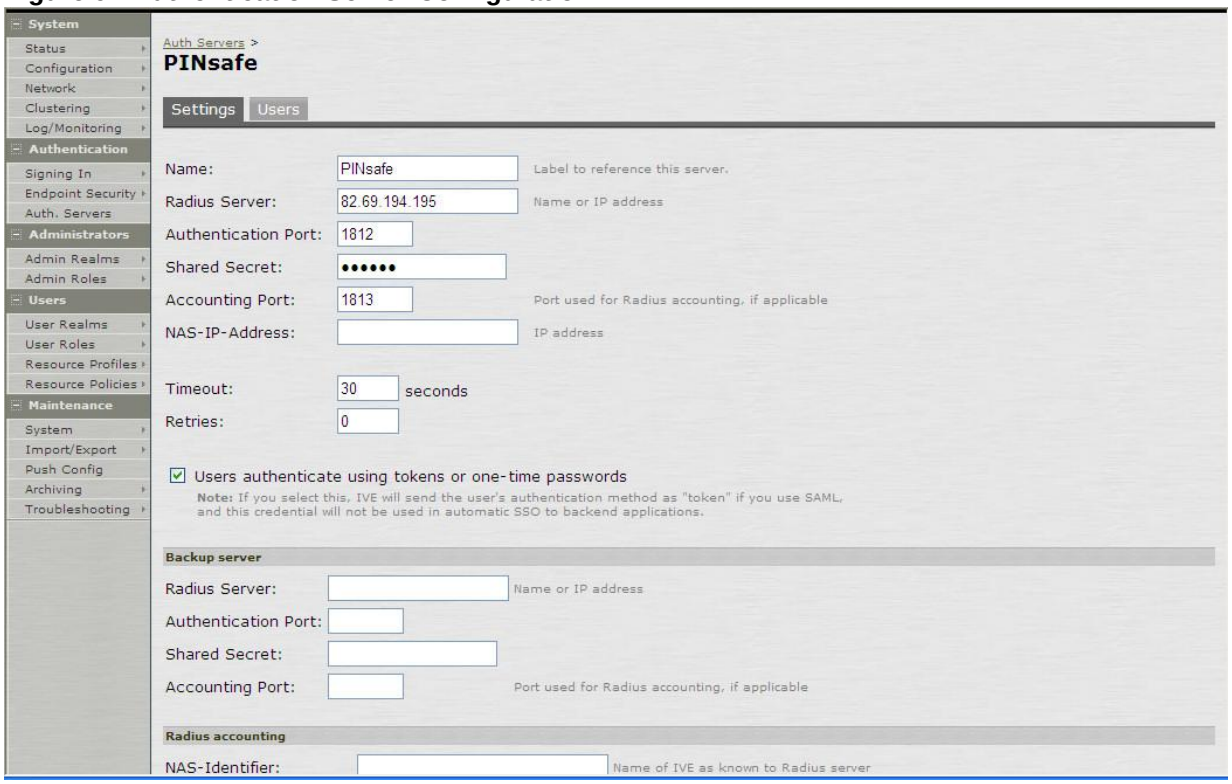


Figure 9 - Authentication Server Configuration



3.7. Authentication Realm configuration

A new realm “PINsafe Realm” was created by selecting User Realms, then New and then configured to use the Authentication Server “PINsafe”. Basic Role Mappings were defined so that authentication users were assumed to be members of appropriate role group. Additional authentication servers may also be configured. Ensure that the setting for ‘Username is’ then ‘predefined as’ is <USERNAME> and not <USER>, (using <USER> will send across the Domain Name /User Name for RADIUS authentication).

Figure 10 – User Authentication Realms

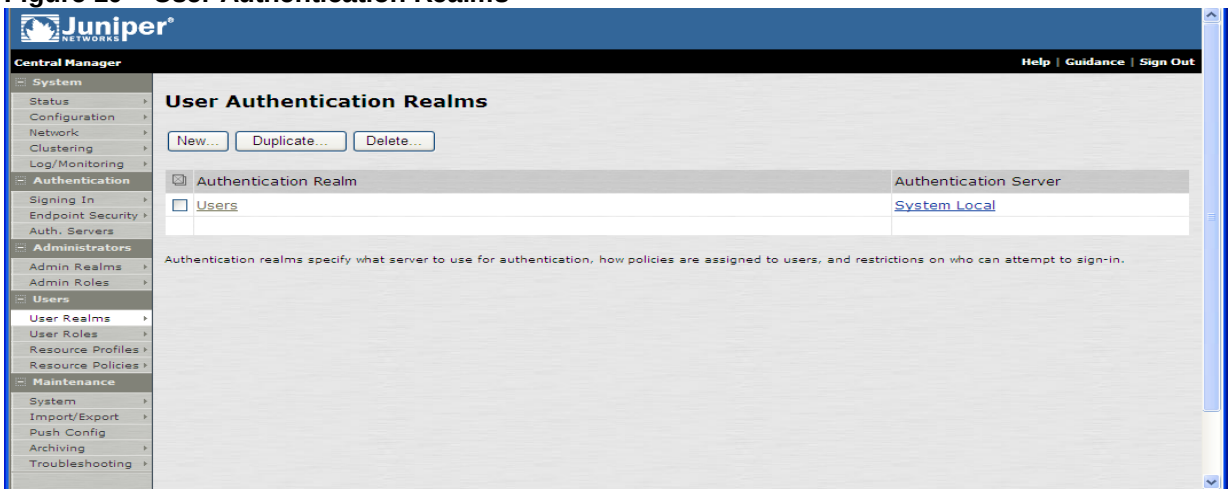


Figure 11 – New Authentication Realm Configuration

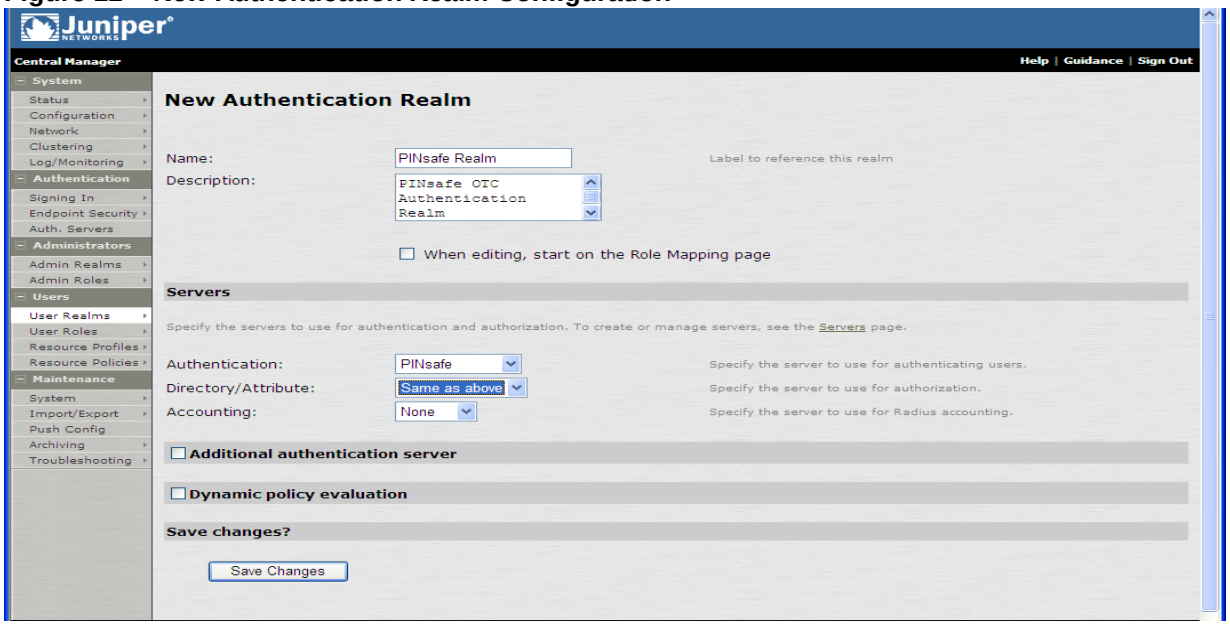


Figure 12 – PINsafe as an Additional Authentication Server

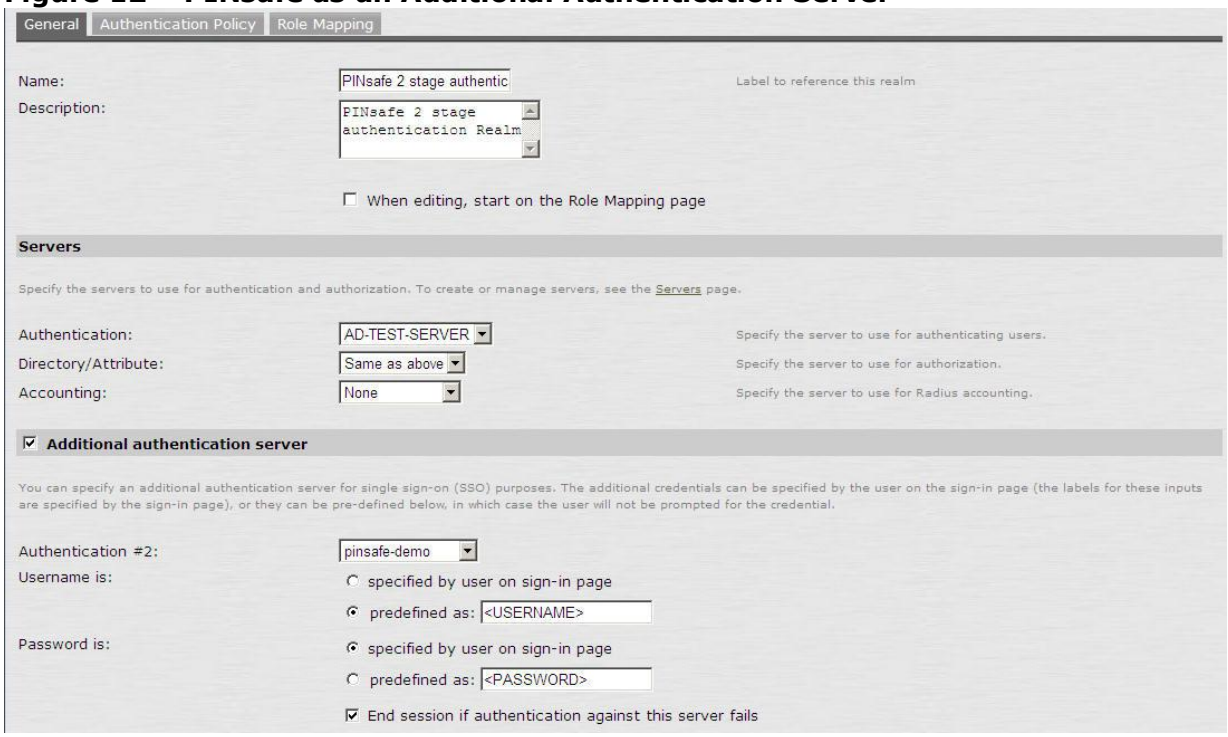
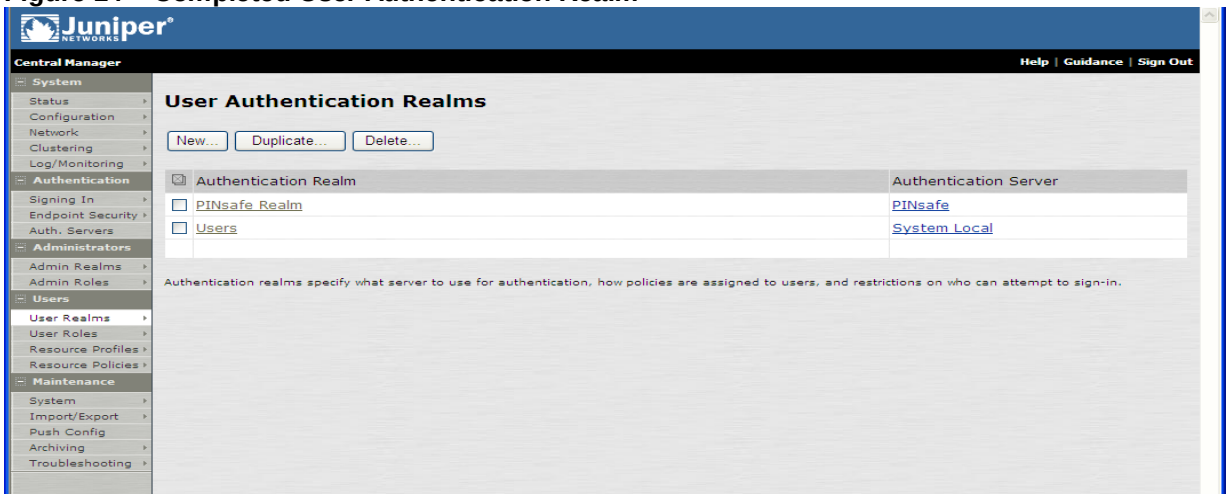


Figure 13 - Realm's Role Mapping

Figure 14 – Completed User Authentication Realm



3.8. Sign In Policy Configuration

In order to isolate the integration from the default operation of the Juniper VPN, a new sign-in policy was created pointing to a specific URL */pinsafe/.

This means that the integration could be tested by browsing to https://SAipAddress/pinsafe/ while with the original configuration was still operational at https://SAipAddress/.

The diagrams below show the sign-in policy configured to use the Swivel sign-in page and realm SwivelRadius1.

Figure 15 – Defined Sign-In Policies

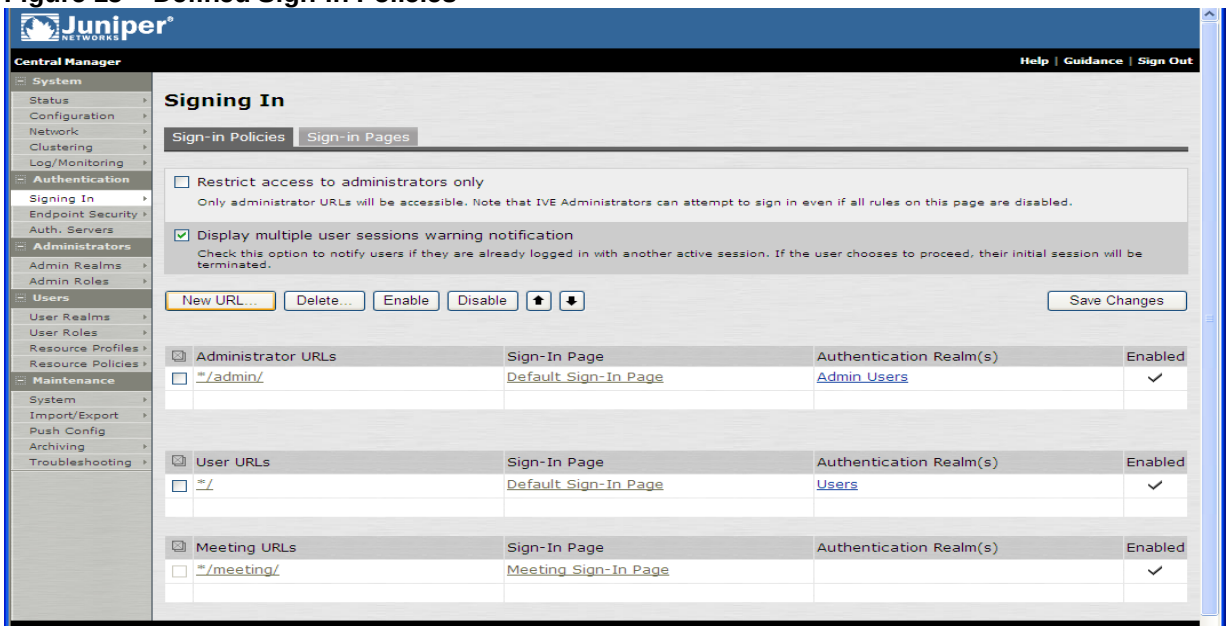


Figure 16 – Sign-In Policy Details

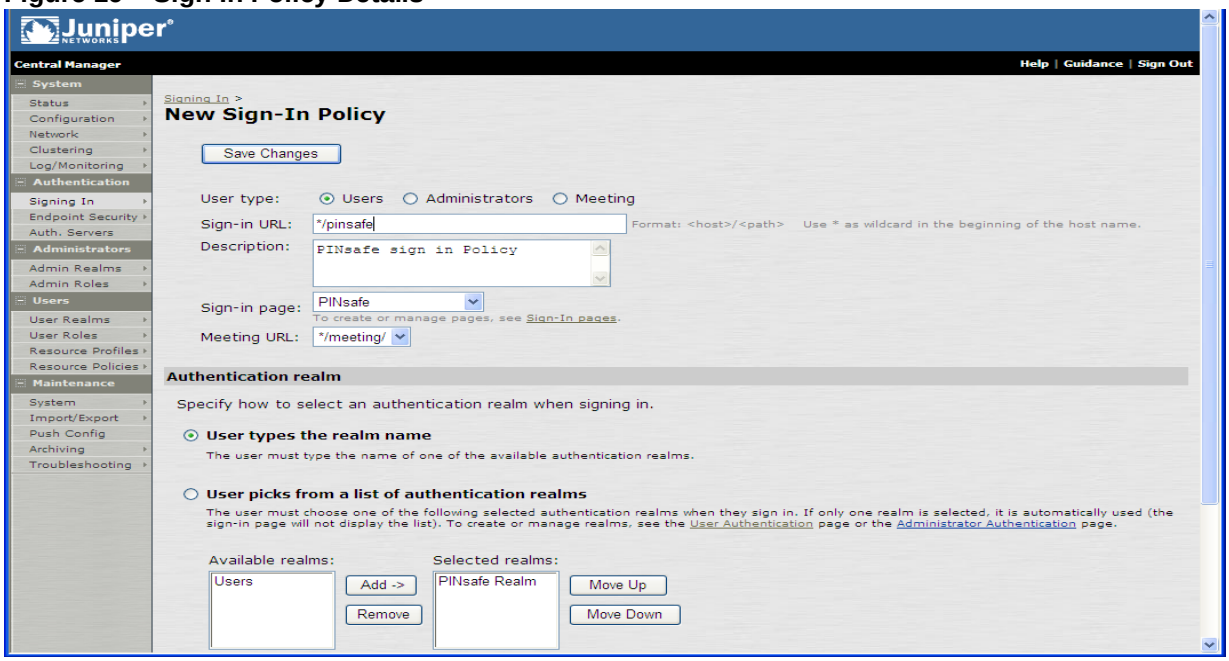
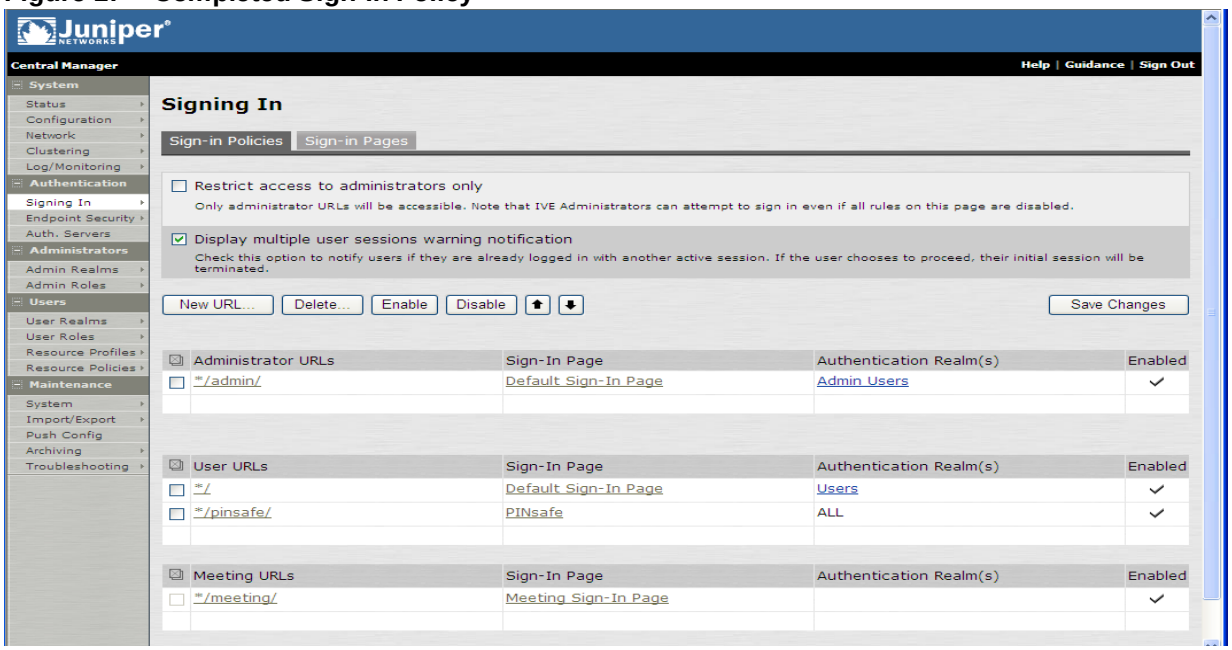


Figure 17 – Completed Sign-In Policy



4. Verifying Installation

Navigate to the Juniper login page. The customisation is visible in the addition of a **One Time Code** field and a **TURing** button. Attempting to login with a correct username and password but no one time code should result in failure. Only when a correct PINsafe one time code is entered in should the user be logged in.

5. Troubleshooting

The Juniper user access log (System>Log/Monitoring>User Access Log) shows entries similar to the following:

Minor	AUT21097	2004/10/08 13:47:57 - [***SAipAddress***] System - Radius Server Swivel1:	Login failed for testUserName because **host 213.152.251.227:1812 is unreachable**.

This suggests that the Juniper server is unable to reach the PINsafe server to make an authentication request, possible because of firewall restrictions.

The Juniper user access log (System>Log/Monitoring>User Access Log) shows entries similar to the following:

Info	AUT21066	2004/10/08 13:47:57 - [***SAipAddress***] testUserName (SwivelRadius1) -	Login failed from 81.157.80.225 for testUserName /SwivelRadius1 using Radius server.

This suggests the Juniper server is sending authentication requests to the PINsafe server, but they are being rejected. Examination of the PINsafe logs might reveal:

LogID	971
TimeStamp	2004-10-08 16:11:10.0
Level	0
Source	Radius Authentication
Address	
Agent	
EventID	RADIUS Log Message
EventResult	-1
Administrator	
Username	
SessionType	
Additional	<255> Access-Reject(3) LEN=51 ***SAipAddress***:12000 Access-Request by testUserName

Single Channel Image. Check the PINsafe server logs to see if a Single Channel Image message is present. If no message is present then no image request has been seen by the PINsafe server. Possible causes are network issues and the script being

in the wrong position. Try in a web browser from the internal network:

http://<pinsafe appliance URL>:8443/proxy/SCImage?username=demouser
(substitute correct port and context name where applicable)

If a single channel image is present check for RADIUS authentication errors.

Try in a web browser from the external network:

https://<turing.mycompany.com >/proxy/SCImage?username=demouser
(substitute correct port and context name where applicable)

Dual Channel and Single Channel RADIUS requests. Check the PINsafe server logs for RADIUS requests. Check name case sensitivity

If the PINsafe server receives the authentication with domain name/user name, then the authentication may fail. On the Juniper SA change the authentication setting for the PINsafe RADIUS server from <USER> to <USERNAME>.

6. Additional Information

For assistance in the PINsafe installation and configuration please contact your reseller or email Swivel Secure support at support@swivelsecure.com