

Juniper ChangePIN

Contents

- [1 Introduction](#)
- [2 Prerequisites](#)
- [3 Baseline](#)
- [4 Architecture](#)
- [5 Installation](#)
 - ◆ [5.1 Swivel Integration Configuration](#)
 - ◆ [5.2 Juniper ChangePIN Integration](#)
 - ◇ [5.2.1 Juniper ChangePIN page options](#)
 - ◇ [5.2.2 Juniper RADIUS Custom rules](#)
 - ◆ [5.3 Additional Installation Options](#)
 - ◇ [5.3.1 Combining Swivel and RSA RADIUS changePIN](#)
- [6 Verifying the Installation](#)
- [7 Uninstalling the Swivel Integration](#)
- [8 Troubleshooting](#)
- [9 Known Issues and Limitations](#)
- [10 Additional Information](#)

Introduction

This document outlines how to integrate the Swivel ChangePIN with Juniper. See also [RADIUS ChangePIN](#) and [ChangePIN How to Guide](#)

Prerequisites

Swivel Server

Juniper SSL VPN version 6 or 7 OS.

[Modified Changepin page for version 6](#)

[Modified Changepin page for version 7](#)

Baseline

Juniper SA 2000 JunOS 6 or 7.

Swivel 3.8

Architecture

A user authenticates against the Juniper server, which passes the RADIUS authentication to the Swivel server. If the user is required to Change their PIN the Swivel server responds with a RADIUS Challenge, and the user is redirected to a change PIN page.

Installation

Configure the Swivel and Juniper so that they are fully working together, see [Juniper SA 6.x Integration](#) or [Juniper SA 7.x Integration](#) or [Juniper SA 8.x Integration](#)

Swivel Integration Configuration

On the Swivel Administration Console select RADIUS then NAS and edit the required Juniper NAS entry Change PIN Warning to Yes, then apply the settings.

NAS:

Identifier:

Check Password with repository:

Username attribute for repository:

Allow alternative usernames:

Alternative username attributes:

Hostname/IP:

Secret:

Group:

EAP protocol:

Authentication Mode:

Vendor (Groups):

Change PIN warning:

Two Stage Auth:

Juniper ChangePIN Integration

Download the login page and add the modified ChangePIN page given above under prerequisites, rename and edit as appropriate, add to the zip file and upload to the Juniper server.

Juniper ChangePIN page options

Edit the following options:

```
var OTC_OPTION = "image"; // button, image, disable
```

image When the user tabs down from the username field, the TURing will automatically show, used for Single Channel access

button The login page will present a TURing button. Click the button to display the TURing, used for Single or Dual Channel access

disable The TURing image will not be shown, used for Dual Channel access.

TURingImage: Is the URL used to generate a TURing image. This should point to the internal IP address of the appliance

```
var TURingImage = "https://turing.swivelsecure.com/proxy/SCImage?username=";
```

Juniper RADIUS Custom rules

On the Juniper Administration console select the Swivel RADIUS server and create a Custom RADIUS rule with the following settings:

Name: ChangePIN

Response Packet Type: Access Challenge

Attribute Criteria: RADIUS Attribute Reply-Message (18)

Attribute Criteria: Operand Matches the expression

Value: changepin

Action: use the appropriately modified page; *Show Next Token page* or *show New Pin Page*

<input type="checkbox"/>	Name	Response Packet Type	Attribute criteria
<input type="checkbox"/>	ChangePIN	Access Challenge	(Reply-Message matches the expression "change

Additional Installation Options

Combining Swivel and RSA RADIUS changePIN

Where Swivel is acting as a proxy RADIUS server for RSA authentication, Swivel can proxy the RADIUS request.

Configure the Swivel RADIUS proxy so that it will authenticate RSA users, see [RADIUS Proxy How to guide](#).

On the Juniper edit the Swivel RADIUS authentication setting to add an additional custom rule with the following settings:

Name: RSACHangePIN

Response Packet Type: Access Challenge

Attribute Criteria: RADIUS Attribute Reply-Message (18)

Attribute Criteria: Operand does not match the expression

Value: changepin

Action: show Generic Login page

Apply the settings

Edit Custom Radius Rule

Name:

If received Radius Response Packet ...

Response Packet Type:

Attribute criteria:

Radius Attribute	Operand	Value	
<input type="text" value="Reply-Message (18)"/>	<input type="text" value="matches the expression"/>	<input type="text"/>	<input type="button" value="Add"/>
Reply-Message	does not match the expression	changepin	<input type="button" value="X"/>

Then take action ...

- show **New Pin** page
- show **Next Token** page
- show **Generic Login** page
- show **user login page** with error message
 -
 - show **Reply-Message** attribute from the Radius server to the user
- send **Access Request** with additional attributes

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

Note: The Juniper displays the Generic login page as *show Defender page*

<input type="checkbox"/>	Name	Response Packet Type	Attribute criteria
<input type="checkbox"/>	ChangePIN	Access Challenge	(Reply-Message matches the expression "change
<input type="checkbox"/>	RSAChangepin	Access Challenge	(Reply-Message does not match the expression "

Verifying the Installation

Login as a Swivel user.

Set the user to be required to change their PIN, the user should be redirected to the ChangePIN page. The user will be required to enter their old OTC, and a new OTC based on what they want their PIN to be. This OTC could be from the TURING, SMS message or mobile app. Remember to never enter the Swivel PIN.

Where RSA authentication is being used, require the user to change their PIN, and they should be redirected to a RSA Change PIN page. The the first time a user accesses the system with a new token the user will be required to enter a new PIN. If the user wanted a PIN of 1234 the would enter 1234 in the box.

The screenshot shows the Juniper Instant Virtual Extranet login interface. At the top, it says "Welcome to the Instant Virtual Extranet". Below this, there is a "Challenge / Response" section with a yellow background. The challenge text reads: "Challenge: Enter a new PIN having from 4 to 8 alphanumeric characters: Enter the challenge string above into your token, and then enter the one-time response in the field below." There is a text input field for the response, and "Sign In" and "Cancel" buttons at the bottom.

The RSA server then send a challenge asking for the PIN to be re-entered to confirm the user has not miss-typed it. The user would again enter 1234.

This screenshot shows the same Juniper Instant Virtual Extranet login interface. The challenge text now reads: "Challenge: Please re-enter new PIN: Enter the challenge string above into your token, and then enter the one-time response in the field below." The response input field contains four asterisks (****), and the "Sign In" and "Cancel" buttons are visible at the bottom.

Once the user has successfully changed their PIN the RSA server asks them to login again with their new PIN plus token code. The user would enter 1234XXXXXX where XXXXXX is the code displayed on the token.

This screenshot shows the Juniper Instant Virtual Extranet login interface. The challenge text reads: "Challenge: PIN Accepted. Wait for the token code to change, then enter the new passcode: Enter the challenge string above into your token, and then enter the one-time response in the field below." There is a text input field for the response, and "Sign In" and "Cancel" buttons at the bottom.

If the RSA server sees the token go out of sync it will ask the user to enter their next token code. The user would now enter XXXXXX where XXXXXX is the next code displayed on the token after the code the user used to authenticate. They do not type their PIN at this stage.



Uninstalling the Swivel Integration

Remove the modified login pages and RADIUS customisation.

Troubleshooting

Check the Swivel logs for authentication, proxy and ChangePIN requests.

Known Issues and Limitations

Where Swivel and RSA change PIN is being used and the user is a Swivel and a RSA user, and dual channel authentication is being used, then the Change PIN will fail for RSA users. for single channel users not using dual channel authentication, the proxy server can be used to detect the presence of a single channel session being started.

Additional Information