



# JUNIPER INTEGRATION

---

HOW TO USE PINSAFE TO AUTHENTICATE A  
JUNIPER SSL VPN

SWIVEL SECURE  
VICTORIA AVENUE  
HARROGATE  
HG1 1EL

# JUNIPER INTEGRATION NOTE

---

## CONTENTS

---

CONTENTS .....	2
INTRODUCTION .....	3
PREQUISITES .....	3
ENHANCEMENT .....	4
Modifying pinsafe.js .....	4
Creating An Anonymous Login Server .....	4
Creating An Anonymous User Role .....	5
Creating An Anonymous User Realm.....	5
Map All Users To The Anon Realm.....	6
Creating a Sign in Policy .....	7
Editing the User Role UI .....	7
Selective Rewriting Rule .....	8
Set Idle Timeout.....	9
Verifying Installation .....	10
Additional Information.....	10
Appendix A PINSAFE.JS EXPLAINED .....	11

---

## INTRODUCTION

---

This document outlines the steps required to implement the enhanced Juniper integration solution. It is an improved solution that removes the requirement for the PINsafe server to have an externally accessible IP address.

---

## PREREQUISITES

---

You require a Juniper VPN server with correct licenses installed to modify and upload the login page. A PINsafe server is required to perform authentication.

If the Single Channel Enhancement is not used to mask the PINsafe server IP address then the PINsafe server must be accessible from the internet to provide the Single Channel images.

The Juniper server used for this document was NetScreen-SA-2000 Advanced - 100 Simultaneous Users, with System Version 5.3R3.1 Release (build 10741).

---

## ENHANCEMENT

---

This section outlines the steps required to mask the PINsafe server so its IP address is not required to be publicly visible when using the Single Channel Turing Image. The basis of the solution is to allow an anonymous user to access the PINsafe server during authentication. Note that this is treated as an additional session and therefore uses an additional license for the process of authentication. The session will timeout and the licence released; the timeout period can be set as required, eg to five minutes.

In this way when the javascript runs in the client browser it actually requests the image via the Juniper SSL server and the SSL proxies the request. Therefore the PINsafe server only needs to be accessible from the SSL server rather than the internet.

### MODIFYING PINSafe.JS

The pinsafe.js java script needs to be modified to point to access the TURING image via the Juniper server as follows:

```
//URL of radiusTuring page on the PINsafe server...  
  
var sUrl="https://<Juniper IP hostname>/pinsafe/SCImage,DanaInfo=<IP of PINsafe  
server>,Port=8080,SSO=U+?username=";
```

### CREATING AN ANONYMOUS LOGIN SERVER

Select the page Authentication/Auth. Servers, from the Select New Server, set it to Anonymous Server then click on New Server, and enter a name for the server, eg PINsafeAnon

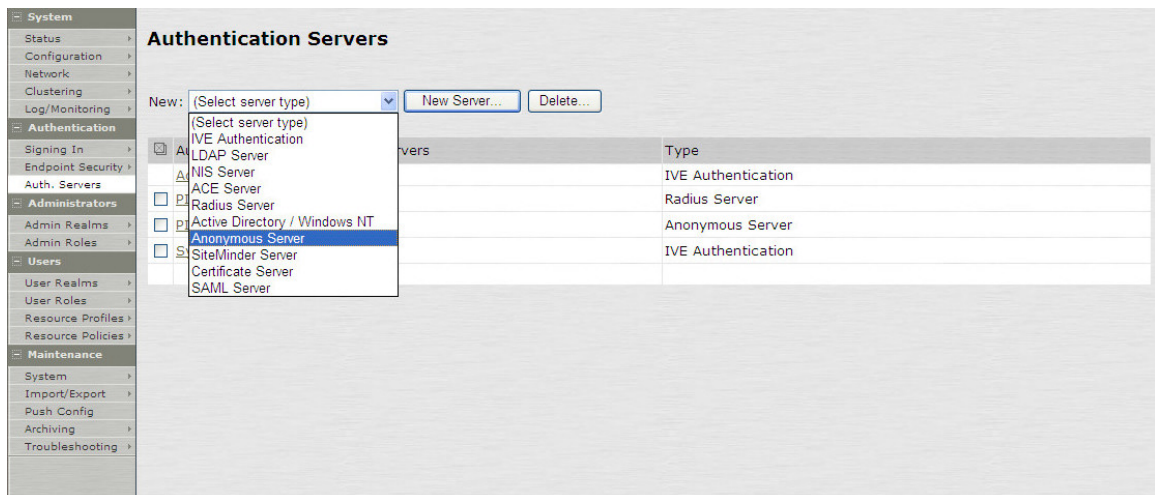


Figure 1. Creating an Anonymous Server

## CREATING AN ANONYMOUS USER ROLE

Select the page Users/User Roles and from this select New Role, enter a name for the role, ensure only UI and Web are selected and then click on Save Changes.

The screenshot displays the 'New Role' configuration interface. On the left is a navigation menu with categories like Authentication, Administrators, Users, and Maintenance. The main content area is titled 'New Role' and contains the following sections:

- Name:** anon
- Description:** Anonymous Role
- Options:** A note states 'Session and appearance options are specified in [Default Options](#). Check the following if this role should override these defaults.' Below this, the following options are checked:
  - Session Options**
  - UI Options**
- Access features:** A note states 'Check the features to enable for this user role, and specify any role-based options. Note that features disabled here may be granted by other roles assigned to the user.' Below this, the following features are checked:
  - Web**Other features listed but unchecked include: Files, Windows; Files, UNIX/NFS; Secure Application Manager (with sub-options for Windows and Java version); Telnet/SSH; Terminal Services; Meetings; Email Client; and Network Connect.

Figure 2. Creating an Anonymous Role

## CREATING AN ANONYMOUS USER REALM

Select the page Users/User Realm and from this select New, enter a name for the realm, and ensure that Authentication is set to the Anonymous Authentication Server created above then click on Save Changes.

**New Authentication Realm**

Name:  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:  Specify the server to use for authenticating users.

Directory/Attribute:  Specify the server to use for authorization.

Accounting:  Specify the server to use for Radius accounting.

Additional authentication server

Dynamic policy evaluation

**Save changes?**

Figure 3. Creating Anonymous Realm

### MAP ALL USERS TO THE ANON REALM

Select the Role Mapping page from User Realm/Anon Realm/Role Mapping, then select new. Assign Users to this realm; as shown below

User Authentication Realms > anon realm >

**Role Mapping Rule**

Rule based on:

Name:  Optional (used with the "select the sets of merged roles" setting)

**Rule: If username...**

If more than one username should match, enter one username per line. You can use \* wildcards.

**...then assign these roles**

Available Roles:

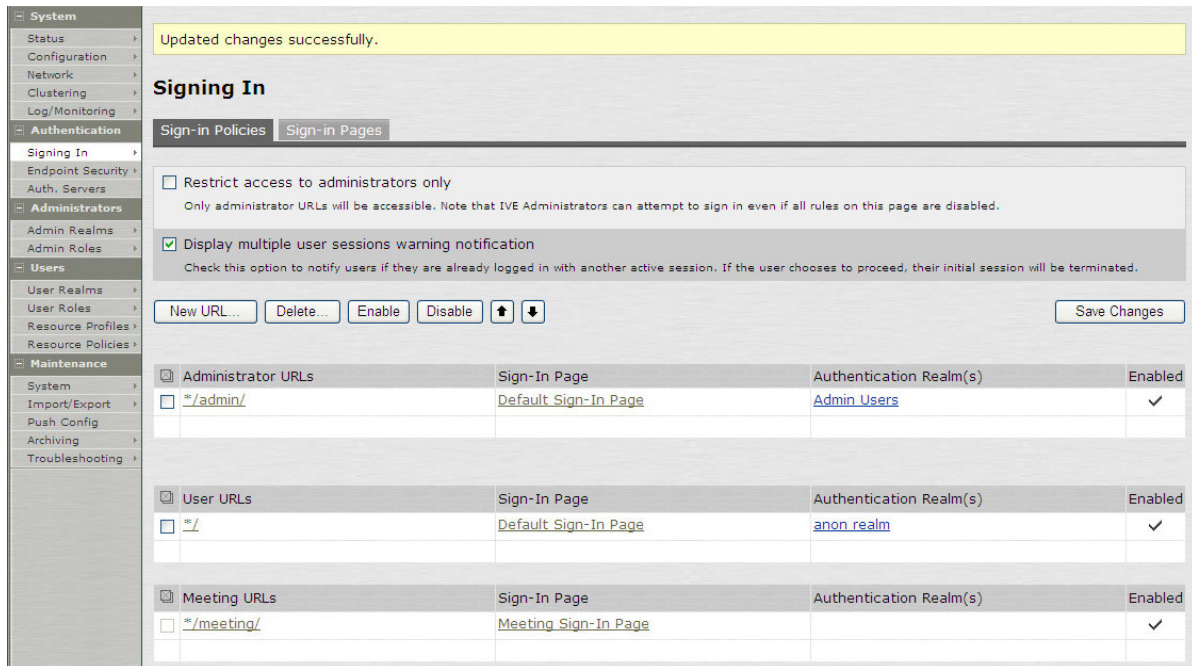
Stop processing rules when this rule matches

**Save changes?**

Figure 4. Mapping Users to the Anonymous Realm

## CREATING A SIGN IN POLICY

Ensure that the correct signing in pages are all in place and set the sign in policy to point at the anonymous realm. Select Authentication/Signing In/Sign-in Policy, select the ./\* URL or the PINsafe login page URL and set the Authentication Realm to the Anonymous realm created, then click on Save Changes.



The screenshot shows the 'Signing In' configuration page. At the top, a yellow banner indicates 'Updated changes successfully.'. Below this, the 'Signing In' section is active, with sub-tabs for 'Sign-in Policies' and 'Sign-in Pages'. There are two checkboxes: 'Restrict access to administrators only' (unchecked) and 'Display multiple user sessions warning notification' (checked). Below these are buttons for 'New URL...', 'Delete...', 'Enable', 'Disable', and 'Save Changes'. A table lists the configured sign-in policies:

URL	Sign-In Page	Authentication Realm(s)	Enabled
<input type="checkbox"/> Administrator URLs			
<input type="checkbox"/> */admin/	Default Sign-In Page	Admin Users	✓
<input type="checkbox"/> User URLs			
<input type="checkbox"/> */	Default Sign-In Page	anon realm	✓
<input type="checkbox"/> Meeting URLs			
<input type="checkbox"/> */meeting/	Meeting Sign-In Page		✓

Figure 5. Setting Signing-In Policy

## EDITING THE USER ROLE UI

Select the UI page from Users/User Role/anonymous role created/General/UI. On the section Start Page click on Custom page and modify the URL to represent the original sign in page which should already have been created.

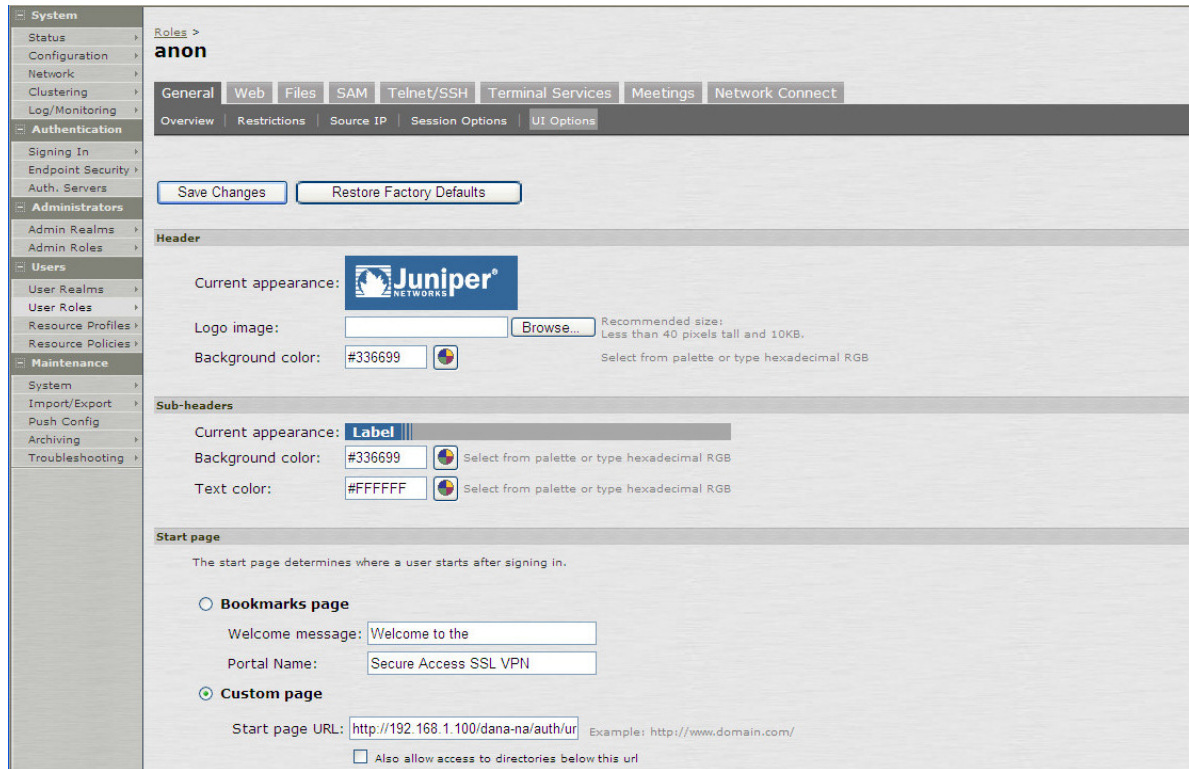


Figure 6. Setting Custom Login page

### SELECTIVE REWRITING RULE

This rule prevents the address details for the server from being over-written, it must be listed before the default rewrite everything rule. Select Resource Policies/Web/Selective Rewriting and then New Policy. Enter a name for the policy and under the resources enter the SSL hostname or IP address, followed by the connection and a \* for sub folders eg:

hostname:80,443/\*

Select Policy Applies to Selected Roles, selecting the anonymous role, and then select the Action 'Don't rewrite content: Do not redirect to target web server', then select Save Changes.



**Name:** PINsafe Selective Rewriting Required: Label to reference this policy.

**Description:** To Stop automatic Rewriting of Rules

**Resources:** Specify the resources for which this policy applies, one per line.  
 \* Resources: Juniper Server IP:80,443/\*  
 Examples:  
 http://\*.domain.com/public/\*  
 https://www.domain.com:443/\*  
 10.10.10.10/255.255.255.0:80,443/public/\*  
 10.10.10.10/24:8000-9000/\*

**Roles:**

Policy applies to ALL roles  
 Policy applies to SELECTED roles  
 Policy applies to all roles OTHER THAN those selected below

**Available roles:** Users  
**Selected roles:** anon

**Action:**

Rewrite content (auto-detect content type)  
 Rewrite content as...  
 HTML  
 Don't rewrite content: Redirect to target web server  
 Don't rewrite content: Do not redirect to target web server  
 Use Detailed Rules (available after you click 'Save Changes')

Figure 7. Selective Rewriting Configuration

**Web Rewriting Policies**

Access SSO Caching Java **Rewriting** Compression Web Proxy Launch JSAM Protocol Options

Selective Rewriting Passthrough Proxy ActiveX Parameter Rewriting

Show policies that apply to: All roles Update

Successfully saved policy: PINsafe Selective Rewriting

New Policy... Duplicate Delete... Save Changes

	Policies	Action	Resources	Applies to role
<input type="checkbox"/>	1. <a href="#">PINsafe Selective Rewriting</a> To Stop automatic Rewriting of Rules	Don't Rewrite (without redirect)	192.168.1.100:80,443/*	anon
<input type="checkbox"/>	2. <a href="#">Initial Rewrite Policy</a> Always rewrite.	Rewrite	*:*/*	All roles

Keyboard shortcuts:  
 Use "<" and ">" keys to move selected items up and down (remember to click Save Changes after rearranging the list). Use **Ctrl+Plus** and **Ctrl+Minus** to expand and collapse all items.

Figure 8. Showing PINsafe re-routing prior to global rewrite policy

### SET IDLE TIMEOUT

Anonymous users count towards the number of concurrent sessions for each login, although they are only briefly used. To prevent the system from filling up with many concurrent anonymous users set the Idle Timeout value to a low value. Select Users/User Roles/ anonymous

role/General/Session Options. Then from the session lifetime section change the Idle Timeout to a value such as 5 minutes.

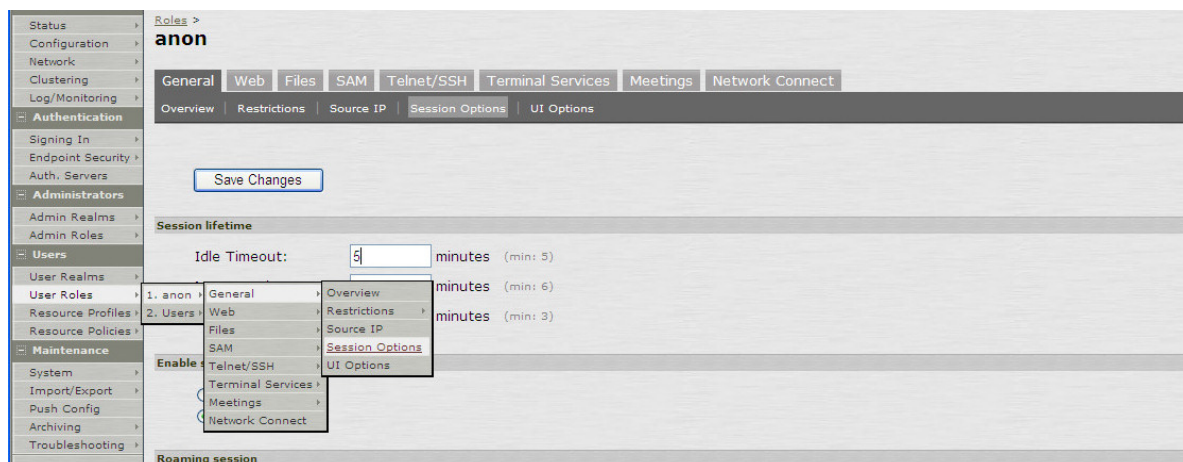


Figure 9. Setting Session Timeout

---

## 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. The Single Channel Turing Image should not reveal the internal IP address of the PINsafe server.

The PINsafe logs will contain entries of all authentication attempts.

---

## ADDITIONAL INFORMATION

---

For assistance in the PINsafe installation and configuration please contact your reseller or email Swivel Secure support at [support@swivelsecure.com](mailto:support@swivelsecure.com)

---

## APPENDIX A PINSAFE.JS EXPLAINED

---

```
//~~~~~  
//  
//Configuration section.....  
  
//Prompt wording...  
var sOTCPrompt = "Enter your OTC:";  
  
//URL of radiusTuring page on the PINsafe server...  
var sUrl="http://172.18.1.20:8080/pinsafe/SCImage?username=";  
  
//Names of the username and password texboxes in the page that's calling this  
script...  
var sNameOfUsernameText = "username";  
var sNameOfPasswordText = "password";  
  
//End configuration section.....  
//  
//~~~~~  
  
//See if we're on the right 'page', ie. username field is present...  
var bExists = (document.getElementById(sNameOfUsernameText)[0] != null);  
  
document.write("<input type=button name=btnTuring value=Turing  
onclick=ShowTuring() class='submitbutton' styleHIDDEN='visibility:hidden;  
position: absolute; left:250;top:302;width:75;'>");  
document.write("<img id=imgTuring name=imgTuring  
style='visibility:hidden;position: absolute; left:100;top:350;'>");  
  
if (bExists){  
    document.getElementById("btnTuring")[0].style.visibility="visible";  
  
    try {  
        var tableCount = document.getElementsByTagName("table").length;  
  
        //Try and determine which page we are on from the table count and update  
the appropriate  
        //table cell with the OTC prompt  
        if (tableCount == 3)  
            document.getElementsByTagName("td")[10].childNodes[0].nodeValue =  
sOTCPrompt;  
        else if (tableCount == 5)
```

This is the prompt that will appear on the login page instead of Password

These are the names of the fields on the login page.

Add the button, but hide it initially. Call ShowTuring when pressed

If we are on a login page, make button visible

Add the TURING image, but hide it initially

Workout where to write OTC prompt

```

        document.getElementsByTagName("td")[13].childNodes[0].nodeValue =
sOTCPrompt;
    } catch (e){
        alert ("An error occurred in PINsafe Extensions:\n\n" + e);

    }

}

function ShowTuring() {

if (bExists) {
    sUser=document.getElementsByName(sNameOfUsernameText)[0].value;

    if (sUser=="") {
        alert ("Please enter your username first!");
        document.getElementsByName(sNameOfUsernameText)[0].focus()
    }else{

        //Find the image using Mozilla compatible pproach...
        varImg = document.getElementById("imgTuring");

        //Set the image SRC and make it visible
        varImg.src = sUrl + sUser;
        varImg.style.visibility = "visible";

        //Alternative approach - show image in Popup
        //window.showModalDialog(sUrl +
sUser,null,"dialogWidth=305px;dialogHeight=110px;status:no;scroll:no;help:no;")

        //Set focus to the OTC input
        document.getElementsByName(sNameOfPasswordText)[0].focus()
    }
}

}

```

If button pressed and username entered, retrieve image from PINsafe