

JUNIPER-PULSE

The specifications and information in this document are subject to change without notice. Companies, names, and data used in examples herein are fictitious unless otherwise noted. This document may not be copied or distributed by any means, in whole or in part, for any reason, without the express written permission of RCDevs Security.

WebADM and OpenOTP are trademarks of RCDevs. All further trademarks are the property of their respective owners.

No guarantee is given for the correctness of the information contained in this document. Please send any comments or corrections to info@rcdevs.com.

How To Enable OpenOTP Authentication On Juniper-Pulse Secure

This document explains how to enable OpenOTP authentication with Radius Bridge and Juniper SSL VPN.

1. WebADM/OpenOTP/Radius Bridge

For this recipe, you will need to have WebADM/OpenOTP installed and configured. Please, refer to [WebADM Installation Guide](#) and [WebADM Manual](#) to do it. You have also to install our [Radius Bridge product](#) on your WebADM server(s).

2. Register Your Juniper VPN In RadiusBridge

On your OpenOTP RadiusBridge server, edit the `/opt/radiusd/conf/clients.conf` and add a RADIUS client (with IP address and RADIUS secret) for your Juniper VPN server.

Example:

```
client <VPN Server IP> {  
  secret = testing123  
  shortname = Juniper-Pulse  
}
```

3. Configuring New Radius Server On Juniper

- › Log in to the Pulse web-based management interface.
- › From the left-hand menu, select Authentication —> Auth. Servers. —> Radius Server —> New Server.
- › On New Radius Server page configure (see example below):
 - › Name - i.e. OpenOTP
 - › NAS-Identifier - any value to describe your Juniper.
 - › Radius Server - your OpenOTP server IP or hostname.
 - › Shared Secret - i.e. testing123 (this value pre-configured to OpenOTP Virtual Machine). Finally, save changes.

Administrator Console

- System**
 - Status
 - Configuration
 - Network
 - IF-MAP Federation
 - Log/Monitoring
- Authentication**
 - Signing In
 - Endpoint Security
 - Auth. Servers
- Administrators**
 - Admin Realms
 - Admin Roles
- Users**
 - User Realms
 - User Roles
- Maintenance**
 - System
 - Import/Export
 - Archiving
 - Troubleshooting

[Auth Servers](#) >

New Radius Server

Name: Label to reference this server.

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

Primary Server

Radius Server: Name or IP address

Authentication Port:

Shared Secret:

Accounting Port: Port used for Radius accounting, if applicable

NAS-IP-Address: IP address

Timeout: seconds

Retries:

☐ 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 SAML, and this credential will not be used in automatic SSO to backend applications.

4. Enabling Challenge-Response (OTPPrompt)

On your new RADIUS server settings page, scroll down to section Custom Radius Rules and click New Radius Rule... button. In subsequent window configure (see example below):

- > Name - i.e. OTPPromptRule
- > At Response Packet Type choose Access-Challenge.
- > At Attribute criteria:
- > Choose Reply-Message for Radius Attribute.
- > Operand must match the expression.
- > Value must be "(.*)", without the quotes.
- > Click Add.

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	matches the expression	(.*)	<input checked="" type="checkbox"/>

- > Under then take action to select the Show Generic Login Page radio-button.

- › Click Save to complete configuring a new RADIUS server.

5. Activate New RADIUS Server

In the left-hand menu, select User Realms → Create New Authentication Realm. In subsequent window configure (see example below):

- › Name - i.e. OpenOTP Realm (this value will be shown in Realms drop-down on your login page).
- › For Authentication under Servers, choose RADIUS server created in previous steps (OpenOTP).
- › Click the Save Changes to complete configuring a new authentication realm.

The screenshot shows the 'Administrator Console' interface. On the left is a navigation menu with categories: System, Authentication, Administrators, Users, and Maintenance. The 'Authentication' section is expanded, showing 'Signing In', 'Endpoint Security', and 'Auth. Servers'. The 'Auth. Servers' option is selected. The main content area is titled 'New Authentication Realm'. It contains the following fields:

- Name:** A text input field containing 'OpenOTP Realm'.
- Description:** A text area with up and down arrow icons.
- ☐ When editing, start on the Role Mapping page

Below these fields is a section titled 'Servers' with a grey header. Under this section, there is a text instruction: 'Specify the servers to use for authentication and authorization. To create or manage servers, see the [Servers](#) page.' Below this instruction are three dropdown menus:

- Authentication:** A dropdown menu with 'OpenOTP' selected.
- Directory/Attribute:** A dropdown menu with 'Same as above' selected.
- Accounting:** A dropdown menu with 'None' selected.

- › In the left-hand menu, click Sign-In → Sign-In Policies.
- › Select the Sign-In policy to which you like to tie the new Realm with, i.e. Default Sign-In Policy (/).
- › Select User Picks from a List of Authentication Realms under Authentication Realms (see example below):
- › From a list of Available Realms, add your new Authentication Realm to list of Selected Realms.
- › Click Save Changes and your Juniper/Pulse configuration is complete, and you can start to log in by using OpenOTP.

Administrator Console

System

Status

Configuration

Network

IF-MAP Federation

Log/Monitoring

Authentication

Signing In

Endpoint Security

Auth. Servers

Administrators

Admin Realms

Admin Roles

Users

User Realms

User Roles

Maintenance

System

Import/Export

Archiving

Troubleshooting

Signing In >

*/

Save Changes

User type:

☒ Users
 ☐ Administrators

Sign-in URL:

*/

Format: <host>/<path>/;

Description:

Default User Sign In

Sign-in page:

Default Sign-In Page

To create or manage pages, see [Sign-In pages](#).

Authentication realm

Specify how to select an authentication realm when signing in.

☐ User types the realm name

The user must type the name of one of the available authentication realms.

☒ User picks from a list of authentication realms

The user must choose one of the following selected authentication realms when they sign in. If only one realm is selected, the user must choose that realm. See [Authentication page](#).

Available realms:

Add ->

Remove

Selected realms:

OpenOTP Realm

Move Up

Move Down

Note

Don't forget to authorize the communication on 1812 UDP port (default RADIUS port for the authentication) from your Juniper-Pulse system to your WebADM instance at the firewall level.

6. Example Login

OTP Token Note

This chapter assumes you have already enrolled your token to OpenOTP, or that you are logging in with a Token less mode (i.e. SMS or Email OTP).

- > Go to your Juniper sign-in URL.
- > From Realm, drop-down choose the OpenOTP Authentication Realm.
- > Enter your domain login name and password:



**Welcome to the
Secure Access SSL VPN**

Username Please sign in to begin your secure session.

Password

Realm

› Page will refresh to prompt you to enter your OTP.



**Welcome to the
Secure Access SSL VPN**

Challenge / Response

Challenge: Please enter your Authenticator code:

Enter the challenge string above into your token, and then

Response:

› Enter the OTP delivered to you via SMS, Email or provided by your OATH Token, Yubikey or similar device. You should be successfully logged in now!

This manual was prepared with great care. However, RCDevs Security S.A. and the author cannot assume any legal or other liability for possible errors and their consequences. No responsibility is taken for the details contained in this manual. Subject to alternation without notice. RCDevs Security S.A. does not enter into any responsibility in this respect. The hardware and software described in this manual is provided on the basis of a license agreement. This manual is protected by copyright law. RCDevs Security S.A. reserves all rights, especially for translation into foreign languages. No part of this manual may be reproduced in any way (photocopies, microfilm or other methods) or transformed into machine-readable language without the prior written permission of RCDevs Security S.A. The latter especially applies for data processing systems. RCDevs Security S.A. also reserves all communication rights (lectures, radio and television). The hardware and software names mentioned in this manual are most often the registered trademarks of the respective manufacturers and as such are subject to the statutory regulations. Product and brand names are the property of RCDevs Security. © 2024 RCDevs Security S.A., All Rights Reserved