

# VPN INTEGRATION WITH RCDEVS CLOUD SOLUTIONS

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](mailto:info@rcdevs.com).

# VPN Integration with RCDevs cloud solutions

[VPN](#) [Virtual Private Network](#) [Token](#) [RCDevs in the Cloud](#) [Cloud Services](#) [Cloud Authentications](#)

## 1. Overview

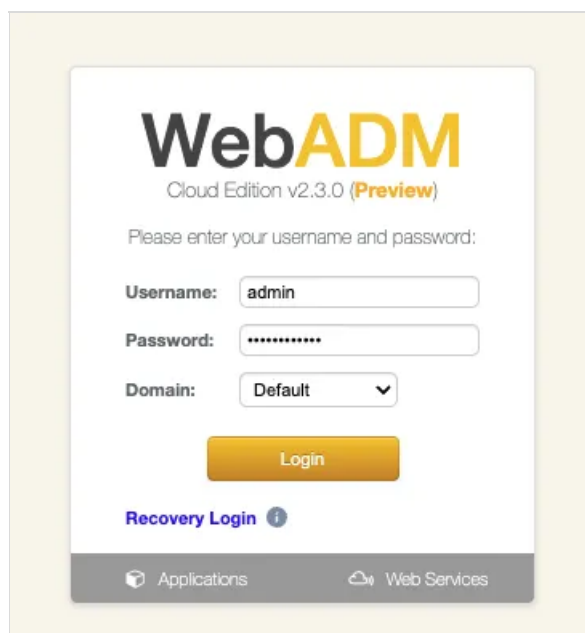
In this documentation, we will focus on configuring your On-Premise VPN server with the OpenOTP Cloud solution (either Mutualized Cloud or Dedicated Cloud). Typically, VPN integration involves using the Radius, LDAP or SAML/OpenID with some VPN solutions. For SSL VPNs working with SAML or OpenID, that documentation is not explaining how to configure your VPN with SAML/OpenID. Please, refer to [OpenID/SAML documentation](#). However, it's important to note that the Radius protocol was not specifically designed for transport over the internet. For this reason, RCDevs recommends deploying the [OpenOTP Cloud Virtual Appliance](#), which includes Radius and LDAP Bridges components. This approach ensures a more secure integration. If you choose not to deploy the OpenOTP Cloud Virtual Appliance, you have the option to contact RCDevs to inquire about alternative solutions. However, it's important to understand that using the Radius protocol directly over the internet without proper precautions carries certain risks, and it is done at your own discretion. When the OpenOTP Cloud Bridge VM is set up, communication between your infrastructure and the RCDevs cloud infrastructures utilizes the HTTPS protocol with client/server certificate validation or API key authentication. This ensures a secure connection. If the OpenOTP Cloud Bridge VM is not implemented within your network, the LDAP and Radius protocols will be transmitted over the internet. It is crucial to consider security implications and evaluate the level of risk associated with the chosen integration method. RCDevs is available to assist and provide guidance in ensuring a secure and reliable VPN integration with the OpenOTP Cloud solution.

## 2. User creation, activation and token enrollment

The following steps outline how to create a user account in WebADM, activate the account, enroll a software token using the Push mechanism, and conduct a test login via the WebADM Admin portal prior to commencing your integration.

### 2.1 Account Creation

Login on WebADM Admin portal with your Administrator account.



The image shows a screenshot of the WebADM Cloud Edition v2.3.0 (Preview) login interface. The form is titled 'WebADM Cloud Edition v2.3.0 (Preview)' and prompts the user to 'Please enter your username and password:'. It includes input fields for 'Username' (containing 'admin'), 'Password' (masked with dots), and 'Domain' (a dropdown menu set to 'Default'). A yellow 'Login' button is positioned below the fields. At the bottom left, there is a link for 'Recovery Login' with an information icon. The footer contains two links: 'Applications' and 'Web Services'.

Click on the create button in order to create a test account.

**LDAP Server 2 (RCDevs Directory)**

RCDevs Directory (3)

- cn=admin
- cn=other\_admins
- dc=WebADM

Create / Search  
Details / Check

**WebADM Cloud Edition v2.3.0 (Preview)**  
Copyright © 2010-2023 RCDevs Security, All Rights Reserved

Home Admin **Create** Search Import Databases Applications About Logout

Hello Admin (cn=admin)  
Connected as Super Administrator to webadm2.openotp

**License Details**

License Status: **Valid** (Virtual)  
Hosted Tenant: **YOANN**  
User Quota: 5 active users  
Host Quota: 0 active host  
Support Services: **Yes** (Generate a support ticket file)

**Activated Services**

Internal PKI Services: ✓ (no new certificate today)  
Electronic Signature: ✓ (no signature & no seal today)  
Mobile User Badging: ⚠ (badging not enabled)  
Mobile Push Service: ✓ (no push sent today)  
SMS Gateway Service: ✓ (no SMS sent today)  
SMTP Email Relay: ✓ (no email sent today)

**Application Status**

MFA Authentication Server: **Ok** (v2.2.4)  
Shared Session Server: **Not Registered**  
SMS Hub Server: **Not Registered**  
SSH Public Key Server: **Ok** (v2.1.1)  
QR Login & Signing Server: **Not Registered**  
Demo Account Registration: **Not Registered**  
OpenID & SAML Provider: **Not Configured**  
Secure Password Reset: **Ok** (v1.3.0)  
User Self-Service Desk: **Ok** (v1.4.0)  
User Self-Registration: **Ok** (v1.4.0)  
OpenOTP Cloud Tenant Registration: **Not Registered**

**Configurations Objects**

User Domains: **1** (Details)      Client Policies: **1** (Details)  
Option Sets: **1** (Details)      Admin Roles: **1** (Details)

Show More

Select User/Administrator and then click **Proceed**.

Create New LDAP Object

☐

WebADM Option Set

OptionSet, Mountpoint, Domain, Client...

☐

WebADM Account

LDAP user with WebADM attributes

☒

User / Administrator

Administrator or LDAP user

☐

Static Group

LDAP group of users

☐

Dynamic Group

LDAP group with dynamic contents

☐

UNIX Account

UNIX POSIX Account

☐

UNIX Group

UNIX POSIX Group

☐

Organizational Unit

LDAP organizational unit container

☐

Organisation

LDAP organization container

☐

Country

LDAP country container

☐

Domain

LDAP domain container

☐

Password Policy

LDAP password policy configuration

Proceed

On the next page, provide user's information and then click **Proceed**.

Create Object of Type **User / Administrator**

Mandatory attributes

Container

[ROOT]

Select

Last Name

test

Common Name

user

Optional attributes

Password

\*\*\*\*\*

Country

[Not Set]

Description / Note

First Name

Email Address

test\_user@domain.com

Mobile Phone Number

Use international format with space separator (ex. +33 612345678).

Organization

Login Name

test\_user

User Certificate

You can create a user certificate one object is created.

Preferred Language

[Not Set]

Organizational Unit

Proceed

A recap is prompted, check your inputs and click **create object**.

Create Object of Type **User / Administrator**

Confirm object creation for *cn=user*

| Attribute     | Value                       |
|---------------|-----------------------------|
| DN            | <u>cn=user</u>              |
| Last Name     | <u>test</u>                 |
| Common Name   | <u>user</u>                 |
| Password      | <u>****</u>                 |
| Email Address | <u>test_user@domain.com</u> |
| Login Name    | <u>test_user</u>            |

Create Object

Your user account is now created.

Object cn=user ⓘ

LDAP Actions

Delete this object
Copy this object
Move this object
Export to LDIF
Change password
Create certificate
Advanced edit mode

Object Details

Object class(es): person  
Account is unique: **Yes** (in [ROOT])  
Account badged-in: **No**  
User activated: **No** **Activate Now!** ⓘ

Object Name

user

Rename

Add Attribute (9)

Country

▼

Add

Add Extension (2)

UNIX Account

▼

Add

Last Name

test

[add values]

Email Address

test\_user@domain.com

[add values] [delete attribute]

✉

Login Name

test\_user

[add values] [delete attribute]

Apply Changes

Re-Encrypt

Delete Selected

## 2.2 Account Activation

Now, we need to activate the account. On the user account, in **object details**, click **Activate now** button followed by **Proceed** button.



Add Extension **WebADM Account** to **cn=user**

Optional attributes

WebADM Settings

You can edit this attribute once object is created.

WebADM User Data

This attribute cannot be created manually.

WebADM Voice Model

You cannot set this attribute manually!

Preferred Language

[Not Set] ▼

Mobile Phone Number

Use international format with space separator (ex. +33 612345678).

Description / Note

Proceed
Cancel

Finally click on **Extend object** :

Add Extension **WebADM Account** to **cn=user**

The object will be extended with the objectclass **WebADM Account**.  
No new attribute will be added to the object during extension.

Extend Object
Cancel

Account is now activated. You can now see the **Application Actions** menu.

Object **cn=user**

LDAP Actions

Delete this object

Copy this object

Move this object

Export to LDIF

Change password

Create certificate

Unlock WebApp access

Advanced edit mode

Object Details

Object class(es): **person, webadmAccount**  
Account is unique: **Yes** (in [ROOT])  
Account badged-in: **No**  
WebADM settings: **None [CONFIGURE]**  
WebADM data: **None [EDIT]**  
User activated: **Yes Deactivate**  
Logs and inventory: **WebApp, WebSrv, Inventory, Record**

Application Actions

Secure Password Reset (1 actions)

User Self-Registration (1 actions)

MFAAuthentication Server (16 actions)

SSH Public Key Server (3 actions)

Object Name

user

Rename

Add Attribute (12)

Country

Add

Add Extension (1)

UNIX Account

Add

Last Name

test

[add values]

Email Address

test\_user@domain.com

[add values] [delete attribute]

Login Name

test\_user

[add values]

Apply Changes | Re-Encrypt | Delete Selected

## 2.3 Token Enrollment

We are going now to enroll a software token. We advise you to use [OpenOTP Token application](#) in order to take advantage of all features provided by OpenOTP. In **Application Actions** menu, click on **MFA Authentication Server** > **Register/Unregister OTP Tokens**. Select **I use a QRCode-based Authenticator** (time-based or event-based), then the enrollment QRCode is prompted. Open the OpenOTP Token application (or another authenticator app), then click the camera button and scan the QRCode.

Register / Unregister OTP Tokens for **cn=user**

You must register a Hardware or Software Token for the user to start using it.  
The registration consists in synchronizing a Secret Key and an initial Token state.

Instructions to register a QRCode-based Software Token:

1. Install the software Token on the mobile device.
2. Start your software Token and Scan the QRCode displayed below.
3. Click the 'Register' button below after scanning.

Detached registration let you send the QRCode to the user via email for self-registration.  
The registration is done when the user scans the QRCode within the configured expiration time.  
The protection PIN can optionally be sent via SMS.

Register Token:

Primary Token ▾



☐ I use a Hardware Token (Inventoried)

☐ I use a Yubikey Token (Inventoried or YubiCloud)


☒ I use a QRCode-based Authenticator (Time-based)

☐ I use a QRCode-based Authenticator (Event-based)

☐ I use another Token (Manual Registration)

QRCode:

(Enlarge)



Optional Information

Expiration Date:

Edit

Registered UserID:

test\_user ▾

Registered Domain:

Default ▾

Mobile Push Data:

[Waiting for Mobile Response]

Detached Registration

Expiration Time:

30 Mins ▾

QRCode Format:

JPG ▾

Send QRCode:

☒ Yes (Email) ☐ No

Enrolment PIN:

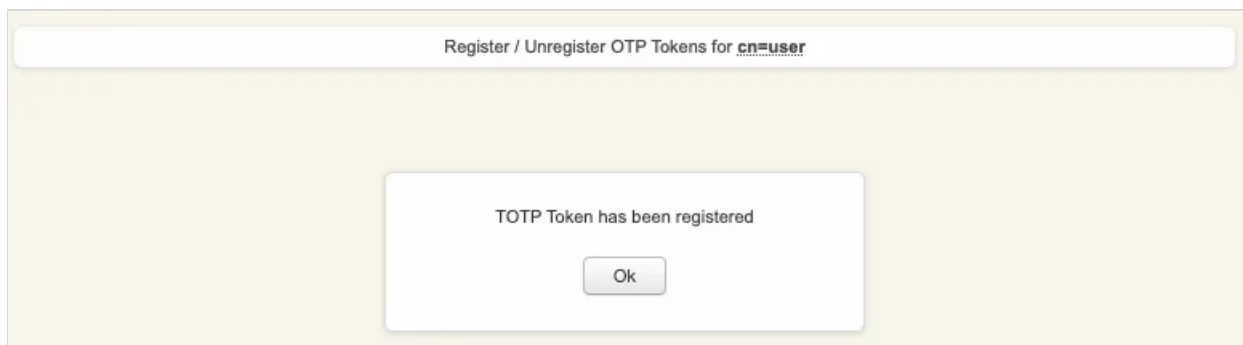
867440

Register

Detach

Ok

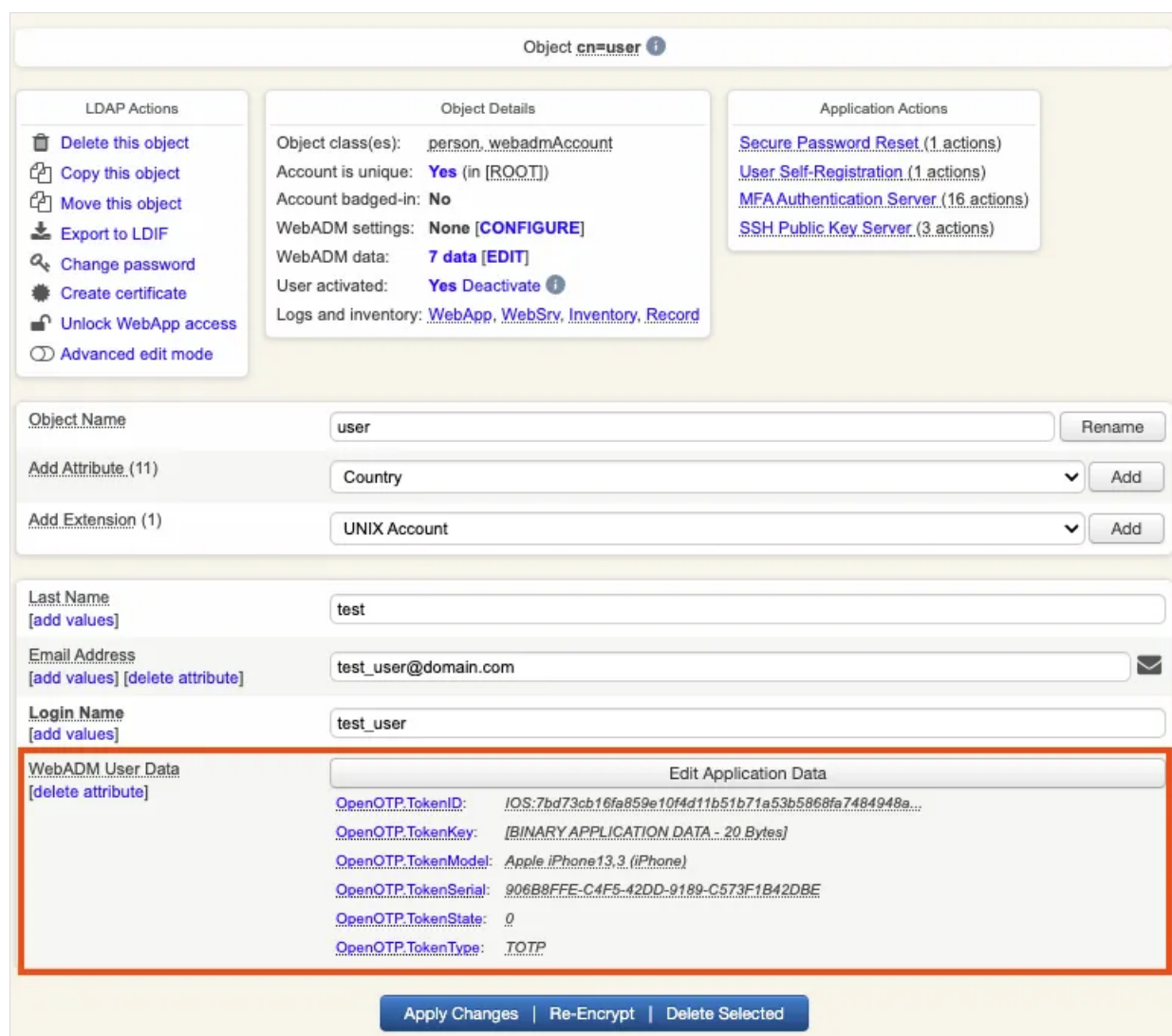
If the QRCode has been scanned with OpenOTP token, you don't need to click **Register** button. If the QRCode has been scanned with another token application, you need to click **Register** button once the token is registered on your device.



Your token has been registered successfully, we can now try to perform a login with it.

## 2.4 Test login

Come back on the user account, you will see now the token metadata registered on the account:





The enrollment here has been performed with OpenOTP Token and Push mechanism are by default enabled. We will now perform a test login with Push authentication.

In **Application Actions** menu, click on **MFA Authentication Server** >  
**Test OTP & FIDO Authentication**

You must register a hardware or software token before a user can start using it.



#### Register / Unregister FIDO Devices

You must register a FIDO Device before a user can start using it.



#### Register / Unregister Voice Biometrics

Enrol your voice fingerprint for voice biometrics authentication.



#### Resynchronize Tokens

Event-based and time-based tokens can get out of sync. You can use the action to resync the Token counter or clock drift.



#### Manage OTP PIN Prefix

Set an OTP PIN if you want the OTP passwords to be prepended by a static PIN password. Any OTP password will have to be prefixed by the static PIN code in the form [PIN][OTP].



#### Manage OCRA Token PIN Code

Only OCRA Tokens support a PIN code feature. Use this action to set or reset the PIN code on the user account.



#### Manage Emergency OTP

An emergency OTP is an auto-expirable static OTP which can be used when the user cannot use his usual OTP/FIDO method and requires a temporary access.



#### Manage Printed OTP List

You can use this action to register, remove, display and download user OTP Lists.



#### Manage Application Passwords

You can use this action to register, remove and display per-application passwords.



#### Unblock Account

You can use this action to unblock an account after the max authentication attempts has been reached.



#### Import OATH-PSKC File

You can use the action to import a PSKC (RFC-6030) OATH Token key file.



#### Export OATH-PSKC File

You can use the action to export the registered OATH Token to a PSKC (RFC-6030) file.



#### Test OTP & FIDO Authentication

You can use this action to simulate a user authentication.



#### Test Signature & Confirmation

You can use this action to test a transaction confirmation or qualified signature.



#### Display Pending Transactions

Review or cancel pending confirmations and signatures for the user.



#### Check on a Remote Worker

Require the remote user to badge (in check mode) and confirm his location information.

Cancel

You arrive at the following page:

Test OTP & FIDO Authentication for **cn=user**

You can use this page to test a user OpenOTP authentication request.  
Some fields are optional and depend on your OpenOTP configuration.

**Server Status: Accepting Requests**

Server: MFAAuthentication Server 2.2.4 (WebADM 2.3.0)  
System: Linux 5.14.0-284.11.1.el9\_2.x86\_64 x86\_64 (64 bit)  
Listener: 127.0.0.1:8080 (HTTP/1.1 SSL)  
Uptime: 2763s (0 days)  
Cluster Node: 2/2 (Session Server 2)  
Local Memory: 0M (42M total)  
Shared Memory: 5M (0M total)  
Connectors: OK (4 alive & 0 down)

Login Method: ☒ Normal ☐ Simple

Username:

Domain:

LDAP Password:

OTP Password:

Simulated Client:

Simulated Source:

Simulated Options:

Request Settings:

Virtual Attributes:

Browser Context:

Debug Mode: ☐ (enable debug logs for this request)

Start

Cancel

Provide the LDAP password that you previously configured during the user account creation, then click **Start**. A push notification should be prompted on your phone. Approve the request. The test login has been performed successfully.

Test OTP & FIDO Authentication for **cn=user**

Result: **Success**

Message: Authentication success

Ok

Cancel

If you didn't register the token with OpenOTP token application, then an OTP challenge is sent if you only provided the LDAP password. In that case, provide the OTP code generated by your token application and click **Continue**.

Test OTP & FIDO Authentication for `cn=user`

Result:

Challenge (OTP)

Message:

Enter your TOKEN password

Timeout:

56 seconds

OTP Password:

Continue

Cancel

The test login has been performed successfully.

If the test login failed, you can browse the WebADM server logs to identify the problem. You can access the logs by accessing the [Databases](#) tab > WebADM Server Log File. The following [troubleshooting documentation](#) will provide help and resolution on common issues.

WebADM Cloud Edition v2.3.0 (Preview)  
Copyright © 2010-2023 RCDev's Security. All Rights Reserved.

Home

Admin

Create

Search

Import

Databases

Applications

About

Logout

SQL Databases and Log Files

SQL Log Tables

Administrator Logs

Admin Portal logs (admin audit)

Manager Logs

Manager Interface logs (admin audit)

WebApp Logs

Web Application logs (user audit)

WebSrv Logs

Web Service logs (user audit)

Alert Logs

System Alerts from applications

SQL Data Tables

Localized Messages

Message translations for applications and services

Inventoried Devices

OpenOTP hardware Tokens and SpanKey PIV keys

Recorded Sessions & Transactions

Transaction records and SpanKey sessions' audit

Physical Access & Mobile Badging

Dashboard with badging records and presence reports

Client, Server and Mobile Certificates

Provides review and revocation for services your certificates

Web Services API Keys

Access Tokens required for Web services with secure access

System Log Files

WebADM Shared Event Logs

WebADM mixed event logs from all cluster nodes

WebADM Server Log File

WebADM local event logs from this server

### 3. VPN Setup with the VM bridges

This scenario assumes that you prioritize maximum security for the communication between your infrastructure and the openotp.com infrastructure. To achieve this, it is recommended to deploy our OpenOTP Cloud Bridge VM, which can be set up

following the instructions provided in the OpenOTP Cloud Bridge VM setup documentation.

The OpenOTP Cloud Bridge VM is a preconfigured virtual machine that includes both the Radius Bridge and LDAP Bridge components. In most cases, the Radius Bridge component will be sufficient, as the majority of VPNs support RADIUS AAA authentication servers.

Alternatively, if you prefer, you can build your own server with the necessary configurations to provide similar functionality. However, using the preconfigured OpenOTP Cloud Bridge VM ensures a streamlined and efficient setup process.

By deploying the OpenOTP Cloud Bridge VM or setting up a similar server, you can establish a secure and reliable connection between your infrastructure and the openotp.com infrastructure, enabling seamless integration and authentication for your VPN.

This scenario assumes that you want to be as most secure as possible regarding communications between your infrastructure and openotp.com infrastructure. This involves deploying our [OpenOTP Cloud Bridge VM](#). Optionally, you can also build yourself a server that will provide exactly the same thing. This VM is a preconfigured VM which runs Radius Bridge and LDAP Bridge. For most of VPNs, Radius Bridge will be enough as 98% of VPNs support RADIUS AAA authentication servers.

## 4. VPN Setup without VM bridges

If you wish to set up your VPN without deploying the [OpenOTP Cloud Bridge VM](#) on-premise, you need to follow the steps outlined below:

- › Request RCDevs to enable the Radius Service for your tenant and provide them with your public IP(s) and your tenant ID. The communication with the Cloud Radius service is filtered by IP addresses, so your public IP(s) need to be declared in the Radius service in order to allow communications. If your public IP(s) are dynamic, you must deploy the [OpenOTP Cloud Bridge VM](#). This is necessary as RCDevs does not want to open the Radius APIs to the entire internet for security reasons. The tenant ID can be found on your [WebADM Home page](#) > [License Details](#) > [Hosted Tenant](#) value.



LDAP Server 2 (RCDevs Directory)

RCDevs Directory (3)

- cn=admin
- dc=WebADM
- ou=Users (1)
  - cn=MyFirstUser

Create / Search  
Details / Check

Create / Search  
Details / Check

WebADM Enterprise Edition v2.3.0

Copyright © 2010-2023 RCDevs Security, All Rights Reserved

HomeAdminCreateSearchImportDatabasesApplicationsAboutLogout

Hello Admin (cn=admin)

Connected as Super Administrator to webadm2.hosting

License Details

License Status: Valid (Virtual)  
Hosted Tenant: TRIALFDN6JL  
User Quota: 2 active users  
Host Quota: 0 active host  
Support Services: Yes (Generate a support ticket file)

Activated Services

Internal PKI Services: (no new certificate today)  
Electronic Signature: (no signature & no seal today)  
Mobile User Badging: (no user badging today)  
Mobile Push Service: (no push sent today)  
SMS Gateway Service: (no SMS sent today)  
SMTP Email Relay: (5 email sent today)

Application Status

MFA Authentication Server: Ok (v2.2.4)  
Shared Session Server: Ok (v1.1.0)  
SMS Hub Server: Ok (v1.3.0)  
SSH Public Key Server: Ok (v2.1.1)  
OpenID & SAML Provider: Not Configured  
Secure Password Reset: Ok (v1.3.0)  
User Self-Service Desk: Ok (v1.4.0)  
User Self-Registration: Ok (v1.4.0)

Configurations Objects

User Domains: 1 (Details)  
Option Sets: 1 (Details)  
Client Policies: 1 (Details)  
Admin Roles: 0 (Details)

Show More

Once you have provided RCDevs with the requested information, they will provide you with the Radius Secret. This Radius Secret needs to be configured in your Radius server configuration on your VPN server. To ensure a secure communication between your VPN server and the OpenOTP cloud infrastructure, it's important to configure the Radius Secret correctly. The Radius Secret acts as a shared secret key between your VPN server and the OpenOTP cloud infrastructure, allowing them to authenticate and communicate securely.

- › Configure a Radius Server as the Authentication server in your VPN configuration, targeting your tenant's or your private cloud's URL on **openotp.com**.

For example, if your OpenOTP tenant URL is "<https://fdn6jl.eu1.openotp.com>", you should configure "fdn6jl.eu1.openotp.com" as the server hostname with the port **1812** using **UDP** on your VPN server.

If your VPN server does not support hostnames, you can use the following IP addresses for the OpenOTP cloud infrastructure:

Name: openotp.com  
Address: 146.59.203.4  
Address: 146.59.206.40

Name: eu1.openotp.com  
Address: 87.98.155.89  
Address: 178.32.96.77

Please note that the IP addresses mentioned above are placeholders, and you should obtain the actual IP addresses from RCDevs for your specific OpenOTP cloud infrastructure region. Ensure that you configure the server hostname or IP address and the port correctly in your VPN server configuration to establish a successful connection with the OpenOTP cloud infrastructure.

- › **The Radius timeout** should be configured to at least 30 seconds.
- › **The Radius retry** should be configured to 0 or 1.
- › **The Radius accounting** is not supported by OpenOTP, so it is useless to configure it on your VPN server.
- › **The Radius secret** or **Shared secret** is provided by RCDevs.
- › The **password protocol** which should be used is PAP.

It's important to note that in the scenario described here, you don't need to set up the Radius Bridge component, as it is hosted by RCDevs. The documentation will provide guidance on the necessary configurations and settings for integrating your VPN with OpenOTP cloud without the need for setting up the Radius Bridge. By following the instructions provided in the VPN provider documentation and the RCDevs documentation, you will be able to configure your VPN to work seamlessly with OpenOTP cloud for multi-factor authentication.

## 5. References and Advanced configuration

For more information regarding the configuration of your VPN, please refer to the documentation provided by your VPN provider. Additionally, you can consult the [RCDevs documentations](#).

Refer to the following link for advanced configuration of [Radius Bridge](#),

*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*