



# OPENOTP CLOUD BRIDGES

## VM

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).

## 1. Overview

This documentation provides a step-by-step guide on how to configure the OpenOTP Cloud Bridge Virtual Appliance. The appliance is a pre-installed Rocky Linux 9.1 with the necessary RCDevs software packages. It includes the following components:

- › [Radius Bridge](#) (installed in /opt/radiusd/).
- › [LDAP Bridge](#) (installed in /opt/ldapproxy).

RCDevs strongly recommends using the Virtual Appliance or deploying LDAP and Radius Bridges on a dedicated server within your infrastructure. This ensures the secure communication of these protocols without transporting them over the internet.

To deploy and configure that virtual appliance, you must have your [OpenOTP Cloud Tenant](#) created or your dedicated hosted infrastructure deployed. For that documentation my tenant URL is <https://fdn6jl.eu1.openotp.com>

## 2. Setups

### 2.1 General information

To download the Appliance, please visit the [RCDevs Website](#) and download the ZIP archive. The Appliance is available in both VMX and OVF formats, compatible with VMware ESX, ESXi, Workstation, and Oracle VirtualBox. After downloading, unzip the archive and follow these steps:

1. In your VMware environment, select “Import Appliance”.
2. Choose the VMX or OVF file from the extracted files.

#### Important

Avoid copying and running the appliance directly without importing it. Running the appliance directly may result in a read-only filesystem error during the boot process.

If necessary, you can adjust the CPU and memory settings of the Appliance. By default, it is configured with 1 virtual CPU and 2GB of memory.

If you decide to use the VMX import format (instead of the preferred OVF format), you’ll need to set up the VM system manually and use the VMX file as the SCSI storage file. The following configuration information may be helpful:

- › Keep the boot console open during the boot process to monitor any startup errors.
- › The Appliance is set to obtain its IP address via DHCP.

During the first boot, this script runs only once and does not require a login password. You can access the console or use SSH to perform the initial setup. If needed, you can restart the appliance setup script using the **vm\_init** command.

The OpenOTP Cloud bridge VM setup script ask and perform the following:

1. Set the root password to access the virtual machine later.
2. Configure your time zone.
3. Configure the network interface.
4. Setup Radius Bridge (radiusd) component with your OpenOTP cloud infrastructure. (optional)
5. Setup LDAP Bridge (ldap) component with your OpenOTP cloud infrastructure. (optional)

Point 4 and 5 are optional but if you are configuring that appliance it is to configure at least one of these services.

During this setup, you will need to access your WebADM Admin Portal in order to approve the certificate requests of Radius and LDAP Bridge products.

First step when you start the Virtual Appliance is to reset the root password and test that you can access the VM with the new password configured.

```
-----  
Welcome to RCDevs VMWare Appliance package webadm is not installed!  
-----
```

```
Please enter a new root password for console and ssh login: xxxxxxxx  
Please enter it again: xxxxxxxx  
Updating password  
Please try a ssh login in an other session, does it work? (y/[n]): y
```

Try to log in through SSH with root account and your freshly configured password.

```
Please identify a location so that time zone rules can be set correctly.  
Please select a continent or ocean.  
1) Africa  
2) Americas  
3) Antarctica  
4) Arctic Ocean  
5) Asia  
6) Atlantic Ocean  
7) Australia  
8) Europe  
9) Indian Ocean  
10) Pacific Ocean  
11) none - I want to specify the time zone using the Posix TZ format.
```

```
#? 8
```

We choose the time zone, for example, Luxembourg in Europe.

Please select a country.

- |                         |                   |                   |
|-------------------------|-------------------|-------------------|
| 1) Albania              | 18) Guernsey      | 35) Poland        |
| 2) Andorra              | 19) Hungary       | 36) Portugal      |
| 3) Austria              | 20) Ireland       | 37) Romania       |
| 4) Belarus              | 21) Isle of Man   | 38) Russia        |
| 5) Belgium              | 22) Italy         | 39) San Marino    |
| 6) Bosnia & Herzegovina | 23) Jersey        | 40) Serbia        |
| 7) Britain (UK)         | 24) Latvia        | 41) Slovakia      |
| 8) Bulgaria             | 25) Liechtenstein | 42) Slovenia      |
| 9) Croatia              | 26) Lithuania     | 43) Spain         |
| 10) Czech Republic      | 27) Luxembourg    | 44) Sweden        |
| 11) Denmark             | 28) Macedonia     | 45) Switzerland   |
| 12) Estonia             | 29) Malta         | 46) Turkey        |
| 13) Finland             | 30) Moldova       | 47) Ukraine       |
| 14) France              | 31) Monaco        | 48) Vatican City  |
| 15) Germany             | 32) Montenegro    | 49) Åland Islands |
| 16) Gibraltar           | 33) Netherlands   |                   |
| 17) Greece              | 34) Norway        |                   |
- #? 27

The following information has been given:

Luxembourg

Therefore TZ='Europe/Luxembourg' will be used.

Local time is now: Tue May 16 16:06:47 CEST 2023.

Universal Time is now: Tue May 16 14:06:47 UTC 2023.

All following options are set with the default value in square brackets. You can keep it by pressing enter.

This VM is running with dynamic IP assignment (DHCP)

The current IP address is 192.168.1.69

Do you want to configure a static IP ([y]/n)?

y

Please type the fixed IP address [192.168.1.69]:

192.168.1.69

Please type the network mask [255.255.255.0]:

255.255.255.0

Please type the gateway address [192.168.1.1]:

192.168.1.1

Please type your primary DNS server IP [8.8.8.8]:

8.8.8.8

Please type your secondary DNS server IP []:

Fixed IP address: 192.168.1.69

Network address: 192.168.1.0

Network mask: 255.255.255.0

Gateway IP address: 192.168.1.1

Primary DNS server: 8.8.8.8

Do you confirm ([y]/n):

y

Restarting network...

Please enter the hostname [bridge.rcdevs.local]:

bridge.support.rcdevs.com

The global VM configuration is done and next step is the Radius Bridge product configuration.

## 2.2 Radius Bridge

### 2.2.1 Configuration script

The setup continues as follows, where I have to provide the FQDN of my server for SSL certificate generation and my WebADM/OpenOTP tenant URL:

Do you want to configure radiusd? ([y]/n)? y

Checking system architecture...Ok

Enter the server fully qualified host name (FQDN): bridge.support.rcdevs.com

If WebADM is running on this server then press Enter.

Else enter one of your running WebADM server IP or hostname.

Note: You can use host:port if WebADM uses a custom HTTPS port.

Enter WebADM server IP or hostname: fdn6jl.eu1.openotp.com

At this step, you need to go to the WebADM interface and accept the SSL certificate request.

```
Found one server URL: https://fdn6jl.eu1.openotp.com:8443/openotp/  
Retrieving WebADM CA certificate... Ok  
Retrieving WebADM CA trusted bundle... Ok  
The setup needs now to request a signed SSL server certificate.  
This request should show up as pending in your WebADM interface and an administrator must accept it!  
Waiting 5 minutes for approbation...
```

Once accepted, you will have the following output:

```
Waiting 5 minutes for approbation... Ok  
Updating configuration file... Ok  
Setting file permissions... Ok  
Do you want OpenOTP RADIUS Bridge to be automatically started at boot (y/n)? y  
Adding systemd service... Ok  
Do you want to register OpenOTP RADIUS Bridge logrotate script (y/n)? y  
Adding logrotate script... Ok  
OpenOTP RADIUS Bridge has successfully been setup.
```

The Radius Bridge setup is finished and the setup script continue with the LDAP Bridge configuration which is optional. For full configuration of Radius Bridge component, please refer to the [Radius Bridge](#) documentation.

### 2.2.2 RADIUS Clients declaration

Please refer to the following documentation section to declare a [Radius client](#) in your radius bridge configuration. By default, all Radius clients are allowed with the shared secret 'testing123'.

### 2.2.3 Advanced configuration

For full configuration and understanding of LDAP Bridge component, please refer to the [RADIUS Bridge documentation](#).

## 2.3 LDAP Bridge

### 2.3.1 Overview

LDAP Bridge allows authentication to be delegated to an OpenOTP server transparently, without changing the LDAP back-end. From the client applications perspective, the main change is that it will use the LDAP Bridge as an LDAP server, instead of the backend-end LDAP server. LDAP Bridge works by relaying LDAP messages to a back-end LDAP server. It intercepts user bind (LDAP authentication) operations and makes an OpenOTP call to authenticate the request with OpenOTP. It then sets the result of the bind request to the authentication result of the OpenOTP call.



## ⚠ Important

LDAP Bridge works with Users' Distinguished Name (DN) attribute to authenticate users' credentials with the LDAP backend and with OpenOTP. That is why, the DN structure must be the same on your LDAP architecture and on OpenOTP Cloud.

E.g: If the DN of my user is `cn=my_user,ou=users,dc=domain,dc=com` in my Active Directory, then in OpenOTP cloud, the DN of my account must be `cn=my_user,ou=users` where `users` is an Organizational Unit containing the object `my_user`. Do not consider the LDAP treebase (`dc=domain,dc=com`) on OpenOTP Cloud as you can not configure it by your own.

In that example, the IP of my domain controller is 192.168.4.2.

### 2.3.2 Configuration script

Now, we are going to configure LDProxy:

```
Do you want to configure ldproxy ([y]/n):y
Checking the system architecture...Ok
Enter the LDAP server IP or hostname [localhost]: 192.168.4.2
Enter the LDAP server port [389]: 389
Enter the LDAP protocol (ldap/ldaps) [ldap]: ldap
Enter a bindable LDAP account from the back-end with no specific permission:
cn=read_only_account,cn=users,dc=support,dc=rcdevs,dc=com
Enter the LDAP account password: xxxxxxxx
Enter the WebADM server IP or hostname [localhost]: fdn6jl.eu1.openotp.com
Found one server URL: https://fdn6jl.eu1.openotp.com:8443/openotp/
Retrieving the WebADM CA certificate... Ok
The setup needs now to request a signed SSL server certificate.
This request should show up as pending in your WebADM interface and an administrator must accept it!
Waiting 5 minutes for approbation...
```

Approve the SSL certificate request from your WebADM Admin GUI, then you are prompted for the following:

```
Waiting 5 minutes for approbation... Ok
Updating the OpenOTP configuration file... Ok
Do you want OpenOTP LDAP Bridge to be automatically started at boot (y/n)[y]? y
Adding the systemd service... Ok
Do you want to register OpenOTP LDAP Bridge logrotate script (y/n)[y]? y

Adding the logrotate script... Ok
OpenOTP LDAP Bridge has successfully been set up.
Starting the OpenOTP LDAP Bridge... Ok

You can connect your server via SSH with 'ssh root@192.168.1.69'.

You can login RCDevs WebADM Admin Portal at 'https://fdn6jl.eu1.openotp.com'.

Press any key to finish!
```

LDProxy is now configured. You can configure your client application(s) using LDAP protocol targeting LDProxy service (port 10389 or 10636) instead of your LDAP backend.

### 2.3.2 Advanced configuration

For full configuration and understanding of LDAP Bridge component, please refer to the [LDProxy documentation](#).

*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*