



READ-ONLY ACTIVE DIRECTORY WITH WEBADM

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.

Copyright (c) 2010-2017 RCDevs SA. All rights reserved.

<http://www.rcdevs.com>

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

Limited Warranty

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

Read-Only Active Directory with WebADM

[Active Directory](#)

How To Configure WebADM with a Read-Only Active Directory

Important Note

An enterprise license is mandatory for that setup since WebADM 1.6.6

In some circumstances, we can not write in the LDAP backend. In that case, we need to store some configurations in a local LDAP database and users extra information in a SQL database.

In this example, we will start with a WebADM server running with a local MariaDB and RCDevs Directory Server. It could be the [VMWare Appliance](#) or a new installation [WebADM Installation Guide](#). We will configure it to use a read-only Active Directory server.

1. WebADM Configuration

We edit `/opt/webadm/conf/webadm.conf` and change `webadm_account_oclasses` and `webadm_group_oclasses` parameters. It should contain the following class:

```
webadm_account_oclasses "person"  
webadm_group_oclasses "group", "groupOfNames", "groupOfUniqueNames", "groupOfURLs",  
"posixGroup"
```

We change also the data store to SQL:

```
data_store SQL
```

We restart WebADM:

```
/opt/webadm/bin/webadm restart
```

2. Container Creation

In WebADM, we create a container for the mount point. We click on `Create`, we select `Domain` and we click on `Proceed`:

—

We enter a name for the domain, for example, `test`, and we click on `Proceed`:

☐

We click on **Create Object** :

☐ ☐

3. Mount Point Creation

To create a Mount Point, click on **Admin** tab and click on **LDAP Mount Points** box:

☐

We click on **Add MountPoint** :

☐

We add a name and click on **Proceed** :

☐

We click on **Create Object** :

☐

We click on **Select** and choose the container previously created for *Mount DN*. Now, we add the IP address of the Active Directory server in *Host Name(s)* field, the port number, the tree base of the AD and AD user and password to connect to the LDAP.

Note

The AD user should have read access on the Active Directory.

We click on **Apply** :

☐ ☐

4. Local Domain Creation

Now, we create a local domain for the mount point. A local domain works only with one LDAP backend, so the default local domain works only with OpenLDAP.

We click on **Admin** tab and on **Local Domains** box:

☐

Click on **Add Domain** :

We enter the name of the domain and click on **Proceed**.

Click on **Create Object**:

We select the mount point as *User Search Base*. We can add domain name aliases, like *test.local* if needed, and we click on **Apply**:

It's done:

Now, we can try an authentication by following this documentation [Authentication](#). We need to select the right local domain during the authentication. Otherwise, OpenOTP won't be able to find the user.

This manual was prepared with great care. However, RCDevs 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 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 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 S.A. The latter especially applies for data processing systems. RCDevs 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 S.A. © 2021 RCDevs SA, All Rights Reserved