



AUTHENTICATION

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.

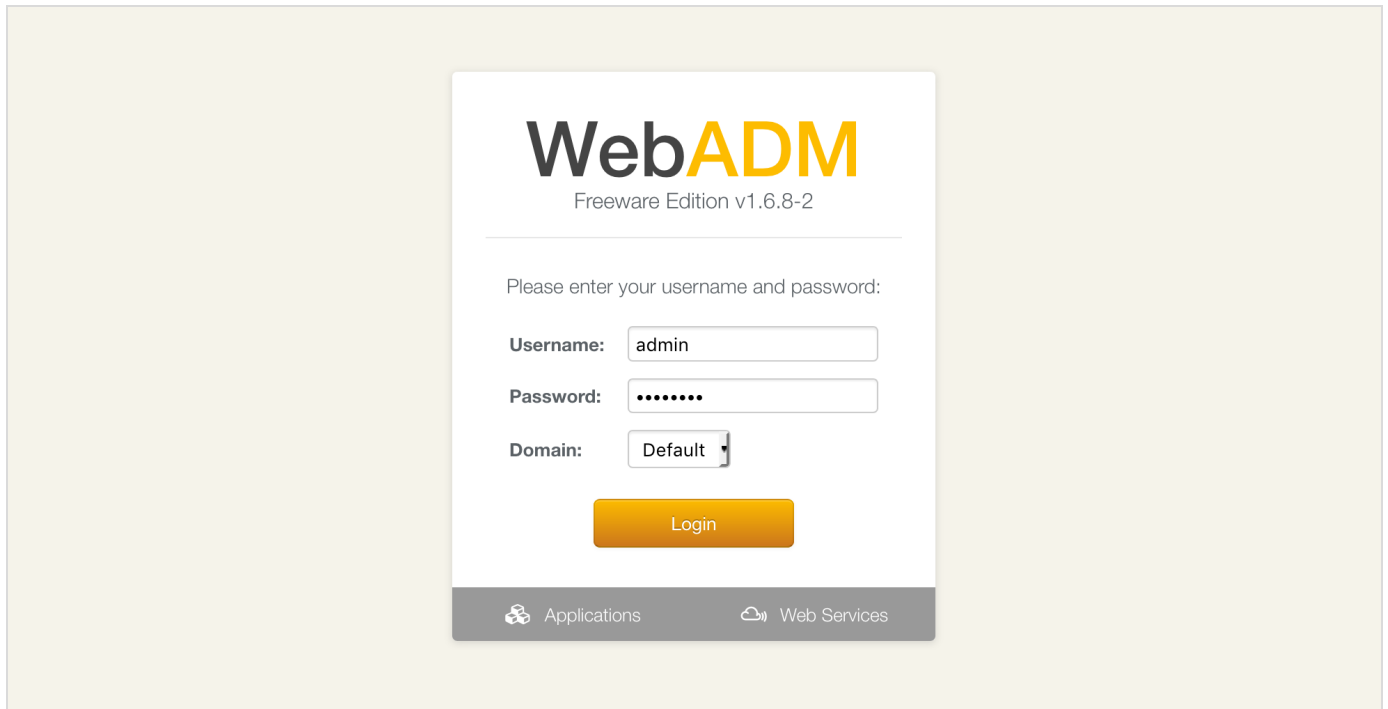
Authentication

[LDAP](#)

Test Double Authentication with a User

1. User Activation

Once WebADM is installed and configured, we can connect to it with a web browser.



We select the user to activate in the LDAP tree on the left, for example, *Admin*, or we create a new user by clicking on [Create](#) .
Once the user is selected, we click on [Activate Now!](#) :

LDAP Server (OpenLDAP)

OpenLDAP (2)

- dc=WebADM
- o=Root (2)
 - cn=admin
 - cn=ppolicy
- Create / Search Details / Check
- Create / Search Details / Check

WebADM Freeware Edition v1.6.8-2

Copyright © 2010-2018 RCDevs SA, All Rights Reserved

Home | Admin | Create | Search | Import | Databases | Statistics | Applications | About | Logout

Object **cn=admin,o=Root (Super Administrator)**

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

User activated: **No Activate Now!**

Object Name: Rename

Add Attribute (10): Add

Add Extension (2): Add

Last Name: [add values]

Group Membership: [add values] [delete attribute] Goto

Apply Changes / Delete Selected

If present, we fill mandatory attributes and **Proceed** :

LDAP Server (OpenLDAP)

OpenLDAP (2)

- dc=WebADM
- o=Root (2)
 - cn=admin
 - cn=ppolicy
- Create / Search Details / Check
- Create / Search Details / Check

WebADM Freeware Edition v1.6.8-2

Copyright © 2010-2018 RCDevs SA, All Rights Reserved

Home | Admin | Create | Search | Import | Databases | Statistics | Applications | About | Logout

Add Extension **WebADM Account** to **cn=admin,o=Root**

In order to add the objectclass **WebADM Account** you must specify at least 1 new mandatory attribute(s).

Mandatory attributes

Login Name

Optional attributes

WebADM Settings You can edit this attribute once object is created.

WebADM User Data This attribute cannot be created manually.

Preferred Language

Mobile Phone Number

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

Email Address

Description / Note

Proceed Cancel

We click on **Extend Object** :

The screenshot shows the WebADM Freeware Edition v1.6.8-2 interface. On the left is a navigation tree for the LDAP Server (OpenLDAP) with nodes for 'OpenLDAP (2)', 'dc=WebADM', 'o=Root (2)', 'cn=admin', and 'cn=ppolicy'. The main area displays the 'Extend Object' dialog for the object 'cn=admin,o=Root'. The dialog title is 'Add Extension WebADM Account to cn=admin,o=Root'. It contains the text: 'The object will be extended with the objectclass **WebADM Account**. The following 1 new attribute(s) will be added during extension.' Below this is a table with two columns: 'Attribute' and 'Value'. The table contains one row: 'Login Name' with the value 'admin'. At the bottom of the dialog are two buttons: 'Extend Object' and 'Cancel'.

Now, the user is activated. We can register a new token. We click on **MFA Authentication Server** :

The screenshot shows the WebADM Freeware Edition v1.6.8-2 interface displaying the details for the object 'cn=admin,o=Root (Super Administrator)'. The left navigation tree is the same as in the previous screenshot. The main area is titled 'Object cn=admin,o=Root (Super Administrator)'. It is divided into three sections: 'LDAP Actions', 'Object Details', and 'Application Actions'. 'LDAP Actions' includes options like 'Delete this object', 'Copy this object', 'Move this object', 'Export to LDIF', 'Change password', 'Create certificate', 'Unlock WebApp access', and 'Advanced edit mode'. 'Object Details' lists: 'Object class(es): person, webadmAccount', 'Account is unique: Yes (in o=root)', 'WebADM settings: None [CONFIGURE]', 'WebADM data: None [EDIT]', 'User activated: Yes Deactivate', and 'Logs and inventory: WebApp, WebSrv, Inventory'. 'Application Actions' lists various servers like 'Secure Password Reset (1 actions)', 'User Self-Registration (1 actions)', 'MFA Authentication Server (13 actions)', 'SMS Hub Server (1 actions)', 'SSH Public Key Server (3 actions)', and 'QR Login & Signing Server (8 actions)'. Below these sections are form fields for 'Object Name' (admin), 'Add Attribute (11)' (Description / Note), 'Add Extension (1)' (UNIX Account), 'Last Name' (admin), 'Login Name' (admin), and 'Group Membership' (cn=super_admins,dc=WebADM). At the bottom is a button labeled 'Apply Changes / Delete Selected'.

2. OTP Soft Token Enrollment

We click on **Register / Unregister OTP Tokens** :

LDAP Server (OpenLDAP)

WebADM Freeware Edition v1.6.8-2
Copyright © 2010-2018 RCDevs SA, All Rights Reserved

API

Home | Admin | Create | Search | Import | Databases | Statistics | Applications | About | Logout

OpenOTP User Actions for **cn=admin,o=Root** (13)

Find below the user actions supported by **MFA Authentication Server** (OpenOTP).

Register / Unregister OTP Tokens

You must register a hardware or software Token before a user can start using it.
You can use this action to update inventory data and enable/disable Tokens too.

For the test, we select **I use a QRCode-based Authenticator**. We need a software token app on our smartphone. We can find here, a list of [compatible software tokens](#). Once installed we scan the QR Code with the app and click on **Register**:

LDAP Server (OpenLDAP)

WebADM Freeware Edition v1.6.8-2
Copyright © 2010-2018 RCDevs SA, All Rights Reserved

API

Home | Admin | Create | Search | Import | Databases | Statistics | Applications | About | Logout

Register / Unregister OTP Tokens for **cn=admin,o=Root**

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.

Register 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:

We click on **OK** :

The screenshot shows the WebADM Freeware Edition v1.6.8-2 interface. The left sidebar displays the LDAP Server (OpenLDAP) tree with nodes for OpenLDAP (2), dc=WebADM, o=Root (2), cn=admin, and cn=ppolicy. The main content area shows the 'Register / Unregister OTP Tokens for cn=admin,o=Root' page. A modal dialog box is centered on the screen with the text 'TOTP Token has been registered' and an 'Ok' button.

We check that the new token is registered:

The screenshot shows the WebADM Freeware Edition v1.6.8-2 interface. The left sidebar is the same as in the previous screenshot. The main content area shows the 'Register / Unregister OTP Tokens for cn=admin,o=Root' page. The page displays the following information:

- 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.
- 1/3 Token is already registered for user:
- Buttons: Primary Token, **TOTP**, Remove, Disable
- Instructions to register an inventoried Hardware Token:
 1. Type the serial number displayed on the back side of the Token.
 2. Click the 'Register' button below.
- Register Token: Primary Token (dropdown menu)
- WARNING: Primary Token is already registered.**
You must remove Token first in order to re-register!
- Ok button

Now, we can try an authentication, we click on **MFA Authentication Server** :

3. Authentication Test

LDAP Server (OpenLDAP)

WebADM Freeware Edition v1.6.8-2
Copyright © 2010-2018 RCDevs SA, All Rights Reserved

Home | Admin | Create | Search | Import | Databases | Statistics | Applications | About | Logout

Object **cn=admin,o=Root (Super Administrator)**

LDAP Actions	Object Details	Application Actions
<ul style="list-style-type: none"> Delete this object Copy this object Move this object Export to LDIF Change password Create certificate Unlock WebApp access Advanced edit mode 	<p>Object class(es): person, webadmAccount</p> <p>Account is unique: Yes (in o=root)</p> <p>WebADM settings: None [CONFIGURE]</p> <p>WebADM data: 4 data [EDIT]</p> <p>User activated: Yes Deactivate </p> <p>Logs and inventory: WebApp, WebSrv, Inventory</p>	<ul style="list-style-type: none"> Secure Password Reset (1 actions) User Self-Registration (1 actions) MFA Authentication Server (13 actions) SMS Hub Server (1 actions) SSH Public Key Server (3 actions) QR Login & Signing Server (8 actions)

Object Name: Rename

Add Attribute (10): Add

Add Extension (1): Add

Last Name: [add values]

Login Name: [add values]

WebADM User Data: [delete attribute]

Group Membership: [add values] [delete attribute] Goto

Edit Application Data

OpenOTP.TokenKey: *[BINARY DATA - 20 Bytes]*

OpenOTP.TokenState: *0*

OpenOTP.TokenType: *TOTP*

Apply Changes / Delete Selected

We scroll down and click on **Test User Login**:

LDAP Server (OpenLDAP)

WebADM Freeware Edition v1.6.8-2
Copyright © 2010-2018 RCDevs SA, All Rights Reserved

Home | Admin | Create | Search | Import | Databases | Statistics | Applications | About | Logout

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 User Authentication**
You can use this action to test a user authentication with OpenOTP.
- Test User Confirmation**
You can use this action to test a transaction confirmation with OpenOTP.

Cancel

We insert the LDAP password and the OTP, and we click on **OK**:

The screenshot shows the WebADM Freeware Edition v1.6.8-2 interface. The left sidebar displays the LDAP Server configuration tree with nodes for OpenLDAP (2), dc=WebADM, o=Root (2), cn=admin, and cn=ppolicy. The main content area is titled 'Test User Authentication for cn=admin,o=Root'. It includes a server status section showing 'Accepting Requests' and various system metrics. Below this is a form with the following fields: Login Method (Normal selected), Username (admin), Domain (Default), LDAP Password (masked), OTP Password (masked), Simulated Client (Default), Simulated Source, Simulated Options, Request Settings, and Browser Context (cfa3e345b7f16b1bb3c0936b54e2231b). 'Start' and 'Cancel' buttons are at the bottom.

We are authenticated!

The screenshot shows the same WebADM interface as above, but the result of the authentication is displayed. The 'Result' is 'Success' and the 'Message' is 'Authentication success'. 'Ok' and 'Cancel' buttons are at the bottom.

4. Logs

Now we can check the log, we click on **Databases** tab:

We click on **WebADM Server log Files**. It corresponds to the `/opt/webadm/log/webadm.log` file:

The screenshot displays the WebADM Freeware Edition v1.6.8-2 interface. The top navigation bar includes Home, Admin, Create, Search, Import, **Databases**, Statistics, Applications, About, and Logout. The left sidebar shows the LDAP Server (OpenLDAP) tree with nodes for OpenLDAP (2), dc=WebADM, o=Root (2), cn=admin, and cn=ppolicy. The main content area is divided into several sections: WebApp Logs (Web Application logs), WebSrv Logs (Web Service logs), Alert Logs (System Alerts from applications), SQL Data Tables (Localized Messages, Inventoried Devices, Recorded Sessions), and System Log Files (WebADM Server Log Files, PKI Server Log File, Watchd Server Log File, Session Server Log File, Background Job Log File). The WebADM Server Log Files section is highlighted, showing a list of log files with their descriptions.

Each authentication is identified by an ID. Here, it is **T3DSOZ9A**.

```
[2017-07-21 07:29:24] [127.0.0.1] [OpenOTP:T3DS0Z9A] New openotpNormalLogin SOAP
request
[2017-07-21 07:29:24] [127.0.0.1] [OpenOTP:T3DS0Z9A] > Username: admin
[2017-07-21 07:29:24] [127.0.0.1] [OpenOTP:T3DS0Z9A] > Domain: Default
[2017-07-21 07:29:24] [127.0.0.1] [OpenOTP:T3DS0Z9A] > LDAP Password: xxxxxxxx
[2017-07-21 07:29:24] [127.0.0.1] [OpenOTP:T3DS0Z9A] > OTP Password: xxxxxx
[2017-07-21 07:29:24] [127.0.0.1] [OpenOTP:T3DS0Z9A] > Client ID: OpenOTP
[2017-07-21 07:29:24] [127.0.0.1] [OpenOTP:T3DS0Z9A] > Source IP: 192.168.3.155
[2017-07-21 07:29:24] [127.0.0.1] [OpenOTP:T3DS0Z9A] > Context ID:
d10243968f7e608fe4743d8a43747123
[2017-07-21 07:29:24] [127.0.0.1] [OpenOTP:T3DS0Z9A] Registered openotpNormalLogin
request
[2017-07-21 07:29:24] [127.0.0.1] [OpenOTP:T3DS0Z9A] Resolved LDAP user:
cn=admin,o=Root
[2017-07-21 07:29:24] [127.0.0.1] [OpenOTP:T3DS0Z9A] Started transaction lock for user
[2017-07-21 07:29:24] [127.0.0.1] [OpenOTP:T3DS0Z9A] Found 37 user settings:
LoginMode=LDAPOTP,OTPTType=TOKEN,OTPLength=6,ChallengeMode=Yes,ChallengeTimeout=90,Enable1
1:HOTP-SHA1-6:QN06-
T1M,SMSType=Normal,SMSMode=Ondemand,MailMode=Ondemand,LastOTPTime=300,ListChallengeMode=5
[2017-07-21 07:29:24] [127.0.0.1] [OpenOTP:T3DS0Z9A] Found 3 user data:
TokenType,TokenKey,TokenState
[2017-07-21 07:29:24] [127.0.0.1] [OpenOTP:T3DS0Z9A] Found 1 registered OTP token
(TOTP)
[2017-07-21 07:29:24] [127.0.0.1] [OpenOTP:T3DS0Z9A] Requested login factors: LDAP &
OTP
[2017-07-21 07:29:24] [127.0.0.1] [OpenOTP:T3DS0Z9A] LDAP password Ok
[2017-07-21 07:29:24] [127.0.0.1] [OpenOTP:T3DS0Z9A] TOTP password Ok (token #1)
[2017-07-21 07:29:24] [127.0.0.1] [OpenOTP:T3DS0Z9A] Updated user data
[2017-07-21 07:29:24] [127.0.0.1] [OpenOTP:T3DS0Z9A] Sent success response
```

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. © 2019 RCDevs SA, All Rights Reserved