



# 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 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).

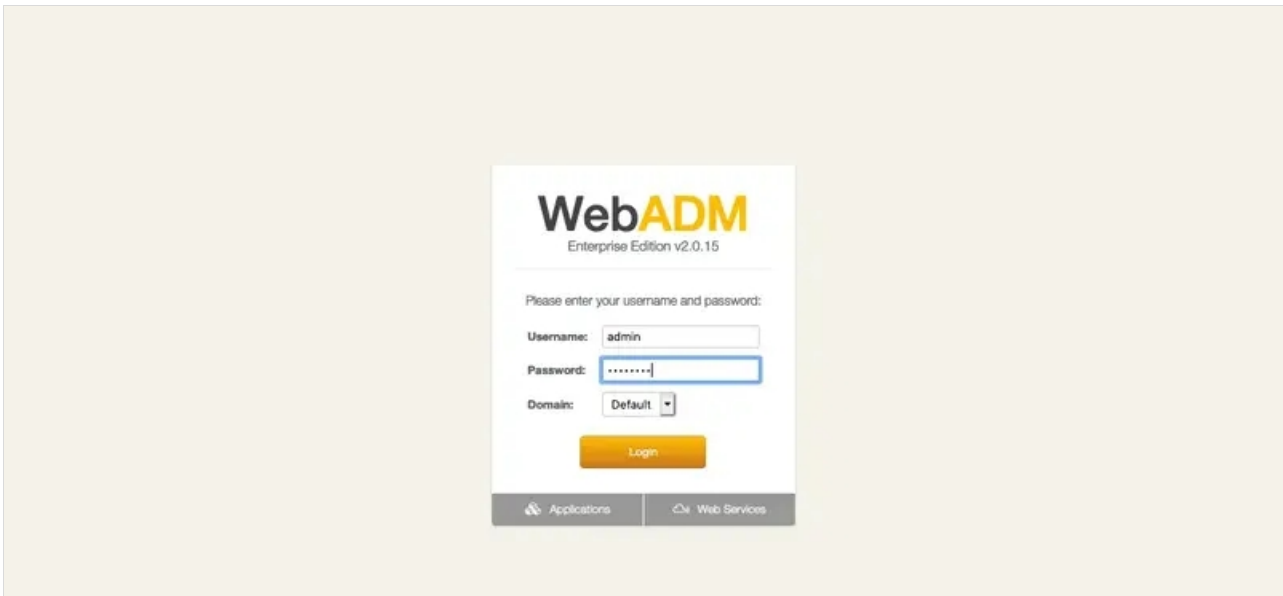
# Authentication

[Authentication](#) [Enrollment](#)

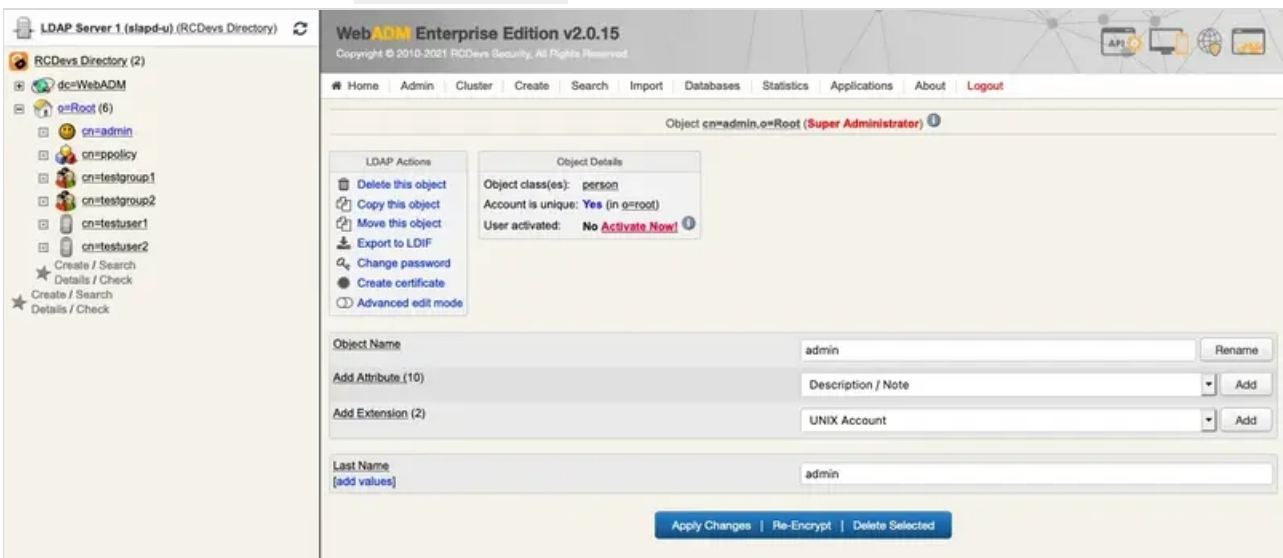
## Test Double Authentication with a User

### 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!](#):



If present, we fill mandatory attributes and [Proceed](#):

**WebADM Enterprise Edition v2.0.15**  
 Copyright © 2010-2021 RCDevs Security, All Rights Reserved

Home | Admin | Cluster | 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.

**WebADM Voice Model** You cannot set this attribute manually!

**Preferred Language**

**Mobile Phone Number**

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

**Email Address**

**Description / Note**

We click on **Extend Object** :

**WebADM Enterprise Edition v2.0.15**  
 Copyright © 2010-2021 RCDevs Security, All Rights Reserved

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

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

The object will be extended with the objectclass **WebADM Account**.

The following 1 new attribute(s) will be added during extension.

Attribute	Value
Login Name	admin

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

WebADM Enterprise Edition v2.0.15  
Copyright © 2010-2021 RCDevs Security, All Rights Reserved

Home Admin Cluster 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
- Unlock WebApp access
- Advanced edit mode

**Object Details**

Object class(es): person, webadmAccount  
 Account is unique: Yes (in o=root)  
 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)
- MFA Authentication Server (14 actions)
- SSH Public Key Server (3 actions)
- Register / Unregister OTP Tokens
- Register / Unregister FIDO Devices
- Register / Unregister Voice Biometrics
- Resynchronize Tokens
- Manage OTP PIN Prefix
- Manage OCRA Token PIN Code
- Manage Emergency OTP
- Manage Printed OTP List
- Manage Application Passwords
- Unblock Account
- Import OATH-PSKC File
- Export OATH-PSKC File
- Test User Authentication
- Test User Confirmation

Object Name: admin [Rename]

Add Attribute (12): Description / No [Add]

Add Extension (1): UNIX Account [Add]

Last Name: admin [add values]

Login Name: admin [add values]

Apply Changes | Re-Encrypt | Delete Selected

## 2. OTP Soft Token Enrollment


We click on [Register / Unregister OTP Tokens](#):

WebADM Enterprise Edition v2.0.15  
Copyright © 2010-2021 RCDevs Security, All Rights Reserved

Home Admin Cluster Create Search Import Databases Statistics Applications About Logout

OpenOTP User Actions for cn=admin,o=Root (14)

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.

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](#):

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.

Detached registration let you send the QRCode to the user (ex. via email) for self-registration.  
The registration is done when the user scans the QRCode within the configured expiration time.  
A protection PIN code should always be used when sending the QRCode via email or 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:

Registered UserID: admin

Registered Domain: Default

Mobile Push Data: [\[Waiting for Mobile Response\]](#)

Detached Registration

Expiration Time: 30 Mins

QRCode Format: JPG

Send QRCode: [Do Not Send]

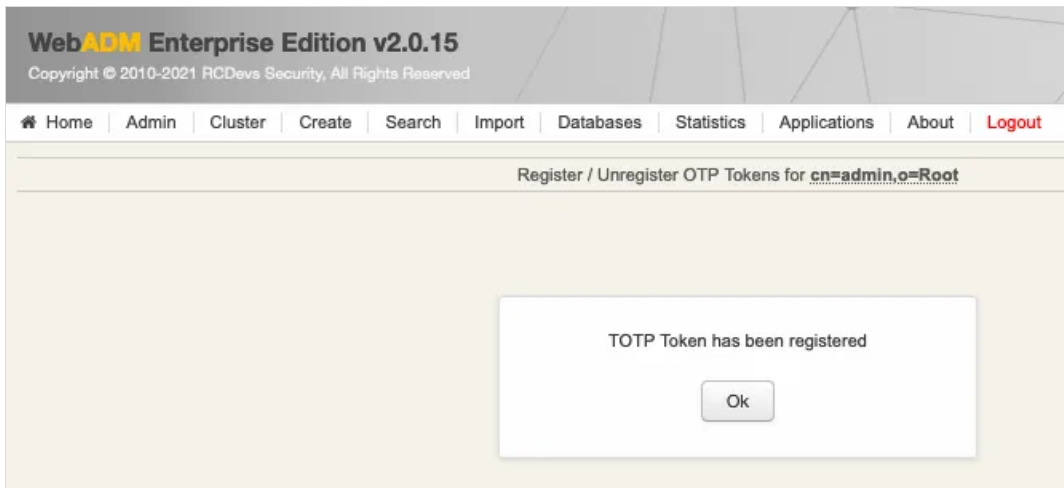
Enrolment PIN: 385376

Register

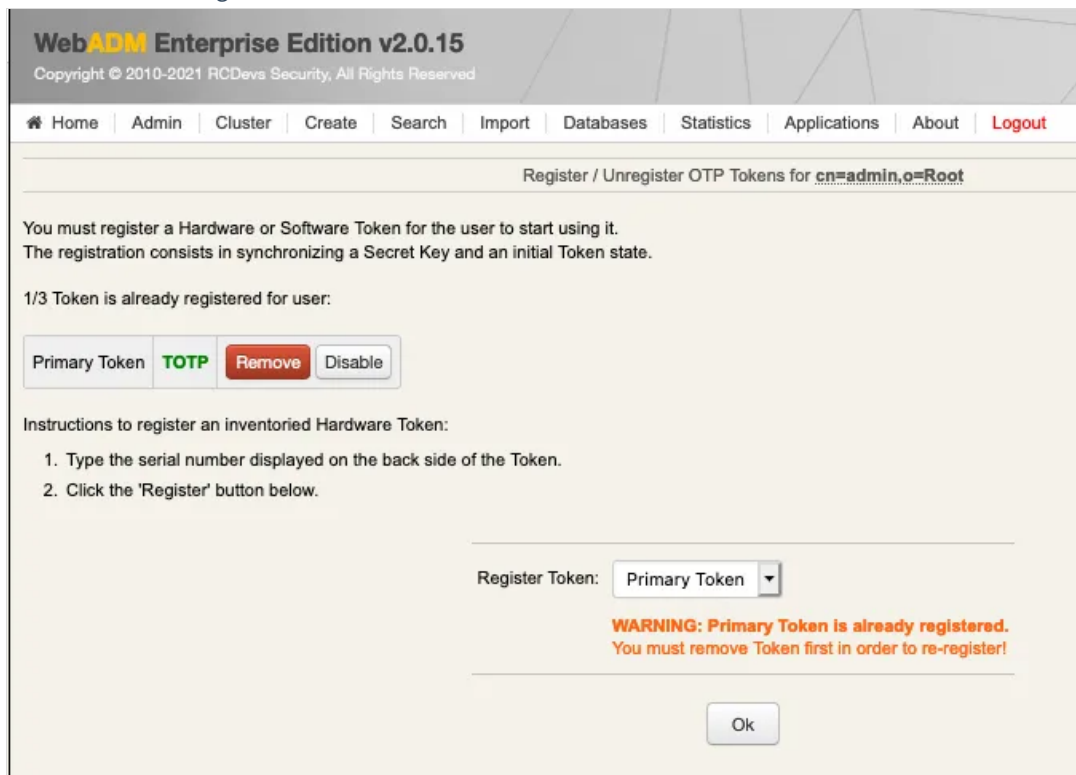
Detach

Cancel

We click on **OK**:



We check that the new token is registered:



Now, we can try an authentication, we click on [MFA Authentication Server](#):

### 3. Authentication Test

WebADM Enterprise Edition v2.0.15  
Copyright © 2010-2021 RCDevs Security, All Rights Reserved

Home Admin Cluster 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
- Unlock WebApp access
- Advanced edit mode

**Object Details**

Object class(es): person\_webadmAccount

Account is unique: Yes (in o=root)

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)
- MFA Authentication Server (14 actions)
- SSH Public Key Server (3 actions)
- Register / Unregister OTP Tokens
- Register / Unregister FIDO Devices
- Register / Unregister Voice Biometrics
- Resynchronize Tokens
- Manage OTP PIN Prefix
- Manage OCRA Token PIN Code
- Manage Emergency OTP
- Manage Printed OTP List
- Manage Application Passwords
- Unblock Account
- Import OATH-PSKC File
- Export OATH-PSKC File
- Test User Authentication
- Test User Confirmation

Object Name: admin [Rename]

Add Attribute (12): Description / No [Add]

Add Extension (1): UNIX Account [Add]

Last Name: admin [add values]

Login Name: admin [add values]

Apply Changes | Re-Encrypt | Delete Selected

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

WebADM Enterprise Edition v2.0.15  
Copyright © 2010-2021 RCDevs Security, All Rights Reserved

Home Admin Cluster Create Search Import Databases Statistics Applications About Logout

**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**:

**WebADM Enterprise Edition v2.0.15**  
Copyright © 2010-2021 RCDevs Security, All Rights Reserved

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

Test User Authentication for cn=admin,o=Root

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: MFA Authentication Server 1.5.7 (WebADM 2.0.15)  
System: Linux 5.8.0-44-generic x86\_64 (64 bit)  
Listener: 10.1.0.105:8080 (HTTP/1.1 SSL)  
Uptime: 178050s (2 days)  
Cluster Node: 1/3 (Session Server 1 (webadm-u))  
Local Memory: 0M (33M total)  
Shared Memory: 2M (256M 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)

We are authenticated!

**WebADM Enterprise Edition v2.0.15**  
Copyright © 2010-2021 RCDevs Security, All Rights Reserved

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

Test User Authentication for cn=admin,o=Root

Result: **Success**

Message: Authentication success

## 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 Enterprise Edition v2.0.15 web interface. At the top, the title bar reads "WebADM Enterprise Edition v2.0.15" with a copyright notice "Copyright © 2010-2021 RCDevs Security, All Rights Reserved". Below the title is a navigation menu with the following items: Home, Admin, Cluster, Create, Search, Import, Databases, Statistics, Applications, About, and Logout. The "Databases" tab is currently selected. The main content area is divided into several sections:

- WebApp Logs**: Web Application logs (user audit)
- WebSrv Logs**: Web Service logs (user audit)
- Alert Logs**: System Alerts from applications
- SQL Data Tables**: A section header for the following items:
  - Localized Messages**: Message translations for applications and services
  - Inventoried Devices**: OpenOTP hardware tokens and SpnKey PIV keys
  - Recorded Sessions & Transactions**: Transaction records and SpanKey sessions' audit
  - Client & Server Certificates**: Provides revocation for services' client certificates
- System Log Files**: A section header for the following items:
  - WebADM Server Log Files**: WebADM server activity events (highlighted in red)
  - PKI Server Log File**: WebADM PKI server events

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

```
[2017-07-21 07:29:24] [127.0.0.1] [OpenOTP:T3DSOZ9A] New openotpNormalLogin SOAP request
[2017-07-21 07:29:24] [127.0.0.1] [OpenOTP:T3DSOZ9A] > Username: admin
[2017-07-21 07:29:24] [127.0.0.1] [OpenOTP:T3DSOZ9A] > Domain: Default
[2017-07-21 07:29:24] [127.0.0.1] [OpenOTP:T3DSOZ9A] > LDAP Password: xxxxxxxx
[2017-07-21 07:29:24] [127.0.0.1] [OpenOTP:T3DSOZ9A] > OTP Password: xxxxxx
[2017-07-21 07:29:24] [127.0.0.1] [OpenOTP:T3DSOZ9A] > Client ID: OpenOTP
[2017-07-21 07:29:24] [127.0.0.1] [OpenOTP:T3DSOZ9A] > Source IP: 192.168.3.155
[2017-07-21 07:29:24] [127.0.0.1] [OpenOTP:T3DSOZ9A] > Context ID:
d10243968f7e608fe4743d8a43747123
[2017-07-21 07:29:24] [127.0.0.1] [OpenOTP:T3DSOZ9A] Registered openotpNormalLogin request
[2017-07-21 07:29:24] [127.0.0.1] [OpenOTP:T3DSOZ9A] Resolved LDAP user: cn=admin,o=Root
[2017-07-21 07:29:24] [127.0.0.1] [OpenOTP:T3DSOZ9A] Started transaction lock for user
[2017-07-21 07:29:24] [127.0.0.1] [OpenOTP:T3DSOZ9A] Found 37 user settings:
LoginMode=LDAPOTP,OTPTType=TOKEN,OTPLength=6,ChallengeMode=Yes,ChallengeTimeout=90,EnableLog
1:HOTP-SHA1-6:QN06-
T1M,SMSType=Normal,SMSMode=Ondemand,MailMode=Ondemand,LastOTPTime=300,ListChallengeMode=
[2017-07-21 07:29:24] [127.0.0.1] [OpenOTP:T3DSOZ9A] Found 3 user data:
TokenType,TokenKey,TokenState
[2017-07-21 07:29:24] [127.0.0.1] [OpenOTP:T3DSOZ9A] Found 1 registered OTP token (TOTP)
[2017-07-21 07:29:24] [127.0.0.1] [OpenOTP:T3DSOZ9A] Requested login factors: LDAP & OTP
[2017-07-21 07:29:24] [127.0.0.1] [OpenOTP:T3DSOZ9A] LDAP password Ok
[2017-07-21 07:29:24] [127.0.0.1] [OpenOTP:T3DSOZ9A] TOTP password Ok (token #1)
[2017-07-21 07:29:24] [127.0.0.1] [OpenOTP:T3DSOZ9A] Updated user data
[2017-07-21 07:29:24] [127.0.0.1] [OpenOTP:T3DSOZ9A] Sent success response
```

*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*