

# CLOUD MOBILE BADGING

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).

# Cloud Mobile Badging

[iOS](#) [Android](#) [Token](#) [RCDevs in the Cloud](#) [Cloud Services](#)

## 1. Overview

This document provides instructions on how to set up and utilize the mobile badging feature of OpenOTP in a cloud tenant. The configuration process is similar to the one explained in the [OpenOTP badging documentation](#).

To enable that feature in your WebADM infrastructure you must meet the following requirements :

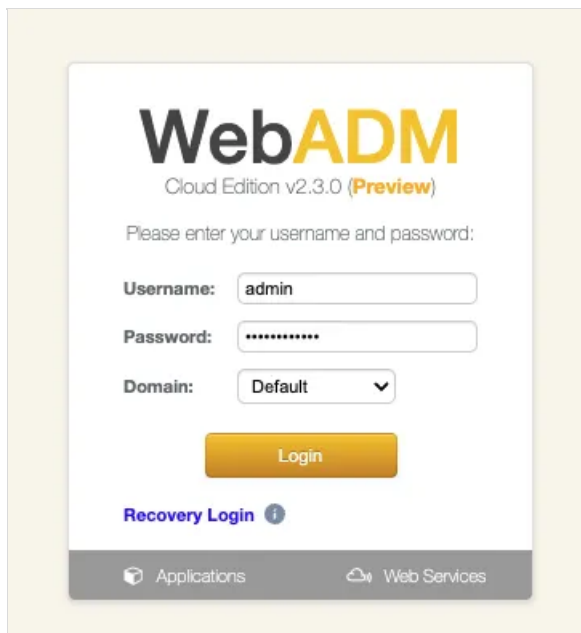
- > Having a tenant well configured with its license. Check this documentation to [configure your tenant](#).
- > [Install the mobile application](#) OpenOTP Token, with a minimal version of 1.5.16

## 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 asks the user to 'Please enter your username and password:'. It contains three input fields: 'Username' with the value 'admin', 'Password' with masked characters '.....', and 'Domain' with a dropdown menu showing 'Default'. Below these fields is a yellow 'Login' button. At the bottom of the form, there is a link for 'Recovery Login' with an information icon. The footer of the page shows 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...

☐ **User / Administrator**  
Administrator or LDAP user

☐ **Dynamic Group**  
LDAP group with dynamic contents

☐ **UNIX Group**  
UNIX POSIX Group

☐ **Organisation**  
LDAP organization container

☐ **Domain**  
LDAP domain container

☐ **WebADM Account**  
LDAP user with WebADM attributes

☐ **Static Group**  
LDAP group of users

☐ **UNIX Account**  
UNIX POSIX Account

☐ **Organizational Unit**  
LDAP organizational unit container

☐ **Country**  
LDAP country 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**  Rename

**Add Attribute (9)**  Add

**Add Extension (2)**  Add

**Last Name**  [add values]

**Email Address**  [add values] [delete attribute] ⓘ

**Login Name**  [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**

**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)

MFA Authentication 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

Email Address

test\_user@domain.com

Login Name

test\_user

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:

Registered UserID:  ▼

Registered Domain:  ▼

Mobile Push Data: [Waiting for Mobile Response]

### Detached Registration

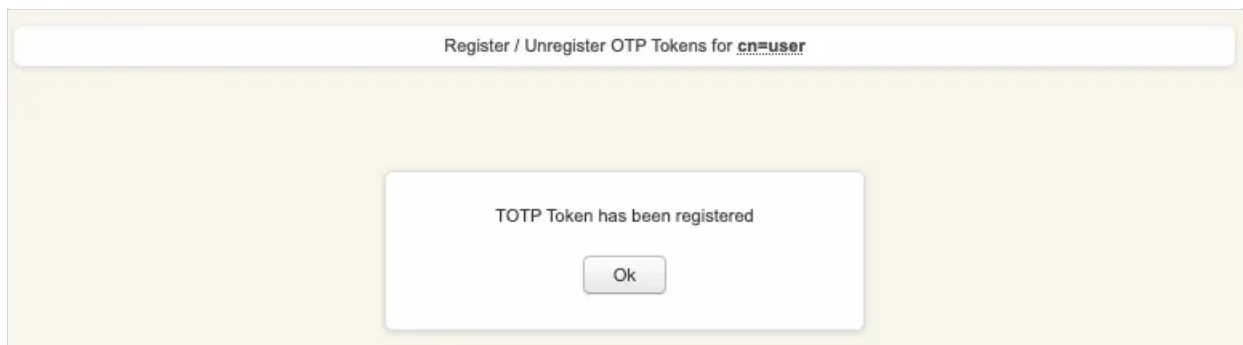
Expiration Time:  ▼

QRCode Format:  ▼

Send QRCode: ☒ Yes (Email) ☐ No

Enrolment PIN:

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:

**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: **7 data** [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](#) (16 actions)
- [SSH Public Key Server](#) (3 actions)

**Object Name** `user` Rename

**Add Attribute (11)** `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]

**WebADM User Data** [delete attribute]

**Edit Application Data**

- `OpenOTP.TokenID:` `IOS:7bd73cb16fa859e10f4d11b51b71a53b5868fa7484948a...`
- `OpenOTP.TokenKey:` `[BINARY APPLICATION DATA - 20 Bytes]`
- `OpenOTP.TokenModel:` `Apple iPhone13,3 (iPhone)`
- `OpenOTP.TokenSerial:` `906B8FFE-C4F5-42DD-9189-C573F1B42DBE`
- `OpenOTP.TokenState:` `0`
- `OpenOTP.TokenType:` `TOTP`

Apply Changes Re-Encrypt Delete Selected

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** >





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


[Home](#) | [Admin](#) | [Create](#) | [Search](#) | [Import](#) | [Databases](#) | [Applications](#) | [About](#) | [Logout](#)


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 RCDevS 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. OpenOTP Badging configuration

To configure the mobile badging feature, follow these steps:

1. Access the **WebADM Admin GUI** and navigate to the **Applications** tab.
2. Look for the MFA Authentication Server section and click on the **CONFIGURE** link associated with it.
3. On the subsequent page, locate the **Mobile Badging** section. Here, you can enable or modify the Mobile Badging feature and choose from three available modes: **BADGE**, **CHECK**, and **MIXED**.

In the **BADGE** mode, you can utilize the time-tracking feature for badging in and out, along with implementing badged-only access policies. The **CHECK** mode allows you to perform check-ins only, without the time-tracking or badged-only access policies. The **MIXED** mode combines the features of both the **BADGE** and **CHECK** modes, utilizing geolocation information.

Make the desired selections and configurations in the Mobile Badging section according to your requirements.

The screenshot shows the 'Mobile Badging' configuration window. It has a title bar 'Mobile Badging'. Inside, there are several sections: 1. 'Mobile Badging' with a checked checkbox and a dropdown menu set to 'BADGE'. Below this are three bullet points explaining the modes: '- BADGE: Badge-in and badge-out with time-tracking and badged-only access policies.', '- CHECK: Badge-in only (no badge-out and no time-tracking).', and '- MIXED: Check from office location and Badge-in elsewhere.' 2. 'Data Collection' with a checked checkbox and four sub-options: 'GPS' (checked), 'DN' (checked), 'IP' (checked), and 'Mobile' (checked), with a '[None]' option (unchecked). Below this is a text line: 'Data to be collected in the exportable XML data during mobile badge-in and badge-out.' 3. 'Timestamping' with a checked checkbox and a dropdown menu set to 'LocalCA'. Below this is a text line: 'Seal and timestamp the collected badging details with your local CA or eIDAS.' followed by a note: 'Note: eIDAS requires your license to include the Sign & Seal options for OpenOTP!'. 4. 'Allowed Locations' with a checked checkbox and a text input field containing 'LU,FR'. To the right of the input field is an 'Edit' button. Below this is a text line: 'When enabled badge-in is limited to the listed countries.'

Mixed to [client policies](#), you can prevent a user to login on a system if he didn't badge-in during the current day.

On the previous image, we can see that 3 other options are available in the Mobile Badging section.

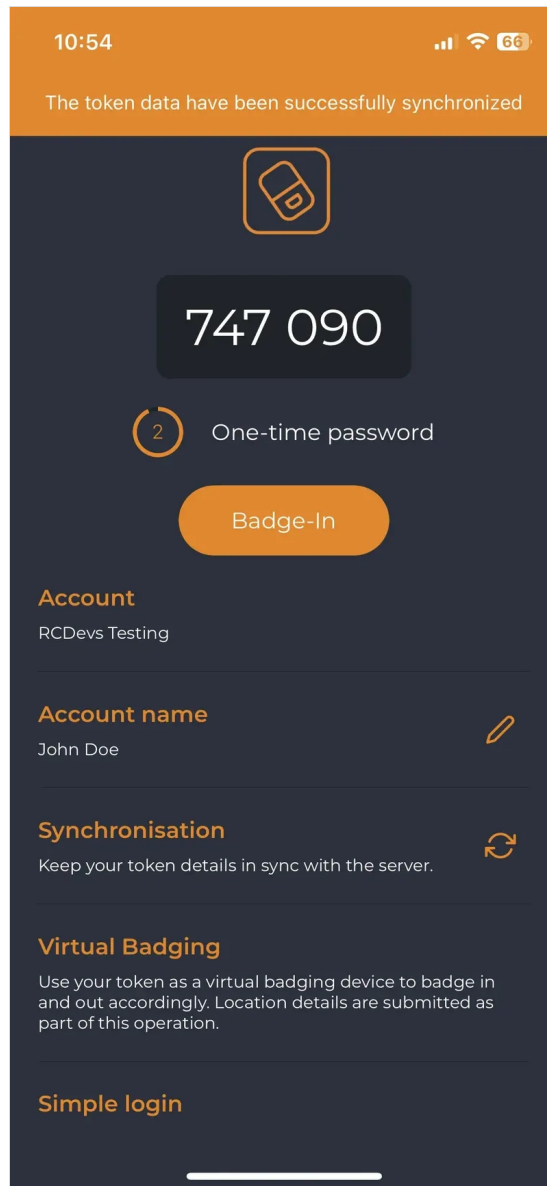
Firstly, we can choose which are the information gathered by checking Data Collection and then checking every option that you want between GPS, DN, IP and Mobile. Those data will be stored in the SQL database configured with your WebADM and are submitted from the mobile to your OpenOTP mobile endpoint URL directly. They are never forwarded through RCDevs cloud infrastructure and RCDevs do not have any access to those data.

The following option concerns the certificate used for the timestamping of each operation. The first choice is the local CA and the second is eIDAS which requires Sign option part of your OpenOTP license with signature credits purchased and available with your license.

Regarding the last option, it is about the possibility to allow only certain location(s) from where the badging operation is allowed (users loations). By checking this option, you can choose the countries where the badging operation will work. If not enabled, then all locations are allowed.

## 4. Badging operations

Once you have a token registered, you can click on it, and then you will see the option to badge-in.



Then, when you click on the buttons **Badge In** or **Badge Out**, a confirmation message will appear at the top of the screen.



10:56



Badging operation completed successfully.



306 065

20

One-time password

Badge-Out

### Account

RCDevs Testing

### Account name

John Doe



### Synchronisation

Keep your token details in sync with the server.

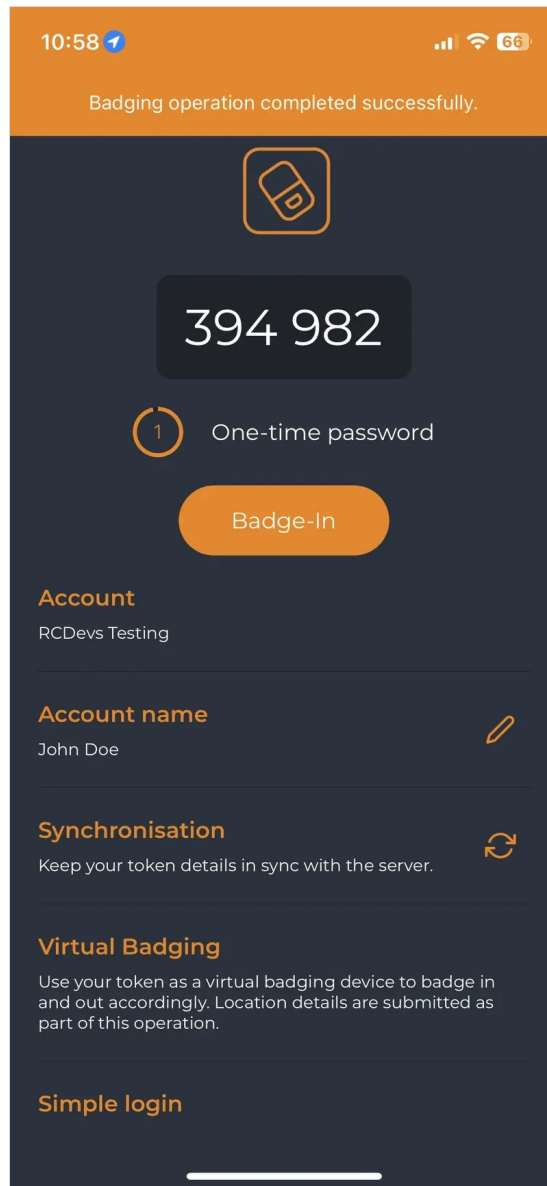


### Virtual Badging

Last Check-In: 2 Dec 2022 at 10:56:39

Use your token as a virtual badging device to badge in and out accordingly. Location details are submitted as part of this operation.

### Simple login



The time between the use of the two buttons is held in WebADM to calculate the time that the user has been badged in.

## 5. Audits and Logs

All badging operations performed by a user are stored in an SQL database. You can have a look on the audit part from

**Databases** menu > **Physical Access and Mobile Badging**.

Database Viewer for Physical Access & Mobile Badging (2 results out of 2 log items)

Filters (1)

DN

Equals

cn=remi

Remove

Action

Equals

Add Filter

This Minute

This Hour

Today

This Week

This Month

Display Options

Retrieve max

1000

Page results

35

Refresh

Log Actions

Delete selected items

Export as CSV / XML

Statistics as CSV / XML

Draw source map

Statistic Options

Show first

ALL

Group by

None

Database Pruning

Delete log entries older than

6

Month

Clean

<input type="checkbox"/>	<input type="radio"/> Action	<input type="radio"/> User DN	Time	User IP	Location	<input type="radio"/> Country	Collected Details
<input type="checkbox"/>	Badged Out	cn=remi	2023-05-17 13:57:20	213.135.242.3	49.5021696 5.9444448		<div>FullName: remi (Download XML)</div> <div>Organization: Rémi</div> <div>ServerTime: 2023-05-17 13:57:20</div> <div>MobileTime: 2023-05-17T11:57:20.086Z</div>
<input type="checkbox"/>	Badged In	cn=remi	2023-05-17 13:57:10	213.135.242.3	49.5021696 5.9444448		<div>FullName: remi (Download XML)</div> <div>Organization: Rémi</div> <div>ServerTime: 2023-05-17 13:57:10</div> <div>MobileTime: 2023-05-17T11:57:09.428Z</div>

Back to Access & Badging Viewer

## 6. Advanced configuration

For advanced configuration of mobile badging feature of OpenOTP, please refer to the [mobile badging 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*