

USER SELF-REGISTRATION

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.

User Self-Registration

[Web-Application](#)

1. Overview

User Self-Registration (SelfReg) application is a web application provided by RCDevs installed on the WebADM server. This application allows users to manage their OTP Token and U2F key enrollment. Users are also able to manage their OTP list and SSH key for SpanKey.

The SelfReg application is similar to the User Self-Service Desk, the only difference between both applications is that the User Self-Registration can be accessed only with a WebADM Administrator request. To allow the user, the Administrator will send a Self-Registration request to the user and this user will receive a one time link to access the application. Once logged on the application, the access link is revoked and the user cannot re-access the application using the access link any more.

Note

To be able to use SelfReg, any LDAP user must be a WebADM account. That means usable LDAP accounts are those containing the webadmAccount LDAP object class. You can enable the WebADM features on any LDAP user/group by extending it with the webadmAccount object class (from object extension list).

The installation of SelfReg is straightforward and only consists of either running the self-installer, or install the corresponding package through RCDevs repository. It is also included in the webadm_all_in_one package.

After installation, this is required to register and configure the application in WebADM. You do not have to modify any files in the SelfReg install directory! The web application configurations are managed and stored in LDAP by WebADM.

2. Installation

The User Self-Registration application can be installed using our package repositories or through a self-installer.

2.1 Install with Redhat Repository

On a RedHat, CentOS or Fedora system, you can use our repository, which simplifies updates. Add the repository:

```
yum install https://repos.rcdevs.com/redhat/base/rcdevs_release-1.1.1-1.noarch.rpm
```

Clean yum cache and install the User Self-Registration (SelfReg):

```
yum clean all  
yum install selfreg
```

The User Self-Registration application is now installed.

2.2 Install with Debian Repository

On a Debian or Ubuntu system, you can use our repository, which simplifies updates. Add the repository:

```
wget https://repos.rcdevs.com/debian/base/rcdevs-release_1.1.1-1_all.deb
apt-get install ./rcdevs-release_1.1.1-1_all.deb
```

Clean cache and install the User Self-Registration (SelfReg):

```
apt-get update
apt-get install selfreg
```

The User Self-Registration application is now installed.

2.3 Install Using the Self-Installer

The installation of the User Self-Registration application is very simple and is performed in less than 5 minutes. Just download the User Self-Registration self-installer package from the RCDevs website and put the installer file on your server. You can use WinSCP to copy the file to your server. To install the User Self-Registration, log into the server with SSH and run the following commands:

```
gunzip selfreg-1.1.x.sh.gz
bash selfreg-1.1.x.sh
```

3. Webapp Integration

You can embed a Web app on your website in an HTML iFrame or Object.

#Example

```
<object data="https://<webadm_addr>/webapps/selfreg?inline=1" />
```

4. Graphical Configuration

Once the application is installed, you have to enable it through the WebADM GUI. To activate it, log in on the WebADM GUI with your super_admin account, click on **Applications** tab, in **Categories** box, on the left, click on **Self-Service**. You should see the User Self-Registration application here.

LDAP Server 1 (slapd-u) (RCDevs Directory)

RCDevs Directory (2)

- dc=WebADM
- o=Root (6)
 - cn=admin
 - cn=ppolicy
 - cn=testgroup1
 - cn=testgroup2
 - cn=testuser1
 - cn=testuser2

Create / Search
Details / Check

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

Registered Applications and Services

Categories	
Authentication	(2)
SMS Relay	(1)
✓ Self-Service	(3)
Single Sign-On	(2)

Web Applications

Secure Password Reset (PwReset) v1.1.2 (Freeware)

Use this Web application to securely reset your LDAP or Domain password when it is lost or expired.

Latest Version: 1.1.2 (Ok)

Status: **Not Registered** [REGISTER]

Available Languages: FR,DE

WebApp URL: <https://192.168.3.185/webapps/pwreset/>

User Self-Service Desk (SelfDesk) v1.2.3 (Freeware)

Use this Web application to edit your account details, reset password, manage OTP tokens or FIDO devices...

Latest Version: 1.2.3 (Ok)

Status: **Enabled** [CONFIGURE] [REMOVE]

Available Languages: FR,DE

WebApp URL: [https://waproxy-u", "waproxy-d", "waproxy-c/selfdesk/](https://waproxy-u) (Proxied)

User Self-Registration (SelfReg) v1.2.2 (Freeware)

Use this Web application to self-register your OTP token or FIDO device after receiving a one-time email or SMS.

Latest Version: 1.2.2 (Ok)

Status: **Not Registered** [REGISTER]

Available Languages: FR,DE

WebApp URL: <https://192.168.3.185/webapps/selfreg/>

Click on the **REGISTER** button to enable the Application and you can now **CONFIGURE** it.

Under the configuration menu, many settings can be configured as you can see on the screenshots below.

WebADM Enterprise Edition v2.0.15

Copyright © 2010-2021 RCDevs Security, All Rights Reserved

API

HomeAdminClusterCreateSearchImportDatabasesStatisticsApplicationsAboutLogout

Object Settings for cn=SelfReg,dc=WebApps,dc=WebADM

Web Application Settings

☐ Disable WebApp

☐ Yes
 ☒ No (default)

☐ Hide WebApp

☐ Yes
 ☒ No (default)

Hide application from WebApps portal.

☐ Publish on Reverse Proxy / WAProxy

☐ Yes
 ☒ No (default)

Make WebApp accessible from WAProxy reverse-proxies.

☒ Default Domain

Default

This domain is automatically selected when no domain is provided.

☐ Enable Group Settings

☒ Yes (default)
 ☐ No

Resolve application settings on user groups (direct and indirect).
Warning: Impacts performances.

☐ Require Access Unlock

☐ Yes
 ☒ No (default)

Login is not permitted unless the user is temporarily authorized.
 To authorize a user, use the 'Unlock WebApp access' action for the user.
 IMPORTANT: Self-service applications published on the Internet without MFA should be locked.

☐ Non-locked IP Addresses

Comma-separated list of IP addresses with netmasks for which access is never locked (ex: 192.168.1.0/24).

☐ Allowed IP Addresses

Comma-separated list of IP addresses with netmasks (ex: 192.168.1.0/24).
 If not set then any source IP is allowed. The localhost is always allowed.

☐ Custom CSS File

Edit

CSS files and additional custom resources must be stored under /opt/webadm/lib/htdocs/custom/.

☐ Default Language

EN

☐ Require LDAP password

☐ Yes
 ☒ No (default)

☐ Require User Certificate

☐ Yes
 ☒ No (default)

If enabled, a user certificate must be provided to enter the application.

Allowed Features

☐ Token1
 ☐ Token2
 ☐ Token3
 ☐ FIDO
 ☐ OTPList
 ☐ AppKeys
 ☐ SSHkey

☐ Allow Self-Registration

The settings below allow the admin to manage how many tokens can be managed by the user, which features will be allowed on the App, which kind of token the user can enroll, etc.

WebADM Enterprise Edition v2.0.15

Copyright © 2010-2021 RCDDevs Security, All Rights Reserved

Home

Admin

Cluster

Create

Search

Import

Databases

Statistics

Applications

About

Logout

Allowed Features

☒ Allow Self-Registration

☒ Token1
☒ Token2
☐ Token3
☒ FIDO
☐ OTPList
☐ AppKeys
☐ SSHkey
☐ Voice
☐ PKI
☐ [None]

Selection of OpenOTP Token types users are able to register.

If not set, any of the listed items can be registered.

OTP Token Management

☒ Allowed Token Types

☐ HARDWARE-OATH
☒ HARDWARE-YUBIKEY
☒ QRCODE-TOTP
☐ QRCODE-HOTP
☐ MANUAL-YUBIKEY
☐ MANUAL-TOTP
☐ MANUAL-HOTP
☐ MANUAL-OCRA

Selection of OpenOTP Token types users are able to register.

Hardware options are used for inventoried Tokens and YubiKeys.

If not set, any Token type can be registered.

☒ Default Token Type

QRCODE-TOTP

If set, this Token type is pre-selected in the Token registration form.

The SSH key management/renewal can be done through the User Self-Registration application too.

Below the SSH Key management settings, another part called Mail/SMS Link allows you to configure the Registration URL, the delivery mode (Mail/SMS) and the link expiration time. This URL should be adjusted when you are running the Application through the WAProxy. Otherwise, the users will access the application through the WebADM server directly.

URL example when a user accesses the app through the WebADM server: `https://webadm-ip/webapps/selfreg/`

URL example when a user accesses the app through the WAProxy: `https://waproxy-ip/selfreg/`

SSH Key Management

☐ Allowed SSH Key Types ☐ HARDWARE ☐ SOFTWARE ☐ EXTERNAL

Selection of SpanKey public key types users are able to register.
HARDWARE option requires inventoried SSH PIV devices.
EXTERNAL let the user copy/paste an existing SSH public key.
If not set, any key type can be self-registered.

☐ Key Password Length

Minimum password length for newly-generated software SSH private keys.
Set '0' to disable password requirement.

Mail / SMS Link

☒ Registration URL

External WebApp URL or reverse proxy mapping.

☐ Link Delivery Mode

MAIL: Self-registration request is sent to user email address(es).
SMS: Self-registration request is sent to user mobile number(s).
MAILSMS: Self-registration request is sent via both email and SMS.

☐ Link Expiration Time

Default time after which the one-time link automatically expire (in seconds).

Email & SMS Settings

☒ Email Subject

Note: Sender email should be configured with 'org_from' setting in WebADM config file.

☐ Secure Email ☐ Yes ☒ No (default)

Encrypt email with the user certificate public key (S-MIME).

☐ SMS Message Type

Flash (class 0) SMS are not stored on the mobile phone.

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

Home

Admin

Cluster

Create

Search

Import

Databases

Statistics

Applications

About

Logout

Misc Settings

☐ Token Download URL

The Software Token download page on an external website.
When configured, a download button is included in the OTP section.
Ex. <https://www.rcdevs.com/solutions/tokens/software/>

☒ Email Message

Hello %USERNAME%,

This self-registration request will expire %TIMEOUT%.
Please click on the link below to start self-registration.
%URL%.

Localized

%USERNAME%: The user common name.
%USERID%: The user login name.
%DOMAIN%: The user domain name.
%URL%: The one-time link (URL).
%TIMEOUT%: The link expiration date.

Self-registration URL: %URL%

Localized

See Email Message above for available variables.

Apply

Cancel

Reset

Other settings can be adjusted like you want to...

Click on **Apply** and the configuration is done.

5. Send a Self-Registration Request to a User

To send a self-registration request to a user, you have 2 ways:

- > Auto send a link when the Token user is expired,

This setting is available since the OpenOTP v1.3.12-1. When the user will login and his token is expired, the authentication will fail and a self-reg link will be sent to the user.

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

User Notifications

☒ Send Expire Notification MAIL ▼

Send a notification email/SMS to the user when his LDAP password or OTP Token expired.
The email subject and sender address are defined in the MAIL OTP Settings.
The SMS sender number is defined in the SMS OTP Settings.

☐ Send Blocking Notification MAIL ▼

Send a notification email/SMS to the user when his account gets blocked.
The email subject and sender address are defined in the MAIL OTP Settings.
The SMS sender and message type are defined in the SMS OTP Settings.

☒ Send Self-Registration Links ☒ Yes ☐ No (default)

Automatically send a self-registration email/SMS to the user has no Token registered or Token expired.
This feature applies to the expiration of OTP List and Application Passwords too.
Note: Requires the SelfReg WebApp to be installed.

☒ Send Password Reset Links ☒ Yes ☐ No (default)

Automatically send a password reset email/SMS to the user password expired or must be changed.
Note: Requires the PwReset WebApp to be installed.

> Manually send a link.

To manually send a self-reg link, go to the WebADM Admin GUI, click on the related user on the left tree. In

Application Actions box, click on **User Self-Registration**.

LDAP Server 1 (slapd-u) (RCDevs Directory)

RCDevs Directory (2)

- dc=WebADM
- o=Root (6)
 - cn=admin
 - cn=ppolicy
 - cn=testgroup1
 - cn=testgroup2
 - cn=testuser1
 - cn=testuser2

Create / Search Details / Check
Create / Search Details / Check

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=testuser1,o=Root

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): webadmAccount, person, posixAc...</p> <p>Account is unique: Yes (in o=root)</p> <p>WebADM settings: None [CONFIGURE]</p> <p>WebADM data: 8 data [EDIT]</p> <p>User activated: Yes Deactivate</p> <p>Logs and inventory: WebApp, WebSrv, Inventory, Record</p>	<ul style="list-style-type: none"> Secure Password Reset (1 actions) User Self-Registration (1 actions) MFA Authentication Server (14 actions)

You can select the method you want to use to send the request (SMS/Mail) and you can also write a message to the user:

LDAP Server 1 (slapd-u) (RCDevs Directory)

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

Send Registration Email / SMS for cn=testuser1,o=Root

Self-registration sends a one-time link to the user by email and/or SMS.
The link is usable only once and automatically expires after the expiration time specified below.
The SelfReg WebApp address contained in the link can be specified in the SelfReg configurations.

Username: testuser1

Domain: Default

Message Type: MAIL

Use Secure Mail: ☐ Yes ☒ No

Link Expiration: 1 Hour

Message Comments: Hello,
You have one hour before the link expires.

Restricted Application: Any

Focused Item: None

Send Cancel

Click on **Send** button and the selfreg request is sent to the user.

The user will receive something like this:

Subject **OpenOTP/SpanKey Self-Registration**

Hello testuser1,

This self-registration request will expire 2021-03-23 12:49:27.
Please click on the link below to start self-registration.

<https://waproxy-u/selfreg/?id=0e26846a6c9e8494ddd4331e6525e21d>.

Hello,

You have one hour before the link expires.

He has to click on the link and will be redirected to the Application.

User Self-Registration

Welcome to the Self-Registration Portal at 192.168.3.185.
Your login password is required to continue.



Username: testuser1

Password:

Login Cancel

 Provided by RCDevs Security SA

Log in with his credentials and the user is logged on the application. Now the user can manage what the admin has allowed him

to manage.

User Self-Registration


Home

OTP

Logout


Hello testuser1.
Welcome to the Self-Registration Portal at 192.168.3.185.

Manage your OTP Token or FIDO Device




- Download a Software/Mobile Token.
- Register your Hardware or Software Token.
- Resynchronize your Hardware or Software Token.
- Test login with your Hardware or Software Token.

Manage your SSH Key



- Register or renew your SSH private key.
- Download your SSH public key for external use.




Provided by RCDevs Security SA

User Self-Registration

Home

OTP

Logout



Register OTP Token(s) to authenticate at 192.168.3.185.
Move your cursor on the (i) icons below for more information.

Authentication Settings

Primary OTP Method: **Token**

Fallback OTP Method: **[Not Set]**

OTP Challenge Timeout: **90 Seconds**

Enable Push Login: **Disabled**

View My

Third Token

OTP Token Status:


Not Registered

User Statistics


Login Count: **7 success & 6 failure**

Last Login: **2021-03-22 15:21:01**


Blocking Status: **Account active (0 login failed)**




Download Token




Register Token



Resync Token



Test Login



Provided by RCDevs Security SA

6. Proxy_user rights for User Self-Registration application

The proxy_user will operate for the end user for every action performed through SelfReg application. This means that the proxy_user account must have the required rights at the AD level to do these actions.

Note

Note that `CN=Users,DC=test,DC=local` used below is the user search base configured under the `WebADM Admin GUI` > `Admin` tab > `Local Domains` > `YOUR_DOMAIN` > `CONFIGURE` > `User Search Base` setting.

6.1 Rights for domain user accounts

For domain users, you have to configure the following rights for the proxy_user:

Token registration rights for a not extended schema

```
dscls "CN=Users,DC=test,DC=local" /I:T /G 'TEST\proxy_user:WPRP;bootfile'
dscls "CN=Users,DC=test,DC=local" /I:T /G 'TEST\proxy_user:WPRP;bootparameter'
dscls "CN=Users,DC=test,DC=local" /I:T /G 'TEST\proxy_user:WPRP;userCertificate'
```

Token registration rights for an extended schema

```
dscls "CN=Users,DC=test,DC=local" /I:T /G 'TEST\proxy_user:WPRP;webadmsetting'
dscls "CN=Users,DC=test,DC=local" /I:T /G 'TEST\proxy_user:WPRP;webadmdata'
dscls "CN=Users,DC=test,DC=local" /I:T /G 'TEST\proxy_user:WPRP;userCertificate'
```

6.2 Rights for domain administrator accounts

For domain admin users, you have to configure the rights on the AdminSDHolder object else, rights will be overridden after an hour.

Token registration rights for a not extended schema

```
dsaclsc"CN=AdminSDHolder,CN=System,DC=test,DC=local" /I:T /G 'TEST\proxy_user:WPRP;bootfile'
dscls "CN=AdminSDHolder,CN=System,DC=test,DC=local" /I:T /G
'TEST\proxy_user:WPRP;bootparameter'
dscls "CN=AdminSDHolder,CN=System,DC=test,DC=local" /I:T /G
'TEST\proxy_user:WPRP;userCertificate'
```

Token registration rights for an extended schema

```
dscls "CN=AdminSDHolder,CN=System,DC=test,DC=local" /I:T /G
'TEST\proxy_user:WPRP;webadmsetting'
dscls "CN=AdminSDHolder,CN=System,DC=test,DC=local" /I:T /G 'TEST\proxy_user:WPRP;webadmdata'
dscls "CN=AdminSDHolder,CN=System,DC=test,DC=local" /I:T /G
'TEST\proxy_user:WPRP;userCertificate'
```

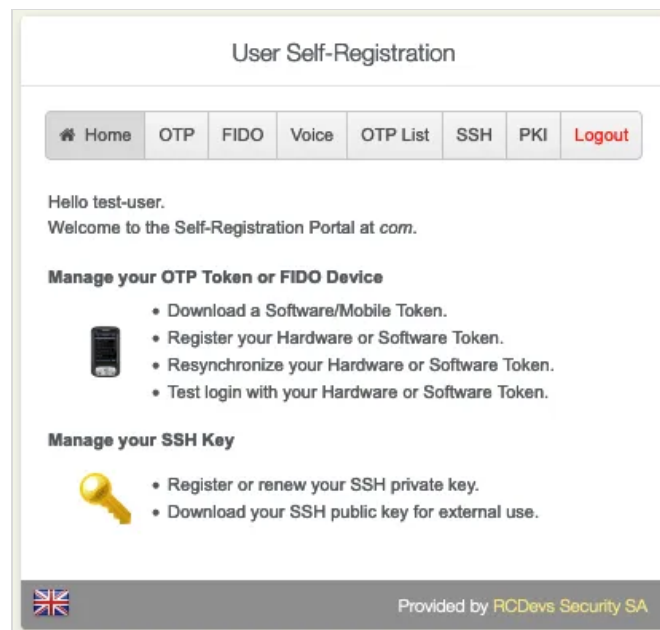
7. Token Enrollment

The **Self-Registration** application is accessible via the following address:

https://YOUR_WEBADM/webapps/selfreg/index.php

and through the **WAProxy** it is:

https://YOUR_WAPROXY/selfreg/index.php



7.1 Software Token

Go to the **OTP** tab. Enroll and manage the **Primary Token**, **Second Token**, etc.

User Self-Registration

Home

OTP

FIDO


Voice

OTP List

SSH

PKI

Logout



Register OTP Token(s) to authenticate at *com*.
Move your cursor on the (i) icons below for more information.

Authentication Settings


Primary OTP Method: Token

Fallback OTP Method: [Not Set]

OTP Challenge Timeout: 90 Seconds

Enable Push Login: Enabled

View My Primary Token

OTP Token Status: Ok (Disable) (Unregister) 

Token Type: OATH Time-based (160 bits)

Time Interval: 30 Seconds



Max Time Offset: 120 Seconds



User Statistics



Login Count: 1 success & No failure



Last Login: 2021-08-13 11:01:18

Blocking Status: Account active (0 login failed)










Download Token

Register Token

Resync Token


Test Login

 Provided by RCDevs Security SA

Click on **View My Primary/Second Token** etc. Click on **Register Token** .

User Self-Registration

[Home](#) [OTP](#) [FIDO](#) [Voice](#) [OTP List](#) [SSH](#) [PKI](#) [Logout](#)



Register OTP Token(s) to authenticate at *com*.
Move your cursor on the (i) icons below for more information.

Authentication Settings


Primary OTP Method: **Token**
Fallback OTP Method: **[Not Set]**
OTP Challenge Timeout: **90 Seconds**
Enable Push Login: **Enabled**


View My Second Token ▾


OTP Token Status: **Not Registered**


User Statistics


Login Count: **1 success & No failure**
Last Login: **2021-08-13 11:01:18**
Blocking Status: **Account active** (0 login failed)

[Download Token](#)

[Register Token](#)

[Resync Token](#)

[Test Login](#)

 Provided by [RCDevs Security SA](#)


Choose between [Hardware](#) , [YubiKey](#) , [QRCode-based](#) or [Manual Registration](#) of the Token.

User Self-Registration

You must first register your Software or Hardware Token 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 your mobile device.
2. Start your software Token and Scan the QRCode displayed below.
3. Click the 'Register' button below after scanning.



☐ I use a Hardware Token (Inventoried)

☐ I use a Yubikey Token (Inventoried / YubiCloud)

☒ I use a QRCode-based Authenticator (Time-based)

☐ I use a QRCode-based Authenticator (Event-based)


☐ I use another Token (Manual Registration) [i](#)

Register As:

Second Token

QRCode:

[\(Enlarge\)](#)



[i](#)


Enter OTP:

.....

[i](#)

Register

Cancel




Provided by [RCDevs Security SA](#)

Enter the **OTP** from the **OpenOTP Smartphone App**. (Only without the **Push Login**.)

User Self-Registration

Your Second Token has been registered

Ok



Provided by [RCDevs Security SA](#)

Click on [Test Login](#) to verify if the **Software Token** has successfully enrolled.

User Self-Registration

Home

OTP

FIDO

Voice

OTP List

SSH

PKI

Logout



Register OTP Token(s) to authenticate at *com*.
Move your cursor on the (i) icons below for more information.

Authentication Settings

Primary OTP Method: **Token**

Fallback OTP Method: **[Not Set]**

OTP Challenge Timeout: **90 Seconds**

Enable Push Login: **Enabled**

View My

Second Token

OTP Token Status: **Ok (Disable) (Unregister)** 

Token Type: **OATH Time-based (160 bits)**

Time Interval: **30 Seconds**


Max Time Offset: **120 Seconds**


User Statistics

Login Count: **1 success & No failure**

Last Login: **2021-08-13 11:01:18**

Blocking Status: **Account active (0 login failed)**










Download Token

Register Token

Resync Token

Test Login



Provided by **RCDevs Security SA**

Enter the **OTP** from the **OpenOTP Smartphone App**. (Only without the **Push Login**.)

User Self-Registration

This page allows you to test an authentication with your OTP methods.

Checking OpenOTP server status... **Ok**

Sending OTP authentication request... **Ok**

Result: **Challenge**

Message: Enter your TOKEN password


Timeout: 74 seconds

OTP:

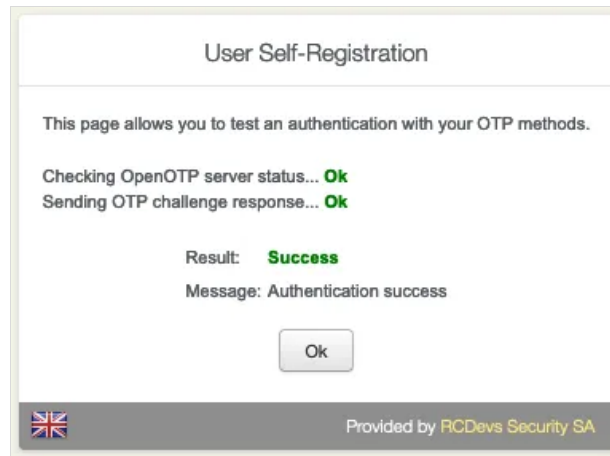
.....

Continue

Cancel



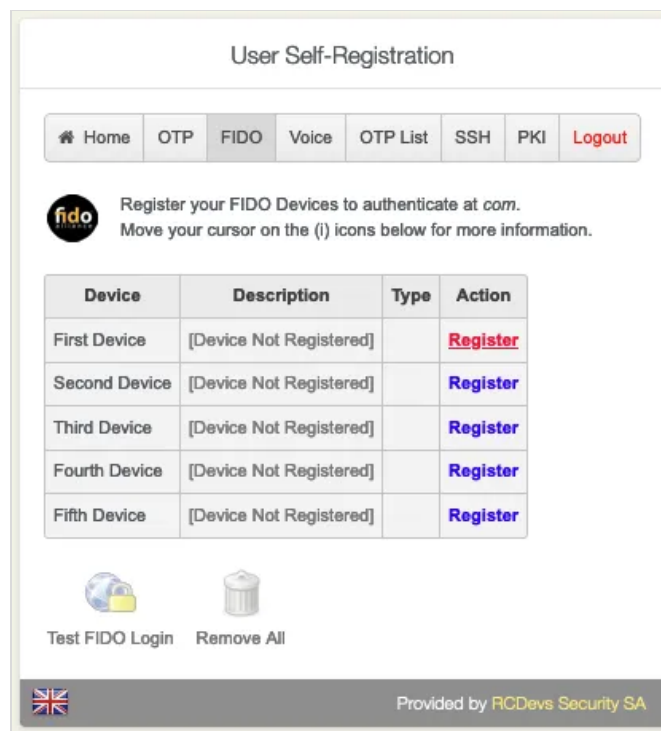
Provided by **RCDevs Security SA**



Click on **Resync Token** if the **Software Token** is out of sync. Always use an **NTP Server** on the **WebADM Servers** and the **Endpoints**.

7.2 Hardware Token

Go to the **FIDO** tab.



Click on **Register** to add the **FIDO Device**.


User Self-Registration

You must first register your FIDO Device or Token to start using it.
If any of the checks below fails then the registration cannot be done.

Your Web browser supports FIDO: **Yes** ⓘ
Self-Registration URL is enabled for FIDO: **No**


Instructions to register your FIDO Device:

- Plug the FIDO Device in a USB port on the computer.
- Click the blinking message below (or press Enter) to initiate the registration.
- When the device starts blinking, press the button to proceed the registration.



Friendly Name: ⓘ

Device Type: **FIDO2**

 Provided by **RCDevs Security SA**


7.3 Voice Registration


Go to the **Voice** tab. The **Voice Registration** consists in speaking several times the same secret passphrase.

User Self-Registration

The voice registration consists in speaking several times the same secret passphrase.
To be secure, the chosen passphrase must be long enough (minimum 3 seconds).

Example passphrase: *Please authenticate me with my voice.*
Or: *My name is test-user and my voice is my password.*



 Provided by **RCDevs Security SA**

Repeat the same **Passphrase**.

User Self-Registration


The voice registration consists in speaking several times the same secret passphrase.
To be secure, the chosen passphrase must be long enough (minimum 3 seconds).

Example passphrase: *Please authenticate me with my voice.*
Or: *My name is test-user and my voice is my password.*

2

Click to Start

Cancel



Provided by [RCDevs Security SA](#)

Again, repeat the same **Passphrase**.

User Self-Registration


The voice registration consists in speaking several times the same secret passphrase.
To be secure, the chosen passphrase must be long enough (minimum 3 seconds).

Example passphrase: *Please authenticate me with my voice.*
Or: *My name is test-user and my voice is my password.*

3

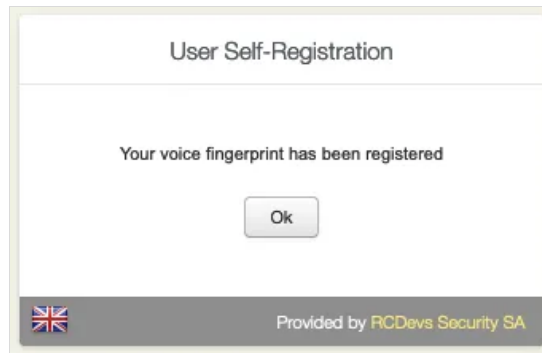
Click to Start

Cancel



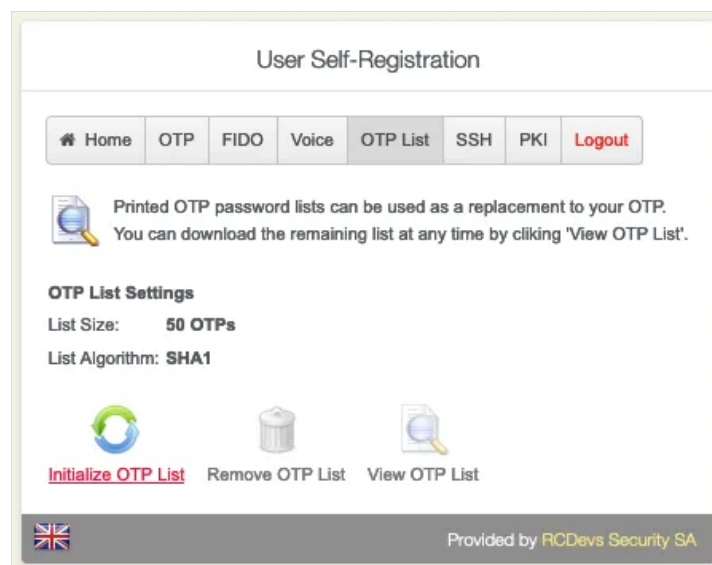
Provided by [RCDevs Security SA](#)

The **Voice Fingerprint** is successfully enrolled.



7.4 OTP List


Go to the **OTP List** tab. A printed **OTP Password List** can be used, for example, as a fallback to your current enrolled OTP Token.



Click on **Initialize OTP List**.

User Self-Registration


You can use this form to register a new OTP password list.
Once registered an OTP List can be used with OpenOTP LIST OTP Type.



List Size: **50 OTPs**
List Algorithm: **SHA1**

Register

Cancel




Provided by **RCDevs Security SA**

Click on **Register**.

User Self-Registration

OTP List successfully registered

Ok



Provided by **RCDevs Security SA**

Click on **Ok** to see the **OTP List**.

User Self-Registration


OpenOTP password List (50 OTPs).

ID	OTP	ID	OTP	ID	OTP	ID	OTP	ID	OTP
1	212158	2	340492	3	430617	4	090294	5	157040
6	700092	7	470329	8	827409	9	454546	10	902798
11	046528	12	463592	13	001088	14	264735	15	780631
16	984493	17	773848	18	726396	19	470119	20	048857
21	652692	22	530004	23	205013	24	681473	25	195507
26	390635	27	851490	28	985598	29	782605	30	027917
31	415546	32	815149	33	348078	34	939086	35	912859
36	622056	37	875979	38	389229	39	393684	40	644050
41	292948	42	893251	43	247663	44	546832	45	658232
46	578243	47	213500	48	869802	49	004415	50	858441

Ok

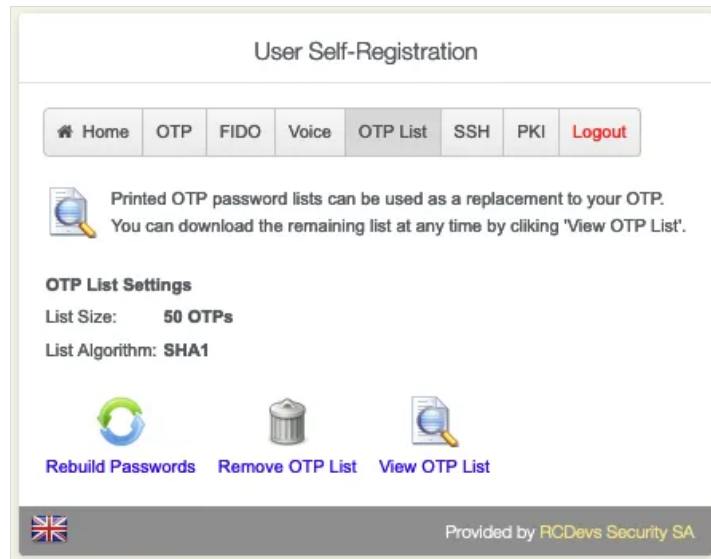
Download HTML

Print



Provided by **RCDevs Security SA**

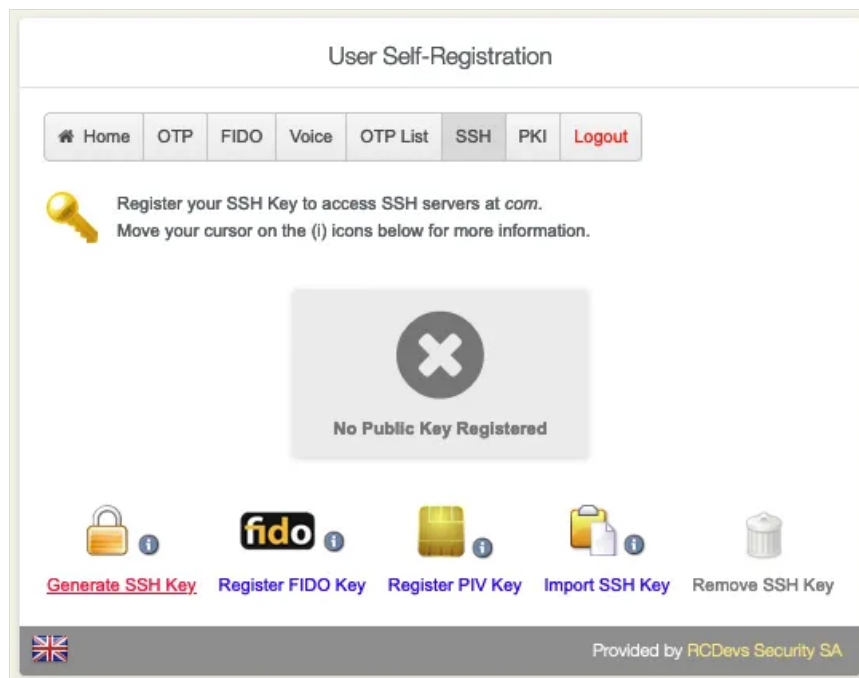
Choose between **Download HTML** or **Print** the **OTP List**.



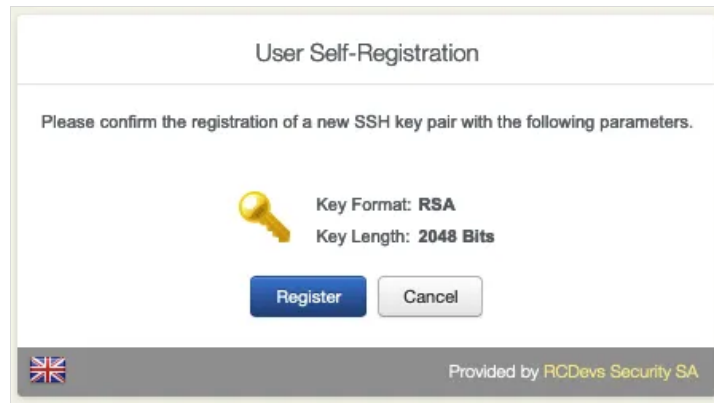
Finally, have the option to [Rebuild Passwords](#), [Remove OTP List](#) or [View OTP List](#).

7.5 SSH Key

Go to the [SSH](#) tab. Choose if you would like to [Generate SSH Key](#), [Register FIDO Key](#), [Register PIV Key](#), [Import SSH KEY](#) or [Remove SSH KEY](#).



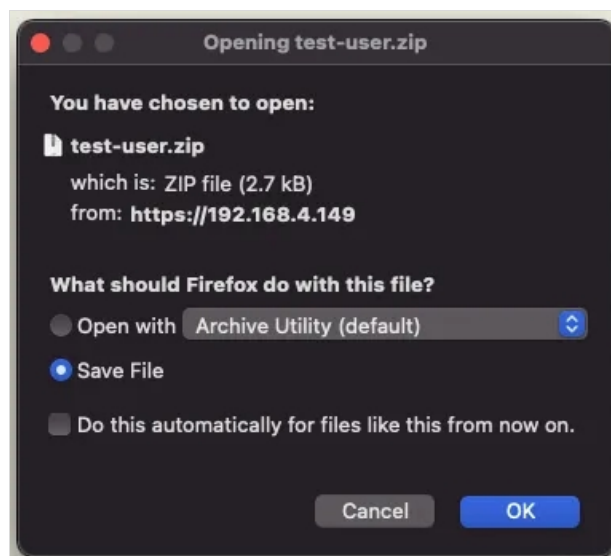
Click on [Generate SSH Key](#) to add the FIDO Device.



Click on **Register**.



Set a strong **Password** and download the **Private Key**.



In the **User Statistics**, there is the **Login Count** and **Last Login**.

User Self-Registration

Home
OTP
FIDO
Voice
OTP List
SSH
PKI
Logout

An SSH public key is already registered on your account and is **VALID**.
 The key does not have an expiration date and will not auto-expire!
 The key does not have a maximum usage count!

SSH Public Key:
(RSA 2048 Bits)

```
ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAQDFJ8/BoQ+0+0
/M76dV83MdpD12uyom7XG8vcEOWg6SLR5Z+Ndz8QcMY4
Y0GbisYDF4dKAcXZoeicGnv
/bm49VSL+DiWVviZ0Xz6oTyxivPGFW36F5LY1oq6
/tT5vbOEfjcEUmtXS
/z//zHiVq5tzdnKd5a01jXBnJFfRcZGaXYAsEDWeq37iT
hw52671DT0a5JnAPxVGv13AwgDJKhRfqE8VgmE0qu0I5i
WfDjO7dHD8DSmcPhHvn6FvV0fAeu8hLrUAu8CEyBRUV4i
H1O+6ZaBEkx0nuM5x+1UeT0gnHishSiCDP8eShoStBm
```

User Statistics

Login Count: **No success & No failure**

Last Login: **Never**

[Renew SSH Key](#)

[Register FIDO Key](#)

[Register PIV Key](#)

[Import SSH Key](#)

[Remove SSH Key](#)

Provided by RCDevs Security SA

7.6 User Certificate

Go to the **PKI** tab. Choose if you would like to **Add New Certificate** or **Get WebADM CA Certificate**.

User Self-Registration

Home
OTP
FIDO
Voice
OTP List
SSH
PKI
Logout

Click the actions in the table below to download, renew or delete your certificates.

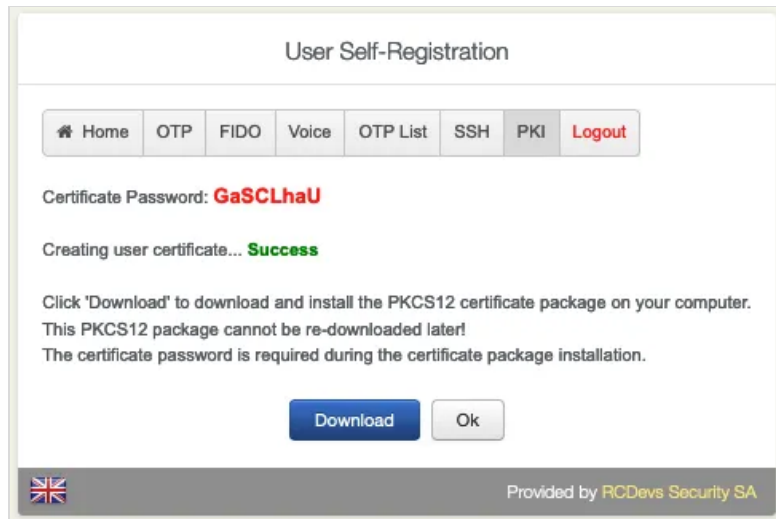
Serial	Name	Valid From	Valid To	Status	Actions
2	Defaulttest-user	13/08/2021	13/08/2022	Valid	

[Add New Certificate](#)

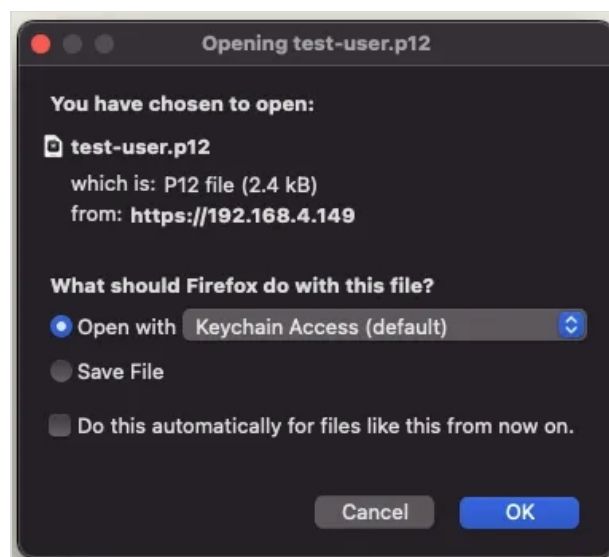
[Get WebADM CA Certificate](#)

Provided by RCDevs Security SA

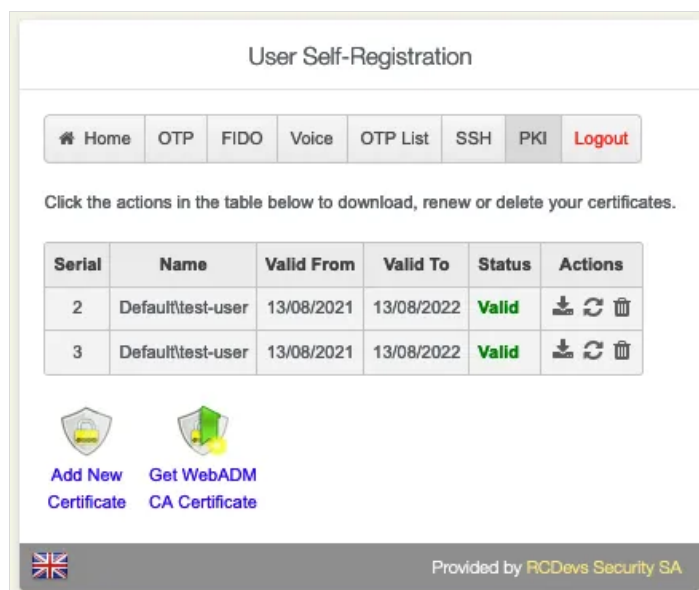
Click on **Add New Certificate**.



Download the **New Certificate**.



Overview of all the users' certificates. **Download**, **Renew** or **Delete** a certificate.



8 Logs

SelfReg application logs are accessible in the **Databases** menu in WebADM:

- You can see full logs in **WebADM Server Log Files** (lines containing **[SelfReg:]** pattern);

```
[2022-02-24 15:01:03] [192.168.4.32:43316] [SelfReg:CFZTJLZH] New login request (UID)
[2022-02-24 15:01:03] [192.168.4.32:43316] [SelfReg:CFZTJLZH] > Request ID: 3c9fc3754f67b9b31748041e688d9f07
[2022-02-24 15:01:03] [192.168.4.32:43316] [SelfReg:CFZTJLZH] > Username: Test User Un
[2022-02-24 15:01:03] [192.168.4.32:43316] [SelfReg:CFZTJLZH] > Domain: Default
[2022-02-24 15:01:03] [192.168.4.32:43316] [SelfReg:CFZTJLZH] Resolved LDAP user: CN=Test User Un,OU=Users,OU=BENOIT,OU=WebADMs,DC=support,DC=rcdevs,DC=com
[2022-02-24 15:01:03] [192.168.4.32:43316] [SelfReg:CFZTJLZH] Resolved LDAP groups: testgroupgetent,groupoutside,authorisedusers,wifi_users
[2022-02-24 15:01:03] [192.168.4.32:43316] [SelfReg:CFZTJLZH] Login session started for CN=Test User Un,OU=Users,OU=BENOIT,OU=WebADMs,DC=support,DC=rcdevs,DC=com
[2022-02-24 15:01:25] [192.168.4.32:43318] [SelfReg:CFZTJLZH] Unregistered TOTP Token
[2022-02-24 15:01:40] [172.16.3.8:59998] [OpenOTP:3UMGIFU2] Received mobile enrol request from 172.16.3.8
[2022-02-24 15:01:40] [172.16.3.8:59998] [OpenOTP:3UMGIFU2] > Session: lmZeXgGfdcZ0E80
[2022-02-24 15:01:40] [172.16.3.8:59998] [OpenOTP:3UMGIFU2] > Secret: 20 Bytes
[2022-02-24 15:01:40] [172.16.3.8:59998] [OpenOTP:3UMGIFU2] > OS Type: AND
[2022-02-24 15:01:40] [172.16.3.8:59998] [OpenOTP:3UMGIFU2] > Push ID: d6NTc7c0Qe-AgM10dR38VA:AP...
[2022-02-24 15:01:40] [172.16.3.8:59998] [OpenOTP:3UMGIFU2] > Serial: 0a0e26281bdf9f08
[2022-02-24 15:01:40] [172.16.3.8:59998] [OpenOTP:3UMGIFU2] > Model: Benoit's S21
[2022-02-24 15:01:40] [172.16.3.8:59998] [OpenOTP:3UMGIFU2] > Clock: 1645711300
[2022-02-24 15:01:42] [192.168.4.32:43320] [SelfReg:CFZTJLZH] Registered TOTP Push Token
[2022-02-24 15:01:52] [192.168.4.32:43322] [SelfReg:CFZTJLZH] Login session stopped for CN=Test User Un,OU=Users,OU=BENOIT,OU=WebADMs,DC=support,DC=rcdevs,DC=com
```

- You can see a list of SelfReg activities in **WebApp Logs** :

WebADM Enterprise Edition v2.1.5
Copyright © 2010-2022 RCDevs Security. All Rights Reserved

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

Database Viewer for **WebApp Logs** (40 results out of 1517 log items)

Filters (1)
Application **Equals** **SelfReg** Remove
Event Time **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"/>	Event Time	<input type="radio"/> Application	<input type="radio"/> User DN	<input type="radio"/> User IP	<input type="radio"/> Session ID	Details
<input type="checkbox"/>	2022-02-24 15:01:52	SelfReg	CN=Test User Un,OU=Users,OU=BE...	192.168.3.127	CFZTJLZH	Logged out
<input type="checkbox"/>	2022-02-24 15:01:42	SelfReg	CN=Test User Un,OU=Users,OU=BE...	192.168.3.127	CFZTJLZH	Registered TOTP Push Token
<input type="checkbox"/>	2022-02-24 15:01:25	SelfReg	CN=Test User Un,OU=Users,OU=BE...	192.168.3.127	CFZTJLZH	Unregistered TOTP Token
<input type="checkbox"/>	2022-02-24 15:01:03	SelfReg	CN=Test User Un,OU=Users,OU=BE...	192.168.3.127	CFZTJLZH	Login to webadm5.support.rcdevs.com
<input type="checkbox"/>	2022-02-24 15:00:45	SelfReg	CN=Test User Un,OU=Users,OU=BE...	192.168.3.127	0DBW7FCG	Logged out
<input type="checkbox"/>	2022-02-24 15:00:15	SelfReg	CN=Test User Un,OU=Users,OU=BE...	192.168.3.127	0DBW7FCG	Registered TOTP Push Token
<input type="checkbox"/>	2022-02-24 14:51:55	SelfReg	CN=Test User Un,OU=Users,OU=BE...	192.168.3.127	0DBW7FCG	Unregistered TOTP Token
<input type="checkbox"/>	2022-02-24 14:51:48	SelfReg	CN=Test User Un,OU=Users,OU=BE...	192.168.3.127	0DBW7FCG	Login to webadm5.support.rcdevs.com

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