



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.

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.

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, SSH key for SpanKey and TiQR Sign. The SelfReg application is similar to the User Self-Service Desk, the only difference between both applications is that the 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 access the application anymore.

2. Installation

The Self-Registration application is included in the Webam_all_in_one package.

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://www.rcdevs.com/repos/redhat/rcdevs_release-1.0.0-0.noarch.rpm
```

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

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

The Self-Registration application is now installed.

2.2 Install with Debian Repository

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

```
wget https://www.rcdevs.com/repos/debian/rcdevs-release_1.0.0-0_all.deb  
apt-get install ./rcdevs-release_1.0.0-0_all.deb
```

Clean cache and install Self-Registration (SelfReg):

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

The Self-Registration application is now installed.

2.3 Install Using the Self-Installer

The installation of RB is very simple and is performed in less than 5 minutes. Just download the RB self-installer package on RCDevs website and put the installer file on your server. You can use WinSCP to copy the file to your server. To install RB, 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. User Self-Registration

The installation of SelfReg is straightforward and only consists of running the self-installer or install the package through RCDevs repository and configure the application in WebADM.

You do not have to modify any files in the SelfReg install directory! The web applications configurations are managed and stored in LDAP by WebADM. To configure SelfReg, just enter WebADM as super administrator and go to the 'Applications' menu. Click SelfReg to enter the web-based configuration.

SelfReg application logs are accessible in the Databases menu in WebADM.

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).

Inline WebApps:

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 Self-Registration application here.

The screenshot displays the WebADM Freeware Edition v1.6.8-4 interface. The left sidebar shows the LDAP Server (OpenLDAP) configuration tree with the 'Self-Service' category selected. The main content area, titled 'Registered Applications and Services', lists three web applications:

- Secure Password Reset (PwReset) v1.0.12 (Freeware)**: Status: Enabled [CONFIGURE] [REMOVE]. WebApp URL: <https://192.168.3.117/webapps/pwreset/>
- User Self-Service Desk (SelfDesk) v1.1.8 (Freeware)**: Status: Enabled [CONFIGURE] [REMOVE]. WebApp URL: <https://192.168.3.117/webapps/selfdesk/>
- User Self-Registration (SelfReg) v1.1.8 (Freeware)**: Status: Not Registered [REGISTER]. WebApp URL: <https://192.168.3.117/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.

LDAP Server (OpenLDAP)

WebADM Freeware Edition v1.6.8-4

Copyright © 2010-2018 RCDevs SA, All Rights Reserved

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

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 WAProxy Yes No (default)
 Make WebApp accessible from WAProxy reverse-proxies.

Default Domain

This domain is automatically selected when no domain is provided.

Group Settings Yes (default) No
 Resolve application settings on user groups (direct and indirect).
 Warning: Impacts performances.

Access Locked 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 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

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

Default Language

Require LDAP password Yes (default) No

Require User Certificate Yes No (default)
 If enabled, a user certificate must be provided to enter the application.

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...

LDAP Server (OpenLDAP)

WebADM Freeware Edition v1.6.8-4
Copyright © 2010-2018 RCDevs SA, All Rights Reserved

API

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

OpenLDAP (2)

- dc=WebADM
- o=Root (3)
 - cn=admin
 - cn=ppolicy
 - cn=test_user
- Create / Search
Details / Check
- Create / Search
Details / Check

Allowed Features

- Allow Self-Registration
 - Token1
 - Token2
 - Token3
 - FIDO
 - OTPList
 - AppKeys
 - SSHkey
 - TiQR
 - [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:

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

The SSH key management/renewal can be done through the 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/`

- OpenLDAP (2)
- dc=WebADM
- o=Root (3)
 - cn=admin
 - cn=ppolicy
 - cn=test_user
- ★ Create / Search
Details / Check
- ★ Create / Search
Details / Check

SSH Key Management

- Allowed SSH Key Types HARDWARE SOFTWARE

Selection of SpanKey public key types users are able to register.
HARDWARE option requires inventoried SSH PIV devices.
MANUAL-PWD issues only password-protected SSH private keys.
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.

LDAP Server (OpenLDAP)

WebADM Freeware Edition v1.6.8-4
Copyright © 2010-2018 RCDevs SA, All Rights Reserved

API

Home | Admin | 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. <http://www.rcdevs.com/tokens/?type=software>

TiQR Download URL

The TiQR mobile download page on an external website.
When configured, a download button is included in the OTP section.
Ex. <http://www.rcdevs.com/tokens/?type=tiqr>

Message Templates

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.

SMS Message

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.

LDAP Server (OpenLDAP)

WebADM Freeware Edition v1.6.8-4
Copyright © 2010-2018 RCDevs SA, All Rights Reserved

API

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

User Notifications

- Send Expire Notification

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 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 on the WebADM Admin GUI, click on the concerned user on the left tree. In **Application Actions** box, click on **User Self-Registration**.

LDAP Server (OpenLDAP)

WebADM Freeware Edition v1.6.8-4
Copyright © 2010-2018 RCDevs SA, All Rights Reserved

API

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

Object **cn=test_user,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): person, webadmAccount</p> <p>Account is unique: Yes (in o=root)</p> <p>WebADM settings: 1 settings [CONFIGURE]</p> <p>WebADM data: None [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)

Click now on **Send Registration Email / SMS**.

LDAP Server (OpenLDAP)

WebADM Freeware Edition v1.6.8-4
Copyright © 2010-2018 RCDevs SA, All Rights Reserved

API

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

SelfReg User Actions for **cn=test_user,o=Root** (2)

Find below the user actions supported by **User Self-Registration** (SelfReg).

Send Registration Email / SMS

This action sends a one-time self-registration link to the user by email and/or SMS. The user just has to click the link and follow the instructions.

Cancel

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 (OpenLDAP)

WebADM Freeware Edition v1.6.8-4
Copyright © 2010-2018 RCDevs SA, All Rights Reserved

API

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

Send Registration Email / SMS for **cn=test_user,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:

Domain:

Message Type:

Use Secure Mail: Yes No

Link Expiration:

Message Comments:

Restricted Application:

Focused Item:

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

The user will receive something like this:

SelfReg@rcvm7.local
OpenOTP/SpanKey Self-Registration
To:

Hello test_user,

This self-registration request will expire 2018-12-17 16:26:51.
Please click on the link below to start self-registration.

<https://192.168.3.117/webapps/selfreg/?id=0ee521a03a031f7439571506ac55d750>.

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 192.168.3.117.
Your login password is required to continue.



Username:

Password:

 Provided by RCDevs Security Solutions

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](#) [FIDO](#) [OTP List](#) [SSH](#) [TiQR](#) [Logout](#)

Hello test_user.
Welcome to the Self-Registration Portal at 192.168.3.117.

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.

Manage your TiQR Mobile Client



- Download the TiQR mobile application.
- Register your TiQR application.
- Test login with your TiQR application.



Provided by [RCDevs Security Solutions](#)

User Self-Registration

[Home](#) [OTP](#) [FIDO](#) [OTP List](#) [SSH](#) [TiQR](#) [Logout](#)



Register OTP Token(s) to authenticate at 192.168.3.117.
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**

View My **Primary Token**

OTP Token Status: **Not Registered**

User Statistics

Login Count: **No success & No failure**
Last Login: **Never**
Blocking Status: **Account active** (0 login failed)



[Register Token](#)



[Resync Token](#)



[Test Login](#)



Provided by [RCDevs Security Solutions](#)

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... That 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

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

Token registration rights for an extended schema

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

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

Token registration rights for an extended schema

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

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