USER SELF-SERVICE DESK

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.

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-Service Desk

Web-Application

1. Overview

This Web application is mostly designed for internal (corporate) use and includes several self-management features like:

- Manage account information such as email, mobile phone numbers, etc..
- Reset LDAP password according to a configurable password policy
- Enroll, re-synchronize and test a Software / Hardware Token or Yubikey
- Enroll the TiQR mobile application
- Manage own user certificates

The installation of SelfDesk is straightforward and only consists of running the self-installer or installing it from the RCDevs repository and configure the application in WebADM.

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

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

Note

To be able to use SelfDesk, 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/selfdesk?inline=1" />
```

2. User Self-Service Desk Installation

The User Self-Service Desk 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-Service Desk (SelfDesk):

```
yum clean all
yum install selfdesk
```

The User Self-Service Desk 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 the User Self-Service Desk application (SelfDesk):

```
apt-get update
apt-get install selfdesk
```

The User Self-Service Desk application is now installed.

2.3 Through the self-installer

Download the Selfdesk package from the RCDevs website, copy it on your WebADM server(s) and run the following commands:

```
[root@webadm1 tmp]# gunzip selfdesk-1.1.8-1.sh.gz
[root@webadm1 tmp]# sh selfdesk-1.1.8-1.sh
Selfdesk v1.1.8-1 Self Installer
Copyright (c) 2010-2018 RCDevs SA, All rights reserved.
Please report software installation issues to bugs@rcdevs.com.

Verifying package update... Ok
Install selfdesk in '/opt/webadm/webapps/selfdesk' (y/n)? y
Extracting files, please wait... Ok
Removing temporary files... Ok
Selfdesk has been successfully installed.
Restart WebADM services (y/n) y
Stopping WebADM HTTP server... Ok
Stopping WebADM Watchd server..... Ok
Stopping WebADM PKI server... Ok
Stopping WebADM Session server... Ok
Checking libudev dependency... Ok
Checking system architecture... Ok
Checking server configurations... Ok

Found Trial Enterprise license (RCDEVSSUPPORT)
Licensed by RCDevs SA to RCDevs Support
Licensed product(s): OpenOTP,SpanKey,TiQR

Starting WebADM Session server... Ok
Starting WebADM PKI server... Ok
Starting WebADM Watchd server... Ok
Starting WebADM HTTP server... Ok

Checking server connections. Please wait...
Connected LDAP server: YO_AD-DC (192.168.3.50)
Connected SQL server: SQL Server (192.168.3.58)
Connected PKI server: PKI Server (192.168.3.54)
Connected Mail server: SMTP Server (78.141.172.203)
Connected Push server: Push Server (91.134.128.157)
Connected Session server: Session Server 2 (192.168.3.55)
Connected License server: License Server (91.134.128.157)

Checking LDAP proxy user access... Ok
Checking SQL database access... Ok
Checking PKI service access... Ok
Checking Mail service access... Ok
Checking Push service access... Ok
Checking License service access... Ok

Cluster mode enabled with 2 nodes (I'm slave)
Session replication status: Active (0.0003 sec)
Please read the INSTALL and README files in /opt/webadm/webapps/selfdesk.
```

Selfdesk is now installed and can be configured under the WebADM Admin GUI.

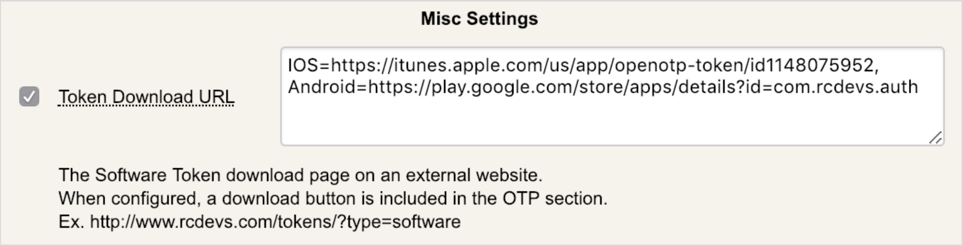
3. Selfdesk configuration

To configure the PWReset application, you have to log in on the WebADM Admin GUI > `Databases` Tab > `Self-Service` > `User Self-Service Desk (selfdesk)` > `CONFIGURE`.

The User Self-Service Desk application can be published through the WebADM Publishing Proxy for the end-user access with the setting `Publish on WAProxy`. This setting is only available when WAProxy is configured with WebADM. Have a look at this documentation to setup WAProxy.

To help you end-users to download a Token application on their phone, you can configure the Token Download URLs setting. For example:

```
IOS=https://itunes.apple.com/us/app/openotp-token/id1148075952,
Android=https://play.google.com/store/apps/details?id=com.rcdevs.auth
```



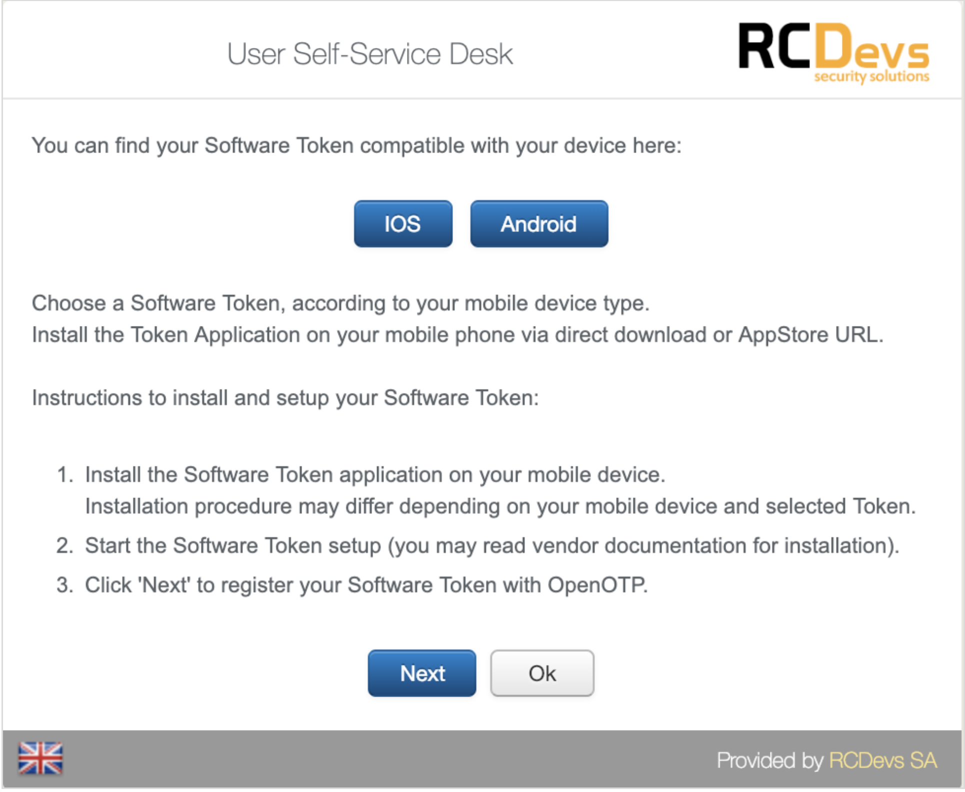
Misc Settings

☑ Token Download URL

```
IOS=https://itunes.apple.com/us/app/openotp-token/id1148075952,
Android=https://play.google.com/store/apps/details?id=com.rcdevs.auth
```

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

It will look like that for the end-user:



User Self-Service Desk

You can find your Software Token compatible with your device here:

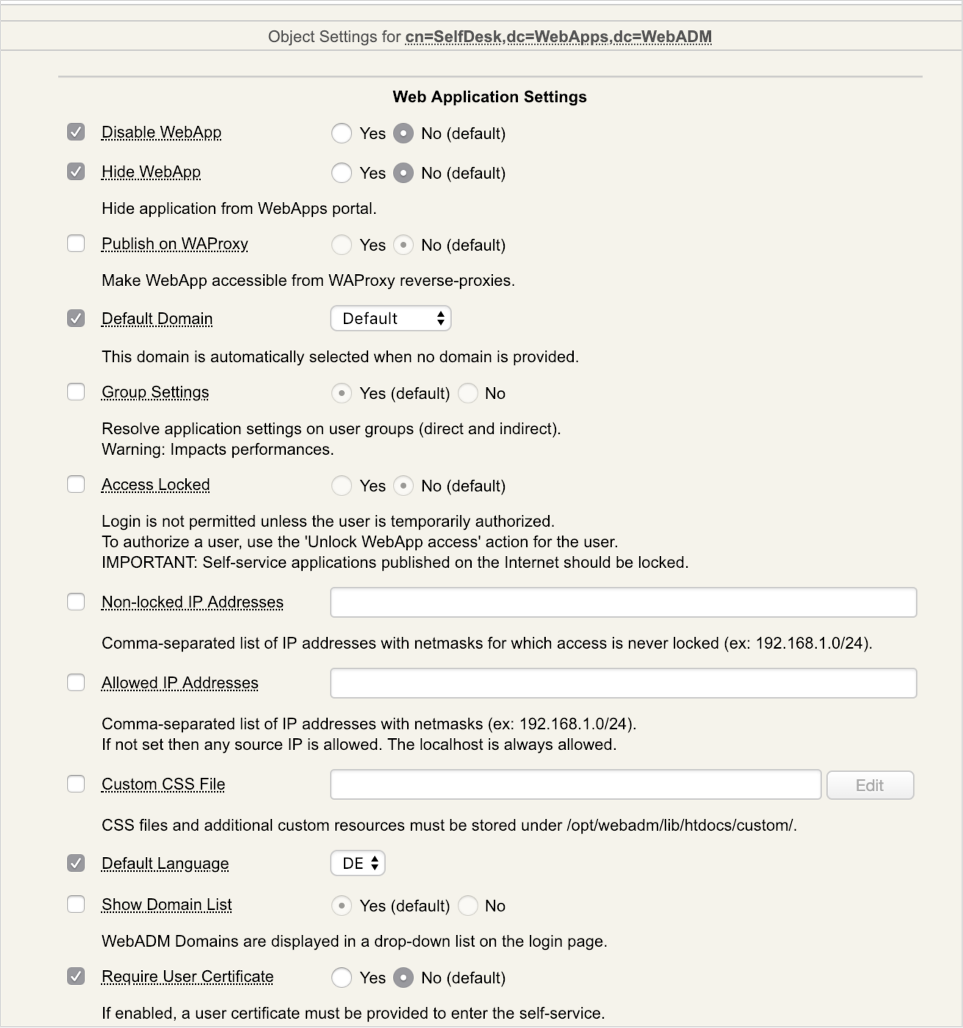
Choose a Software Token, according to your mobile device type.
Install the Token Application on your mobile phone via direct download or AppStore URL.

Instructions to install and setup your Software Token:

1. Install the Software Token application on your mobile device.
   Installation procedure may differ depending on your mobile device and selected Token.
2. Start the Software Token setup (you may read vendor documentation for installation).
3. Click 'Next' to register your Software Token with OpenOTP.

Provided by RCDevs SA

The other settings are described under the User Self-Service Desk configuration page.



Object Settings for cn=SelfDesk,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 Default

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 Edit

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

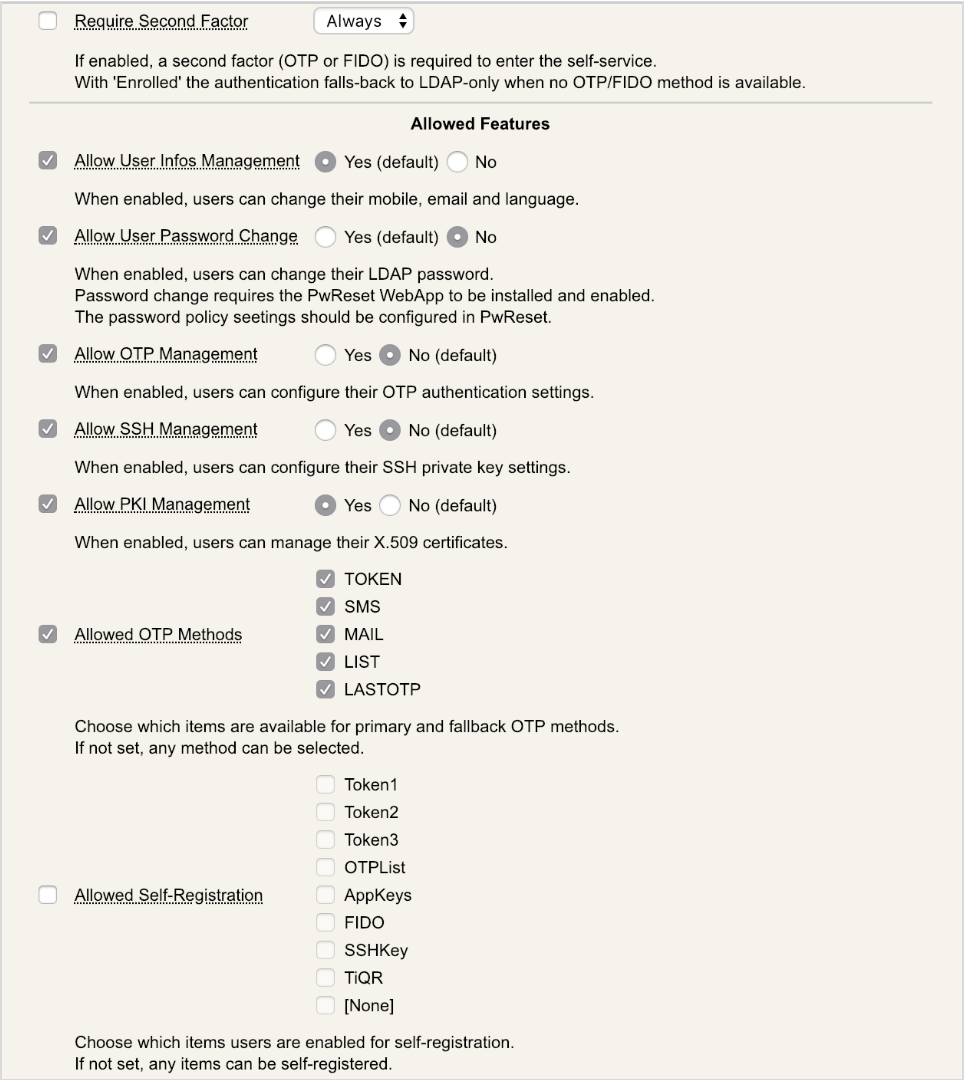
☑ Default Language DE

□ Show Domain List ● Yes (default) ○ No

WebADM Domains are displayed in a drop-down list on the login page.

☑ Require User Certificate ○ Yes ● No (default)

If enabled, a user certificate must be provided to enter the self-service.



☐ Require Second Factor — Always

If enabled, a second factor (OTP or FIDO) is required to enter the self-service.
With 'Enrolled' the authentication falls-back to LDAP-only when no OTP/FIDO method is available.

Allowed Features

☑ Allow User Infos Management ● Yes (default) ○ No

When enabled, users can change their mobile, email and language.

☑ Allow User Password Change ○ Yes (default) ● No

When enabled, users can change their LDAP password.
Password change requires the PwReset WebApp to be installed and enabled.
The password policy seetings should be configured in PwReset.

☑ Allow OTP Management ○ Yes ● No (default)

When enabled, users can configure their OTP authentication settings.

☑ Allow SSH Management ○ Yes ● No (default)

When enabled, users can configure their SSH private key settings.

☑ Allow PKI Management ● Yes ○ No (default)

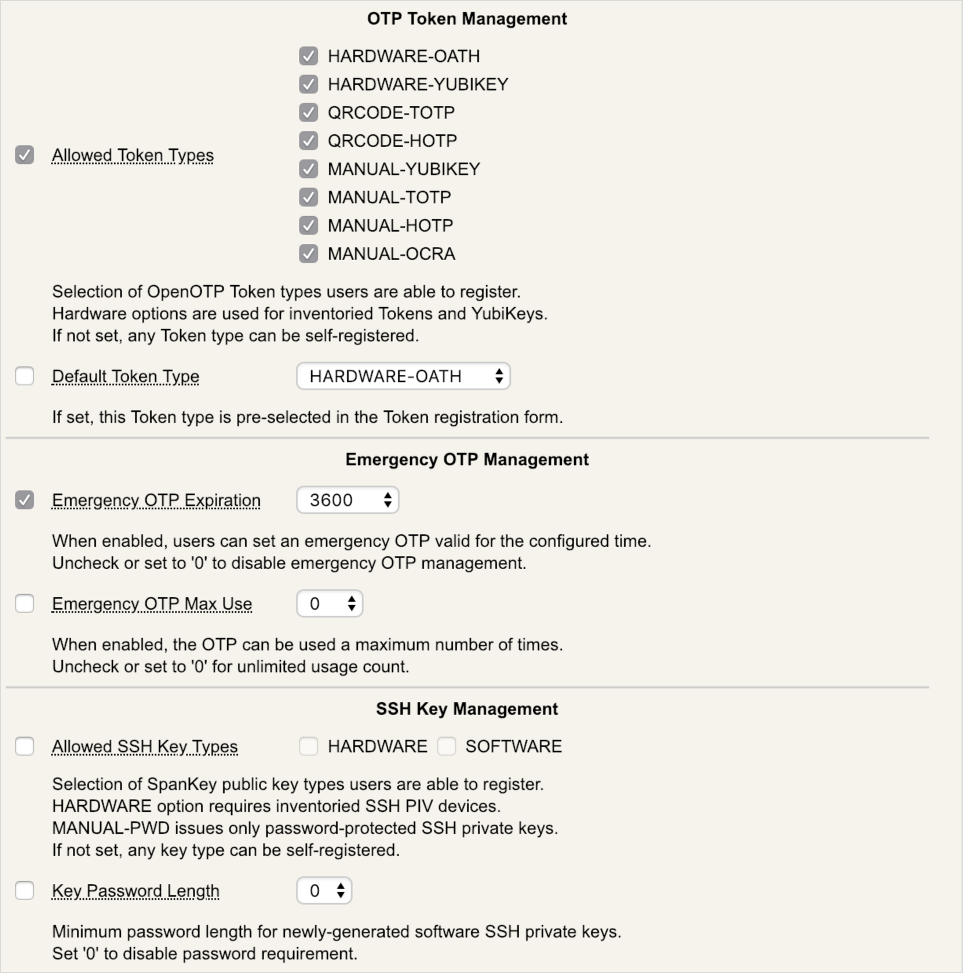
When enabled, users can manage their X.509 certificates.

☑ Allowed OTP Methods
- ☑ TOKEN
- ☑ SMS
- ☑ MAIL
- ☑ LIST
- ☑ LASTOTP

Choose which items are available for primary and fallback OTP methods.
If not set, any method can be selected.

☐ Allowed Self-Registration
- ☐ Token1
- ☐ Token2
- ☐ Token3
- ☐ OTPList
- ☐ AppKeys
- ☐ FIDO
- ☐ SSHKey
- ☐ TiQR
- ☐ [None]

Choose which items users are enabled for self-registration.
If not set, any items can be self-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 self-registered.

☐ Default Token Type: HARDWARE-OATH

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

Emergency OTP Management

☑ Emergency OTP Expiration: 3600

When enabled, users can set an emergency OTP valid for the configured time.
Uncheck or set to '0' to disable emergency OTP management.

☐ Emergency OTP Max Use: 0

When enabled, the OTP can be used a maximum number of times.
Uncheck or set to '0' for unlimited usage count.

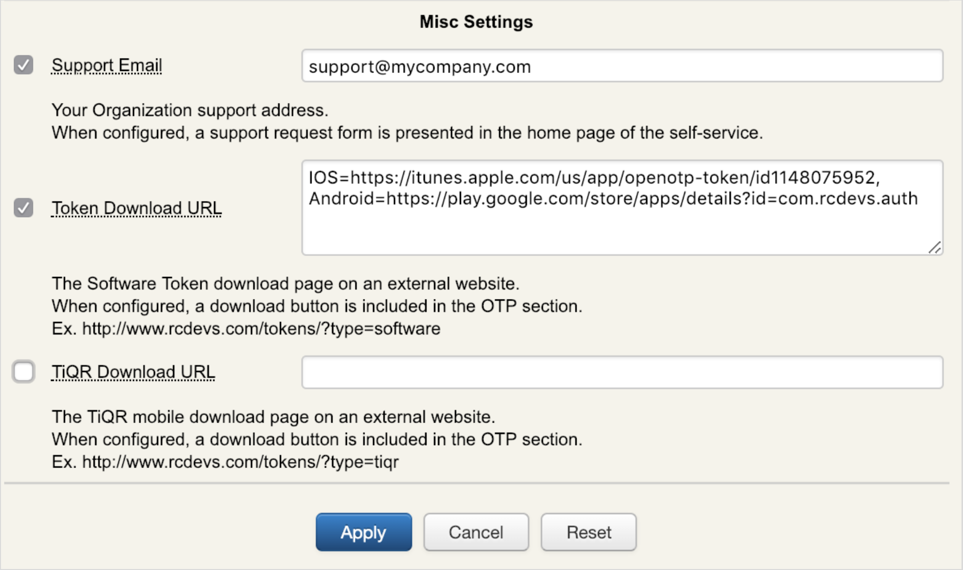
SSH Key Management

☐ 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: 0

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



Misc Settings

☑ Support Email: support@mycompany.com

Your Organization support address.
When configured, a support request form is presented in the home page of the self-service.

☑ Token Download URL:
```
IOS=https://itunes.apple.com/us/app/openotp-token/id1148075952,
Android=https://play.google.com/store/apps/details?id=com.rcdevs.auth
```

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

4. Proxy_user rights on AD for SelfDesk app

The proxy_user will operate for the end user to reset the password, change user account information like mobile, mail, preferred languages… 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.

4.1 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

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

Token registration rights for an extended schema

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

Common attributes rights

```
dsacls "CN=Users,DC=test,DC=local" /G 'TEST\proxy_user:WPRP;mail'
dsacls "CN=Users,DC=test,DC=local" /G 'TEST\proxy_user:WPRP;mobile'
dsacls "CN=Users,DC=test,DC=local" /G 'TEST\proxy_user:WPRP;preferredLanguage'
```

Password reset rights

```
dsacls "CN=Users,DC=test,DC=local" /I:T /G 'TEST\proxy_user:WPRP;userPassword'
dsacls "CN=Users,DC=test,DC=local" /I:T /G 'TEST\proxy_user:WPRP;pwdlastset'
```

4.2 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'
dsacls "CN=AdminSDHolder,CN=System,DC=test,DC=local" /I:T /G
'TEST\proxy_user:WPRP;bootparameter'
```

Token registration rights for an extended schema

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

Common attributes rights

```
dsacls "CN=AdminSDHolder,CN=System,DC=test,DC=local" /G 'TEST\webadm_admins:WPRP;mail'
dsacls "CN=AdminSDHolder,CN=System,DC=test,DC=local" /G
'TEST\webadm_admins:WPRP;mobile'
dsacls "CN=AdminSDHolder,CN=System,DC=test,DC=local" /G
'TEST\webadm_admins:WPRP;preferredLanguage'
```

Password reset rights

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

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