USER SELF-SERVICE DESK

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
- Manage SSH keys (SpanKey)
- Manage PDF Signatures
- 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://repos.rcdevs.com/redhat/base/rcdevs_release-1.1.1-1.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://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-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
```

It will look like that for the end-user:

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

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'
```

Voice rights (if Schema extended)

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

Voice rights (if Schema not extended)

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

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'
```

Voice rights (if Schema extended)

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

Voice rights (if Schema not extended)

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

5. SelfDesk Usage

The `Self-Service` application is accessible via the following address:

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

and through the `WAProxy` it is:

https://YOUR_WAPROXY/selfdesk/index.php

5.1 Manage personnal information

The `Home` tab allow you to view and manage account information such as mobile phone number, e-mail address, the prefered language and change his LDAP password.

Click on `Edit Information` to change the users information.

Click on `Update` to update new information provided on your account.

Click on `Change Password` and follow the instructions provided to change your password.

5.2 OTP Tokens enrollment

Go to the `OTP` tab. Choose the **Authentication Settings** like `Primary/Fallback OTP Method` and `Push Login`.

Click on `Register Token`. Choose between `Hardware`, `YubiKey`, `QRCode-based` or `Manual Registration` of the Token according the type of Token you want to register.

5.2.1 Sofware Token

Press I use QRCode-Base authenticator and then a QRCode is prompted as the below example :

Scan the QRCode with your Token application previously installed on your phone. It should create a token entry in your application and 6 digits code should appears.

Enter the **OTP** provided by the your application. This step is needed only if you are not using Push login. With Push login enabled, you don’t need to provide the OTP as the registration will be done with a communication coming from OpenOTP Token

application (phone) to the server.

Click on `Test Login` to verify if the **Software Token** has successfully enrolled.

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

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

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

5.2.2 Hardware Token (Inventoried)

To register an inventoried hardware token, select the correct option as shown in the screenshot below and you need to provide the serial number written on the back of the token and the OTP in order to validate the enrollment and to initialize the Token.

Press `Next` button and if all information provided can be successfully validated by the server, the token is enrolled on the account.

5.2.3 Yubikey (Inventoried/Yubicloud)

To enroll a Yubikey, select the correct option as shown in the screenshot below and press the Yubikey when you are invited to do it :

If the enrollment finished successfully, a confirmation message like below appears.

5.2.4 VOICE biometric enrollment

Go to the `View My` drop menu and choose **Voice Biometrics** then click on **Click to Register**.

The **Voice Biometrics** consists in speaking several times the same secret passphrase.

Repeat the same **Passphrase**.

Again, repeat the same **Passphrase**.

Finally, repeat one last time the same **Passphrase**.

The **Voice Fingerprint** is successfully enrolled.

Click on `Test Login` to verify if the **Voice Fingerprint** has successfully enrolled.

Hit the `Click to Speak` button and repeat your secret passphrase.

> **Note**
>
> For easy interaction with any integrations, the VOICE password can be provided through OpenOTP Token application if the configuration is allowed in OpenOTP server configuration. The setting to allow that is `Mobile Voice Login` set to `Yes`. VOICE biometric usage for MFA logins requires VOICE option as part of your license. Contact RCDevs Sales team for more information regarding that feature.

5.3 FIDO devices enrollment

Go to the `FIDO` tab and click on the first `Register` button available to register the new **FIDO device**.

Once you are one the following screen, plug the FIDO device you want to register on your computer and press the red message which is blinking.

Once you clicked on the red message, if multiple FIDO devices are detected, you are prompted to choose the one you want to register. I selected my security key.

Then I have to allow the access to my security key in order to perform the registration. The key is now ready to be enrolled and my key (Feitian BioPass FIDO2) is blinking, which means I have to press the key to perform the enrollment.

After pressing the key, the FIDO device is enrolled and can be used to login on systems requiring FIDO authentication.

You can see now, the key registered on the account :

You can test if the key is working correctly by clicking the `Test FIDO login` button. My key is detected by my web browser and is blinking. I have to press the security key in order to be authenticated.

I am successfully authenticated, my FIDO device is correctly registered and ready to be used in my company's FIDO integrations.

5.4 SSH Key enrollment for Spankey usage

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.

Choose the `Key Format` and the `Key Length`.

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

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

5.5 Submit PDF for Signature

The new `Sign` functionality allows the user connected to the Selfdesk application, the possibility to electronically sign a document. That feature is available since WebADM 2.0.23, Selfdesk 1.2.6 and OpenOTP 2.0. It also requires the OpenOTP Token application, the Push functionality must be configured in your WebADM infrastructure and a Push token enrolled on the user account. Go to the `Sign` tab.

You can choose the Signature Mode you want to use. For more information regarding the 2 modes, please refer to the REGULATION (EU) No 910/2014 OF THE EUROPEAN PARLIAMENT.

Drag and drop the document you want to send for Signature or click in the white zone to import the PDF you want to sign. Once the file has been loaded in the Selfdesk application, you will receive a push notification.

Once the document is uploaded, the user receives a notification on the OpenOTP Token application to sign the document.

Click the `Next` button to review the document:

On the next screen, you are prompted on your phone to provide your handwritten signature which will be incorporated into the final document.

I provide my signature :

If the PDF contains multiple pages, you are invited to provide your paraphs, which will be incorporated into all other pages.

I provide my paraphs and then click `Next` :

The transaction is submitted to the server.

After that screen, the PDF is auto-prepared by RCDevs Cloud Services with the handwritten signature at the end of the document and paraphs are added on intermediate pages. On top of that, the PDF is electronically signed and sealed with RCDevs certificates. If you check the signature validity/status, the status of the signature will depend on the type of mode of signature (Advanced/Qualified) that has been chosen at the beginning of the workflow to sign that document. For example, Adobe Reader will by default, show the signature validity in green as soon as the document has been signed with a qualified device. For advanced signature, it may appear in orange if the certificate authority file of RCDevs is not trusted in Adobe Reader.

Once the workflow is finished successfully, you can see the following screen on the SelfDesk application and the version of the

signed PDF is automatically downloaded.

You can verify the electronic signature with Adobe Reader or with a PDF digital signature validator.

See proofs of signatures above.

If you want to involve multiple signatories for the same document, you can send the first signed PDF version to the next person who should sign it. His handwritten signature/paraphs will be added to the document and the cryptographic proof of the signature is added after the existing signature block. Found below, the example of the same document signed by 2 persons :

Signatures status are displayed in green in Adobe Reader because I trusted the RCDevs CA certificate in Adobe Reader :

This is not needed when signatures are produced by qualified devices because Adobe Reader already trust the Certificate Authorities used to provide qualified devices.

5.6 User Certificate enrollment

Go to the `PKI` tab. Choose if you would like to `Add New Certificate`, `Get Other User Certificate` or `Get WebADM CA Certificate`.

Click on `Add New Certificate`.

Download the **New Certificate**.

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