SECURE PASSWORD RESET WEB APPLICATION

📄 Secure Password Reset Web Application

1. Overview

This application allows users to set a new password on their LDAP account when they lost their current password or if it expired. It uses the OpenOTP second login factor (SMS, Token or Yubikey) to authenticate the password reset operation. Alternatively, TiQR (QRCode login) and PKI access with user certificate can be used as authentication back-ends.

RCDevs Password Reset is compliant with any LDAP password including AD Domain passwords, UNIX passwords and even SAMBA accounts. You can define password complexity policies or let the application obey the existing AD password policy. The password complexity configuration includes password size, type of characters, password blacklist and even dynamic complexity requirements per password length.

The installation of PwReset 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 PwReset install directory! The web applications configurations are managed and stored in LDAP by WebADM. To configure PwReset, just enter WebADM as super administrator and go to the `Applications` menu. Click PwReset to enter the web-based configuration.

PwReset application logs are accessible in the `Databases` menu in WebADM.

> 🚩 Note
>
> To be able to use PwReset, some Directory server like Active Directory have to communicate over SSL with WebADM. Please, refer to Active Directory and SSL documentation to setup AD with SSL.

> 🚩 Note
>
> To be able to use PwReset, 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/pwreset?inline=1" />
```

2. PwReset Installation

The Secure Password Reset 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 Secure Password Reset (PwReset):

```
yum clean all
yum install pwreset
```

The Secure Password Reset 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_1.0.1-0_all.deb
apt-get install ./rcdevs-release_1.0.1-0_all.deb
```

Clean cache and install Secure Password Reset application (PwReset):

```
apt-get update
apt-get install pwreset
```

The Secure Password Reset application is now installed.

2.3 Through the self-installer

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

```
[root@webadm1 tmp]# gunzip pwreset-1.0.12-1.sh.gz
[root@webadm1 tmp]# sh pwreset-1.0.12-1.sh
PWReset v1.0.12-1 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 PwReset in '/opt/webadm/webapps/pwreset' (y/n)? y
Extracting files, please wait... Ok
Removing temporary files... Ok
PWReset 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/pwreset.
```

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

3. PwReset configuration

To configure the PwReset application, you have to log in on the WebADM Admin GUI > `Databases` Tab > `Self-Service` > `Secure Password Reset (PwReset)` > `CONFIGURE`.

PwReset 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. If you publish PwReset on WAProxy, take into account the setting `Password Reset URL`. This URL should be edited to point to WAProxy if you sent automatic PwReset link when users password is expired. The default URL for this setting is: `https://WebADM_Server_IP/webapps/pwreset/`. If you publish the PwReset application through WAProxy then the URL must be changed to this:

`https://WAProxy_Server_IP/pwreset/`

The `/webapps/` folder disappear from the URL when you use WAProxy.

A feature dedicated to Active Directory is `Allow Account Unlock` which allows the user to unlock his account by himself at the AD level. The proxy_user must have the right permissions to allow this action. Please refer to this documentation for more information about proxy_user rights on Active Directory.

The other settings are described under the Secure Password Reset configuration page.

4. Proxy_user rights on AD for PwReset

The proxy_user will operate for the user to reset the password. That means that the proxy_user account must have the rights at the AD level to reset users password and to unlock the account if you want to enable this option.

4.1 Domain User accounts

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

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'
```

Unlock account rights :

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

4.2 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.

Password reset rights :

```
dsacls "CN=AdminSDHolder,CN=System,DC=test,DC=local" /G
'TEST\proxy_user:WPRP;userPassword'
dsacls "CN=AdminSDHolder,CN=System,DC=test,DC=local" /G
'TEST\proxy_user:WPRP;pwdlastset'
```

Unlock account rights :

```
dsacls "CN=AdminSDHolder,CN=System,DC=test,DC=local" /G
'TEST\proxy_user:WPRP;lockouttime'
```