SECURE PASSWORD RESET

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.

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.

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 Installation 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 Secure Password Reset (PwReset):

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

The Secure Password Reset application is now installed.

2.2 Installation 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 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 > `Applications` Tab > `Self-Service` > `Secure Password Reset (PwReset)` > `CONFIGURE`.

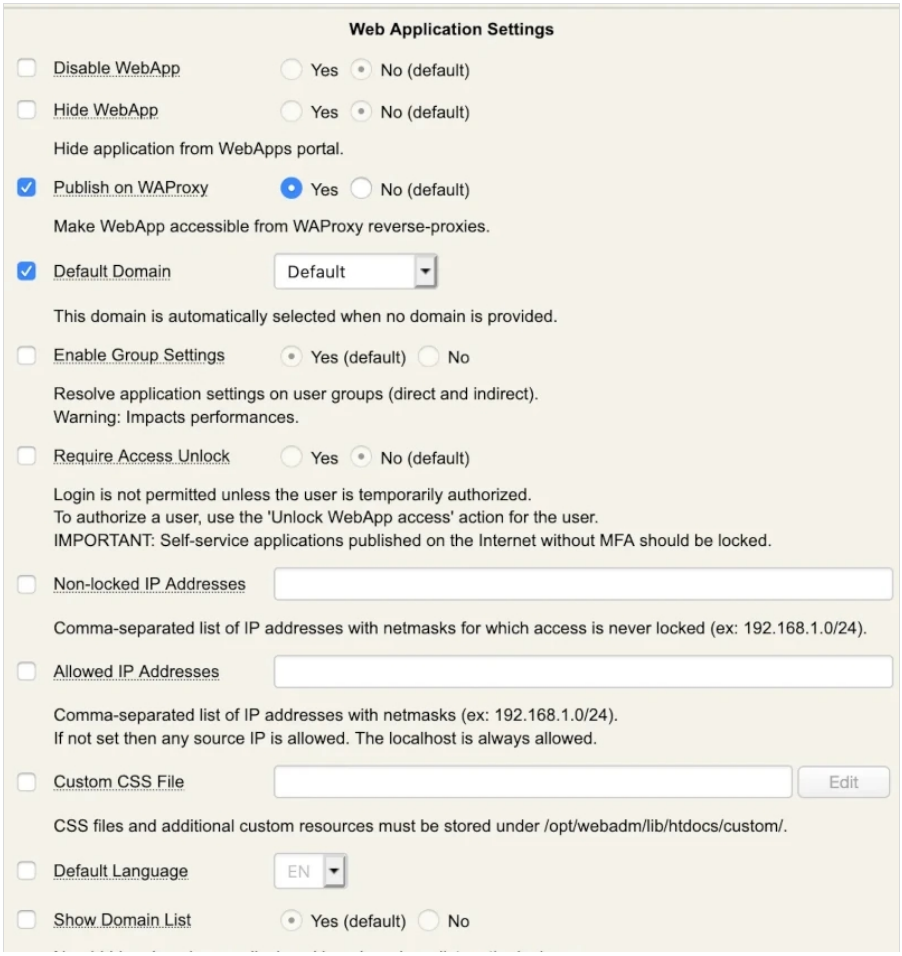
PwReset can be published through the WebADM Publishing Proxy for the end-user access with the setting `Publish on WAProxy`. This setting is only available when WAProxy is configured with WebADM. Have a look at this documentation to set up WAProxy. If you publish PwReset on WAProxy, take into account 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.



Non-hidden domains are displayed in a drop-down list on the login page.
The domain drop-down selector is hidden when there is only one domain available.
You must disable this setting if you need to use user principal names (UPN).

Require Email Link — Yes / No (default)

When enabled, direct access is forbidden and an access email has to be sent via the Manager API.

Require LDAP Password — Yes / No (default)

Require both the LDAP password (expired or not) and the OTP for a password reset.
With PKI login, password is always required.

Hide OTP Password Input — Yes / No (default)

Enabling this feature does not display the OTP password input on the login form.
OTP will also always use the OpenOTP challenge-response mechanism.

Feature Access

Allow Password Reset — Yes (default) / No

Choose wether password reset is allowed or not by default.
You need to set 'No' if you want to allow password reset on a user/group basis.

Allow Account Unlock — Yes / No (default)

Choose wether AD account unlock is allowed or not by default.
Account unlock is not possible if 'Require LDAP Password' is enabled.

Password Policy

Min Password Length — 6 (Default)

Default minimum length is 6 characters.

Max Password Length — 6

Require Numeric Char(s) — Yes / No (default)

Require Alphabetic Char(s) — Yes / No (default)

Require Other Char(s) — Yes / No (default)

Password requires non-alphanumeric character(s).

Require Multi-Case Char(s) — Yes / No (default)

Password requires both upcase and lowcase character(s).

Complexy by Length — 4

Remove requirements above according to the new password length.
Example: With 3 requirements checked, min length set to 8 and this setting set to 5 then:
- Less than 13 chars: Enforce 3/3 requirements.
- From 13 to 17 chars: Enforce 2/3 requirements.
- More than 17 chars: Enforce 1/3 requirement.

Prevent Known Passwords — Yes / No (default)

Password is validated using the 'pwned password' API at haveibeenpwned.com.

Mail / SMS Link

Password Reset URL — https://bercdevs.com/pwreset/

External WebApp URL or reverse proxy mapping.

Link Delivery Mode — MAIL (Default)

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

Link Expiration Time — 3600 (Default)

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

Email & SMS Settings

Email Subject — LDAP Password Reset — Localized

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 — Normal (Default)

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

Authentication Backend

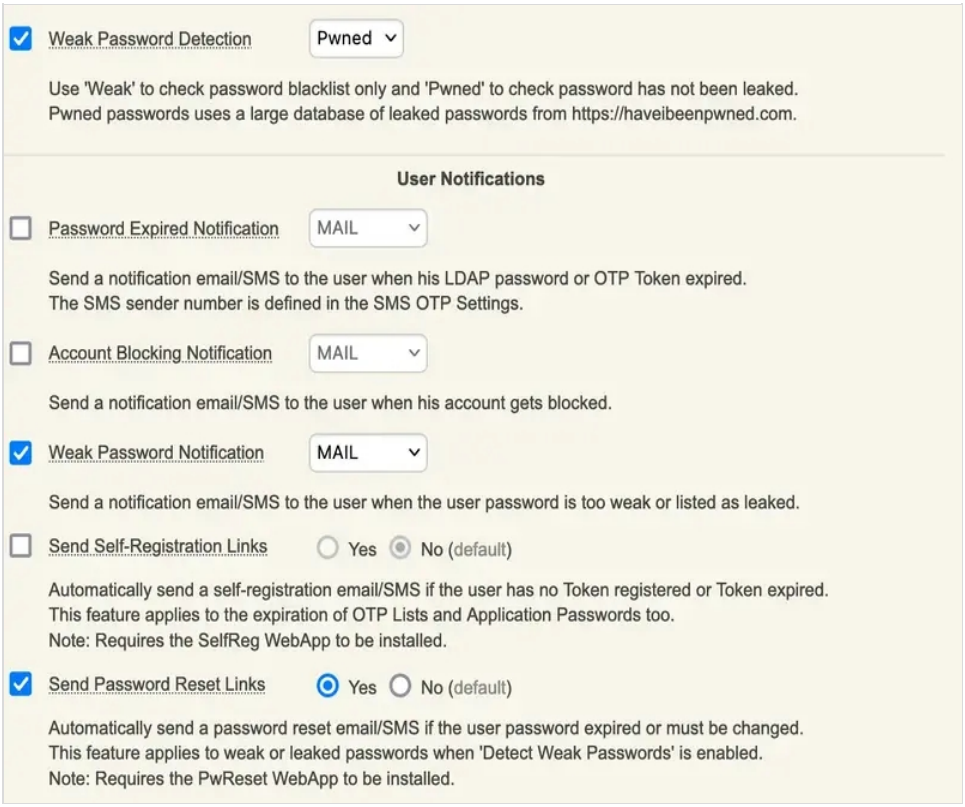
Default Auth Backend — OpenOTP (Default)

3.1 Weak and Pwned password

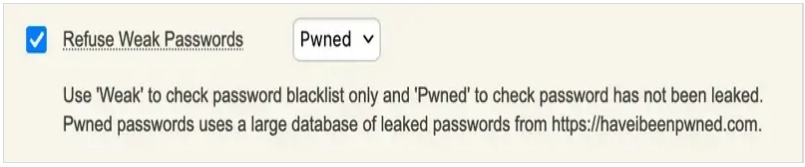
> **Note**
>
> The OpenOTP server and PwReset app include a feature to detect weak or compromised passwords starting from WebADM v2.3.10 / OpenOTP v2.2.11 / PwReset v1.3.2

Weak or compromised passwords refer to passwords that are either easily guessable, simple, or have been exposed through security breaches. WebADM includes the option to detect a weak password and automatically send the user an alert along with a link to reset their password :

OpenOTP :

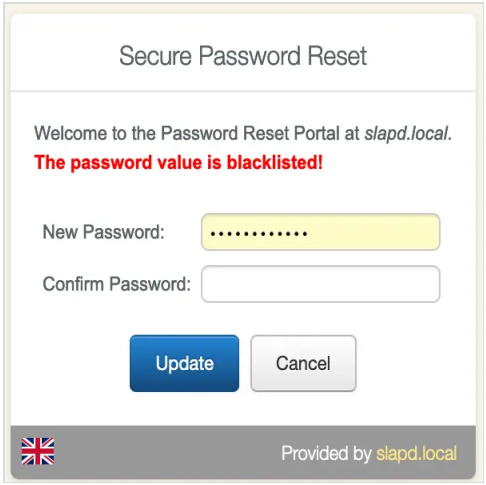


PwReset :

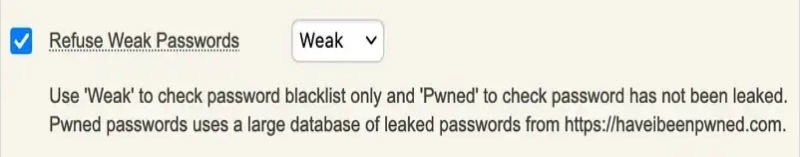


If you choose `Pwned` option, the user must select a strong password that is not known to be compromised on https://haveibeenpwned.com

Here, I tried to set the password as: `Password123`



But if you choose `Weak` option, an alert is sent, but the `Pwned` database is not checked :



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'
```