MAIL OTP

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.
This guide will show how to set up the email settings for sending MAIL OTP. If one needs to change or to add Localized Message then navigate to the following documentation Message Templates.

**2. Config Mail Server**

SMTP mail servers can be used by WebADM for sending emails. Therefore add your mail server settings in the following configuration file `/opt/webadm/conf/servers.xml`. If no server is specified, WebADM will use the local mailer in `/usr/sbin/sendmail` to send emails.

```bash
-bash-4.2# vi /opt/webadm/conf/servers.xml
<?xml version="1.0" encoding="UTF-8" ?>

<Servers>

<!--
******************************************
***  WebADM Remote Server Connections  ***
******************************************
...
<!--
SMTP mail servers can be used by WebADM for sending emails.
If no server is specified, WebADM will use the local mailer
in /usr/sbin/sendmail to send emails.
-->

<!--
<MailServer name="SMTP Server"
    host="localhost"
    port="25"
    user=""
    password=""
    encryption="NONE"
    ca_file="" />

-->

</Servers>
```

Please remove `<!--` and `-->` to activate the MailServer configuration. Replace the default settings with your SMTP mail server settings. Finally, restart WebADM with `/opt/webadm/bin/webadm restart`. Have a look below for an example.
<xml version="1.0" encoding="UTF-8" ?>

<Servers>

<!--
******************************************
***  WebADM Remote Server Connections  ***
******************************************
...
-->

<MailServer name="SMTP Server"
    host="www.rcdevs.com"
    port="25"
    user="loic"
    password="{wcrypt}O0ycjL0MoL51xy6D0vc0MA=="
    encryption="NONE"
    ca_file="" />

</Servers>

-bash-4.2# /opt/webadm/bin/webadm restart
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: LDAP Server (192.168.3.80)
Connected SQL server: SQL Server (192.168.3.80)
Connected PKI server: PKI Server (192.168.3.80)
Connected Mail server: SMTP Server (78.141.172.203)
Connected Push server: Push Server (91.134.128.157)
Connected Session server: Session Server (192.168.3.80)
In this example, the password has been encrypted. This feature requires an Enterprise License and the encryption mechanism is bound to secret data in your encoded license file. Please follow this documentation [RCDevs Utilities and Command Line Tools for WebADM](#).

3. Config Email

3.1 Test Email

First, select the **test_user** on the left side. It has no email address, add it under **Add Attribute** add **Email Address**.
Now, the **test_user** has got an email address.

Let's check if WebADM is able to send an email. Therefore, we click under **Application Actions** on **Secure Password Reset**.
Find below the user actions supported by Secure Password Reset (PwReset).

Send Password Reset Email / SMS

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

Send Password Reset Email / SMS for cn=test_user, o=Root

Password Reset 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 PwReset WebApp address contained in the link can be specified in the PwReset configurations.

Username: test_user
Domain: Default
Message Type: MAIL
Use Secure Mail: Yes
Link Expiration: 1 Hour
Message Comments: Testing

Password reset sent successfully (MAIL)
Hello test_user,

This password reset request will expire 2019-02-27 11:25:11.
Please click on the link below to reset your password.

https://192.168.3.163/webapps/pwreset/?id=5033b3d85eabb0ce4db7ba52f6c645d5.

This is a test mail.

This is the default output, let’s continue with changing the sender’s email.

3.2 Sender Email

To configure the sender email, edit the WebADM configuration file /opt/webadm/conf/webadm.conf by removing the # in front of org_from and replacing the default sender email. Save the changes and restart WebADM with /opt/webadm/bin/webadm restart.

-bash-4.2# vi /opt/webadm/conf/webadm.conf

# WebADM Server Configuration
#
...
# Personalization options
# You can customize your organization's name, logo file and website URL.
# The logo file must be a PNG image under conf/ with a size of 100x50 pixels.
#org_name "RCDevs SA"
#org_logo "rcdevs.png"
#org_site "http://www.rcdevs.com/
#org_from "noreply@rcdevs.com"
...
Let's send again a test mail and verify that the sender email has changed to `noreply@rcdevs.com` instead of the default `PwReset@rcdevs.com`.

noreply@rcdevs.com
LDAP Password Reset
To:

Hello test_user,

This password reset request will expire 2019-02-27 11:35:27.
Please click on the link below to reset your password.

https://192.168.3.163/webapps/pwreset/?id=36ea9fbc4b4f5325216f47ef6d654b7fb.

This is a test mail.

3.3 Alerts

Alerts are always recorded to the SQL Alert log. Additionally, when `alert_email` is defined, the alerts are also sent by email. To activate this feature, edit the configuration file of WebADM `/opt/webadm/conf/webadm.conf` by removing the `#` in front of `alert_email` and replacing the default email. Save the changes and restart WebADM with `/opt/webadm/bin/webadm restart`. 

-bash-4.2# vi /opt/webadm/conf/webadm.conf
#
# WebADM Server Configuration
#
...  
# Personalization options
# You can customize your organization's name, logo file and website URL.
# The logo file must be a PNG image under conf/ with a size of 100x50 pixels.
#org_name "RCDevs SA"
#org_logo "rcdevs.png"
#org_site "http://www.rcdevs.com/"
org_from "noreply@rcdevs.com"
...
Let's engage an alert recorded to the SQL Alert log by setting a wrong time clock on the server. Do the following steps from this documentation NTP (Network Time Protocol). Afterward, restart WebADM.

To alert users via email when a login certificate or ActiveDirectory domain password is near expiration, set user_warning to Yes.

```bash
-bash-4.2# vi /opt/webadm/conf/webadm.conf
#
# WebADM Server Configuration
#
...
# Alerts are always recorded to the SQL Alert log. Additionally, when alert_email
# or alert_mobile is defined, the alerts are also sent by email/SMS.
#alert_email "me@mydomain.com"
#alert_mobile "+33 12345678"
...
```

```
-bash-4.2# vi /opt/webadm/conf/webadm.conf
#
# WebADM Server Configuration
#
...
# Alerts are always recorded to the SQL Alert log. Additionally, when alert_email
# or alert_mobile is defined, the alerts are also sent by email/SMS.
alert_email "testmail@rcdevs.com"
#alert_mobile "+33 12345678"
...
```
The templates for alerting users via email when a login certificate or ActiveDirectory domain password is near expiration are defined by `ldap_expire_xxx` and `cert_expire_xxx` in `/opt/webadm/conf/webadm.conf`. There, the messages can be changed and additional variables can be added. A notification email will be sent 5 days before the user’s password expiration and afterward every day until the password has been changed. The value is hardcoded.

Finally, save the changes and restart WebADM with `/opt/webadm/bin/webadm restart`.

### 3.4 Mail OTP

To receive an OTP via Email, the user must have a mail value configured in mail or othermail attributes. To enable the OTP by Mail, there are multiple ways:

- Under OpenOTP global configuration,
- Under OpenOTP user settings configuration,
- Under OpenOTP client policy configuration,
The **OTP Type** setting must be set to MAIL. In the following scenario, we use option 2 and will configure the WebADM user setting on the user object. On an activated user account, in **object Details** box, click on **CONFIGURE** button:

Choose **OpenOTP** from the **Applications** box and set **OTP Type** to **MAIL**. Note that **MAIL OTP** may require longer timeouts, therefore enable the option **Challenge Session Timeout**. Furthermore, if needed enable the options under **User Notifications** as shown below.
Enable the option **Send Blocking Notification** to send a notification email to the user when his account gets blocked.
Finally, the last options for OpenOTP. OnDemand Email Delivery Mode means a new OTP is sent when the user starts an authentication process. Next chapter, encrypt OTP email with the user certificate public key (S-MIME).

Let's test the Mail OTP by clicking **MFA Authentication Server** under **Application Actions**.
Now click on **Test User Authentication**.
Type in your LDAP password if the Login Mode is set to LDAPOTP. Click the Start button.

Now, switch to your email client and check your mail.
Finally, enter your OTP from the email and click **Continue**.

noreply@rcdevs.com

OpenOTP Login

To:

Hello test_user. Your access code for OpenOTP at 192.168.3.168 is 209931.

Finally, enter your OTP from the email and click **Continue**.

3.5 Encrypt Mail OTP
First, enable the option **Use Secure Email**. Have a look at the previous chapter.

Now, create a certificate through WebADM for the user in question. In this example, select the `test_user` on the left side and click on **Create certificate**.
Now, click the Create Cert button.
Click the **Download PKCS12** button to download the user’s certificate. Import the certificate into your mail client.

Let’s verify if the email is encrypted. Do the same steps as in the previous chapter for the **Test User Authentication**.
Hello test_user. Your access code for OpenOTP at 192.168.3.168 is 947502.

In the header of the email, you can see that it has been encrypted.

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