



EMAIL (OTP, ALERTS)

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.

Email (OTP, Alerts)

[email Alert](#)

1. Overview

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

2. Configure 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-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.

```
-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="www.rcdevs.com"
  port="25"
  user="loic"
  password="{wcrypt}OOycjL0MoL51xy6DOvc0MA=="
  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)
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 4 nodes (I'm master)
-bash-4.2#
```

In this example, the password has been encrypted.

The encryption mechanism is bound to secret data in your encoded license file and is available for free and enterprise licenses starting from version 2 of WebADM. Prior to version 2 of WebADM, this feature requires an Enterprise License. Please follow this documentation [RCDevs Utilities and Command Line Tools for WebADM](#).

3. Configure and test email

3.1 Test Email

First, select the `testuser1` on the left side. It has no email address, add it under `Add Attribute` add `Email Address`.

LDAP Server 1 (slapd-u) (RCDevs Directory) ↻

WebADM Enterprise Edition v2.0.15
Copyright © 2010-2021 RCDevs Security, All Rights Reserved

Home | Admin | Cluster | Create | Search | Import | Databases | Statistics | Applications | About | Logout

Object cn=testuser1,o=Root

LDAP Actions

- Delete this object
- Copy this object
- Move this object
- Export to LDIF
- Change password
- Create certificate
- Unlock WebApp access
- Advanced edit mode

Object Details

Object class(es): webadmAccount, person, posixAc...

Account is unique: **Yes** (in o=root)

WebADM settings: **None [CONFIGURE]**

WebADM data: **8 data [EDIT]**

User activated: **Yes Deactivate**

Logs and inventory: [WebApp](#), [WebSrv](#), [Inventory](#), [Record](#)

Application Actions

- [Secure Password Reset \(1 actions\)](#)
- [User Self-Registration \(1 actions\)](#)
- [MFA Authentication Server \(14 actions\)](#)
- [SSH Public Key Server \(3 actions\)](#)

Object Name: testuser1 Rename

Add Attribute (11): Email Address Add

Login Name [add values]: testuser1

Last Name [add values]: User1

First Name [add values] [delete attribute]: Test

UID Number: 500

GiD Number: 100

Home Directory: /home/testuser1

Login Shell [delete attribute]: /bin/bash

WebADM User Data [delete attribute]

Edit Application Data

OpenOTP.LastLogin: 2021-03-22 15:21:01

OpenOTP.LastOTP: [BINARY APPLICATION DATA - 24 Bytes]

OpenOTP.LoginCount: 7

OpenOTP.RejectCount: 0

OpenOTP.TokenKey: [BINARY APPLICATION DATA - 20 Bytes]

OpenOTP.TokenState: 53980762

OpenOTP.TokenType: TOTP

Group Membership [add values] [delete attribute]

cn=testgroup1,o=Root Goto

cn=testgroup2,o=Root Goto

Apply Changes | Re-Encrypt | Delete Selected

LDAP Server 1 (slapd-u) (RCDevs Directory) ↻

WebADM Enterprise Edition v2.0.15
Copyright © 2010-2021 RCDevs Security, All Rights Reserved

Home | Admin | Cluster | Create | Search | Import | Databases | Statistics | Applications | About | Logout

New Email Address Value(s) for cn=testuser1,o=Root

testmail@rcdevs.com

Proceed Cancel

Now, the `testuser1` has got an email address.

LDAP Server 1 (slapd-u) (RCDevs Directory) WebADM Enterprise Edition v2.0.15
 Copyright © 2010-2021 RCDevs Security, All Rights Reserved

Home | Admin | Cluster | Create | Search | Import | Databases | Statistics | Applications | About | Logout

Object **cn=testuser1,o=Root**

LDAP Actions

- Delete this object
- Copy this object
- Move this object
- Export to LDIF
- Change password
- Create certificate
- Unlock WebApp access
- Advanced edit mode

Object Details

Object class(es): webadmAccount_person_posixAc...

Account is unique: **Yes** (in o=root)

WebADM settings: **None [CONFIGURE]**

WebADM data: **8 data [EDIT]**

User activated: **Yes Deactivate**

Logs and inventory: [WebApp](#), [WebSrv](#), [Inventory](#), [Record](#)

Application Actions

- [Secure Password Reset \(1 actions\)](#)
- [User Self-Registration \(1 actions\)](#)
- [MFA Authentication Server \(14 actions\)](#)
- [SSH Public Key Server \(3 actions\)](#)

Object Name: testuser1 Rename

Add Attribute (10): Description / Note Add

Login Name [add values]: testuser1

Last Name [add values]: User1

First Name [add values] [delete attribute]: Test

UID Number: 500

GID Number: 100

Home Directory: /home/testuser1

Login Shell [delete attribute]: /bin/bash

WebADM User Data [delete attribute] Edit Application Data

OpenOTP.LastLogin: 2021-03-22 15:21:01
 OpenOTP.LastOTP: [BINARY APPLICATION DATA - 24 Bytes]
 OpenOTP.LoginCount: 7
 OpenOTP.RejectCount: 6
 OpenOTP.TokenKey: [BINARY APPLICATION DATA - 20 Bytes]
 OpenOTP.TokenState: 53880762
 OpenOTP.TokenType: TOTP

Email Address [add values] [delete attribute]: testmail@rcdevs.com ✉

Group Membership [add values] [delete attribute]:

- cn=testgroup1,o=Root Goto
- cn=testgroup2,o=Root Goto

Apply Changes | Re-Encrypt | Delete Selected

Let's check if WebADM is able to send an email. Therefore, we click under **Application Actions** on **Secure Password Reset**.

LDAP Server 1 (slapd-u) (RCDevs Directory)

WebADM Enterprise Edition v2.0.15
Copyright © 2010-2021 RCDevs Security, All Rights Reserved

Home Admin Cluster Create Search Import Databases Statistics Applications About Logout

Send Password Reset Email / SMS for **cn=testuser1,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:

Domain:

Message Type:

Use Secure Mail: Yes No

Link Expiration:

Use MFA: Yes No

Message Comments:

LDAP Server 1 (slapd-u) (RCDevs Directory)

WebADM Enterprise Edition v2.0.15
Copyright © 2010-2021 RCDevs Security, All Rights Reserved

Home Admin Cluster Create Search Import Databases Statistics Applications About Logout

Send Password Reset Email / SMS for **cn=testuser1,o=Root**

Password reset sent successfully (MAIL)

PwReset@rcvm7.local
LDAP Password Reset
To:

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"
...
```

```
-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=36ea9fbc4b4f5325216f47efd654b7fb.

This is a test mail.
```

4. Configure 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
#
...
# 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"
...
```

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.

```
noreply@rcdevs.com
WebADM Alert (rcvm7.local)
To:

Server: rcvm7.local
Time: 2019-02-27 10:00:34
Alert: Server time drift of 2703 seconds is detected
```

Utilize the `User Alert Setting` feature to notify users via email when a certificate or Active Directory domain password is approaching its expiration date :

| | | |
|--|--|---|
|  User Domains (3) Associate domain names with LDAP user search bases. |  Client Policies (3) Define custom policy settings for consumer applications. |  Access Devices (0) Hardware devices for badging and physical access control. |
|  LDAP Mount Points (3) Connect secondary LDAP servers to the tree view. |  LDAP Option Sets (1) LDAP subtree customizations, alerts and badging features. |  Administrator Roles (1) Create admin role templates for your 'other' administrators. |

User Alert Settings

User Alerts
 Password
 Certificate
 Badging

Periodically alerts users when passwords or certificates will expire. Password near expiration detection works only with ActiveDirectory. Badging sends a warning to users who forgot to badge-out yesterday.

Alert Period
10 (Default) ▾

Start sending alerts 1 to 30 days before expiration.

Alert Repeat
3 (Default) ▾

Re-send alert messages every 1 to 5 days.

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.

```
-bash-4.2# vi /opt/webadm/conf/webadm.conf
#
# WebADM Server Configuration
#
...
# End-user message templates
# The following variables are available: %USERNAME%, %USERDN%, %USERID%, %DOMAIN%,
%APPNAME%
# Additional variables are available depending on the context: %APPNAME%, %APPID%, %TIMEOUT%,
%EXPIRES%
app_unlock_subject "Unlocked access to %APPNAME%"
app_unlock_message "Hello %USERNAME%,\r\n\r\nYou have a one-time access to the
%APPNAME%.\r\n\r\nYour access will automatically expire %EXPIRES%."
ldap_expire_subject "Login password near expiration"
ldap_expire_message "Hello %USERNAME%,\r\n\r\nYour login password will expire %EXPIRES%.\r\n\r\nPlease
reset your password before expiration!\r\n\r\nRegards"
cert_expire_subject "Login certificate near expiration"
cert_expire_message "Hello %USERNAME%,\r\n\r\nYour login certificate will expire %EXPIRES%.\r\n\r\nPlease
renew your certificate before expiration!\r\n\r\nRegards"
```

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

5. Configure Mail OTP

5.1 Normal 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:

The screenshot displays the WebADM Enterprise Edition v2.0.15 interface. The left sidebar shows the directory structure under 'LDAP Server 1 (slapd-u) (RCDevs Directory)'. The main area is titled 'Object cn=testuser1,o=Root' and contains several sections:

- LDAP Actions:** Delete this object, Copy this object, Move this object, Export to LDIF, Change password, Create certificate, Unlock WebApp access, Advanced edit mode.
- Object Details:** Object class(es): webadmAccount, person, posixAc...; Account is unique: Yes (in o=root); WebADM settings: None [CONFIGURE]; WebADM data: 8 data [EDIT]; User activated: Yes Deactivate; Logs and inventory: WebApp, WebScr, Inventory, Record.
- Application Actions:** Secure Password Reset (1 actions), User Self-Registration (1 actions), MFA Authentication Server (14 actions), SSH Public Key Server (3 actions).
- User Attributes:**
 - Object Name: testuser1
 - Add Attribute (10): Description / Note
 - Login Name: testuser1
 - Last Name: User1
 - First Name: Test
 - UID Number: 500
 - GID Number: 100
 - Home Directory: /home/testuser1
 - Login Shell: /bin/bash
 - WebADM User Data: Edit Application Data (OpenOTP.LastLogin: 2021-03-22 15:21:01, OpenOTP.LastOTP: [BINARY APPLICATION DATA - 24 Bytes], OpenOTP.LoginCount: 7, OpenOTP.RejectCount: 6, OpenOTP.TokenKey: [BINARY APPLICATION DATA - 20 Bytes], OpenOTP.TokenState: 53880762, OpenOTP.TokenType: TOTP)
 - Email Address: benoit@rcdevs.com
 - Group Membership: cn=testgroup1,o=Root, cn=testgroup2,o=Root

At the bottom, there are buttons for 'Apply Changes', 'Re-Encrypt', and 'Delete Selected'.

Choose **MFA Authentication Server** 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.

LDAP Server 1 (slapd-u) | WebADM Enterprise Edition v2.0.15
Copyright © 2010-2021 RCDevs Security, All Rights Reserved

Home Admin Cluster Create Search Import Databases Statistics Applications About Logout

Application Settings for cn=testuser1,o=Root

Applications

- MFA Authentication Server
- SSH Public Key Server
- OpenID & SAML Provider
- Secure Password Reset
- User Self-Service Desk
- User Self-Registration

Authentication Policy

Login Mode LDAPOTP (Default)

The login mode (required login factors) should be adjusted via Client Policies.

- LDAPOTP: Require both LDAP and OTP passwords.
- LDAPU2F: Require both LDAP and FIDO response.
- LDAPMFA: Require LDAP and either OTP or FIDO.
- LDAP: Require LDAP password only.
- OTP: Require OTP password only.

OTP Type MAIL

- TOKEN: OATH HOTP/TOTP/OCRA, YubiKey or MobileOTP Token.
- SMS: SMS one-time password (On-demand or Prefetched).
- MAIL: Email one-time password (On-demand or Prefetched).
- LIST: Pre-generated OATH OTP password list (to be printed).
- VOICE: Voice biometrics authenticator (requires license option).
- PROXY: Forward requests to another RADIUS server (for migrations).

OTP Fallback TOKEN

Fallback OTP Type to be used as secondary authentication method.
SMS/MAIL OTPs are delayed for MobileTimeout seconds before being sent.
LASTOTP let users use the last validated OTP which expires after a delay.
Use DISABLED to disabled fallback if there is a configuration by default.

OTP Password Length 6 (Default)

Note: This setting is ignored for OCRA Tokens as OTP length is part of the OCRA Suite.
Warning: Changing this setting after having registered OATH Tokens will invalidate these Tokens.

OTP PIN Prefix Yes No (default)

When enabled a static prefix has to be prepended to any OTP password in the form [PIN][OTP].
The OTP Prefix must be registered first and must be at least 4 alpha-numeric characters.

Mobile Response Timeout 30 (Default)

Time to wait for mobile response with Token Simple Push before switching to a fallback method.
Changing the default value requires to adjust client timeouts (ex. RADIUS request timeout) accordingly!
Note: This timeout applies to MSS mobile responses as well (MobileID SMS delivery mode).

Challenge Session Timeout 600

Timeout to wait for a challenge response (in seconds).
Note: SMS OTP and MAIL OTP may requires longer timeouts.

User Notifications

Send Expire Notification MAIL

Send a notification email/SMS to the user when his LDAP password or OTP Token expired.
The email subject and sender address are defined in the MAIL OTP Settings.
The SMS sender number is defined in the SMS OTP Settings.

Send Blocking Notification MAIL

Send a notification email/SMS to the user when his account gets blocked.
The email subject and sender address are defined in the MAIL OTP Settings.
The SMS sender and message type are defined in the SMS OTP Settings.

Send Self-Registration Links Yes No (default)

Automatically send a self-registration email/SMS to the user has no Token registered or Token expired.
This feature applies to the expiration of OTP List and Application Passwords too.
Note: Requires the SelfReg WebApp to be installed.

Send Password Reset Links Yes No (default)

Automatically send a password reset email/SMS to the user password expired or must be changed.
Note: Requires the PwReset WebApp to be installed.

Finally, the last options for OpenOTP. OnDemand Email Delivery Mode means a new OTP is sent when the user starts an authentication process.

LDAP Server 1 (slapd-u) | WebADM Enterprise Edition v2.0.15
Copyright © 2010-2021 RCDevs Security, All Rights Reserved

Home Admin Cluster Create Search Import Databases Statistics Applications About Logout

MAIL OTP

Use Secure Email Yes No (default)

Encrypt OTP email with the user certificate public key (S-MIME).

Email Delivery Mode Ondemand (Default)

Ondemand: A new OTP is sent when the user starts an authentication process.
Prefetch: The next OTP is sent after the user performed an authentication.

Let's test the Mail OTP by clicking **MFA Authentication Server** under **Application Actions**.

The screenshot shows the WebADM Enterprise Edition v2.0.15 interface. The main content area displays the details for the user object **cn=testuser1,0=Root**. The interface is divided into several sections:

- LDAP Actions:** A list of administrative actions such as "Delete this object", "Copy this object", "Move this object", "Export to LDIF", "Change password", "Create certificate", "Unlock WebApp access", and "Advanced edit mode".
- Object Details:** Information about the user object, including "Object class(es): webadmAccount, person, posixAc...", "Account is unique: Yes (in e=rcdevs)", "WebADM settings: None [CONFIGURE]", "WebADM data: 8 data [EDIT]", "User activated: Yes Deactivate", and "Logs and inventory: WebApp, WebSrv, Inventory, Record".
- Application Actions:** A dropdown menu showing various actions related to the user's application data, including "Secure Password Reset (1 actions)", "User Self-Registration (1 actions)", "MFA Authentication Server (14 actions)", and "SSH Public Key Server (3 actions)". The "MFA Authentication Server" action is expanded, showing sub-actions like "Register / Unregister OTP Tokens", "Register / Unregister FIDO Devices", "Register / Unregister Voice Biometrics", "Resynchronize Tokens", "Manage OTP PIN Prefix", "Manage OCRA Token PIN Code", "Manage Emergency OTP", "Manage Printed OTP List", "Manage Application Passwords", "Unlock Account", "Import OATH-PSKC File", "Export OATH-PSKC File", "Test User Authentication", and "Test User Confirmation".
- User Attributes:** Fields for "Login Name", "Last Name" (User1), "First Name" (Test), "UID Number" (500), "GiD Number" (100), "Home Directory" (/home/testuser1), "Login Shell" (/bin/bash), "WebADM User Data", "Email Address" (testmail@rcdevs.com), and "Group Membership" (cn=testgroup1,0=Root and cn=testgroup2,0=Root).
- Edit Application Data:** A section showing application-specific data like "OpenOTP.LastLogin: 2021-03-22 15:21:01", "OpenOTP.LastOTP: [BINARY APPLICATION DATA - 24 Bytes]", "OpenOTP.LoginCount: 7", "OpenOTP.RejectCount: 6", "OpenOTP.TokenKey: [BINARY APPLICATION DATA - 20 Bytes]", "OpenOTP.TokenState: 53880762", and "OpenOTP.TokenTypes: TOTP".

At the bottom of the interface, there are buttons for "Apply Changes", "Re-Encrypt", and "Delete Selected".

Now click on **Test User Authentication**.

LDAP Server 1 (slapd-u) (f) WebADM Enterprise Edition v2.0.15
 Copyright © 2010-2021 RCDevs Security. All Rights Reserved

Home Admin Cluster Create Search Import Databases Statistics Applications About Logout

OpenOTP User Actions for cn=testuser1,o=Root (14)

Find below the user actions supported by MFA Authentication Server (OpenOTP).

- Register / Unregister OTP Tokens**
 You must register a hardware or software Token before a user can start using it.
- Register / Unregister FIDO Devices**
 You must register a FIDO Device before a user can start using it.
- Register / Unregister Voice Biometrics**
 Enrol your voice fingerprint for voice biometrics authentication.
- Resynchronize Tokens**
 Event-based and time-based tokens can get out of sync. You can use the action to resync the Token counter or clock drift.
- Manage OTP PIN Prefix**
 Set an OTP PIN if you want the OTP passwords to be prepended by a static PIN password. Any OTP password will have to be prefixed by the static PIN code in the form [PIN][OTP].
- Manage OCRA Token PIN Code**
 Only OCRA Tokens support a PIN code feature. Use this action to set or reset the PIN code on the user account.
- Manage Emergency OTP**
 An emergency OTP is an auto-expirable static OTP which can be used when the user cannot use his usual OTP/FIDO method and requires a temporary access.
- Manage Printed OTP List**
 You can use this action to register, remove, display and download user OTP Lists.
- Manage Application Passwords**
 You can use this action to register, remove and display per-application passwords.
- Unblock Account**
 You can use this action to unblock an account after the max authentication attempts has been reached.
- Import OATH-PSKC File**
 You can use the action to import a PSKC (RFC-6030) OATH Token key file.
- Export OATH-PSKC File**
 You can use the action to export the registered OATH Token to a PSKC (RFC-6030) file.
- Test User Authentication**
 You can use this action to test a user authentication with OpenOTP.
- Test User Confirmation**
 You can use this action to test a transaction confirmation with OpenOTP.

Cancel

https://192.168.3.185:1443/admin/action_page.php?websrv=openotp&page=testlogin&dn=cn=testuser1,o=Root

Type in your LDAP password if the **Login Mode** is set to **LDAPOTP** . Click the **Start** button.

LDAP Server 1 (slapd-u) (F) WebADM Enterprise Edition v2.0.15
 Copyright © 2010-2021 RCDevs Security, All Rights Reserved

Home Admin Cluster Create Search Import Databases Statistics Applications About Logout

Test User Authentication for **cn=testuser1,o=Root**

You can use this page to test a user OpenOTP authentication request. Some fields are optional and depend on your OpenOTP configuration.

Server Status: **Accepting Requests**

Server: MFA Authentication Server 1.5.7 (WebADM 2.0.15)
 System: Linux 5.8.0-44-generic x86_64 (64 bit)
 Listener: 10.1.0.105:8080 (HTTP/1.1 SSL)
 Uptime: 158067s (1 days)
 Cluster Node: 1/3 (Session Server 1 (webadm-u))
 Local Memory: 0M (33M total)
 Shared Memory: 2M (256M total)
 Connectors: OK (4 alive & 0 down)

Login Method: Normal Simple

Username:

Domain:

LDAP Password:

OTP Password:

Simulated Client:

Simulated Source:

Simulated Options:

Request Settings:

Virtual Attributes:

Browser Context:

Debug Mode: (enable debug logs for this request)

Now, switch to your email client and check your mail.

LDAP Server 1 (slapd-u) (F) WebADM Enterprise Edition v2.0.15
 Copyright © 2010-2021 RCDevs Security, All Rights Reserved

Home Admin Cluster Create Search Import Databases Statistics Applications About Logout

Test User Authentication for **cn=testuser1,o=Root**

Result: **Challenge (OTP)**

Message: Enter your TOKEN password

Timeout: 85 seconds

OTP Password:

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](#).

The screenshot shows the WebADM Enterprise Edition v2.0.15 interface. On the left is a tree view of the LDAP Server 1 (slapd-u) structure, including RCDevs Directory (2), dc=WebADM, o=Root (6), and several users and groups. The main panel displays the 'Test User Authentication for cn=testuser1,o=Root' page. The 'Result' is 'Challenge (OTP)', the 'Message' is 'Enter your MAIL password', and the 'Timeout' is '77 seconds'. There is an input field for the 'OTP Password' with six dots, and 'Continue' and 'Cancel' buttons.

The screenshot shows the same WebADM Enterprise Edition v2.0.15 interface. The 'Test User Authentication for cn=testuser1,o=Root' page now shows a 'Result: Success' and a 'Message: Authentication success'. There are 'Ok' and 'Cancel' buttons.

5.2 Encrypt Mail OTP

First, enable the option [Use Secure Email](#) (on an activated user account, go in [object Details](#) box, click on [CONFIGURE](#) button and choose [MFA Authentication Server](#) from the [Applications](#) box)

The screenshot shows the WebADM Enterprise Edition v2.0.15 interface with the 'MAIL OTP' configuration page. The 'Use Secure Email' checkbox is checked, and the 'Email Delivery Mode' is set to 'Ondemand (Default)'. The 'Yes' radio button is selected for the 'Use Secure Email' option. The page also includes explanatory text for 'Ondemand' and 'Prefetch' modes.

Now, create a certificate through WebADM for the user in question. In this example, select the `testuser1` on the left side and click on `Create certificate`.

The screenshot shows the WebADM Enterprise Edition v2.0.15 interface. On the left sidebar, the 'LDAP Server 1 (slapd-u)' tree is expanded to 'o=Root (6)', and 'cn=testuser1' is selected. The 'Create certificate' option is highlighted in the sidebar. The main panel displays the configuration for 'Object cn=testuser1,o=Root'. The 'LDAP Actions' section includes 'Create certificate'. The 'Object Details' section shows 'Object class(es): webadmAccount_person_posixAc...', 'Account is unique: Yes (in o=root)', 'WebADM settings: 1 settings [CONFIGURE]', 'WebADM data: 8 data [EDIT]', 'User activated: Yes Deactivate', and 'Logs and inventory: WebApp, WebSrv, Inventory, Record'. The 'Application Actions' section includes 'Secure Password Reset (1 actions)', 'User Self-Registration (1 actions)', 'MFA Authentication Server (14 actions)', and 'SSH Public Key Server (3 actions)'. The main form contains fields for 'Object Name' (testuser1), 'Add Attribute (9)', 'Login Name' (testuser1), 'Last Name' (User1), 'First Name' (Test), 'UID Number' (500), 'GID Number' (100), 'Home Directory' (/home/testuser1), 'Login Shell' (/bin/bash), 'Email Address' (testmail@rcdevs.com), 'WebADM Settings', 'WebADM User Data', and 'Group Membership' (cn=testgroup1,o=Root and cn=testgroup2,o=Root). At the bottom, there are buttons for 'Apply Changes', 'Re-Encrypt', and 'Delete Selected'.

Now, click the `Create Cert` button.

The screenshot shows the 'New User Certificate Value(s) for cn=testuser1,o=Root' configuration page. The left sidebar is the same as in the previous screenshot. The main panel contains the following fields: 'Certificate validity (in days):' (input field), 'Certificate export format:' (PKCS12), 'Email address:' (testmail@rcdevs.com), 'Send email notification:' (radio buttons for Yes and No, with No selected), 'Certificate usage:' (radio buttons for Admin and User, with User selected), and 'User domain:' (Default). At the bottom, there are buttons for 'Create Cert', 'Import Cert', and 'Cancel'.

Click the `Download` button to download the user's certificate. Import the certificate into your mail client.

LDAP Server 1 (slapd-u)

WebADM Enterprise Edition v2.0.15
Copyright © 2010-2021 RCDevs Security. All Rights Reserved

Home | Admin | Cluster | Create | Search | Import | Databases | Statistics | Applications | About | Logout

New User Certificate for **cn=testuser1,o=Root**

Creating private key... **Success**
Reading infos from LDAP user... **Success**

Certificate details:
- emailAddress: **testmail@rcdevs.com**
- commonName: **Defaulttestuser1**
- userid: **testuser1**
- domainComponent: **Default**
- description: **USER**
- surname: **User1**

Creating a certificate request based on the above details... **Success**
Calling WebADM CA for certificate request signing... **Success**
Checking certificate data... **Success**
Storing certificate in LDAP... **Success**
Updating OCSP cache... **Success**
Creating a PKCS12 package... **Success**

Certificate installation password: fJmp05Q3

The certificate and private key have been bundled into a PKCS12 package.
Click the button below to download the new certificate package.

[Download](#) [Ok](#)

Let's verify if the email is encrypted. Do the same steps as in the previous chapter for the **Test User Authentication**.

noreply@rcdevs.com

OpenOTP Login

To:

Security: Encrypted

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 Security 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 Security 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 Security 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 Security S.A. The latter especially applies for data processing systems. RCDevs Security 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 Security. © 2024 RCDevs Security S.A., All Rights Reserved