EMAIL (OTP, ALERTS)

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#
```

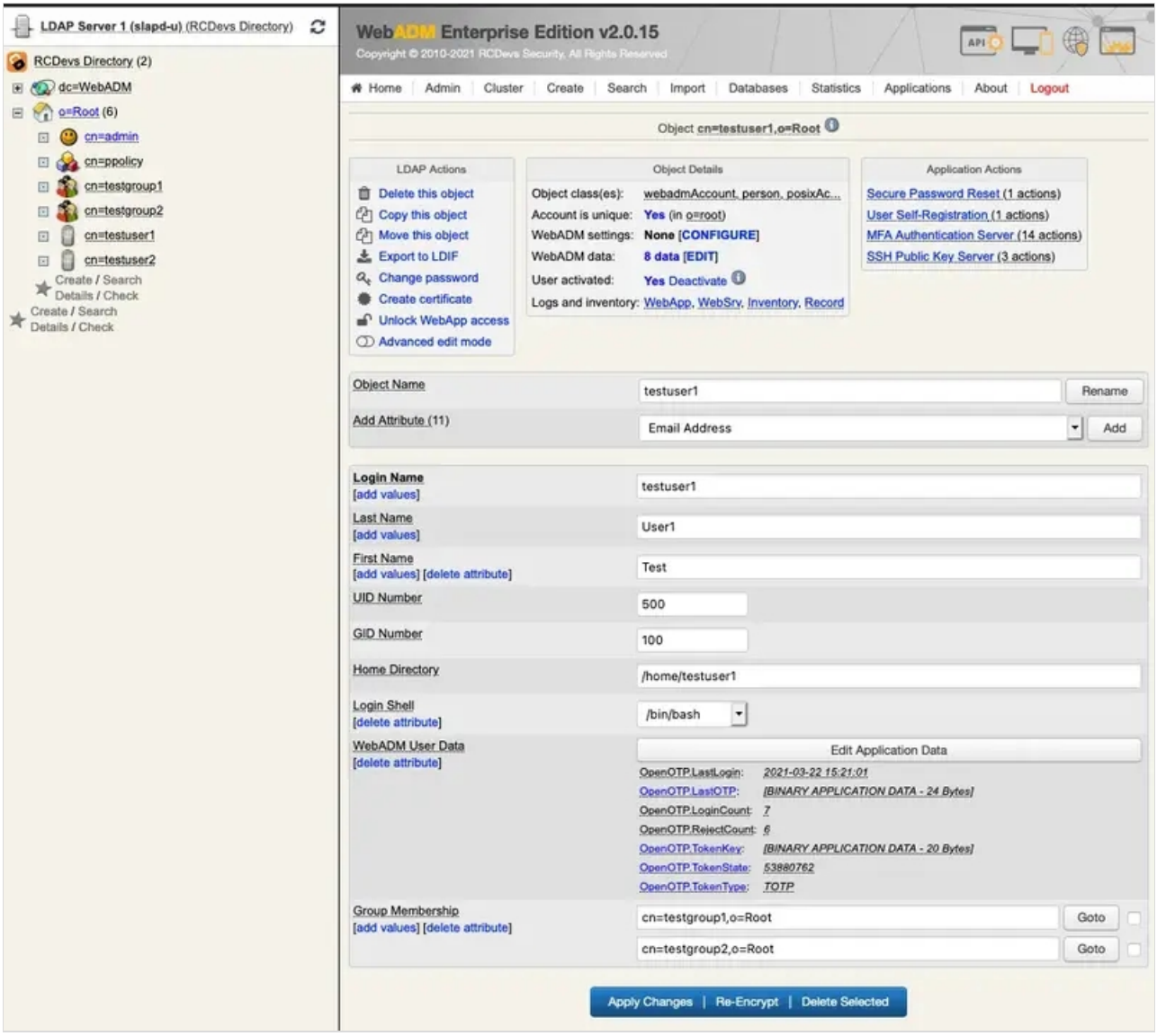
In this example, the password has been encrypted.

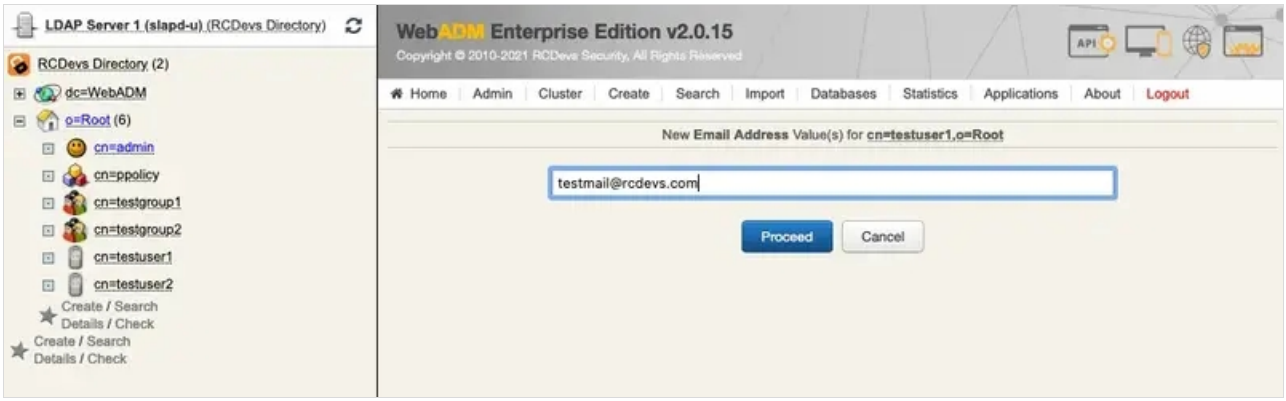
The encryption mechanism is bound to secret data in your encoded license file and is available for free and enterprise licenses starting from version 2 of WebADM. Prior to version 2 of WebADM, this feature requires an Enterprise License. Please follow this documentation RCDevs Utilities and Command Line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

3. Configure and test email

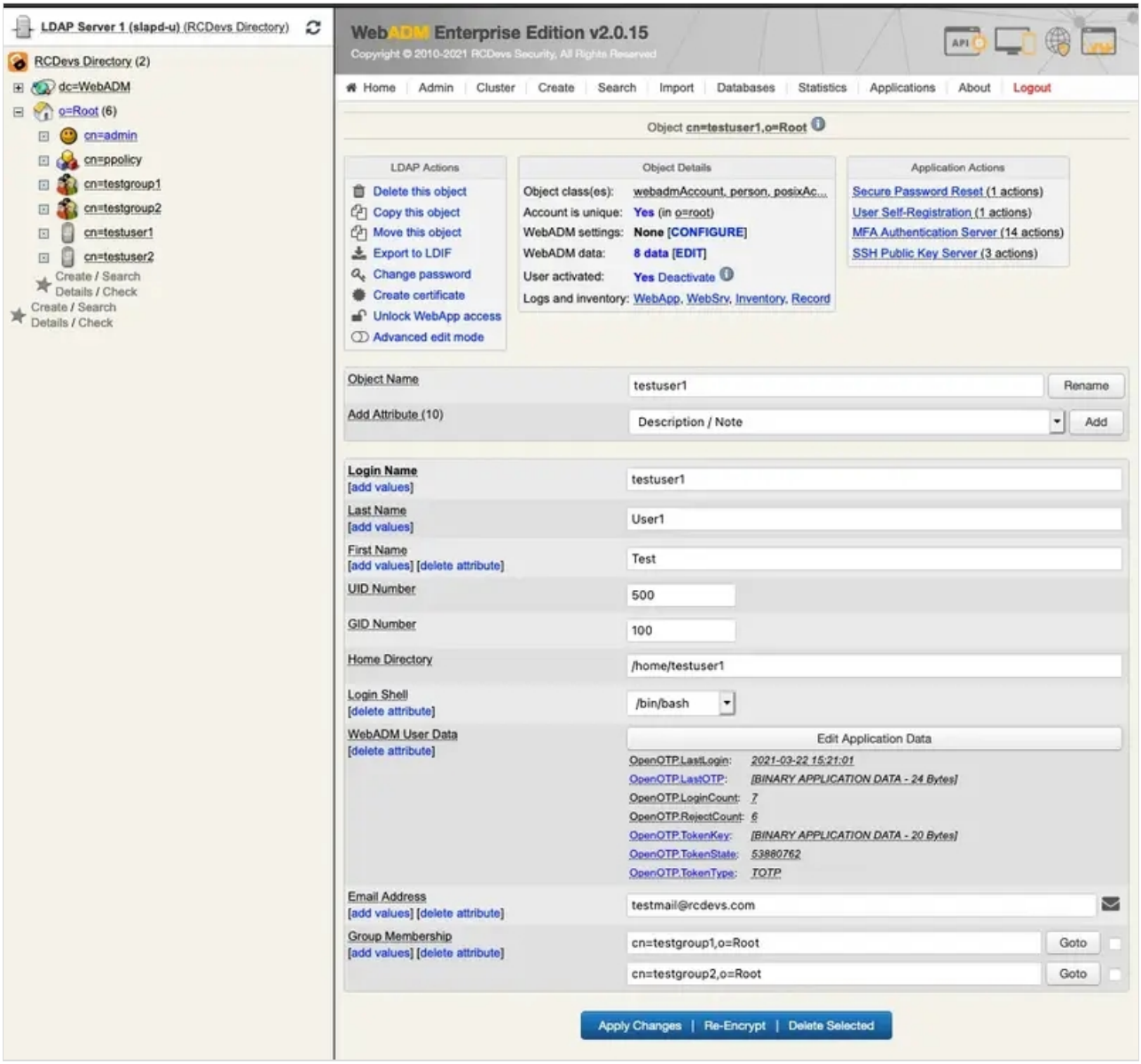
3.1 Test Email

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

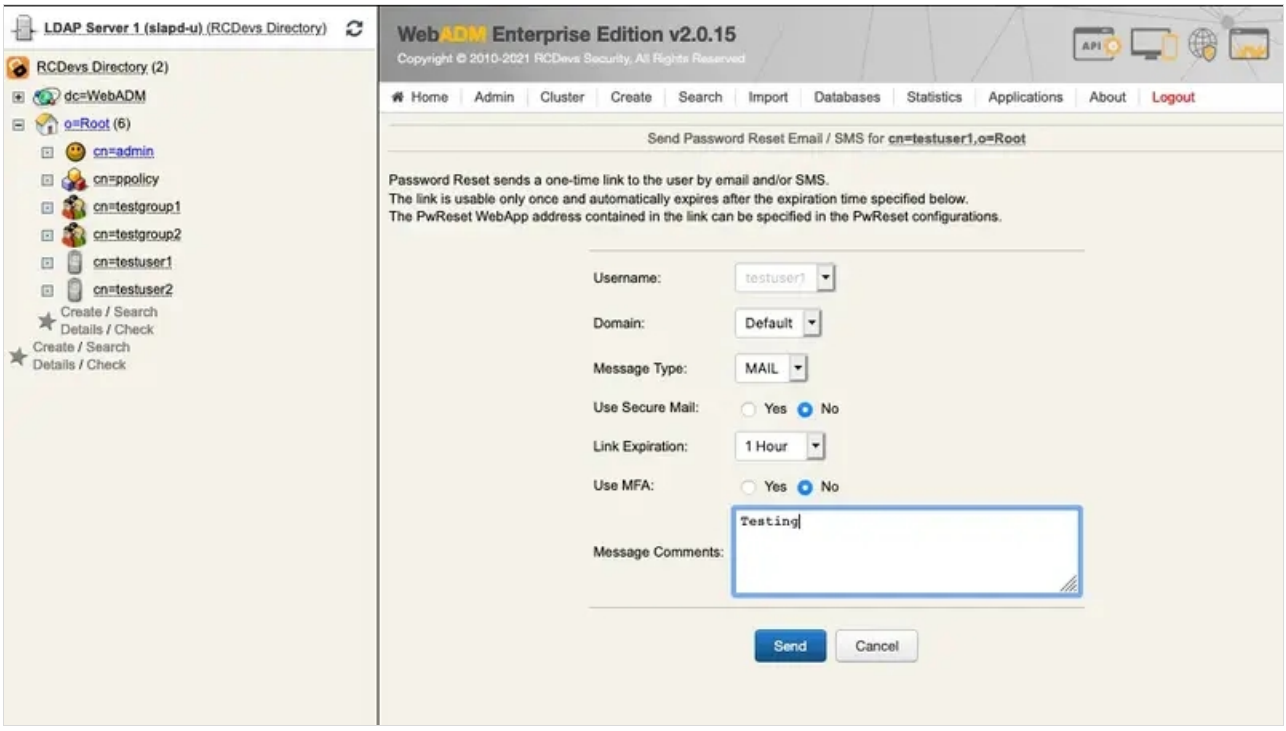


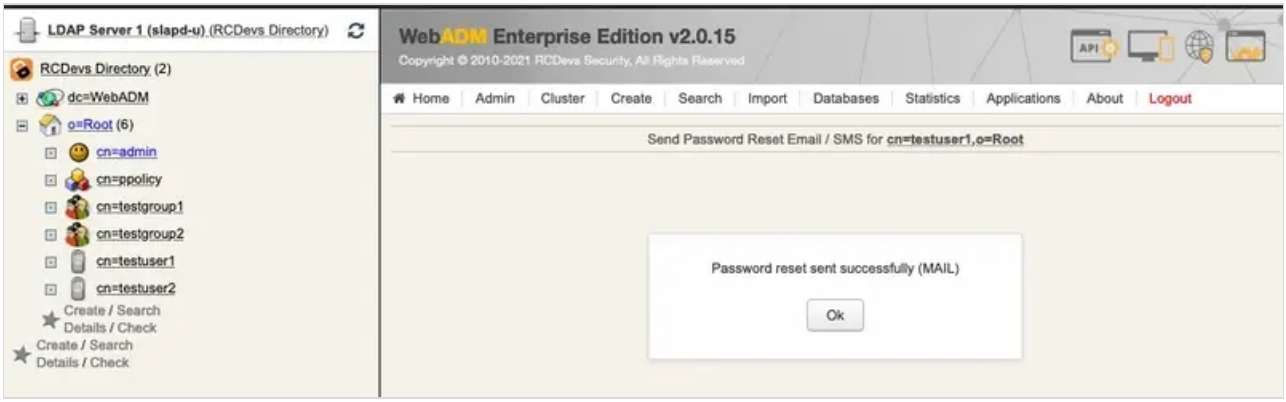


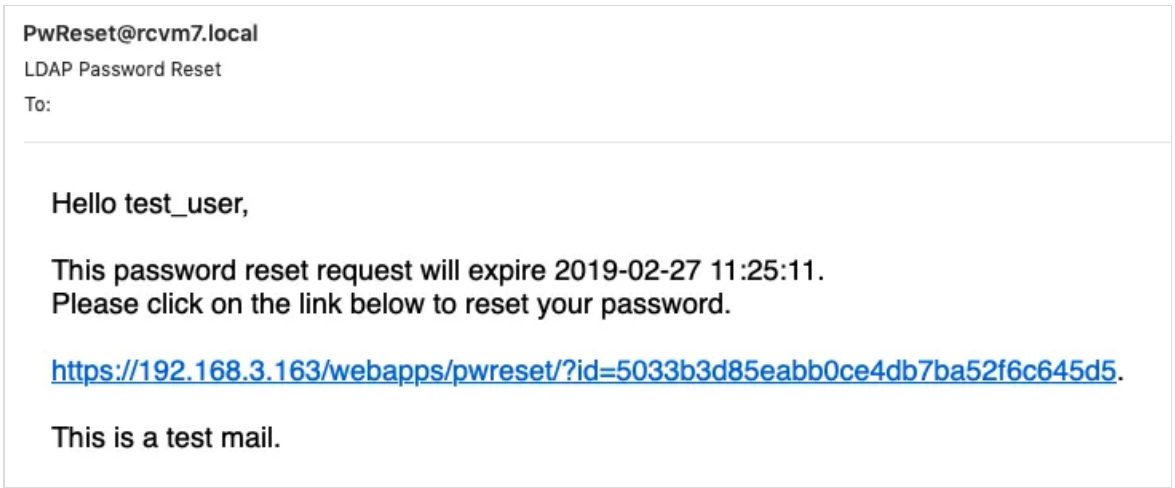
Now, the `testuser1` has got an email address.



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







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

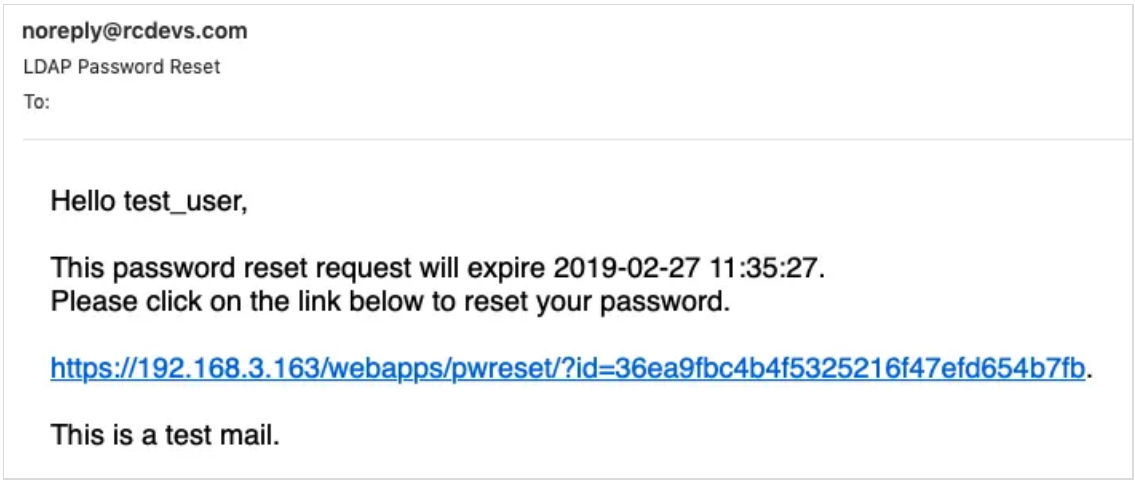
3.2 Sender Email

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`.



4. Configure Alerts

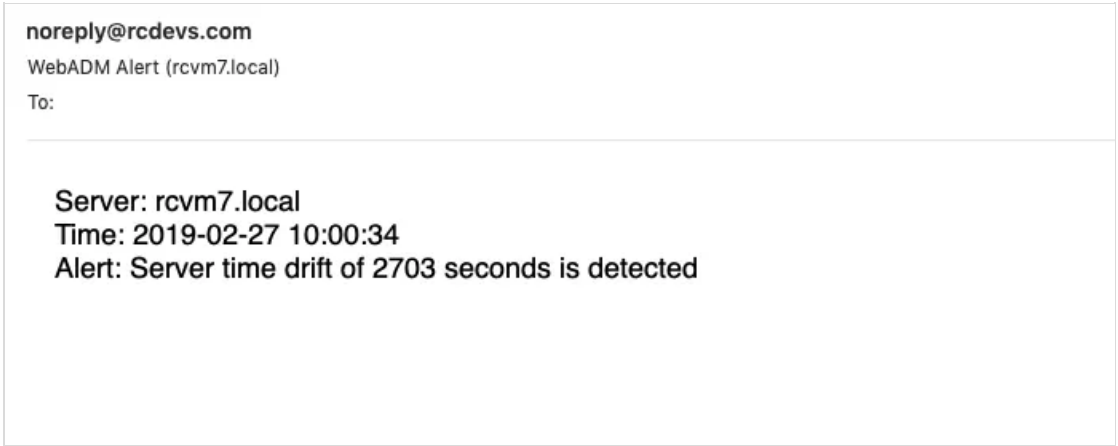
Alerts are always recorded to the SQL Alert log. Additionally, when `alert_email` is defined, the alerts are also sent by email.

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`.

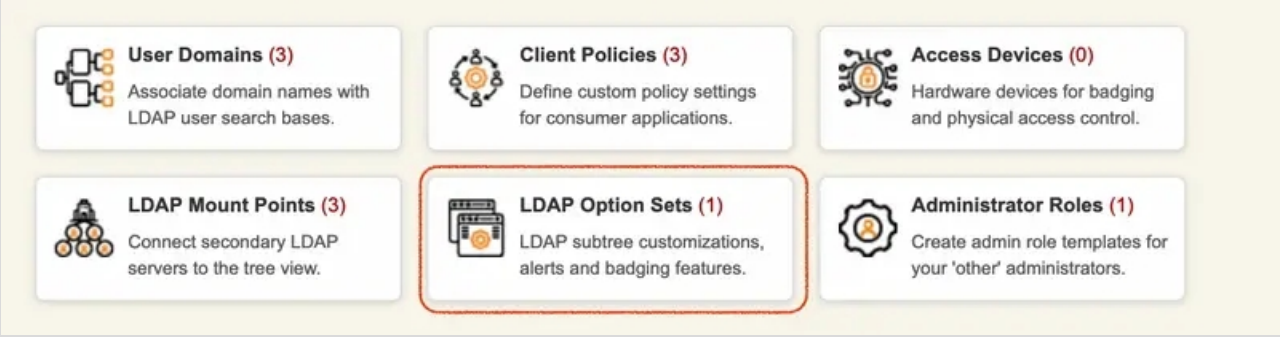
```
-bash-4.2# vi /opt/webadm/conf/webadm.conf
#
# WebADM Server Configuration
#
...
# Alerts are always recorded to the SQL Alert log. Additionally, when alert_email
# or alert_mobile is defined, the alerts are also sent by email/SMS.
#alert_email "me@mydomain.com"
#alert_mobile "+33 12345678"
...
```

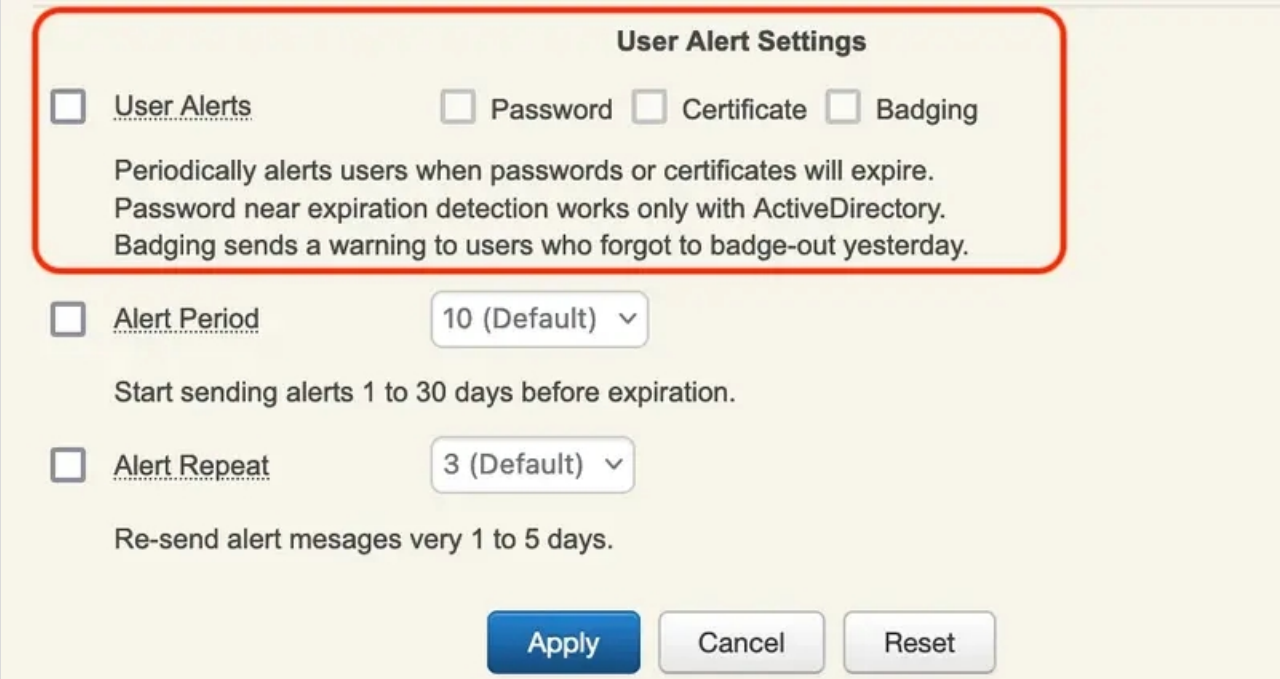
```
-bash-4.2# vi /opt/webadm/conf/webadm.conf
#
# WebADM Server Configuration
#
...
# Alerts are always recorded to the SQL Alert log. Additionally, when alert_email
# or alert_mobile is defined, the alerts are also sent by email/SMS.
alert_email "testmail@rcdevs.com"
#alert_mobile "+33 12345678"
...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

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.



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





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\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\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\nPlease
renew your certificate before expiration!\r\n\r\nRegards"
```

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

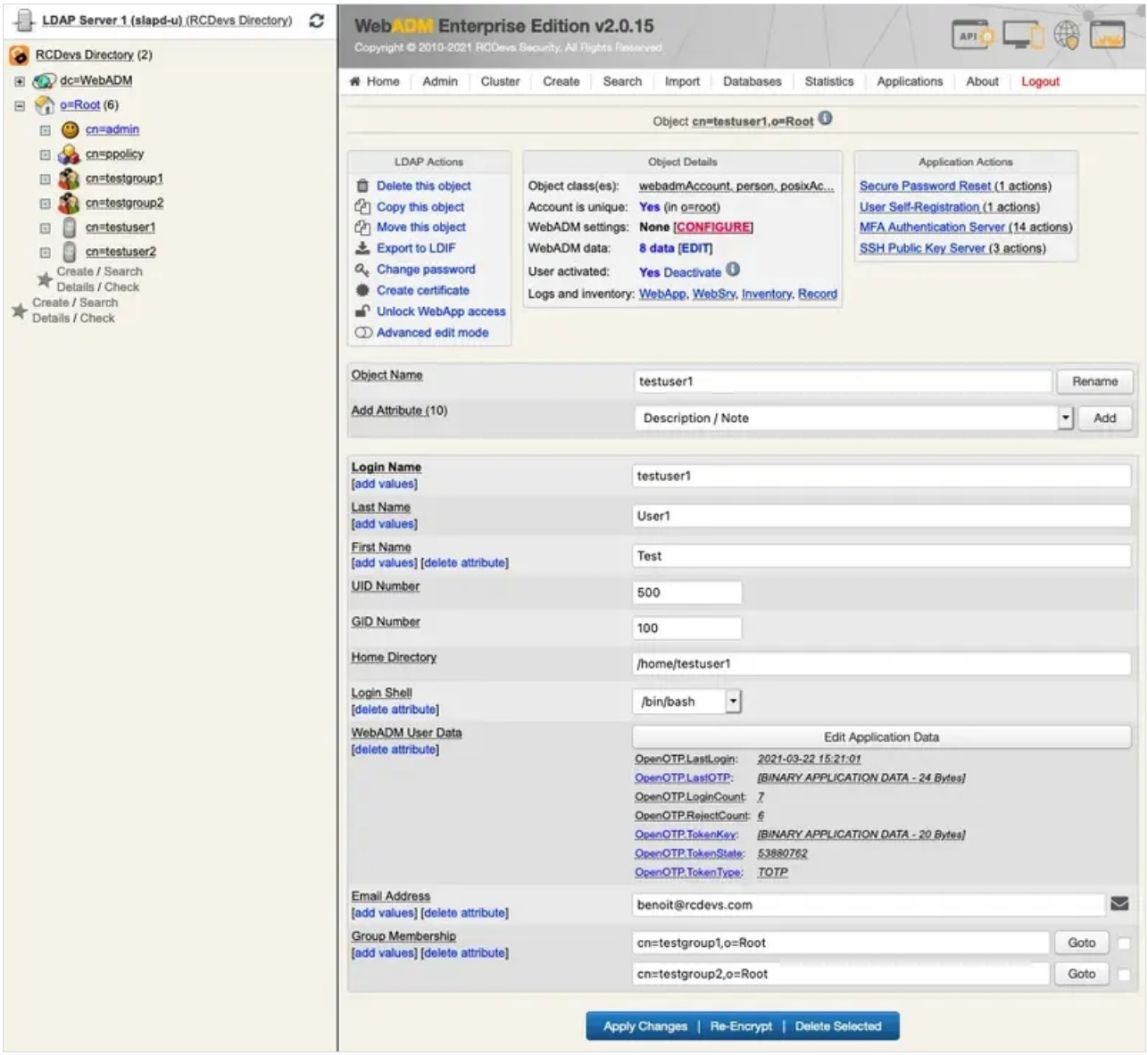
5. Configure Mail OTP

5.1 Normal Mail OTP

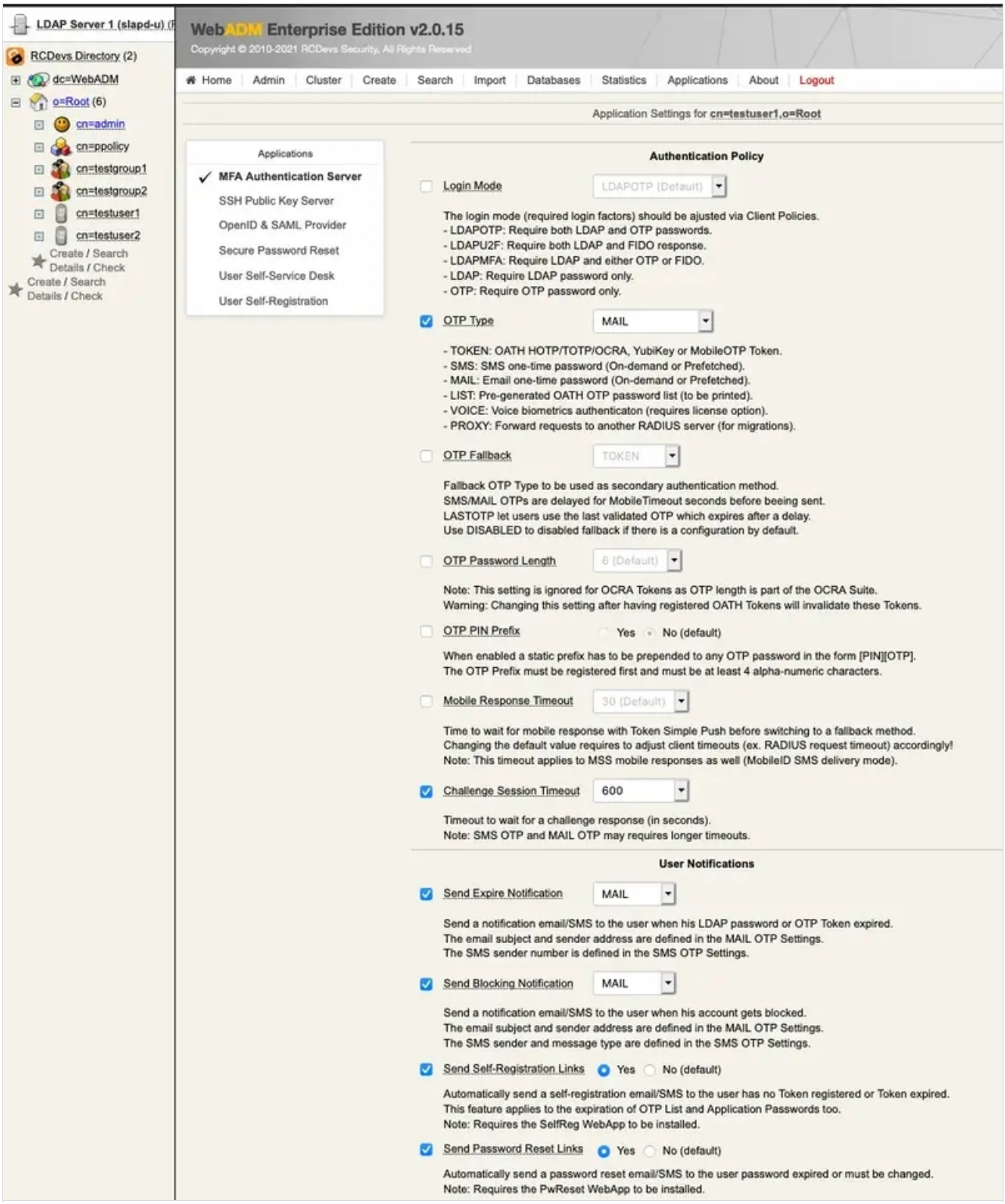
To receive an OTP via Email, the user must have a mail value configured in mail or othermail attributes. To enable the OTP by Mail, there are multiple ways:

- Under OpenOTP global configuration,
- Under OpenOTP user settings configuration,
- Under OpenOTP client policy configuration,

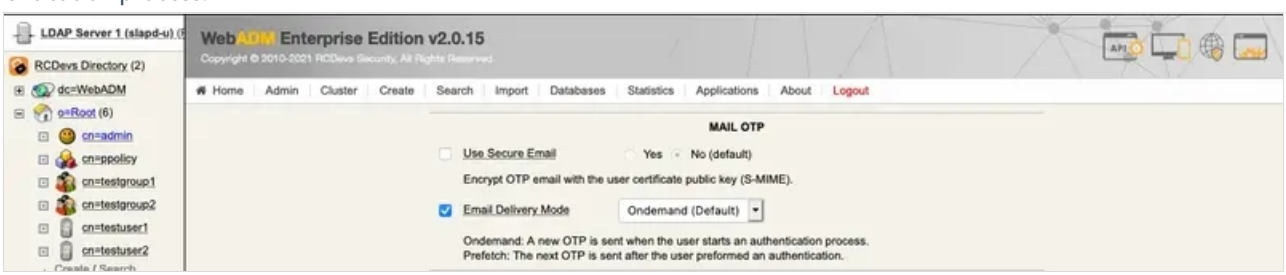
The `OTP Type` setting must be set to MAIL. In the following scenario, we use option 2 and will configure the WebADM user setting on the user object. On an activated user account, in `object Details` box, click on `CONFIGURE` button:



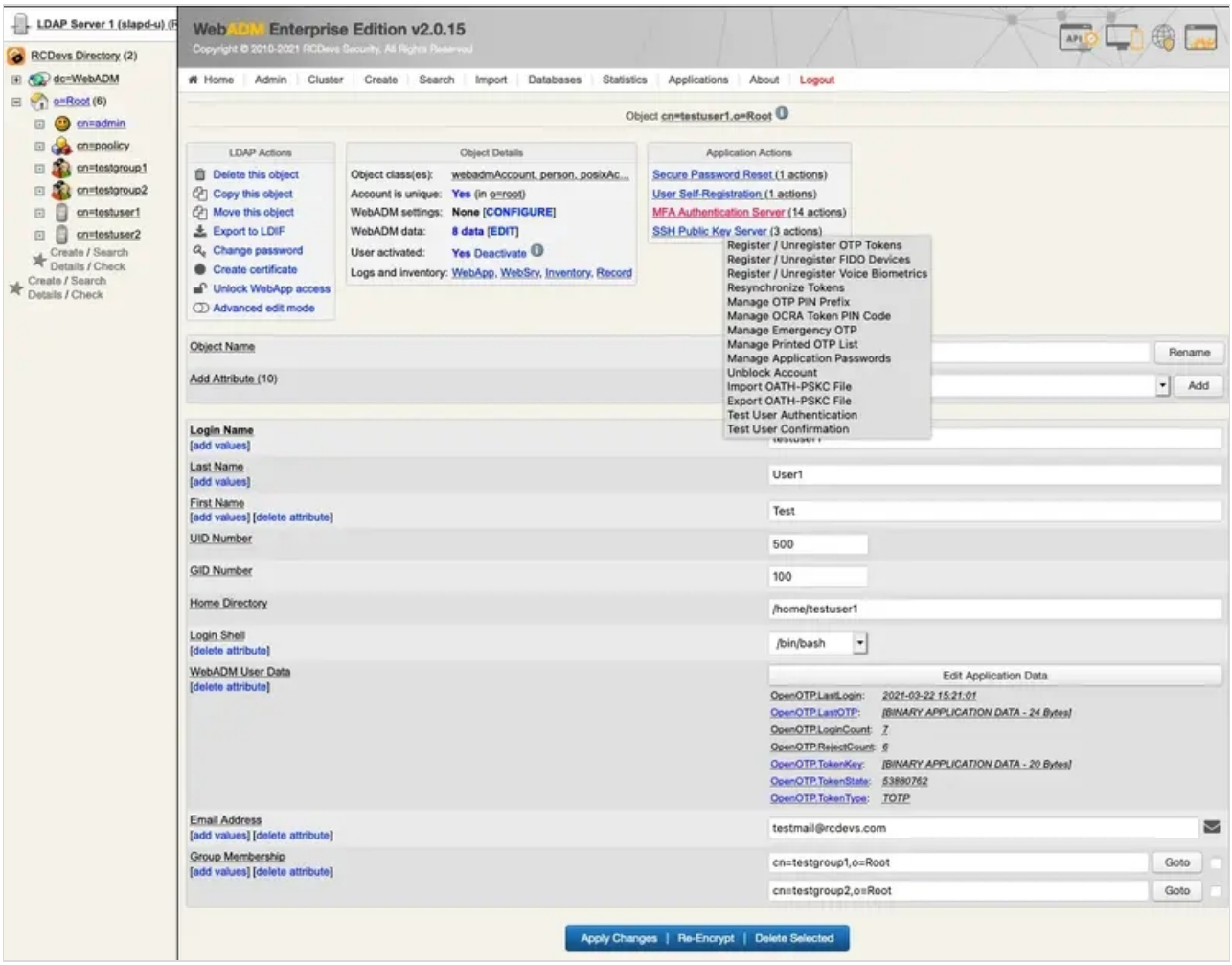
Choose `MFA Authentication Server` from the `Applications` box and set `OTP Type` to `MAIL`. Note that `MAIL OTP` may require longer timeouts, therefore enable the option `Challenge Session Timeout`. Furthermore, if needed, enable the options under `User Notifications` as shown below.



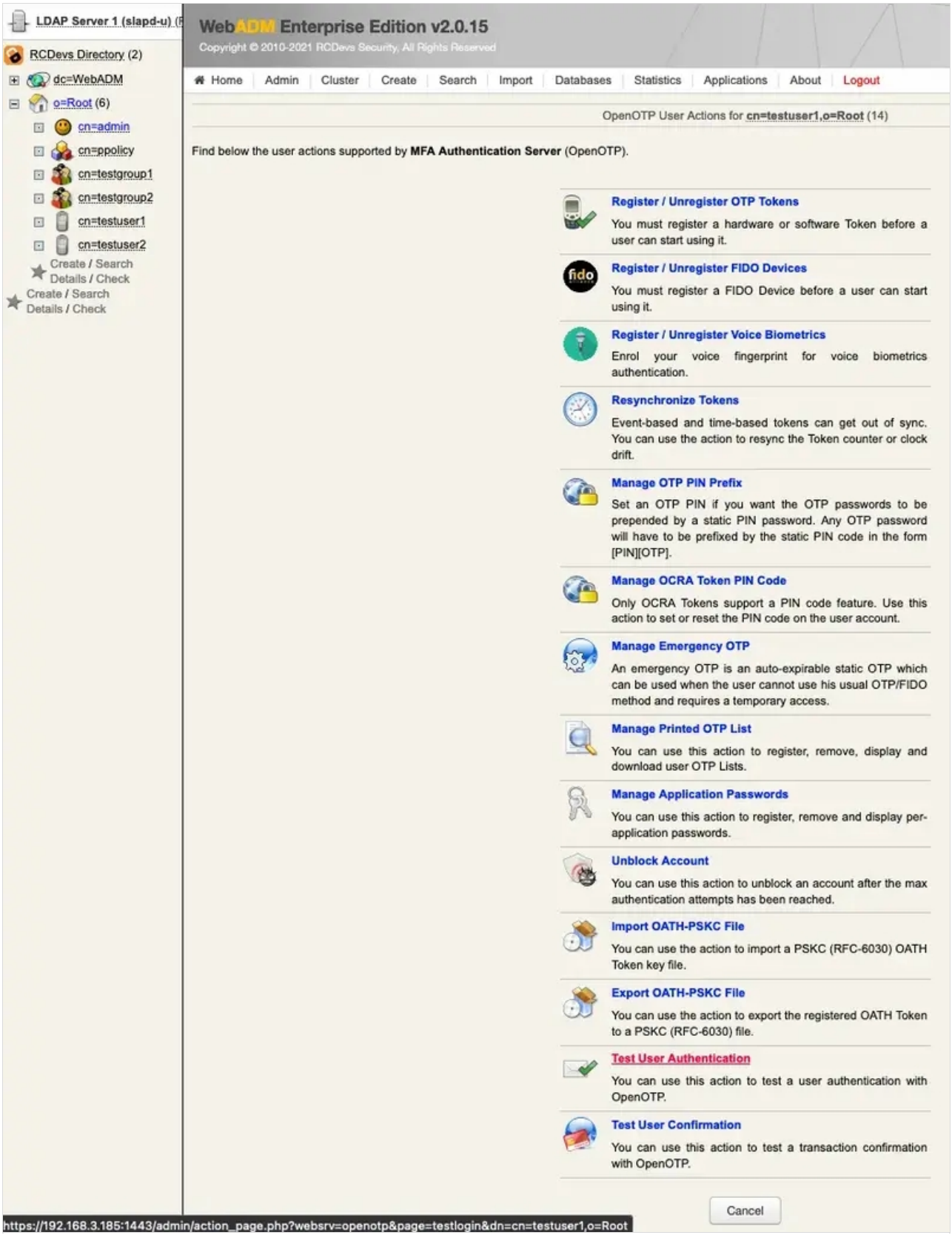
Finally, the last options for OpenOTP. OnDemand Email Delivery Mode means a new OTP is sent when the user starts an authentication process.



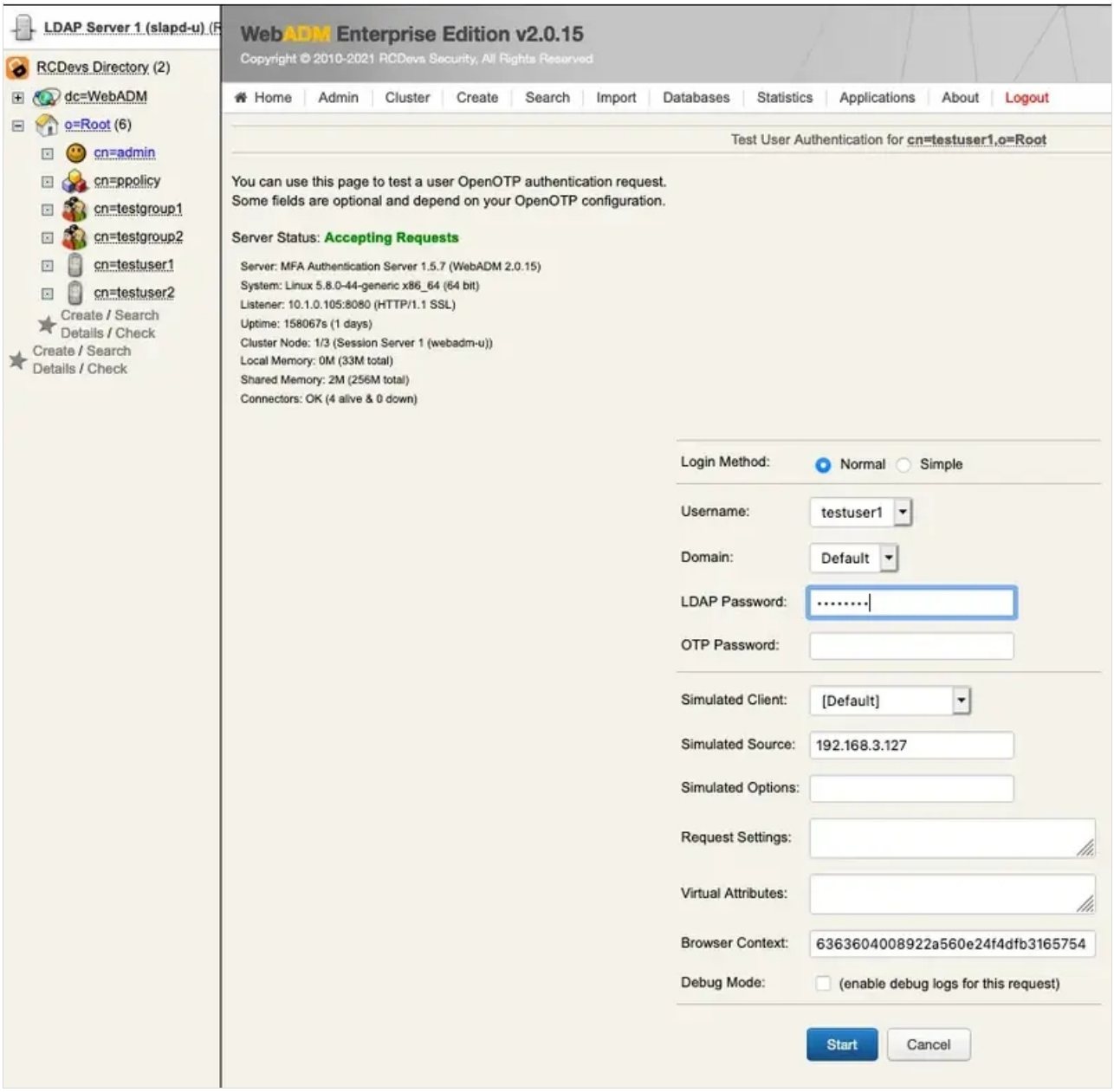
Let's test the Mail OTP by clicking `MFA Authentication Server` under `Application Actions`.



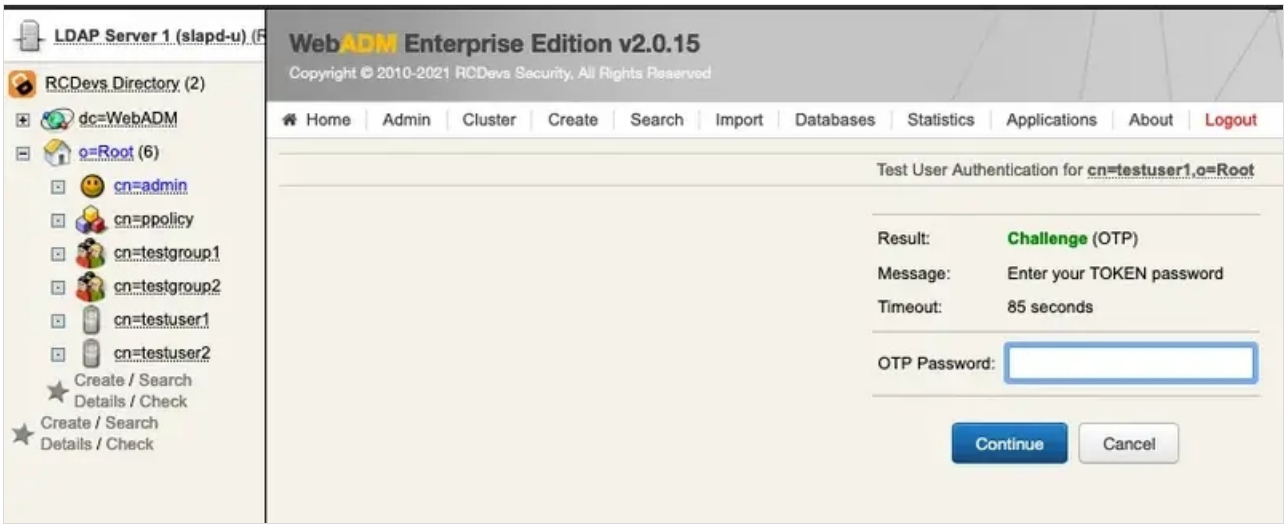
Now click on `Test User Authentication`.

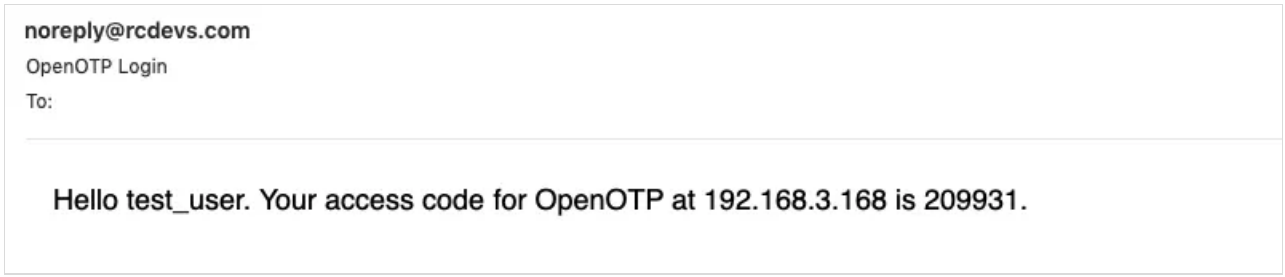


Type in your LDAP password if the `Login Mode` is set to `LDAPOTP`. Click the `Start` button.

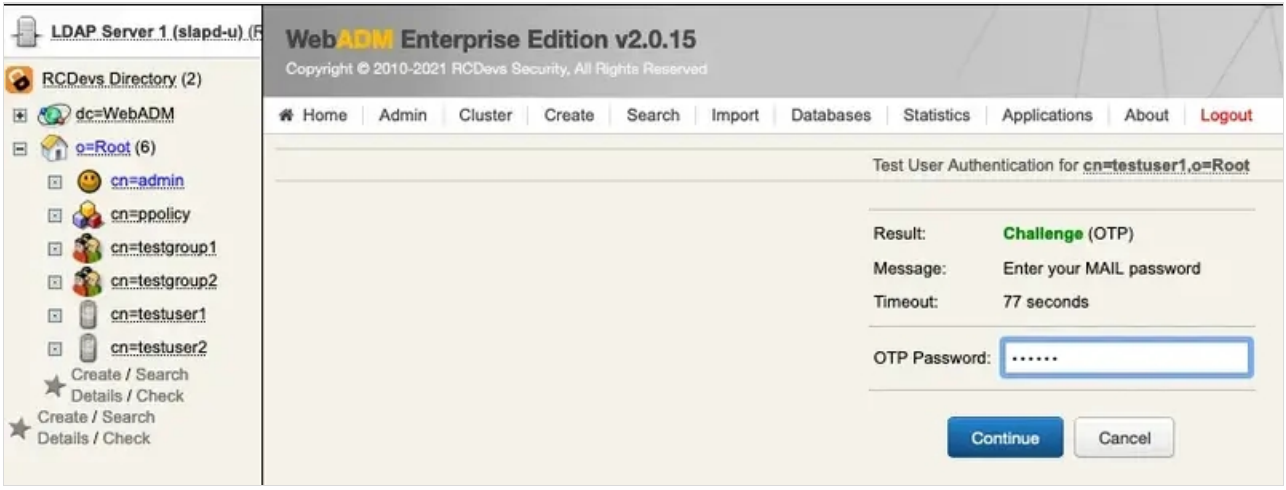


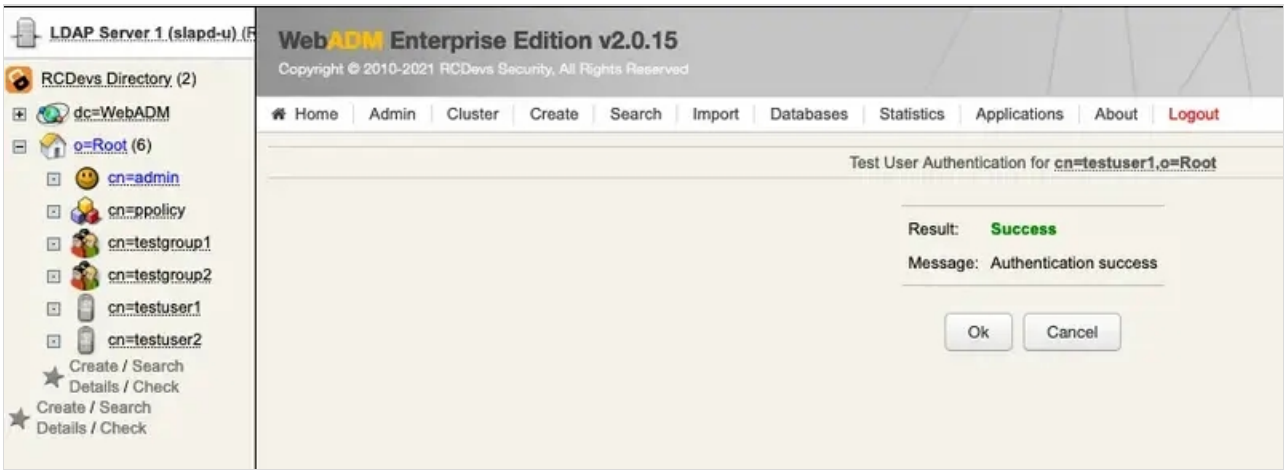
Now, switch to your email client and check your mail.





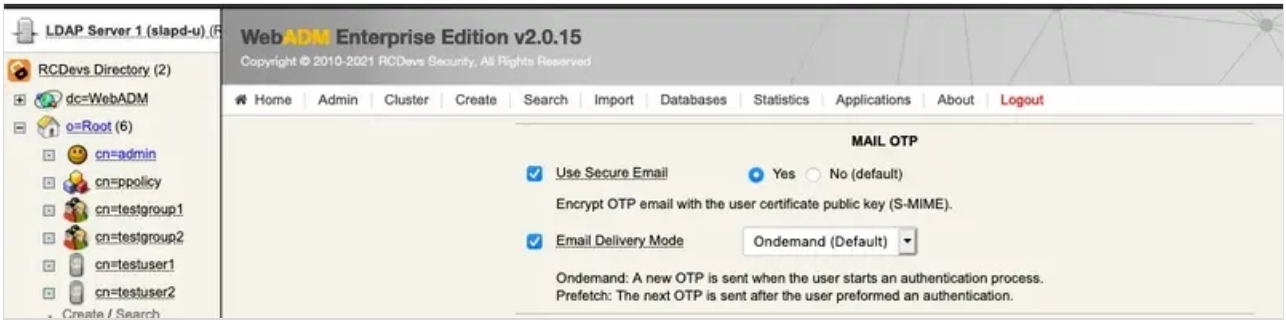
Finally, enter your OTP from the email and click `Continue`.



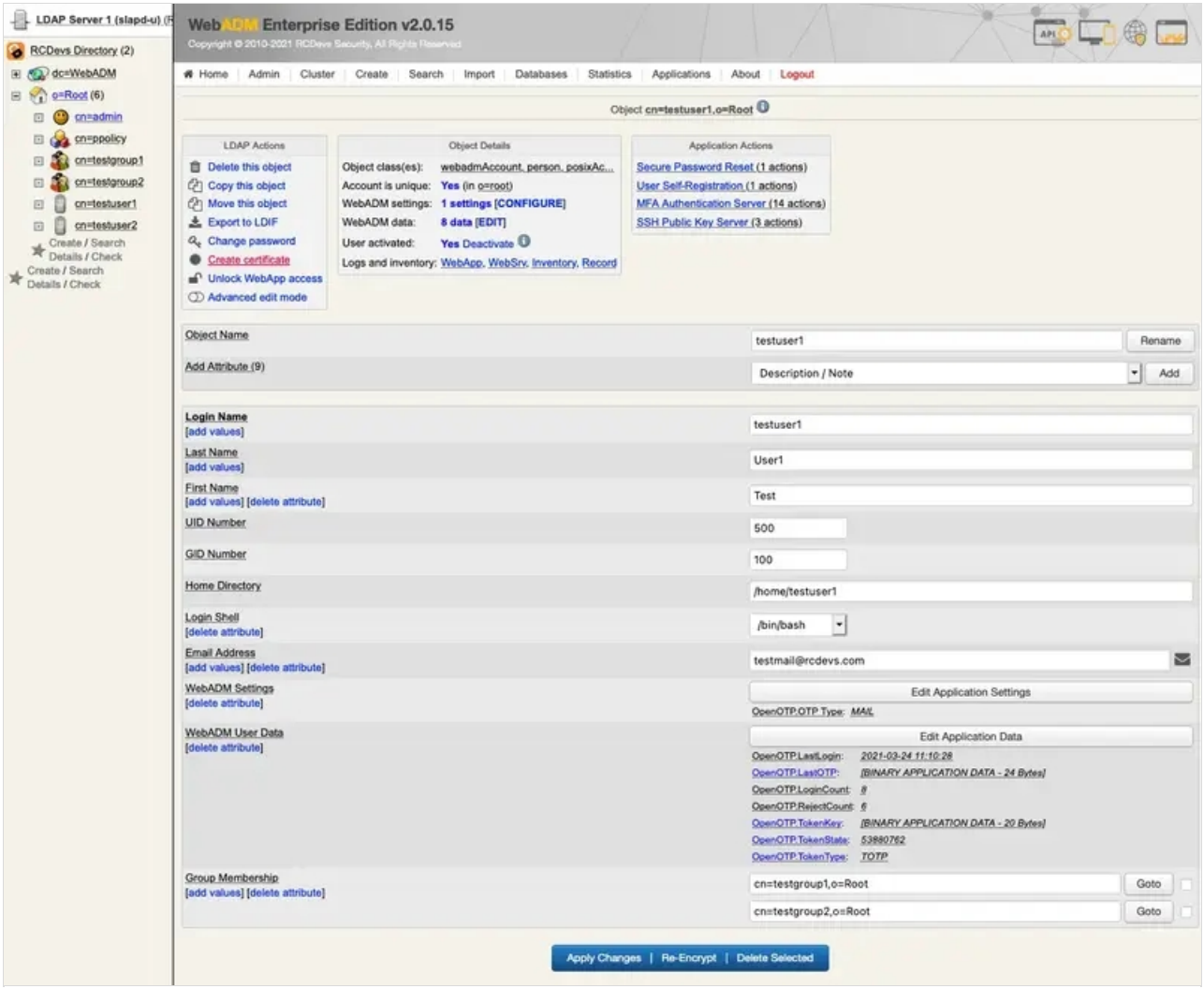


5.2 Encrypt Mail OTP

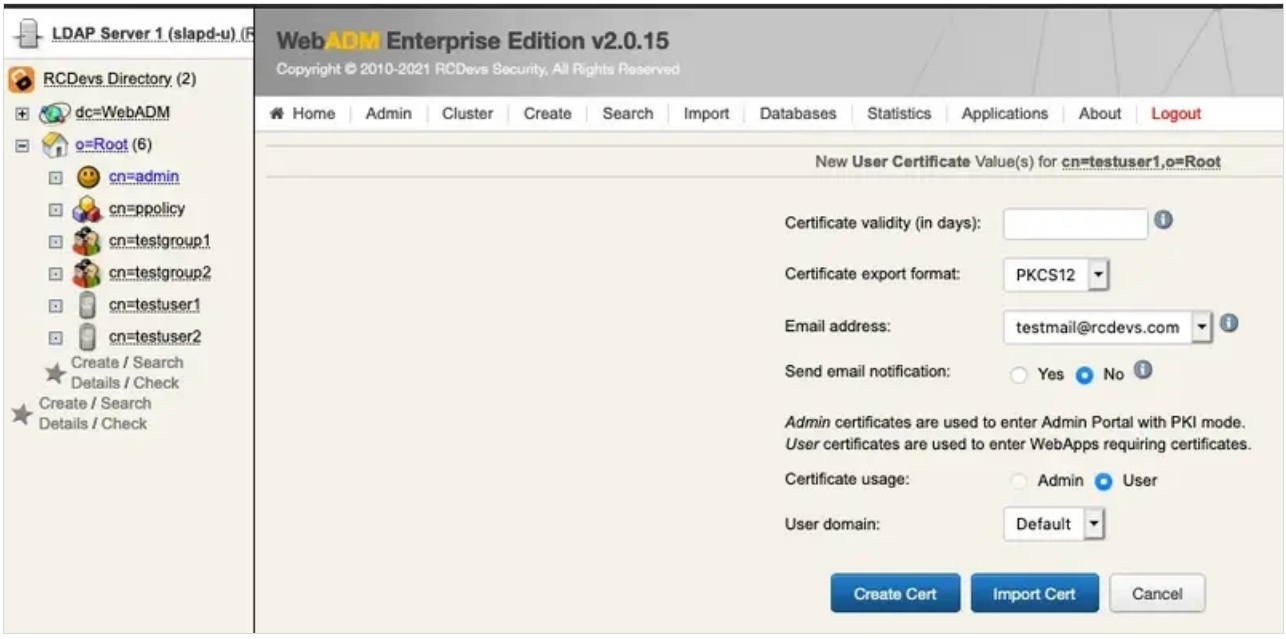
First, enable the option `Use Secure Email` (on an activated user account, go in `object Details` box, click on `CONFIGURE` button and choose `MFA Authentication Server` from the `Applications` box)



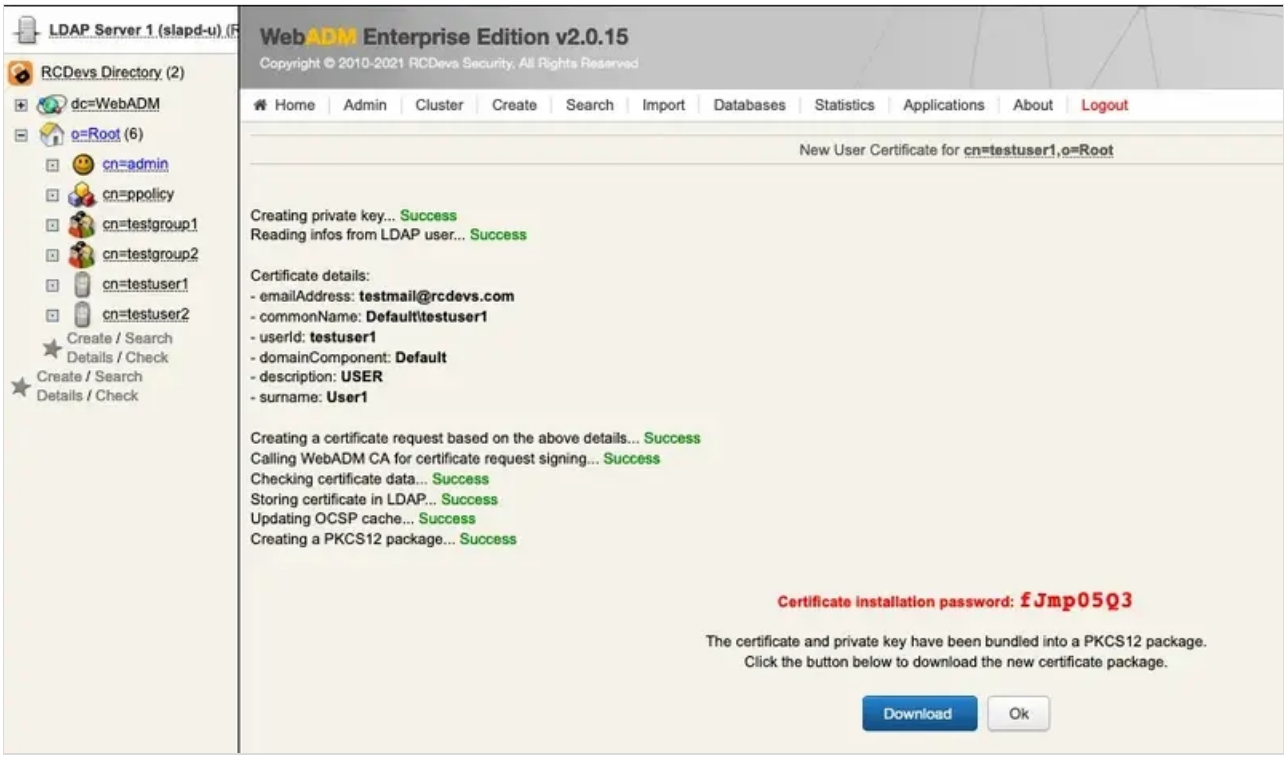
Now, create a certificate through WebADM for the user in question. In this example, select the `testuser1` on the left side and click on `Create certificate`.



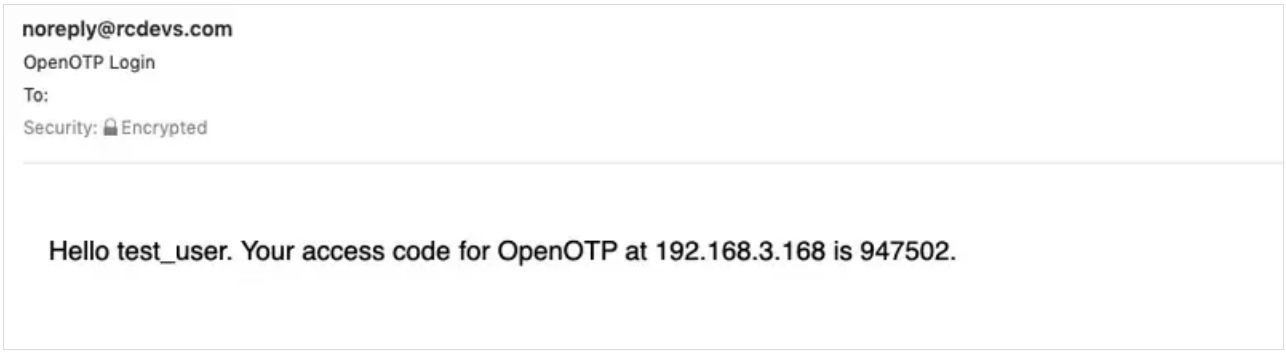
Now, click the `Create Cert` button.



Click the `Download` 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`.



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