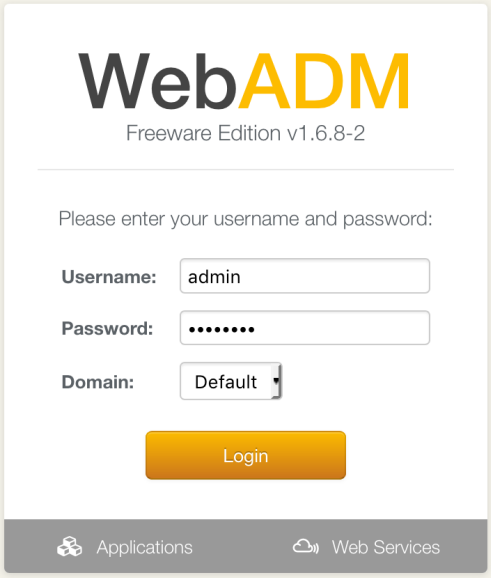
AUTHENTICATION

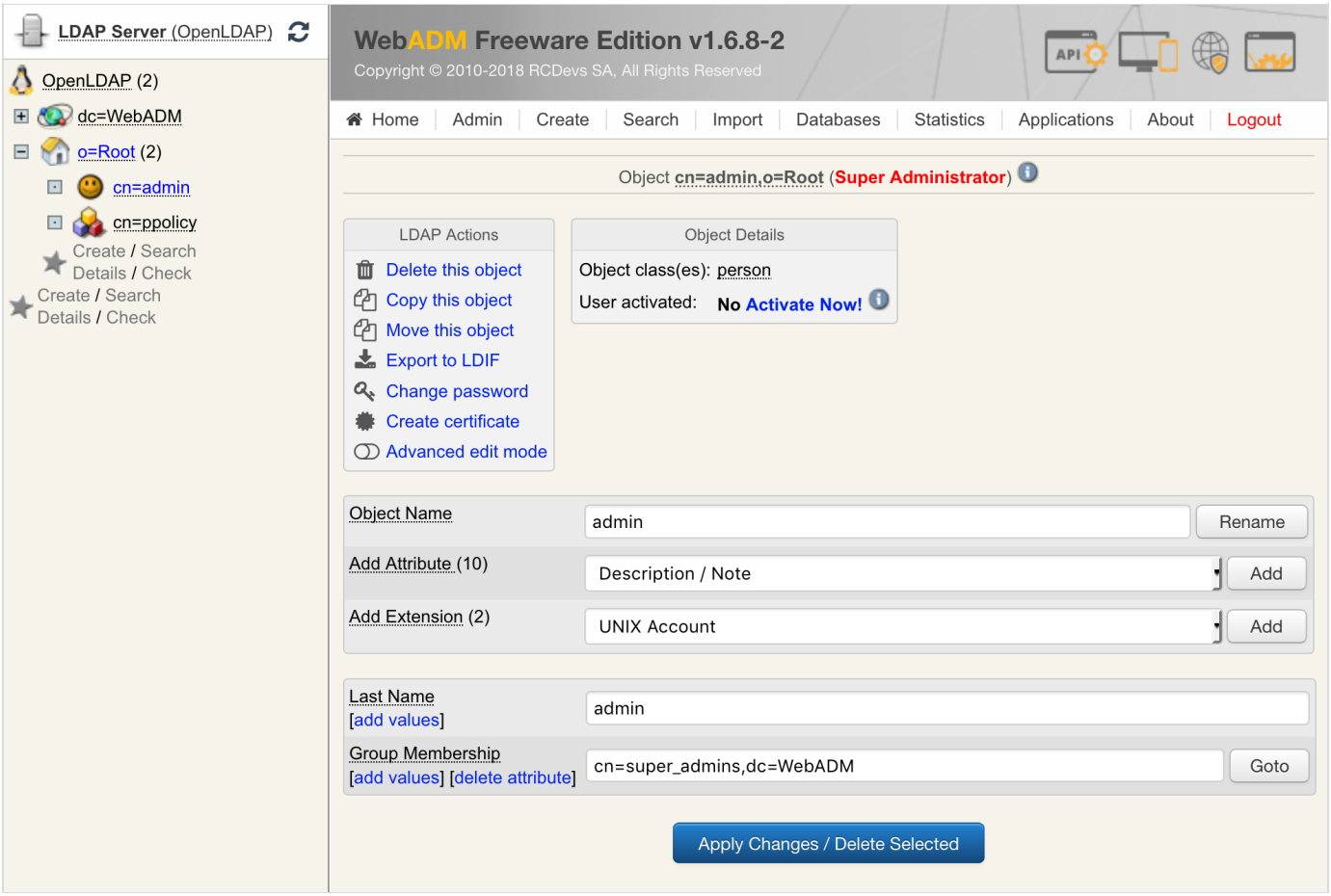
Test Double Authentication with a User

1. User Activation

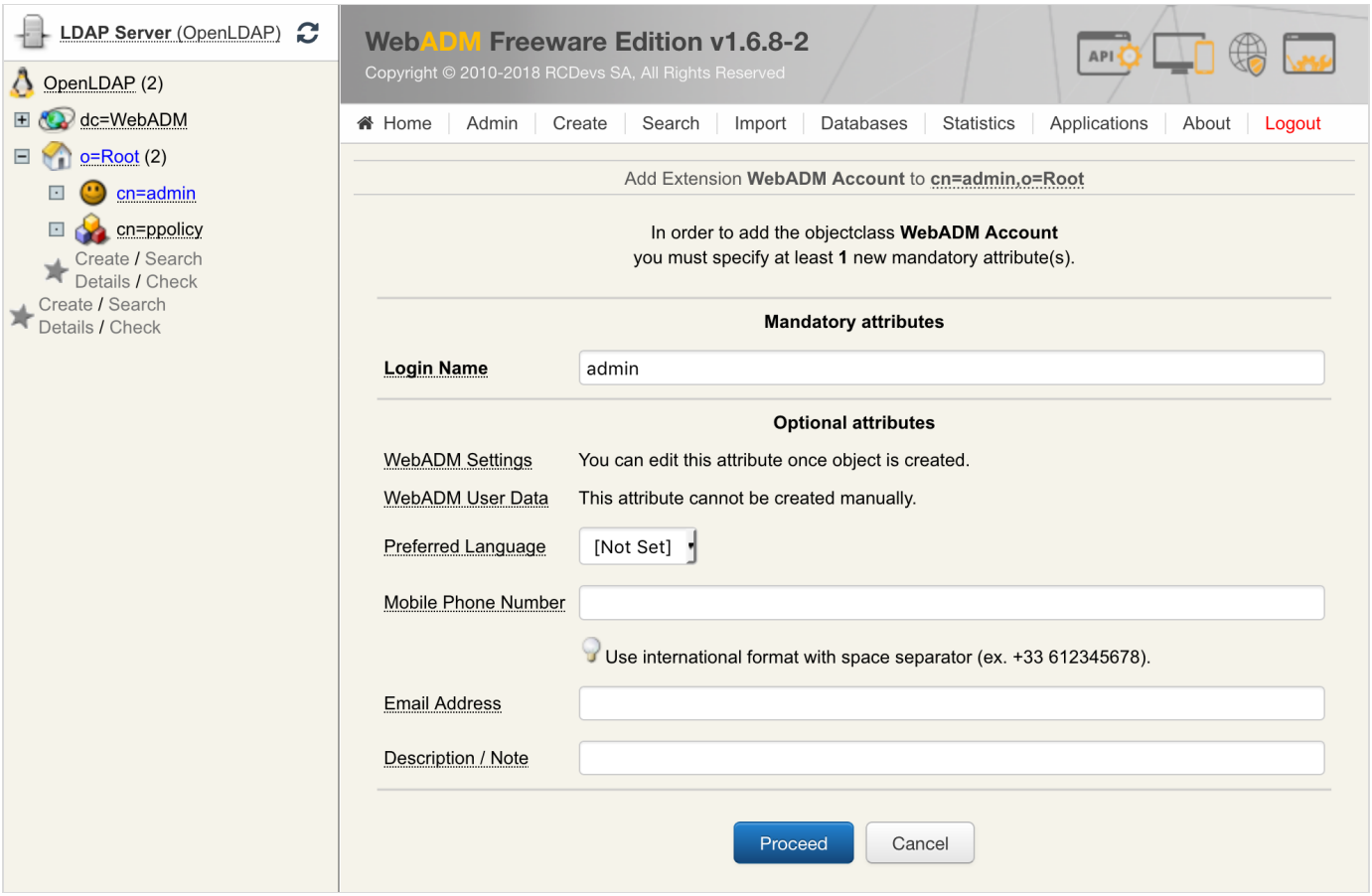
Once WebADM is installed and configured, we can connect to it with a web browser.



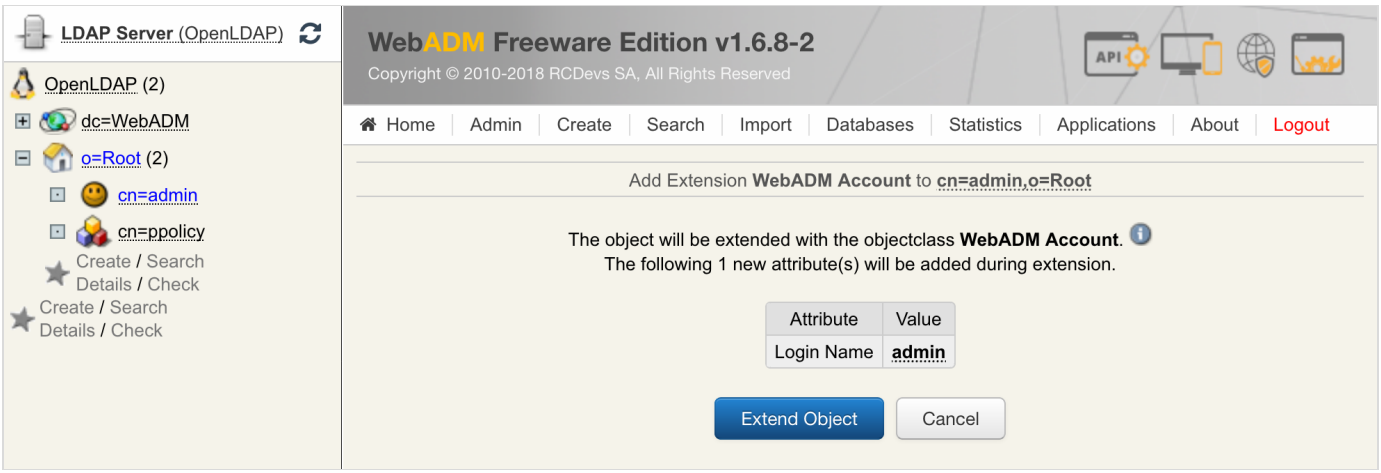
We select the user to activate in the LDAP tree on the left, for example, *Admin*, or we create a new user by clicking on `Create`.
Once the user is selected, we click on `Activate Now!`:



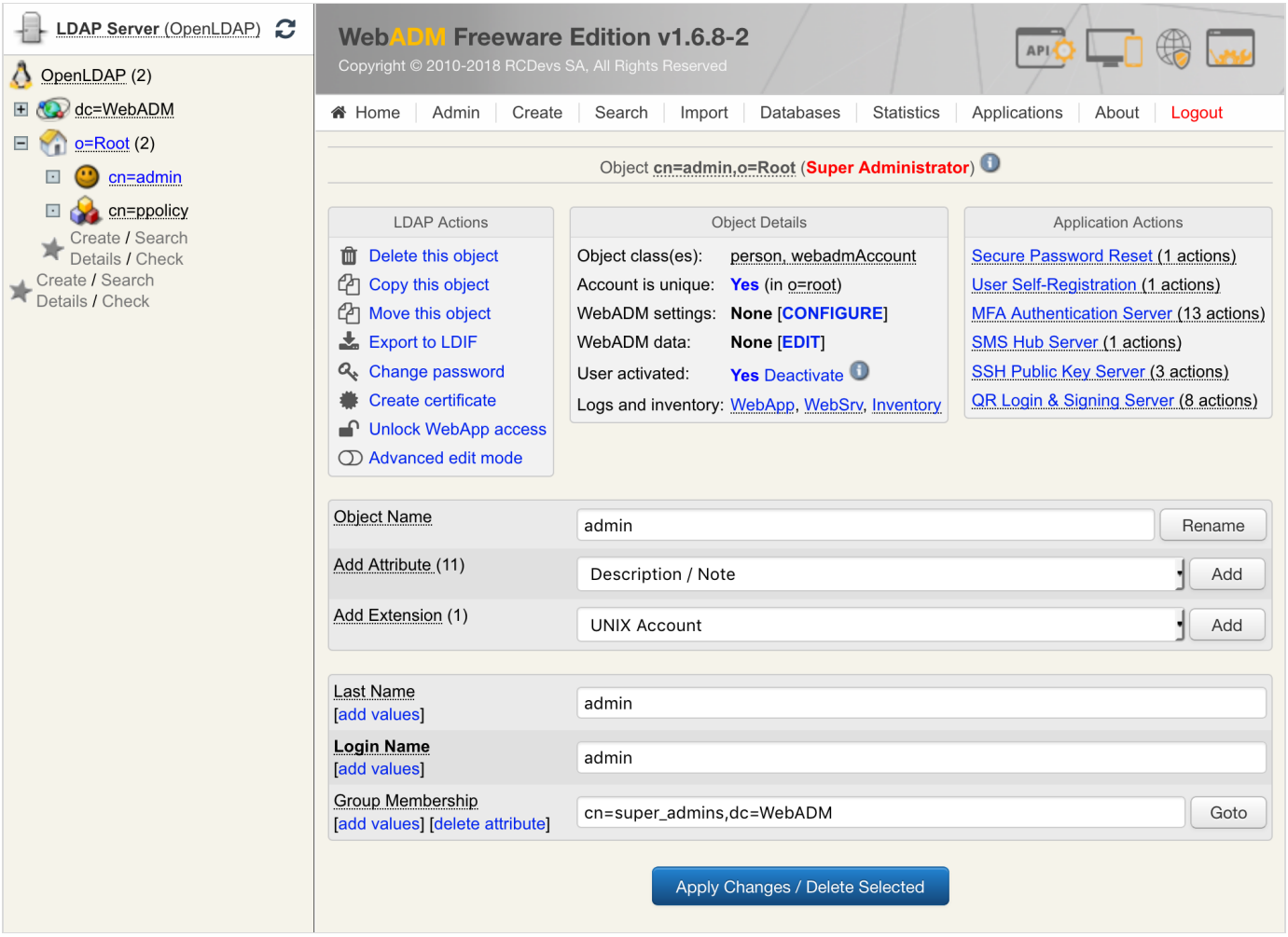
If present, we fill mandatory attributes and `Proceed`:



We click on `Extend Object`:

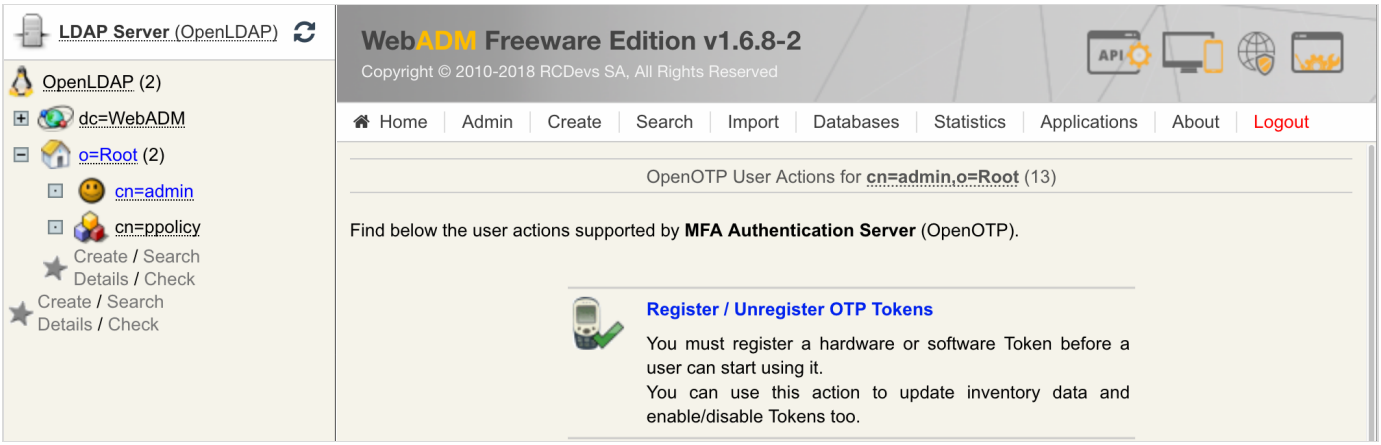


Now, the user is activated. We can register a new token. We click on `MFA Authentication Server`:

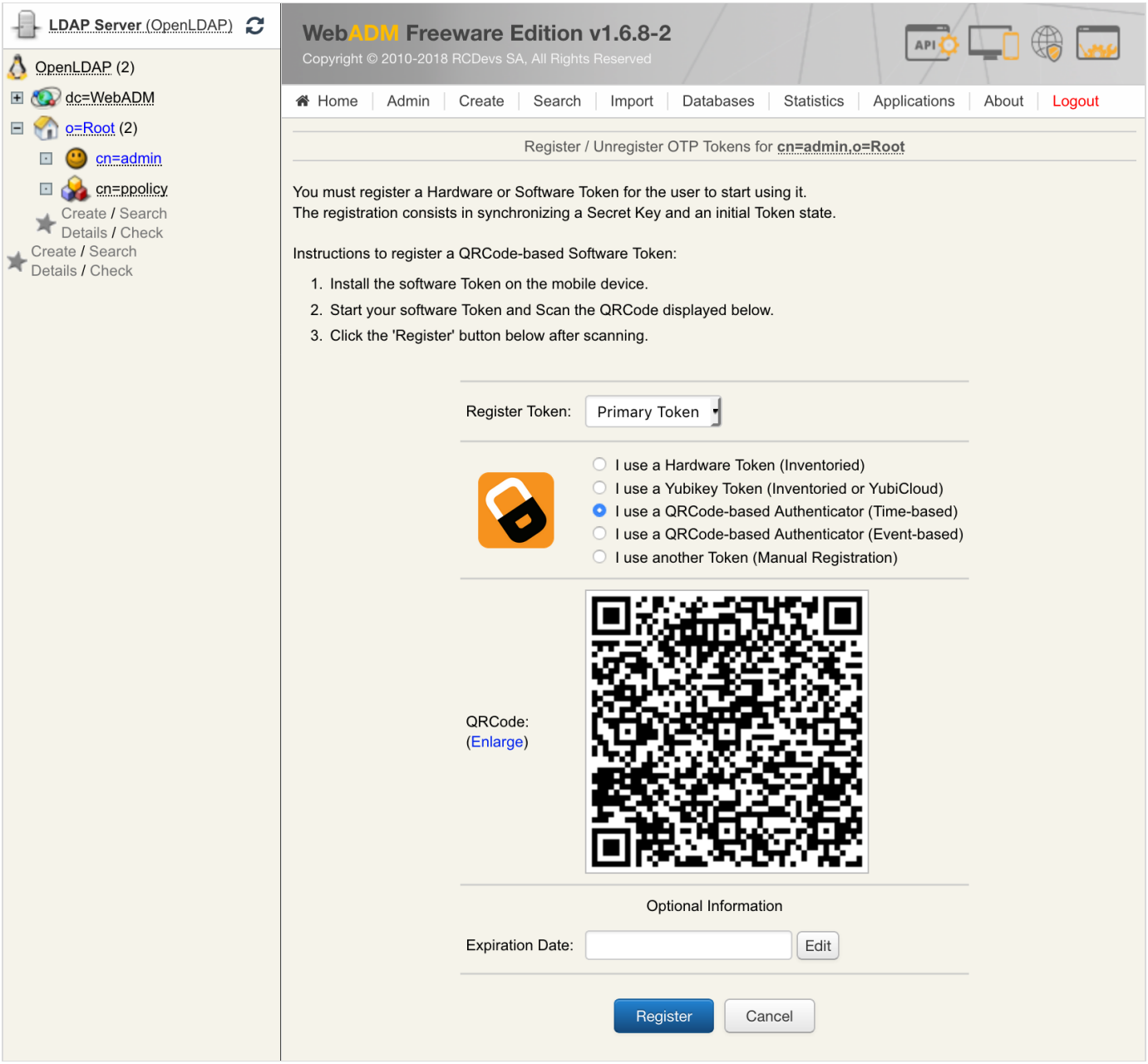


2. OTP Soft Token Enrollment

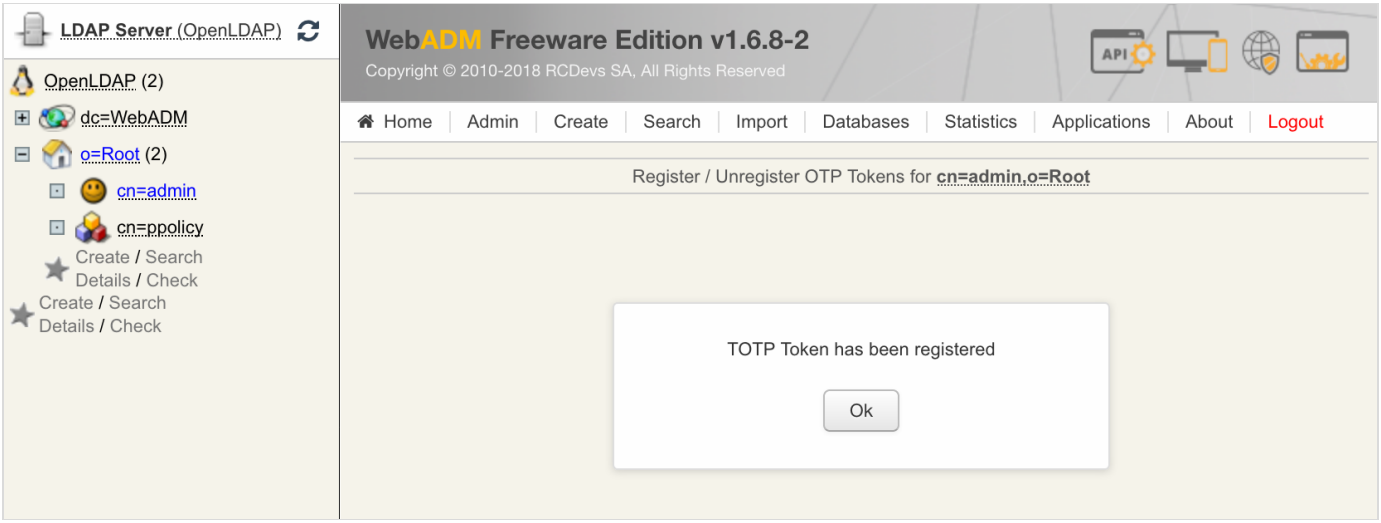
We click on `Register / Unregister OTP Tokens`:



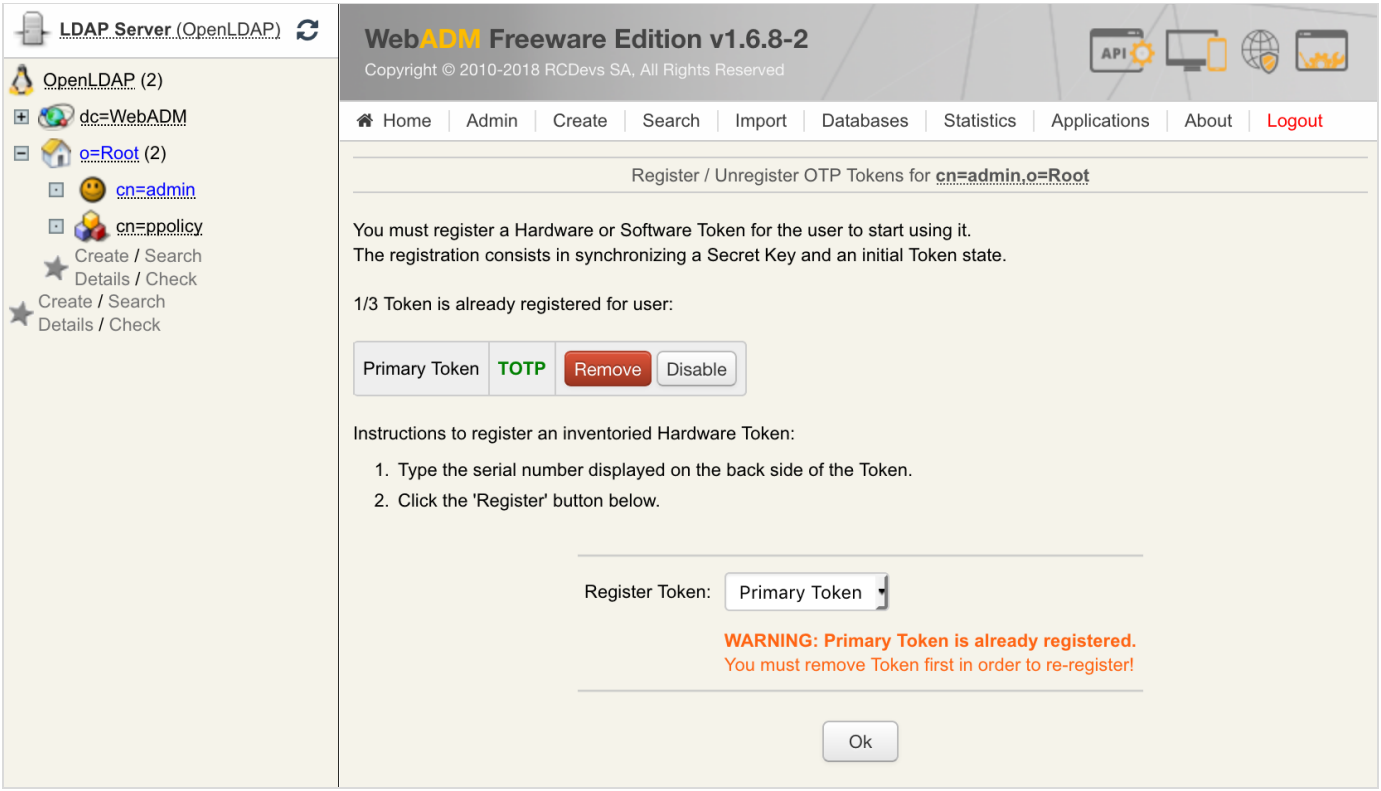
For the test, we select `I use a QRCODE-based Authenticator`. We need a software token app on our smartphone. We can find here, a list of compatible software tokens. Once installed we scan the QR Code with the app and click on `Register`:



We click on `OK`:

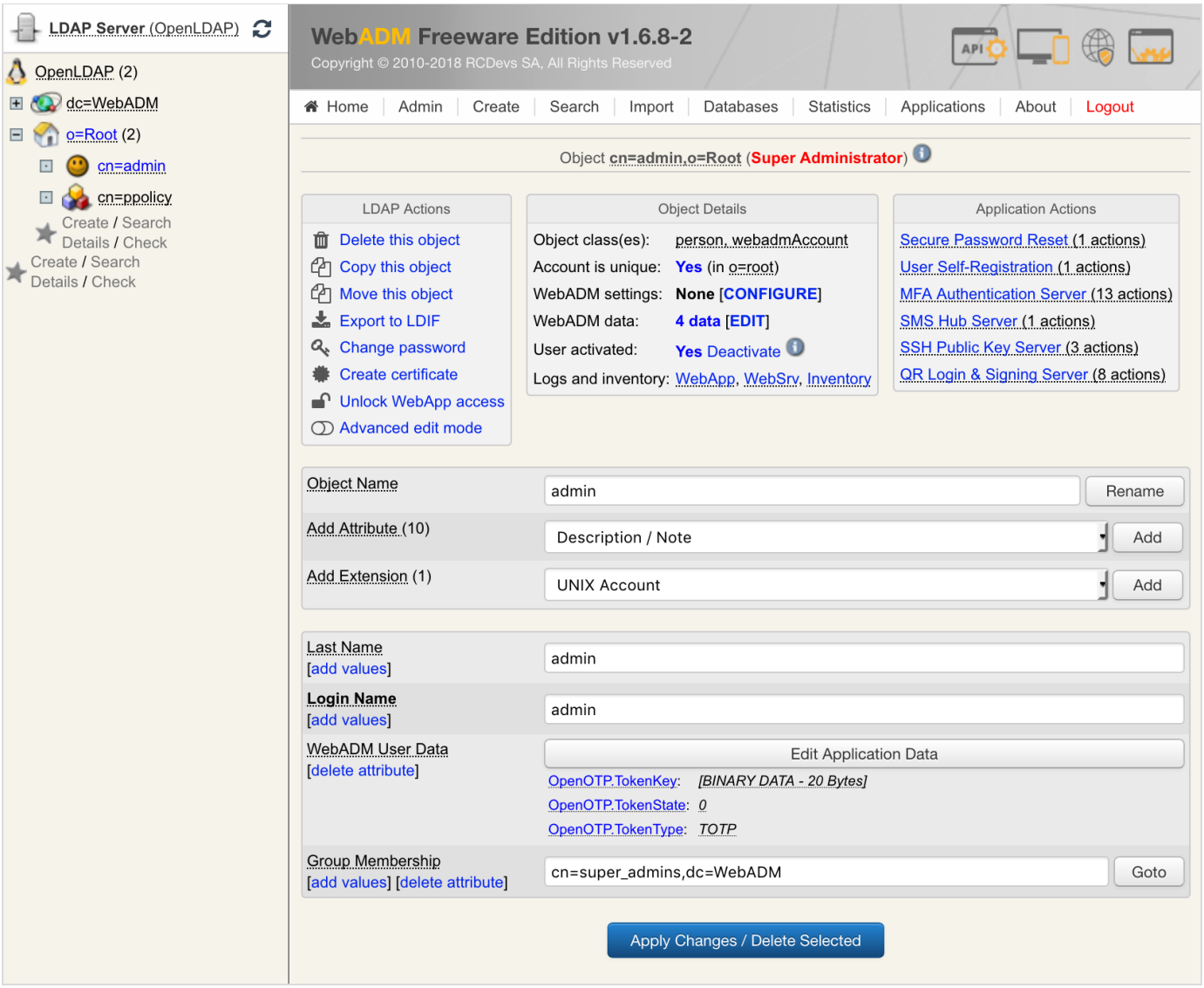


We check that the new token is registered:

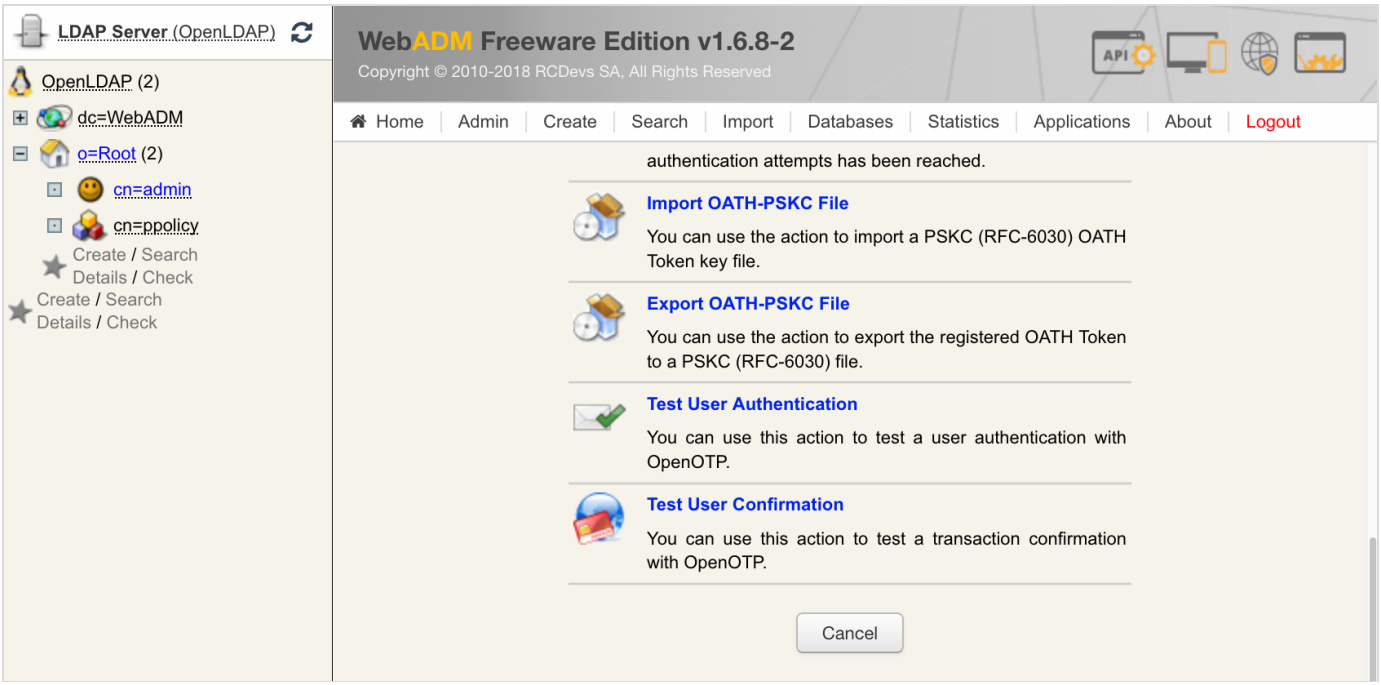


Now, we can try an authentication, we click on `MFA Authentication Server`:

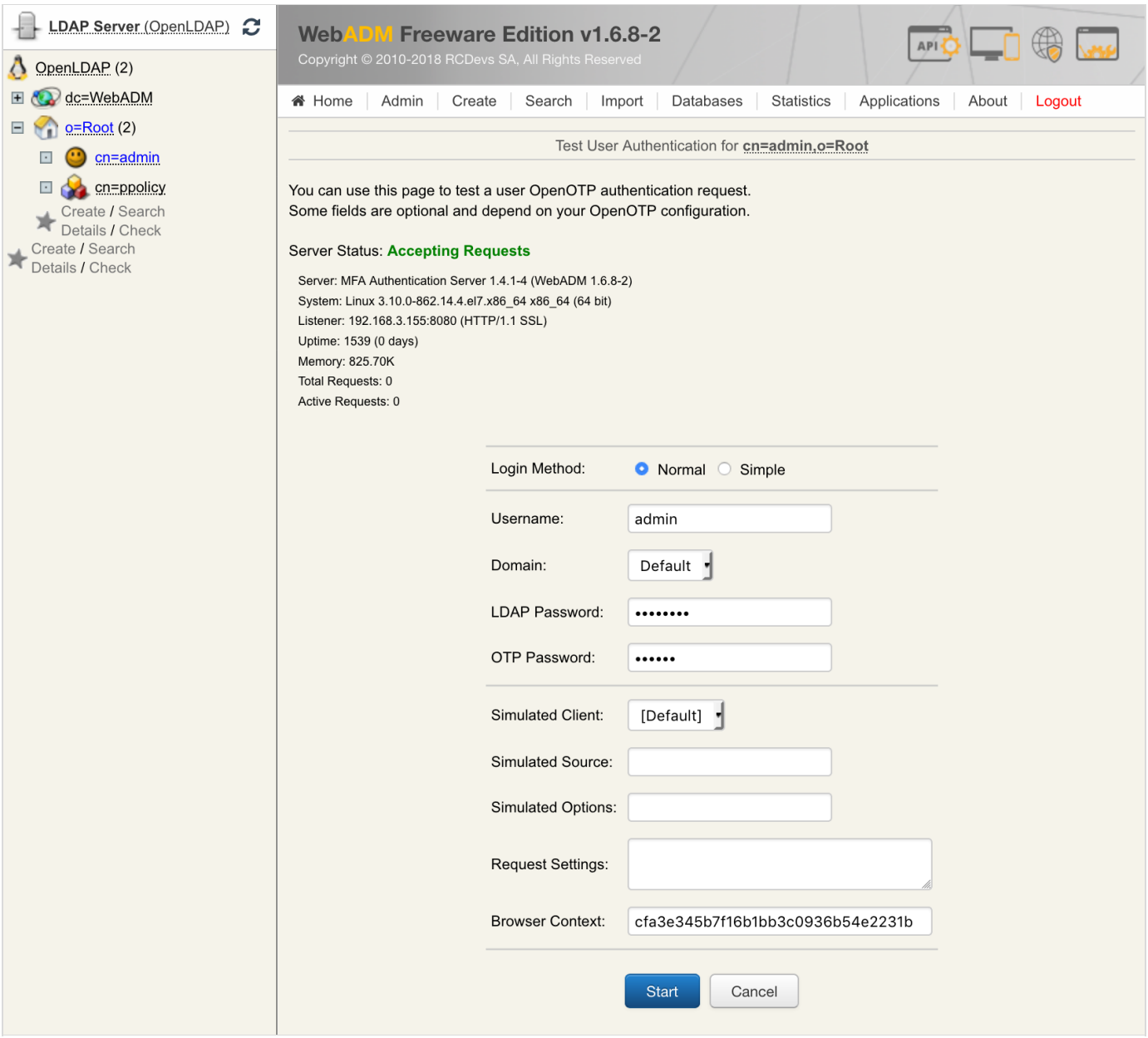
3. Authentication Test



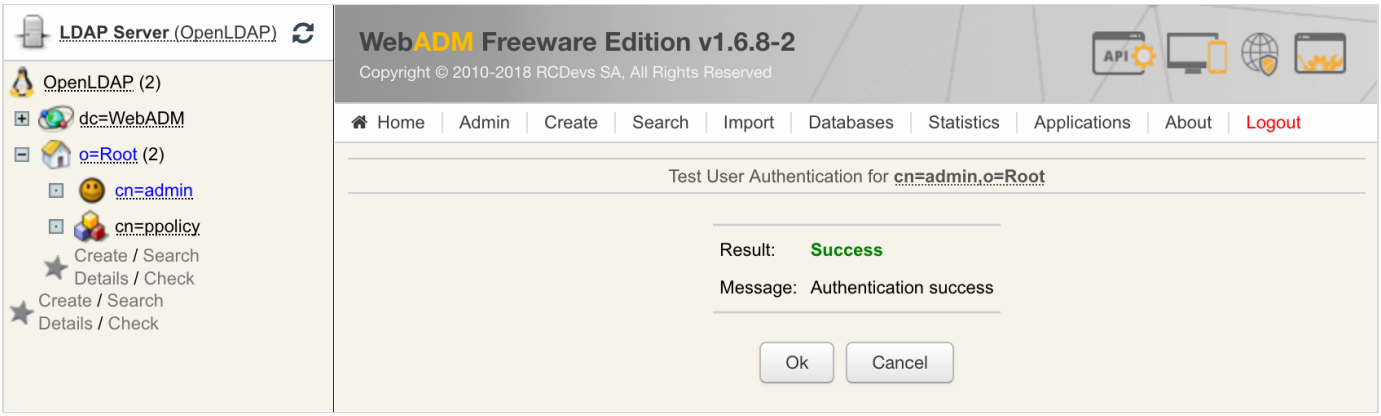
We scroll down and click on `Test User Login`:



We insert the LDAP password and the OTP, and we click on `OK`:



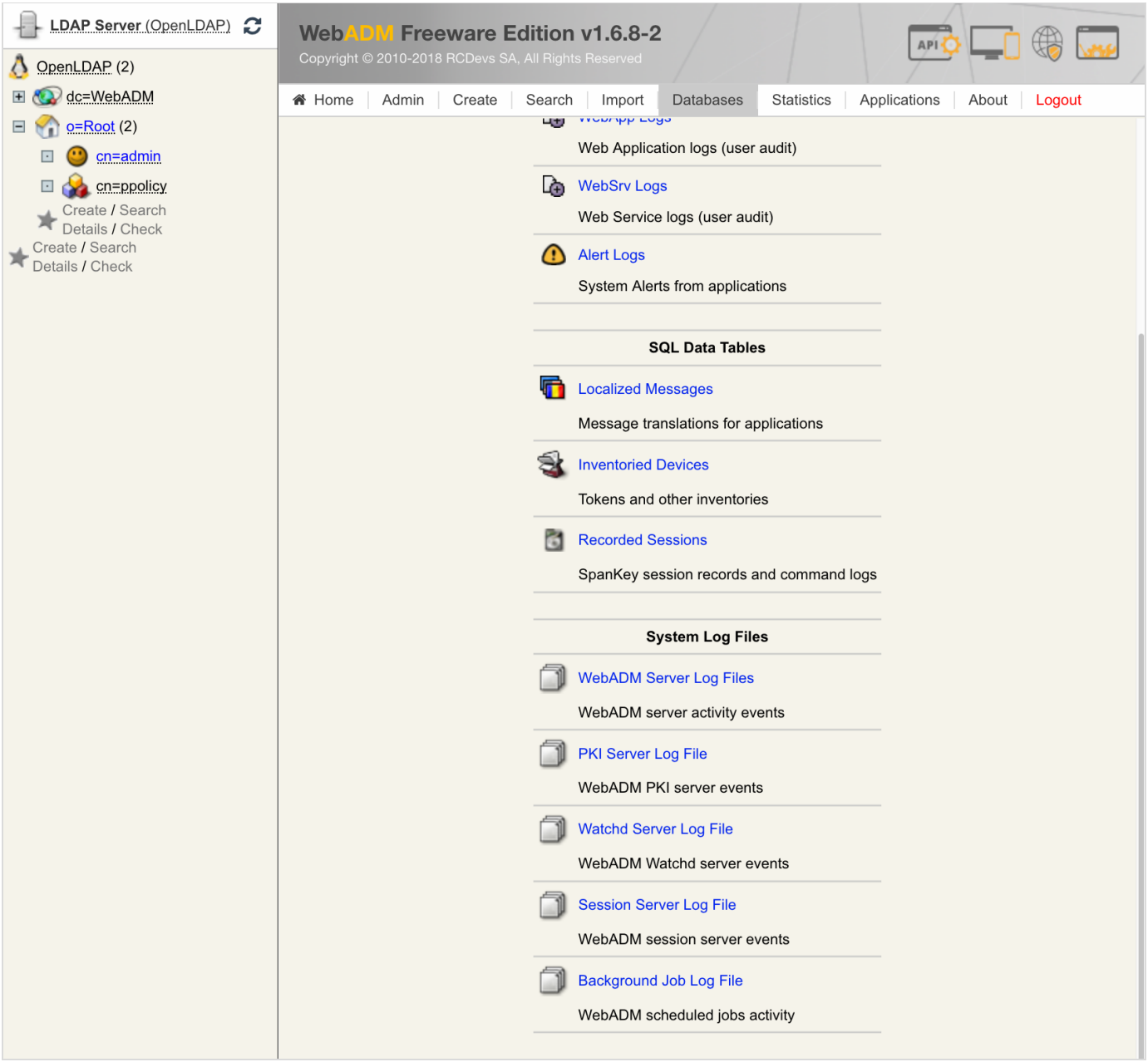
We are authenticated!



4. Logs

Now we can check the log, we click on `Databases` tab:

We click on `WebADM Server log Files`. It corresponds to the `/opt/webadm/log/webadm.log` file:



Each authentication is identified by an ID. Here, it is **T3DSOZ9A**.

```
[2017-07-21 07:29:24] [127.0.0.1] [OpenOTP:T3DSOZ9A] New openotpNormalLogin SOAP
request
[2017-07-21 07:29:24] [127.0.0.1] [OpenOTP:T3DSOZ9A] > Username: admin
[2017-07-21 07:29:24] [127.0.0.1] [OpenOTP:T3DSOZ9A] > Domain: Default
[2017-07-21 07:29:24] [127.0.0.1] [OpenOTP:T3DSOZ9A] > LDAP Password: xxxxxxxx
[2017-07-21 07:29:24] [127.0.0.1] [OpenOTP:T3DSOZ9A] > OTP Password: xxxxxx
[2017-07-21 07:29:24] [127.0.0.1] [OpenOTP:T3DSOZ9A] > Client ID: OpenOTP
[2017-07-21 07:29:24] [127.0.0.1] [OpenOTP:T3DSOZ9A] > Source IP: 192.168.3.155
[2017-07-21 07:29:24] [127.0.0.1] [OpenOTP:T3DSOZ9A] > Context ID:
d10243968f7e608fe4743d8a43747123
[2017-07-21 07:29:24] [127.0.0.1] [OpenOTP:T3DSOZ9A] Registered openotpNormalLogin
request
[2017-07-21 07:29:24] [127.0.0.1] [OpenOTP:T3DSOZ9A] Resolved LDAP user:
cn=admin,o=Root
[2017-07-21 07:29:24] [127.0.0.1] [OpenOTP:T3DSOZ9A] Started transaction lock for user
[2017-07-21 07:29:24] [127.0.0.1] [OpenOTP:T3DSOZ9A] Found 37 user settings:
LoginMode=LDAPOTP,OTPType=TOKEN,OTPLength=6,ChallengeMode=Yes,ChallengeTimeout=90,EnableL
1:HOTP-SHA1-6:QN06-
T1M,SMSType=Normal,SMSMode=Ondemand,MailMode=Ondemand,LastOTPTime=300,ListChallengeMode=S

[2017-07-21 07:29:24] [127.0.0.1] [OpenOTP:T3DSOZ9A] Found 3 user data:
TokenType,TokenKey,TokenState
[2017-07-21 07:29:24] [127.0.0.1] [OpenOTP:T3DSOZ9A] Found 1 registered OTP token
(TOTP)
[2017-07-21 07:29:24] [127.0.0.1] [OpenOTP:T3DSOZ9A] Requested login factors: LDAP &
OTP
[2017-07-21 07:29:24] [127.0.0.1] [OpenOTP:T3DSOZ9A] LDAP password Ok
[2017-07-21 07:29:24] [127.0.0.1] [OpenOTP:T3DSOZ9A] TOTP password Ok (token #1)
[2017-07-21 07:29:24] [127.0.0.1] [OpenOTP:T3DSOZ9A] Updated user data
[2017-07-21 07:29:24] [127.0.0.1] [OpenOTP:T3DSOZ9A] Sent success response
```