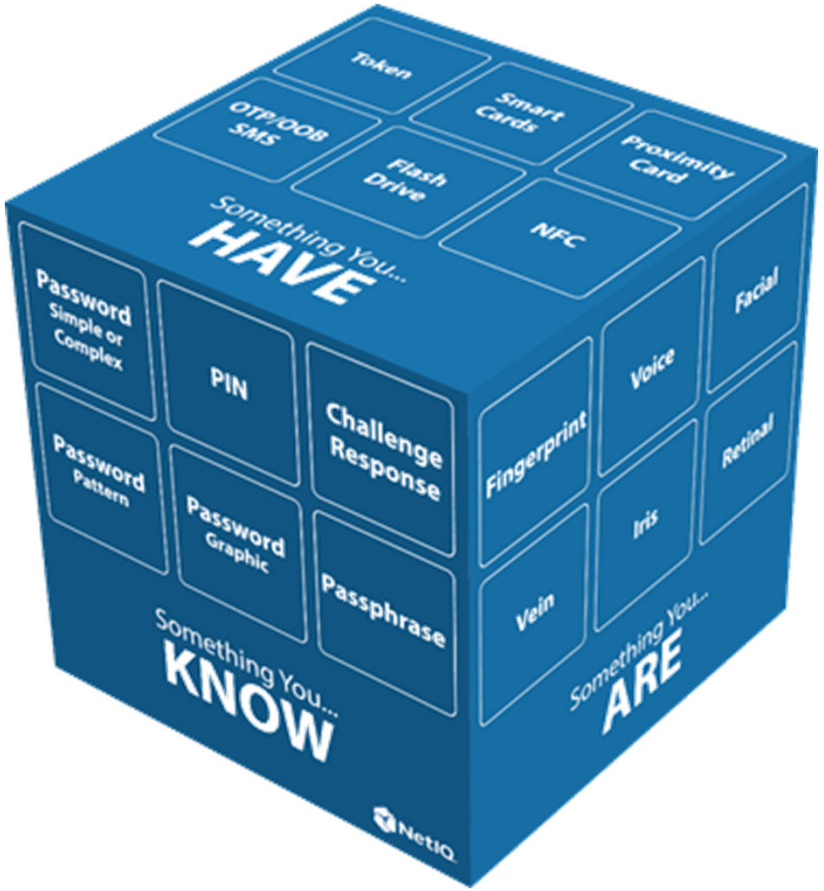

opentext™
Configuring Filr to use MFA
with Advanced Authentication
Robin Redgrave
Solutions Consultant

What is Advanced Authentication

Advanced Authentication delivers:

- Two-Factor Authentication (2FA)
- Multi-Factor Authentication (MFA)



opentext™

Filr Advanced With Advanced Authentication

Gives Multi Factor Authentication

- Ask for more than just a password
- For both Internal and external users (need power external user license)

Advanced Authentication Limited

- An entitlement with Filr Advanced Maintenance
  - Also available with GroupWise, OES, iPrint, ZENworks etc
- Typically, you will use SMS OTP, Email OTP or TOTP for additional authentication
- You will find it available to download in your SLD portal

If you wish to have other methods of authentication

- Buy the full product (smartphone, smartcard, facial recognition, geofencing etc)

opentext™

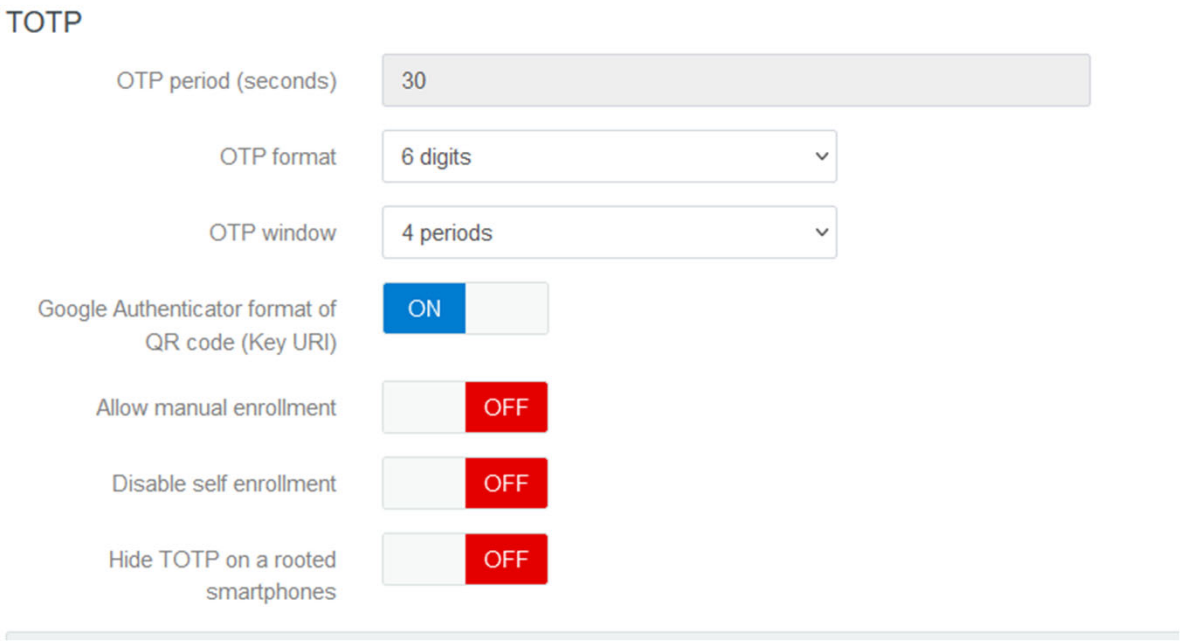

Configuration of AA with Filr

Advanced Authentication Configuration

Set up the methods you plan to use

Add mail config

- Go to policies
- Select mail sender
- Host : Enter mail realy
- Sender email : filr@<company>.com
- Test sending to a user



If required set up SMS

- Supports Twilio or Messagebird
- Also generic settings

If required set up TOTP

- Enable google authenticator format if using Google or MS authenticator

opentext™

Advanced Authentication Configuration
Setting up Repositories

Login to advanced authentication admin

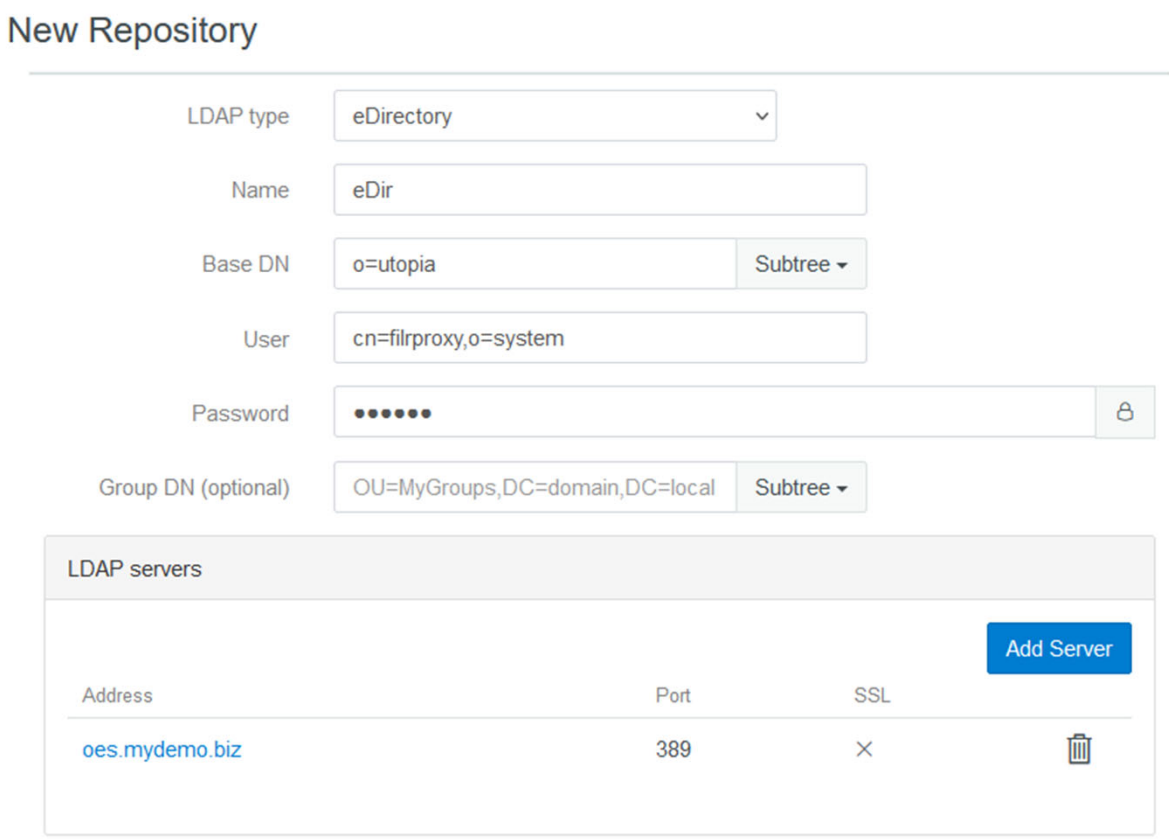
- https://<server>/admin
- User : admin

Add LDAP repository

Point to your LDAP directory

If using MFA for external users

Set up an SQL repository



opentext™

Advanced Authentication Configuration
External User MFA

Allow access from Advanced Authentication to the database

- If you are running the single server install you can run pgRemoteAccess.sh on the Filr web server
  - sh /opt/novell/filr_config/pgRemoteAccess.sh <AA_ip_address/nw_mask>
  - If no IP is specified, access is enabled for all servers (0.0.0.0/0)
  - Or edit /vastorage/postgres/conf/vabase-pg_hba.conf manually
- If using the Database Appliance
  - This should be already enabled, unless you have locked it down
- If using your own database
  - You may need to enable this

Advanced Authentication Configuration

Create chains and events

Create the chain(s) for the authentication methods(s) required

- Add method (eMail OTP/SMS OTP/TOTP)
- Add users/groups that will be using it

Create an event for Filr authentication

- Give it a name, ensure that it is enabled
- Set event type as OAuth2
- Add chain(s) required (the one you just created)

Copy the Client ID and Secret (We need these for Filr)

opentext™

Advanced Authentication Configuration
Filr Configuration

In the Filr admin console enable ‘NetIQ Advanced Authentication’

- For internal LDAP/External users
- Enter in the Server URL (https://<aa server>>
- Paste in the Client ID and secret

The tenant name will typically be ‘TOP’

- Maybe different if you are running with multiple tenants
- Filr Advanced supports multi-tenanting, each ‘zone’ can use a separate AA Tenant

Copy the redirect URLs and paste into the Event in Advanced Authentication Admin

- Edit if using additional host names

Do test to check that it works

opentext™

FilrMFA Configuration

If you need to enrol an authentication method (ie for TOTP)

- You can do it on https://<aa server>

Enable internal/external user MFA in Filr Admin console

If ‘all users’ was selected for your chain then same MFA will work for both user types

Can have different MFA for internal and external users

- Have two chains with different repositories as the users

opentext™

Further Information

Documentation

- Using Multi-Factor Advanced Authentication with Filr

Videos

- Installing the Advanced Authentication appliance - first boot
- Installing the Advanced Authentication appliance - configuration after first boot
- Installing the Advanced Authentication appliance - product configuration
- Configuring Filr to use MFA for internal and external user authentication


opentext™