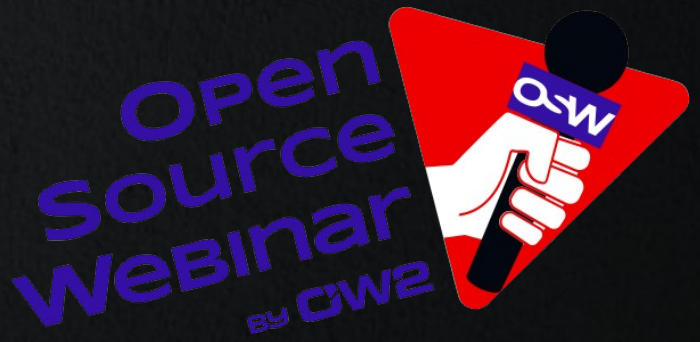
Vorteks

make IT work, make IT free

New features in LemonLDAP::NG



Speaker

David COUTADEUR

IAM Architect

david.coutadeur@worteks.com

@dcoutadeur

david-coutadeur

LemonLDAP::NG
LDAP Tool Box
LSC
FusionIAM

Worteks (\vɔʁ.tɛks\)

Service

Complex infrastructures, cloud, mail, authentication, security

- Studies, audit & consulting
- Technical expertise
- Support
- Training
- R&D and innovation

Edition

V'Sweet — Collaborative portal

V'Opla — Common developement platform

V'IDaaS — Identity and Access Management

Partners

Red Hat Advanced Business Partner Reseller

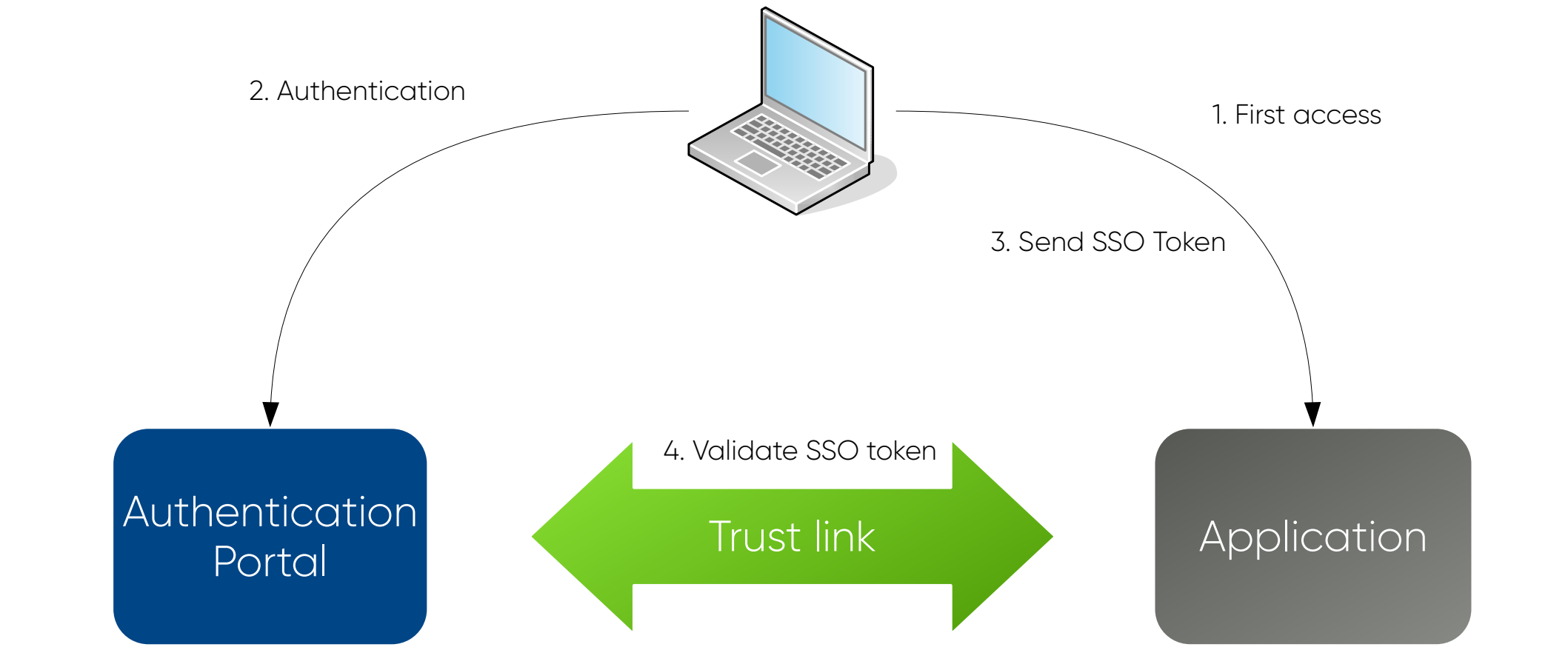
BlueMind

ONLYOFFICE

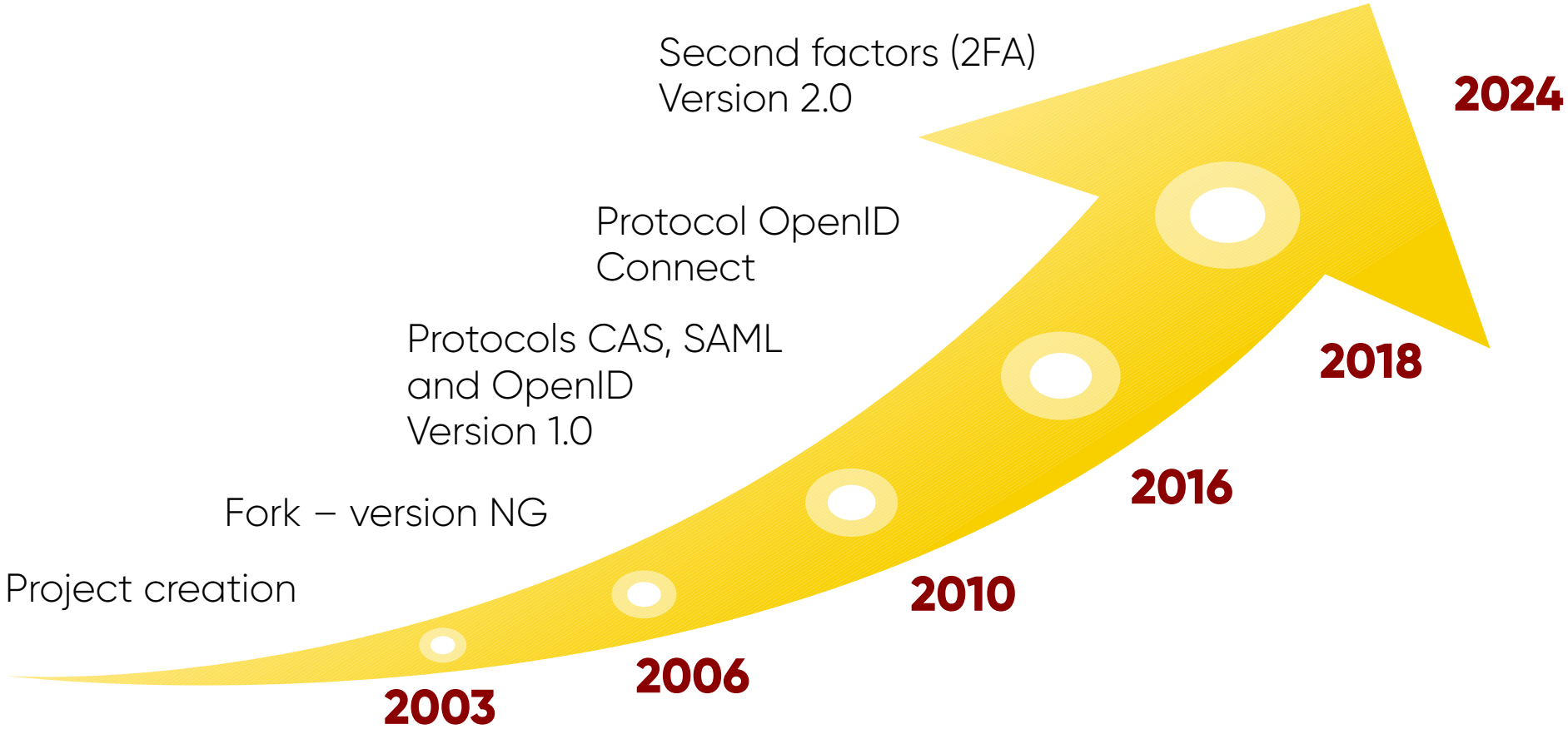
Collabora Online

LemonLDAP::NG

Web Single Sign On

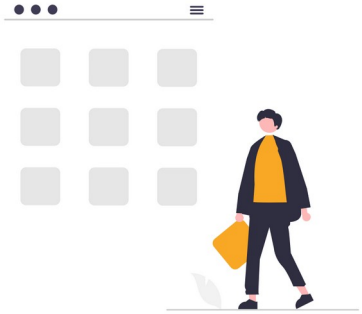


Project history

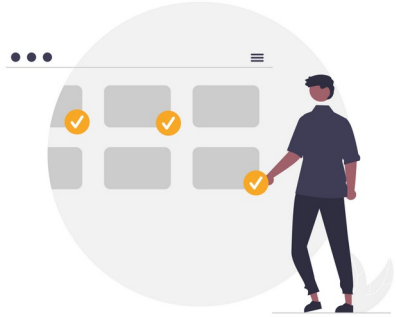


Main features

SSO & Access Control

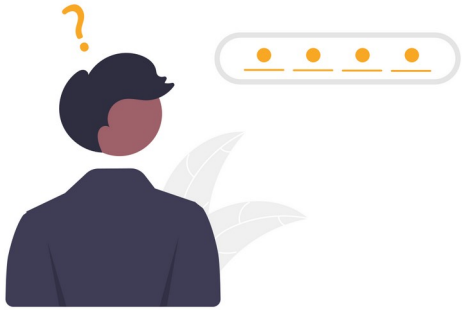


Application menu

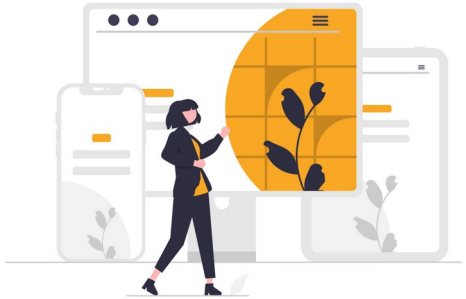


CAS / SAML / OIDC

Second Factor (2FA)



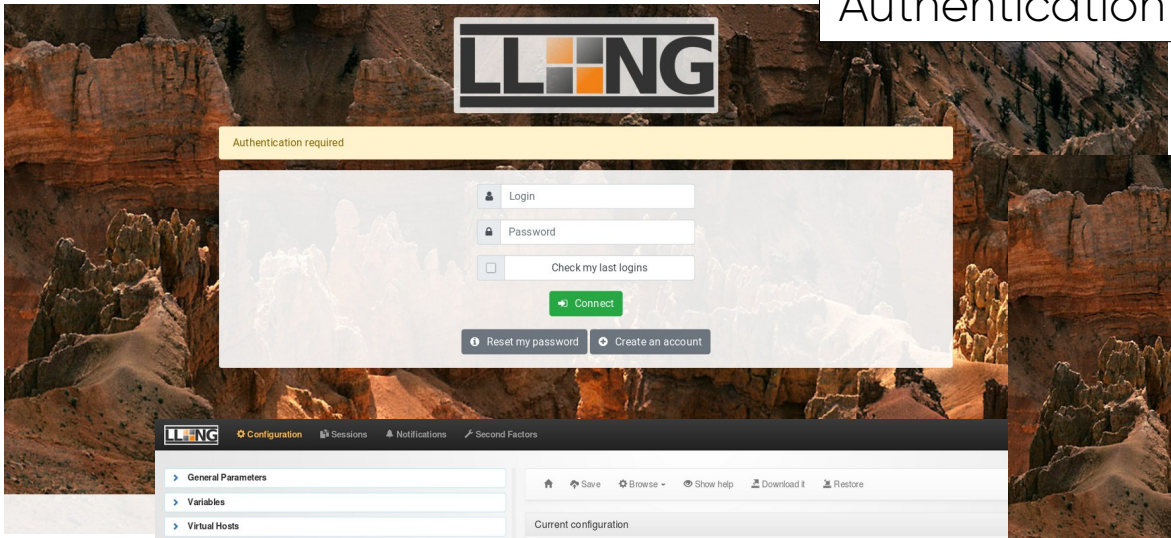
Password management



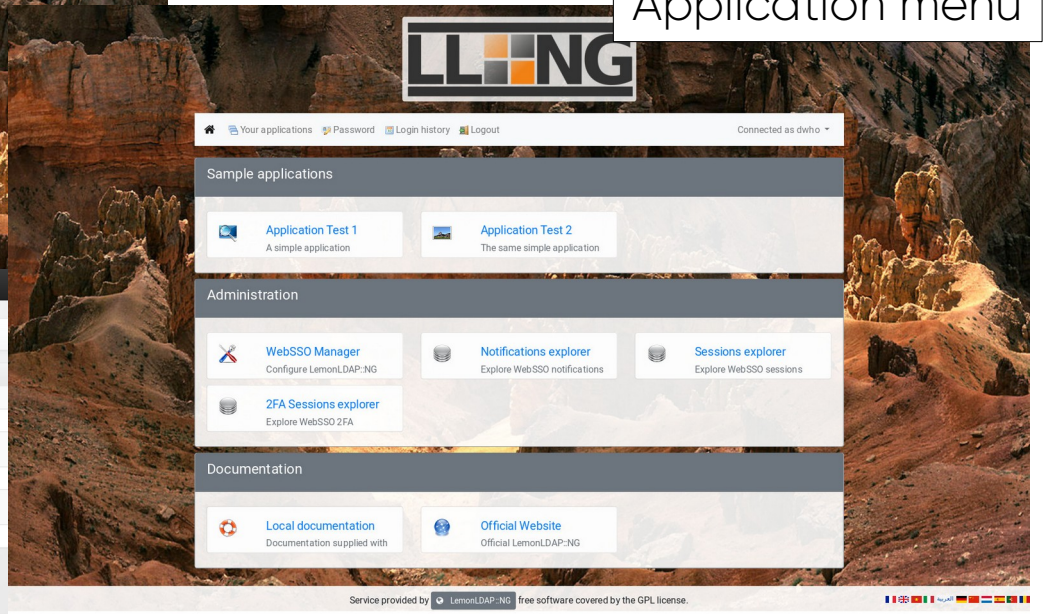
Graphical customization

Screenshots

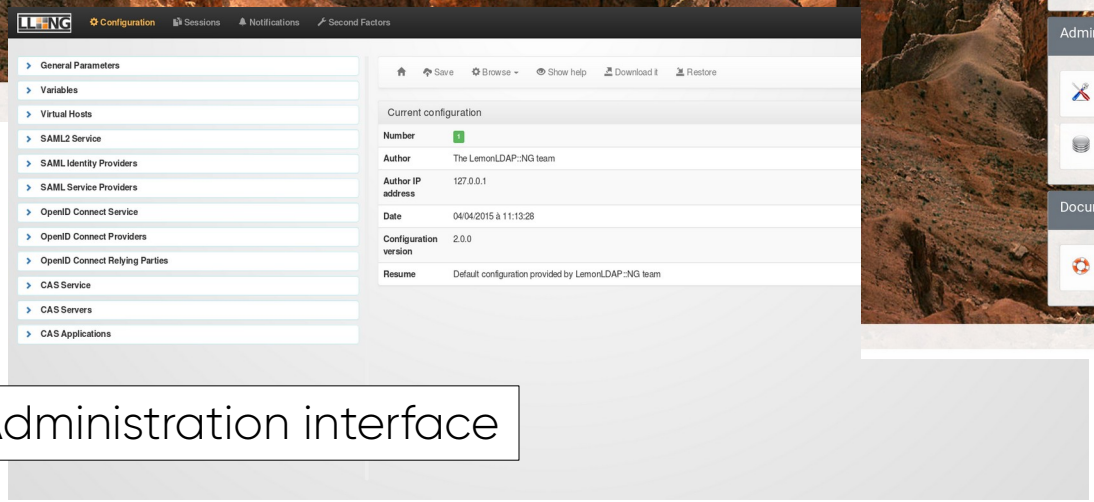
Authentication form



Application menu



Administration interface

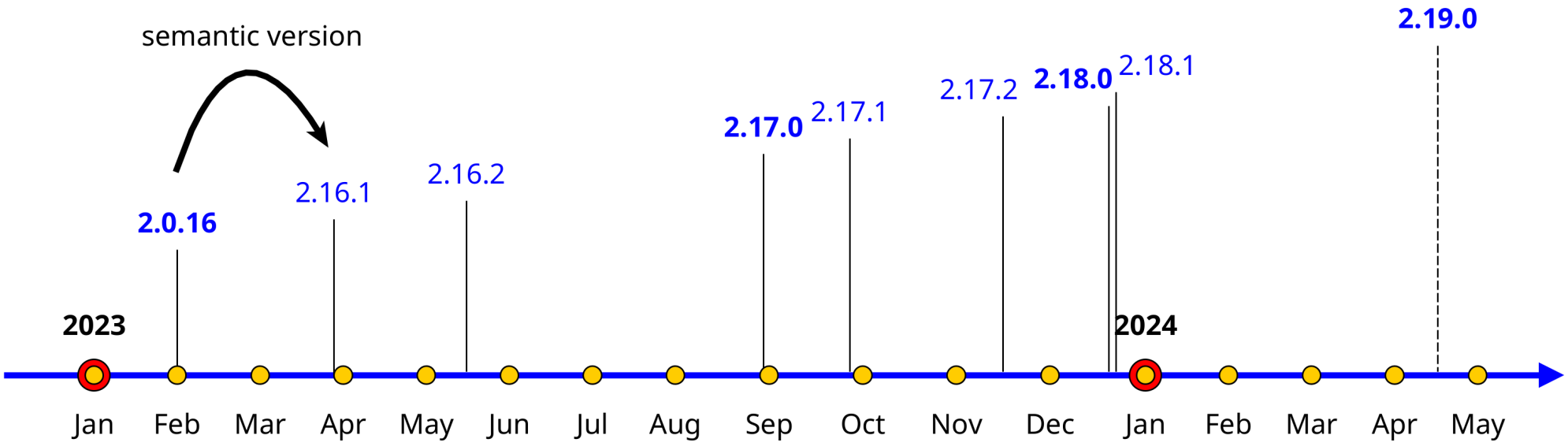


100% Free Software

- License GPL
- OW2 project
- Forge: https://gitlab.ow2.org/lemonldap-ng/lemonldap-ng
- Site: https://lemonldap-ng.org
- OW2 Community Award in 2014
- SSO component of FusionIAM project: https://fusioniam.org/

What's new?

Release cycle



- new minor (2 – 10 issues) every 2 month
- new major (~ 50 issues) every 6 mth – 1 year

2.17.0

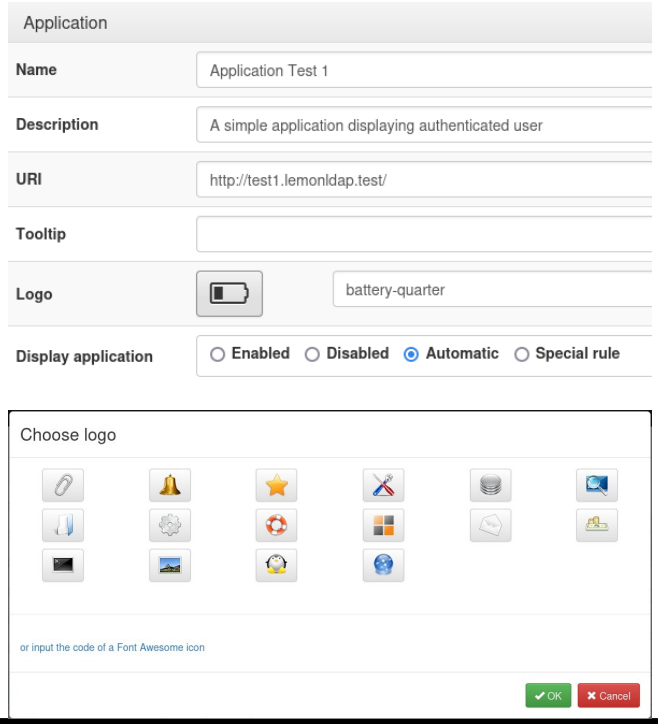
2.17.0

- OIDC: as OP or RP, implement Back-Channel and front-channel logout
  - allows logout spreading

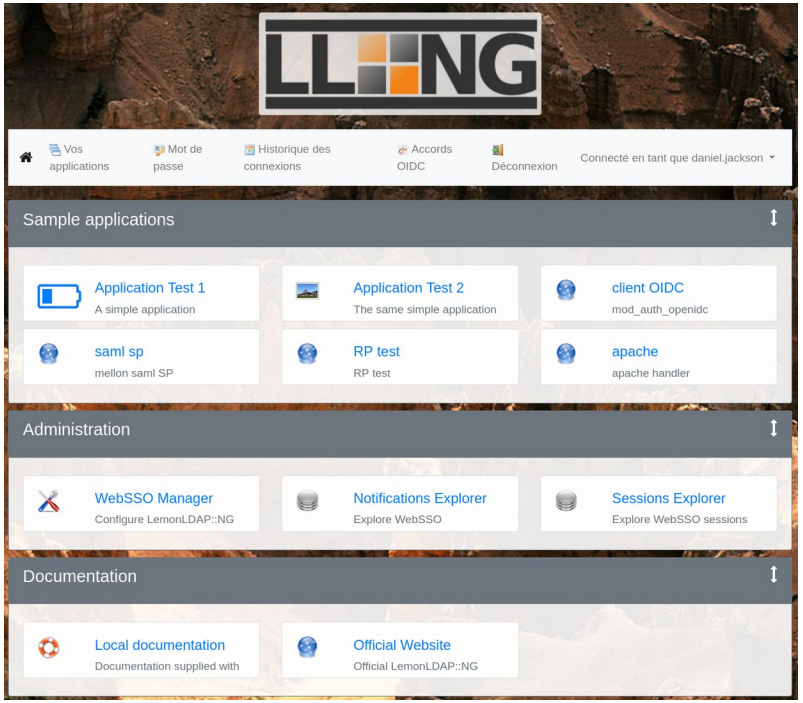
- Add cassandra support for:
  - configuration storage
  - session storage

- Add ability to use applications icons instead of images

configuration



display in portal



2.17.0

- Manager API: add methods to get login history

```
curl -s http://manager-api.lemonldap.test/api/v1/history/daniel.jackson/last | jq .
{
  "ipAddr": "10.0.3.1",
  "date": 1712232938,
  "result": "success",
  "error": "-4"
}
```

2.17.0

- Add a function in Safelib to match IP addresses reliably:
  - Usable in application rules or sessions opening

```
inNetwork("192.168.0.0/24") or inNetwork("127.0.0.1/32")
```

- Allow admin to choose key size during certificate generation for SAML usage (stored in parameter *defaultNewKeySize*)

- Provide all applications informations trought REST service

```
curl -s http://manager-api.lemonldap.test/api/v1/menu/app/1sample/test1 | jq .
{
  "options": {
    "description": "A simple application displaying authenticated user",
    "display": "auto",
    "name": "Application Test 1",
    "logo": "battery-quarter",
    "uri": "http://test1.lemonldap.test/"
  },
  "confKey": "test1",
  "order": 2
}
```

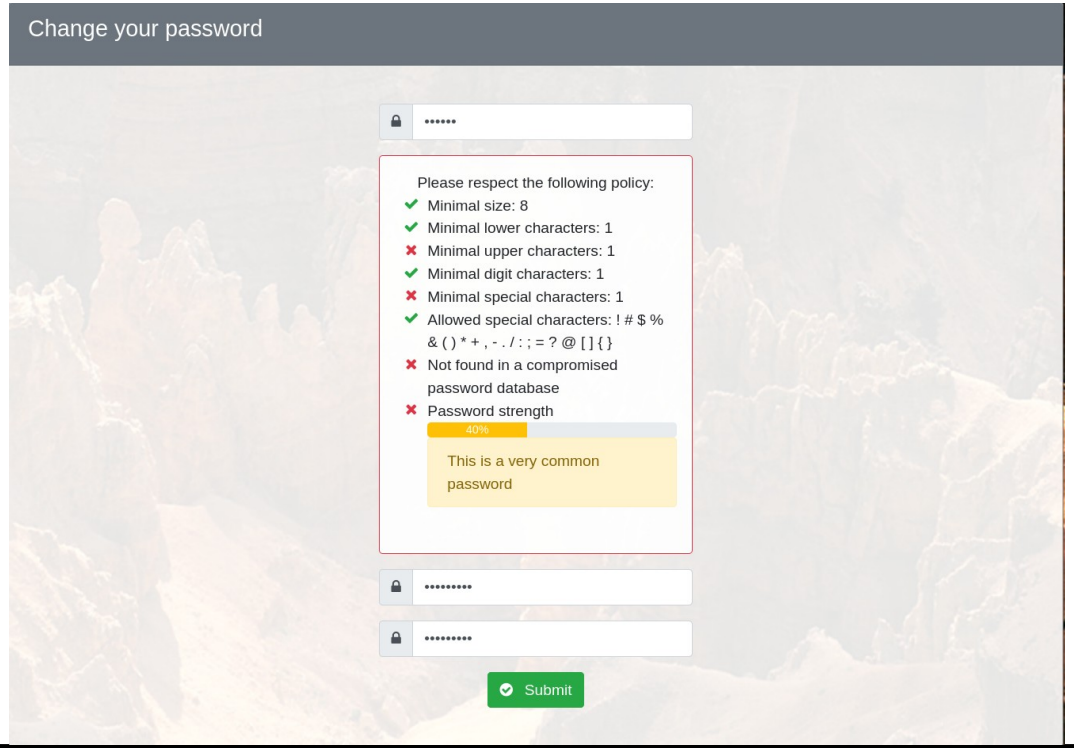
2.18.0

2.18.0

- Send a bulk of reset password links
  - enable the *initialize-password-reset* plugin and define a secret

```
curl -s -X POST -H "Content-Type: application/json" \
      -d '{"mail":"user@domain.com","secret":"mysecret"}' \
      http://auth.lemonldap.test/initializepasswordreset | jq .
{
  "url": "http://auth.domain.com/resetpwd?mail_token=8c717a2eb8233a95181846e0",
  "mail_token": "8c717a2eb8233a95181846e0"
}
```

- implement pluggable password policies and add an indicator of entropy during password change



2.18.0

- possibility to remember second factor / 2FA on a device, to avoid entering it at each authentication
  - through the plugin trustedBrowser (renamed from stayconnected)
  - trustedbrowser can be enabled by a rule
  - then $_trustedBrowser variable can be used in 2FA activation rule

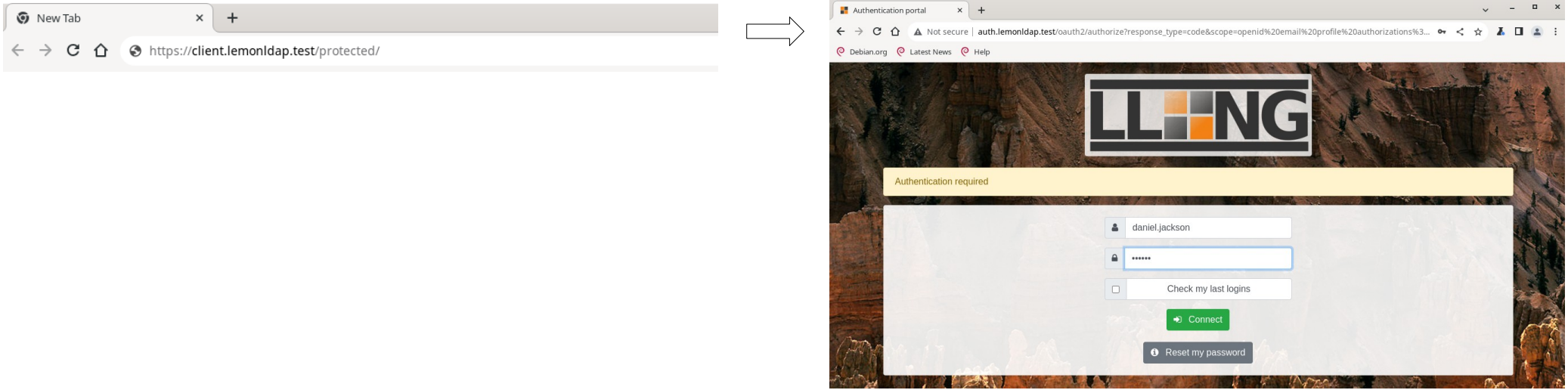
2.18.0

OIDC security:

- encryption of JWT (OIDC)
  - useful if you add some personnal info or right in the ID token
  - encryption of the JSON structure using the JWE specification
- PS256 (probabilistic version of RSA) for ID Token signature
  - different signature at each generation
- Accept EC algorithms for ID token signature: ES256/ES256K/ES384/ES512/EdDSA

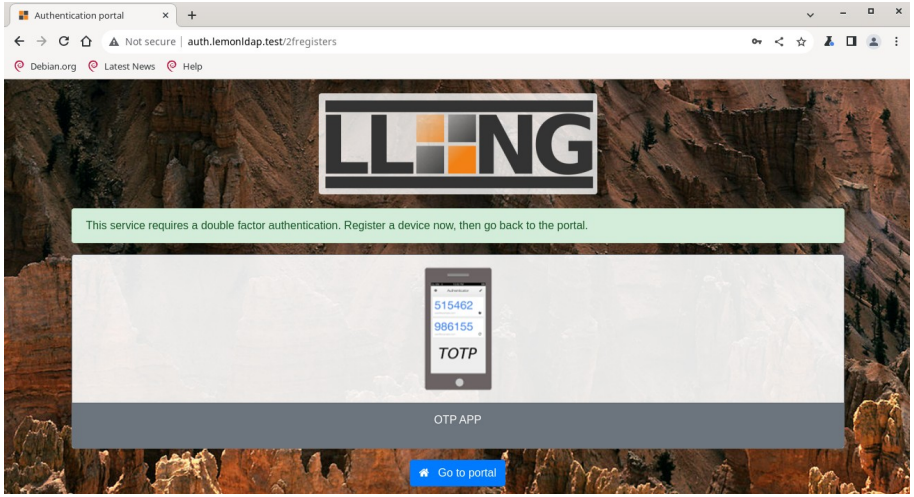
2.18.0

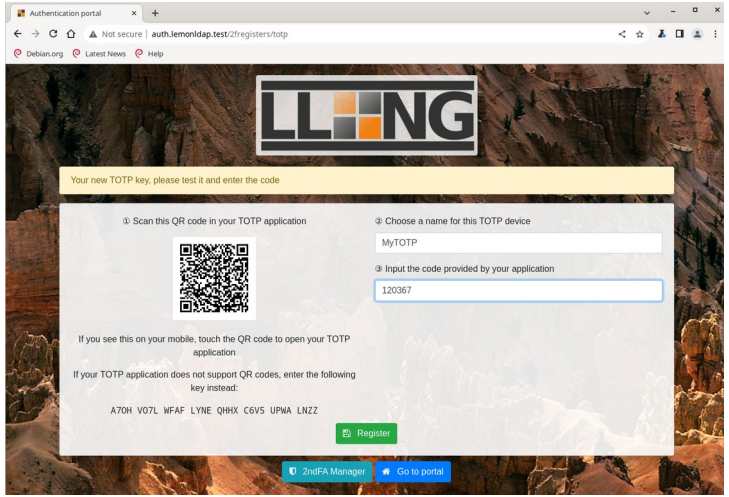
- Continue login after mandatory 2FA registration



2.18.0

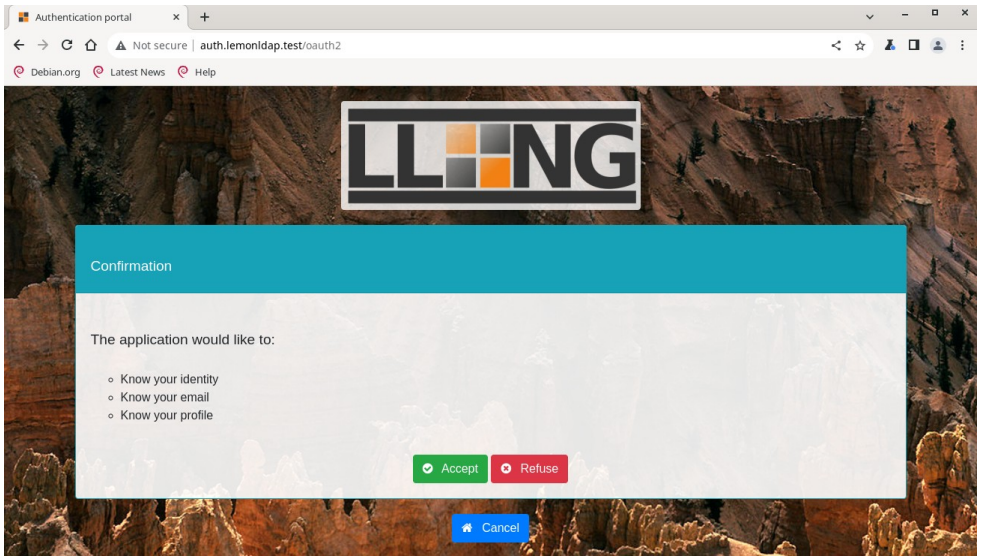
- Continue login after mandatory 2FA registration





2.18.0

- Continue login after mandatory 2FA registration



2.18.0

- Support **attestation** validation in WebAuthn 2FA
  - attestation is a feature in the FIDO and WebAuthn protocols
  - enables each RP to use a cryptographically verified chain of trust from the device's manufacturer to choose which security keys to trust
- New hook before 2FA validation
  - called immediately before LemonLDAP::NG calls the verify method of each second factor implementation
  - can be used to run additional checks

Keep informed about LL::NG

- Register to lemonldap-ng-announces mailing list
  https://mail.ow2.org/wws/subscribe/lemonldap-ng-announces
- Follow project updates
  https://projects.ow2.org/bin/view/lemonldap-ng/
- Social networks:
  - Twitter: https://twitter.com/lemonldapng/
  - Facebook: https://www.facebook.com/lemonldapng/

Thank you

info@worteks.com

@worteks_com

linkedin.com/company/worteks