



# New features in LemonLDAP::NG





Clément OUDOT  
Identity Solutions Manager  
Worteks

@clementoudot  



LemonLDAP::NG  
LDAP Tool Box  
LDAP Synchronization Connector  
FusionIAM  
W'Sweet



KPTN - <https://kptn.org>  
DonJon Legacy  
Improcité

## Service

Complex infrastructures, cloud, mail, authentication, security

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

## Edition



Collaborative portal



Common development platform



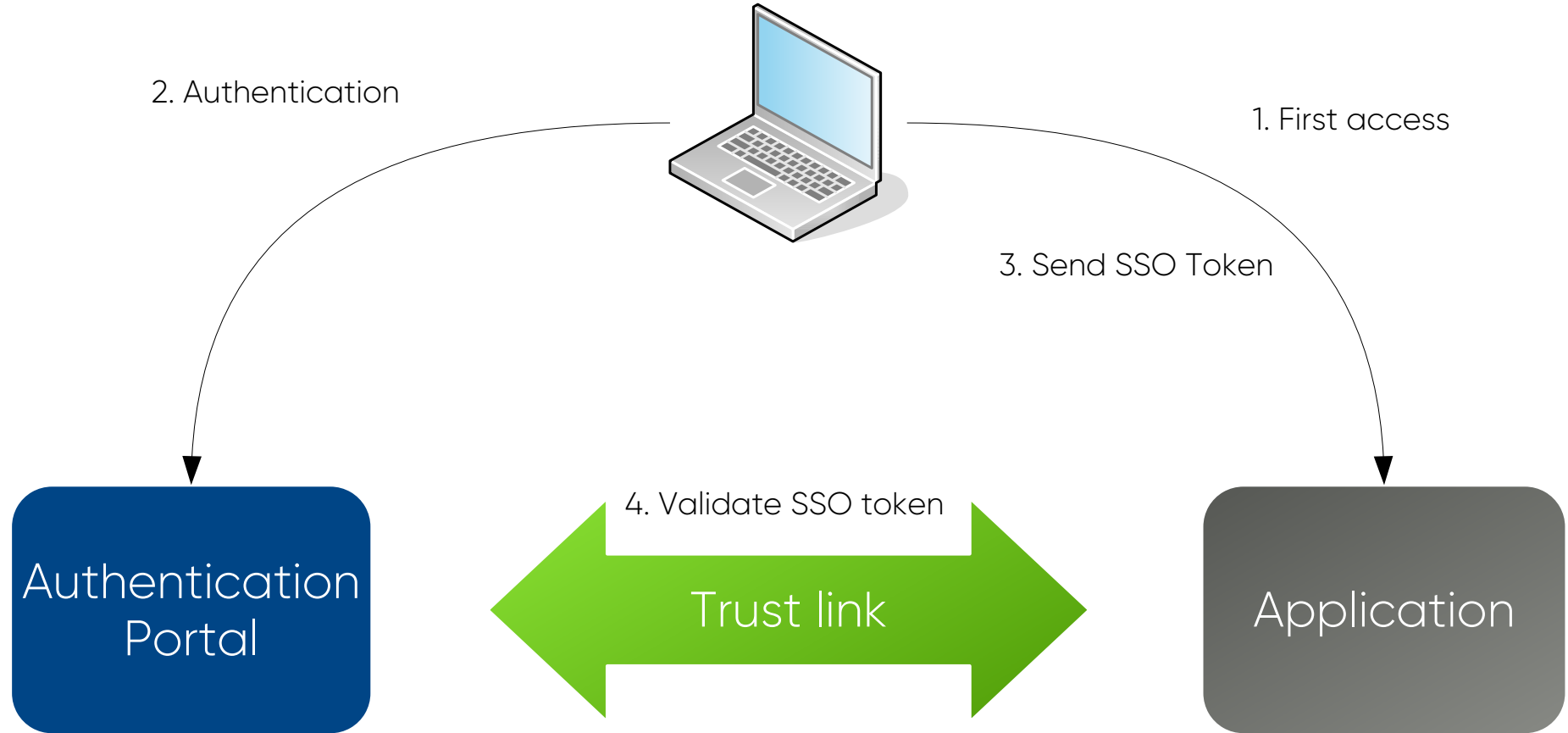
Identity and Access Management

## Partners

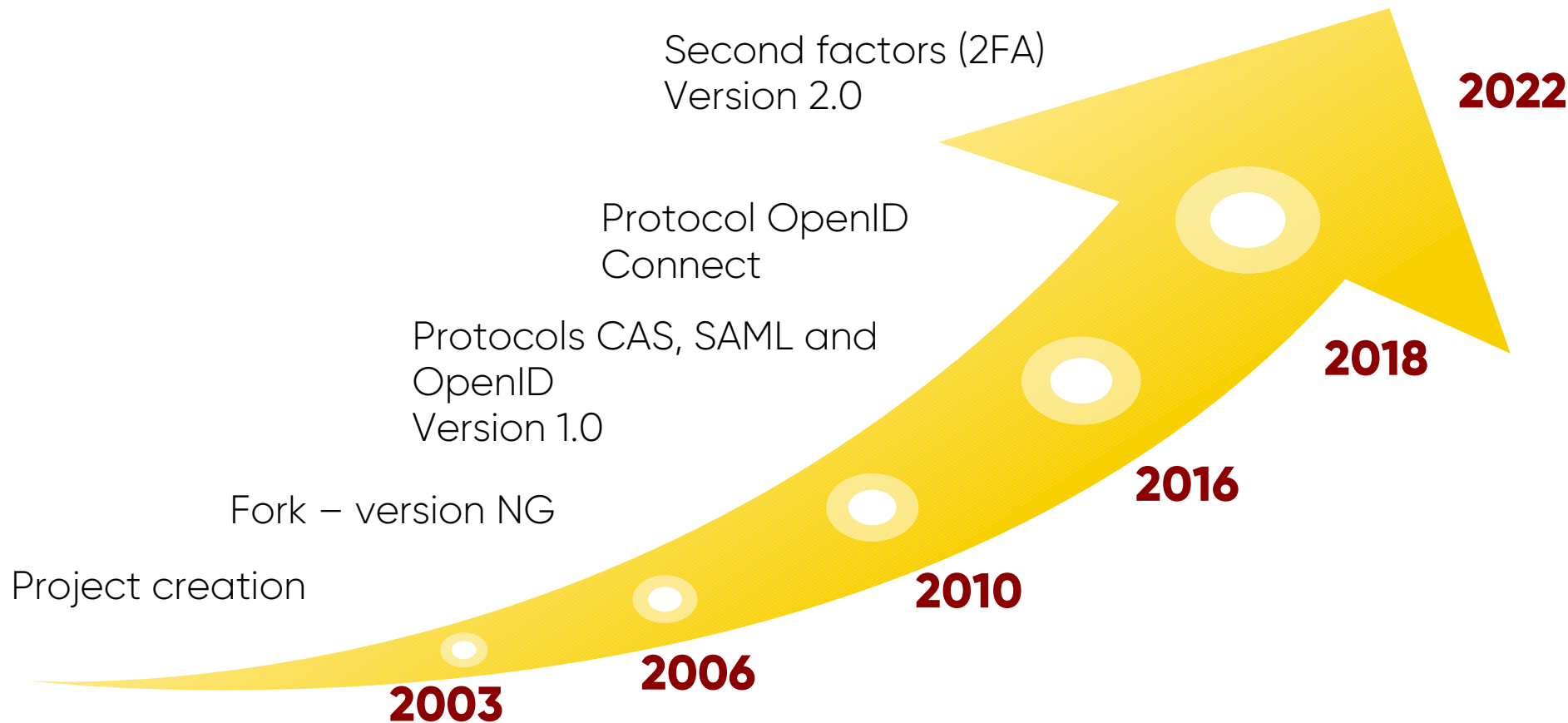


LemonLDAP::NG

# Web Single Sign On



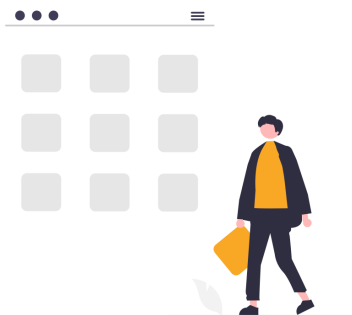
# Project history



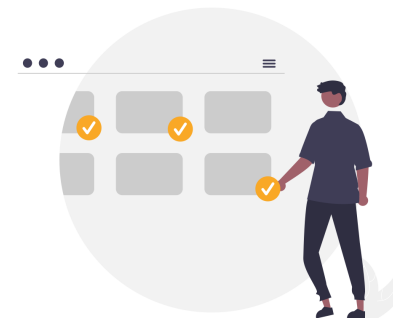
# Main features



SSO & Access Control



Application menu



CAS / SAML / OIDC



Second Factor (2FA)



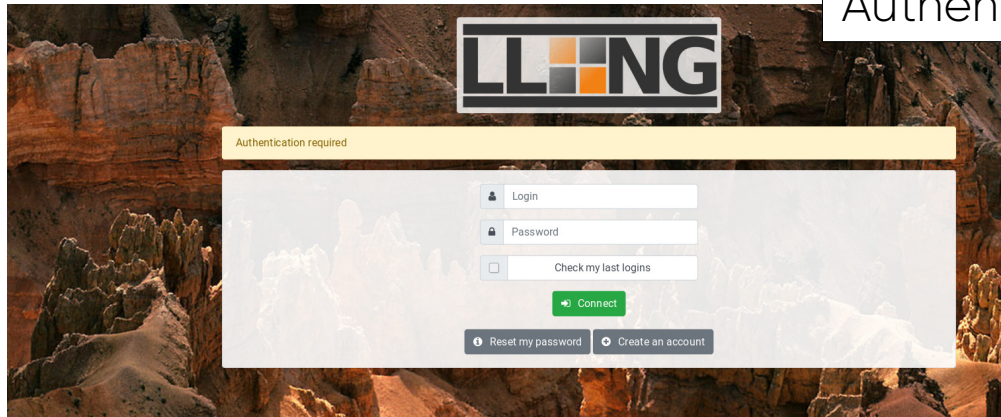
Password management



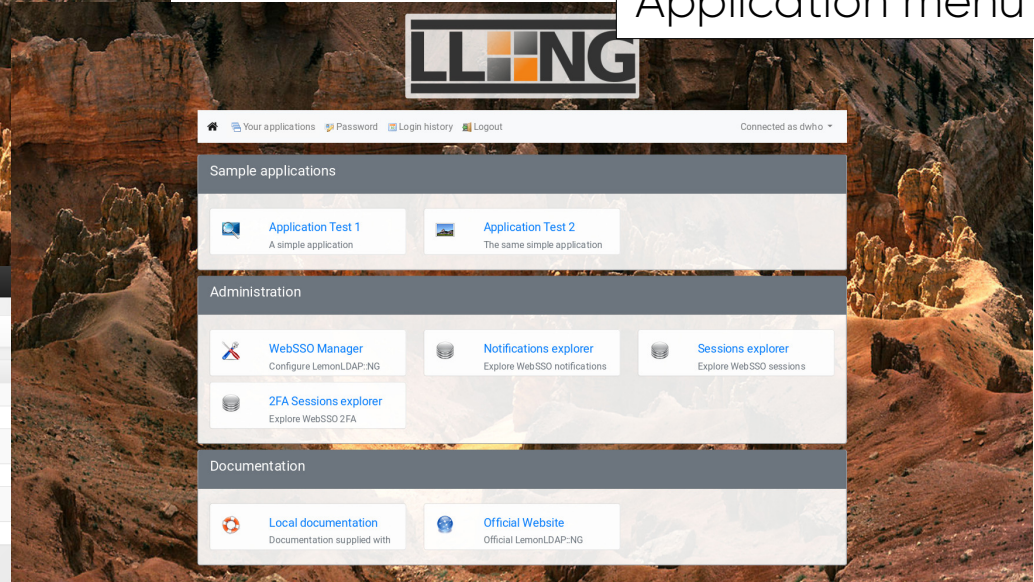
Graphical customization

# Screenshots

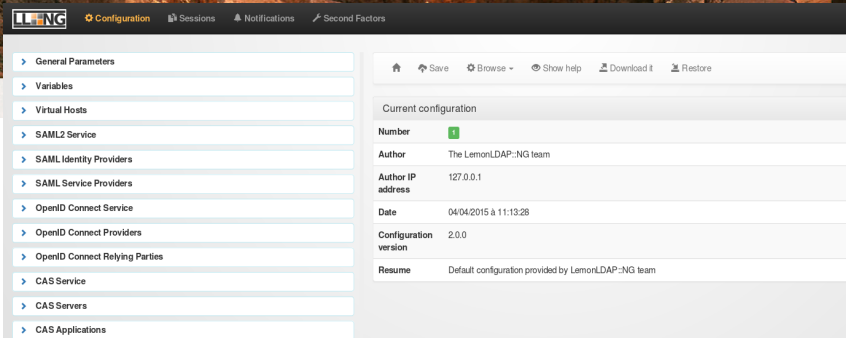
Authentication form



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?



# Back to the future

- Version 2.0 released in december 2018
- Version 2.0 features presented at OW2Con'19  
<https://www.worteks.com/opensource/conferences/2019-06-12-ow2con/>
- In 2022, version 2.0 is still the stable version, but got many improvements since the first release
- Current minor release: 2.0.14

- lemonldap-ng-cli (configuration management):
  - New actions to save and restore a configuration
  - "rollback" action to remove latest configuration and use the previous one
- lemonldap-ng-sessions (sessions management):
  - Inspect all sessions (SSO and persistent)
  - Search on any session key
  - Edit and delete
  - Specific actions for Second Factors and OIDC consents

- REST web services to edit configuration
- Documented with OpenAPI:  
<https://lemonldap-ng.org/manager-api/2.0/>
- Available operations:
  - Add/edit/delete SAML Service Providers
  - Add/edit/delete OIDC Relying Parties
  - Add/edit/delete CAS applications
  - Check API status
  - Manage 2FA registered for a user
  - Edit application menu (categories and applications)

# SAML protocol

- SHA256 is now the default algorithm (instead of SHA1)
- Possibility to directly generate a certificate in Manager instead of publishing only the public key

The screenshot shows the SAML Manager interface with a navigation bar at the top containing icons for home, save, browse, show help, new certificate, and download. The main content area is titled "Signature" and is divided into two columns: "Private key" and "Public key".

**Private key**

```
-----BEGIN RSA PRIVATE KEY-----
MIIEpQIBAAKCAQEAqHKSiuFzLSAe1nbNuJyZhdDuCZzTcKEOnFk+k0Gs5jgcp8TQ
f65Py4zAuExSVhwp1/1WFGocDzp7+4JsQIZkoFbKQIIAAlnskiR6jf30SNyQp1
bz9XEGvpgA5TFYp0Exx6.YXE34zgisLI/MOK+dqGIE31niDrLNdSfgxWytlpCd
in/HVFMuEw25XJdIXWwcoLXGxckmBPMYGNZ7dCpKszUdxBURFGHEWQLGL/MHk2zgj
kW0/OBVmP0aLAG/IYY9dTLKE1K8/DFSdigk8oGxmB2i3FoGAzTq6swyY7ZJge6VB
NCYsf6x3n9AZEeayQBSIs85FTIJXRJ8hEcn3QQIDAQABAoIBAFuaswbDxBbuONb4
IH/9zjkjUk/38SR28bMk9Vqvh9ORlcYCSmaI6RZNzU5JHfjwHey0key1Ocw/nS
VWMp018+049wmQGxT0EtEjzxsRtH/wkYxa0o2xSwxDYwYiSpHersUXBQWUKYI
```

**Public key**

```
-----BEGIN CERTIFICATE-----
MIIDQDCCAlGCCQDPu9MLFZJbWTANBgkqhkiG9w0BAQsFADBlMQswCQYDVQQGEwJG
UJETMBEGA1UECAwKU29tZS1TdGF0ZTENMAsGA1UEBwwETHIvbjEUMBIGA1UECgwL
T3BibikEIEENsdWlxGTAxBG9vBAMMEGF1dGgub3BibmlkLmNsdWlwHhcNMTYwMjAx
MTU1NzQ4WhcNMjYwMTI5MTU1NzQ4WjBIMQswCQYDVQQGEwJGUJETMBEGA1UECAwK
U29tZS1TdGF0ZTENMAsGA1UEBwwETHIvbjEUMBIGA1UECgwLT3BibikEIEENsdWlx
GTAxBG9vBAMMEGF1dGgub3BibmlkLmNsdWlwggEIMA0GCSqGSIb3DQEBAAUAA4IB
DwAwggEKAoIBAQCoKk4XMIIB7Wds1SPzJmEO4JnNwoQ6cWT6TQazmOBynxNB/
rk/LJMC4TFJWHcnX/VYUahwPOnv7gmxB9mSgVspCV8AAIKeySJHqN/IRI2thA/Vv
```

**Replace by file**

Parcourir... Aucun fichier sélectionné.

**Private key password**

\_\_\_\_\_

# OpenID Connect protocol

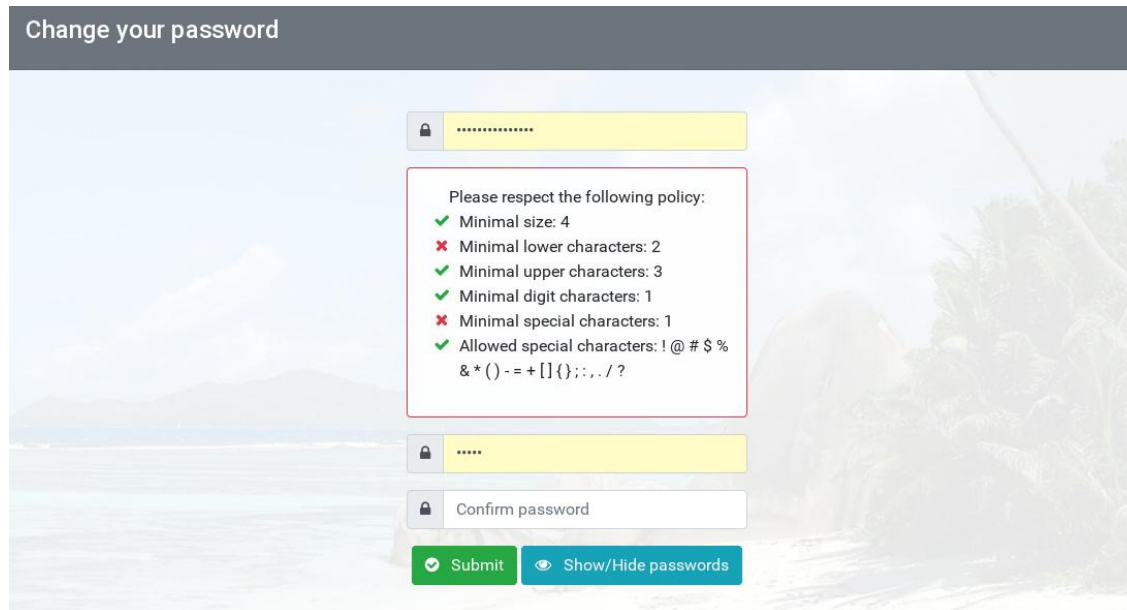
- Refresh tokens: linked to current session or long life tokens (offline mode)
- New OAuth2 endpoint: Introspection
- Possibility to publish claims in ID Token and Access Token
- New grants:
  - Resource Owner Password Credentials Grant
  - Client Credentials Grant

- A new hook system was introduced, allowing to adapt requests/responses outside the core of LemonLDAP::NG :
  - OpenID Connect hooks: `oidcGotRequest`, `oidcGotClientCredentialsGrant`, `oidcGenerateCode`, `oidcGenerateUserInfoResponse`, `oidcGenerateIDToken`, `oidcGenerateAccessToken`, `oidcResolveScope`
  - SAML hooks: `samlGotAuthnRequest`, `samlBuildAuthnResponse`, `samlGotLogoutRequest`, `samlGotLogoutResponse`, `samlBuildLogoutResponse`
  - CAS hooks: `casGotRequest`, `casGenerateServiceTicket`, `casGenerateValidateResponse`
  - Password hooks: `passwordBeforeChange`, `passwordAfterChange`



# Password Policy

- A local password policy can now be configured (minimal size, type of characters, ...)
- A graphical form shows which criteria are filled



Change your password

.....

Please respect the following policy:

- ✓ Minimal size: 4
- ✗ Minimal lower characters: 2
- ✓ Minimal upper characters: 3
- ✓ Minimal digit characters: 1
- ✗ Minimal special characters: 1
- ✓ Allowed special characters: !@#\$%&\*()-+[]{};:./?`

.....

Confirm password

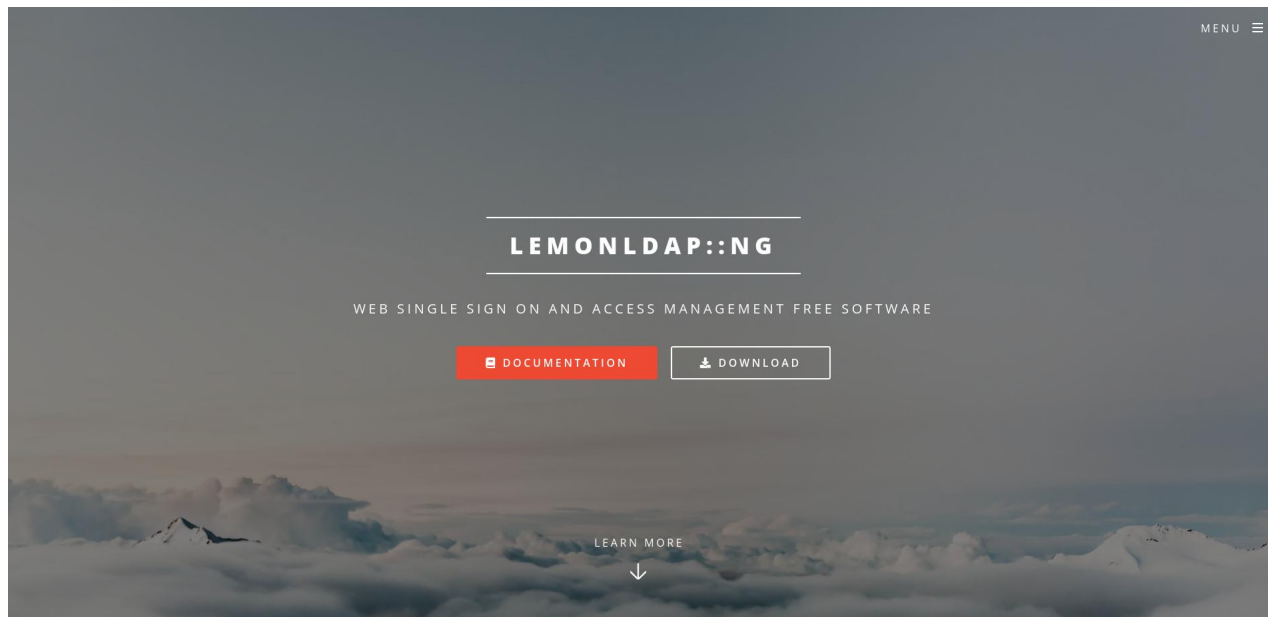
Submit Show/Hide passwords

# Second factors (2FA)

- The 2FA system was created in 2.0. New 2FA backends are now available:
  - Radius
  - WebAuthn (FIDO2)
- The second factor can now be asked only on session upgrade, when authentication level is too low to access an application
- Adaptive Authentication and Risk Based Authentication can be used to require a second factor
- TOTP secrets can now be encrypted

# Documentation and Website

- Documentation was rewritten with Sphinx (reStructuredText)
- Website rebuilt as static pages with Templar



# 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](mailto:info@worteks.com)

 [@worteks\\_com](https://twitter.com/worteks_com)

 [linkedin.com/company/worteks](https://www.linkedin.com/company/worteks)