LemonLDAP::NG Software
SSO Workflow

1. First access

2. Authentication

3. Send SSO Token

4. Validate SSO token

Authentication Portal

Trust link

Application
Main features

- Web Single Sign On
- Access control
- Applications portal
- Authentication modules choice and chain
- Password management, account creation
- Multi-factor authentication (MFA)
- Protection of Web applications and API/WebServices
- Graphical customisation
- Packages for Debian/Ubuntu/RHEL/CentOS
Portal with application menu
# Web Administration Interface

## Current Configuration

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number</td>
<td>1</td>
</tr>
<tr>
<td>Author</td>
<td>The LemonLDAP::NG team</td>
</tr>
<tr>
<td>Author IP address</td>
<td>127.0.0.1</td>
</tr>
<tr>
<td>Date</td>
<td>04/04/2015 à 11:13:28</td>
</tr>
<tr>
<td>Configuration version</td>
<td>2.0</td>
</tr>
<tr>
<td>Resume</td>
<td>Default configuration provided by LemonLDAP::NG team</td>
</tr>
</tbody>
</table>
Command Line Interface

```
root@ader-worteks:~# /usr/share/lemonldap-ng/bin/lemonldap-ng-cli info

Num  : 88
Author : clement
Author IP: localhost
Date  : Tue Dec 18 09:57:58 2018
Log   : Edited by lnConfigEditor

root@ader-worteks:~# /usr/share/lemonldap-ng/bin/lemonldap-ng-cli help
Usage: /usr/share/lemonldap-ng/bin/lemonldap-ng-cli <options> action <parameters>

Available actions:
- help            : print this
- info            : get current configuration info
- update-cache    : force configuration cache to be updated
- get <keys>      : get values of parameters
- set <key> <value>: set parameter(s) value(s)
- addKey <key> <subkey> <value>: add or set a subkey in a parameter
- delKey <key> <subkey>: delete subkey of a parameter

See Lemonldap::NG::Common::Cli(3) or Lemonldap::NG::Manager::Cli(3) for more
root@ader-worteks:~# /usr/share/lemonldap-ng/bin/lemonldap-ng-cli set ldapServer 'ldap://ldap.example.com'
```
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/
CAS, SAML and OpenID Connect

- LL::NG can act as client and as server
- Attributes sharing
- Manage authentication contexts and levels
- Autogeneration of public/private keys
- Access control per services
- Publication of configuration data (metadata)
- Multi-protocols gateway
- Single logout
Second Factor Authentication (2FA)

- LemonLDAP::NG can use the following 2FA:
  - TOTP
  - U2F
  - TOTP or U2F
  - Mail
  - External
  - REST
  - Yubikey
DevOps (SSO as a Service)

- Portal
- Sessions
- Web Application
- Handler

Authentication

Session creation

SSO cookie

Session read

Access rules

Exported headers

rules .json

HTTP headers
OpenID Connect / OAuth2

Portal

Authentication

Session creation

Sessions

OAuth2 Access Token

Session read

Handler

Web Application

HTTP headers
Support of RENATER / eduGAIN via SAML2:

- Service Provider
- Identity Provider

Call to Identity Provider selection page (WAYF) via SAML Discovery Protocol

Metadata bulk import script
Plugin engine

- Portal code was fully rewritten, and it now allows to write plugins
- Plugin examples, provided by default:
  - Auto Signin: direct authentication for some IP
  - Brute Force: protect against brute-force attacks
  - Stay Connected: "remember me" button
  - Public Pages: create static pages using portal skin
  - Impersonation: take the identity of another user
- Write a custom plugin:
  https://lemonldap-ng.org/documentation/latest/plugincustom
The beginning of the journey
Orange is a complex environment...

*With many people and kind of skills*  
*With thousands applications*  
*In a full motion environment*
Orange is a complex environment in complex world...

With many people and kind of skills With thousands applications In a full motion environment

**Long time partnerships**
- Orange people
- Contractors
- Partners
- Universities

**On demand relationships**
- Freelances with few days contracts

- Orange made or bought.
- Including SSO compatibility or not.
- Accessible from Internet or Intranet.
- Security access level specific for each.
- Each application has its own lifecycle.

- Our users want the same quality on work tools than on the personal offer on Internet.
- Rise of « fashion tool ».
...With the constraints and needs than others...

- Provide many types of protocols
- Manage all identification/authentication cases
- Allow access from different contexts
- Guaranty high security level
- Guaranty a high availability level
- Flexible to support future
- Manage all kinds of users
- Have a single system to authenticate users
- Keep things as transparent as possible for users
- Keep it simple, stupid
- Provide many types of protocols

12/06/2019
...So we are building a scalable LemonLDAP::NG infrastructure...

- **HA ext**
  - Lemon ext 1
  - Lemon ext 2
- **HA int**
  - Lemon int 1
  - Lemon int 2
- **Config Sessions**
  - then
  - Kerberos OS
  - OIdC
  - REST → LDAP
  - LDAP
- **Applications**
  - External Accounts
  - Orange Accounts
- **12/06/2019**
...And we are at the beginning of the journey...

We have tested LemonLdap in real conditions on many applications used by innovation people:
...Under industrialisation by a specialized team.

First team to « think »
- Test LemonLdap and try to get its limits
- Test the potential architectures
- Test intégration with about 20 applications (gitlab, nextcloud, jira & confluence, Dokuwiki, Apache 2, Flexible Engine, Grafana, WebCom, WordPress, OpenStack...).
- Test authentication protocols and ways (OTP, ...)

Another team to « build »

Final team to « Run »
- Get the results of the previous level to create an « industrial solution » able to support millions people.
Orange-Worteks Partnership

- Worteks offers a framework contract for support around LemonLDAP::NG and other free softwares, with two parts:
  - Incident management: a ticket can be opened to solve any fault on a production or development system (business hours)
  - Evolutions: a request can be done to fix bugs or code new features in the software
- Any Orange Business Unit can request a contract, prices are already defined
- It can then contribute to LemonLDAP::NG roadmap by requesting evolutions
Thanks to all the contributors

Thank you to all the contributors to this project, for their competence, their good humor and their motivation that are overcoming all the problems that veinly tried to stand up against us:

- **The LemonLDAP::NG Team** (Clément, Xavier and all the others).

- **Worteks** for the support.


- **All others** success keys in this project:
Gendarmerie Nationale
ST(SI)^2
History

• 2002: First WebSSO GN (SiteMinder)
• Licencing cost : 90 k€/year for 5000 users (target ~1 M€/year)
→ Take LemonLDAP over from the Ministry of finance
• 2005: Development of LL::NG (fork), SSO now used by (almost) all civil services
Budget

- Project build (excluding machine cost):
  - Between 2005 and 2015: ~ 150 k€
  - 2015: 100 K€
  - 2016 & 2017: 0 €
  - 2018: 25 k€
  - 2019: 0 €
Technical team for all ST(SI)$^2$ SSO

- X. Guimard: Lead developer LL::NG
- S. Marcq: Project manager
- A. Rosier & C. Maudoux: developers and administrators
Platforms

- Proxyma → GN
- CheopsNG → PN
- PSI → SP (SAML with interior security services)
- Judiweb → SP RIE (government network)
- Curasso & Espresso → internet SSO
- SAML with 12 civil services
Proxyma : SSO GN

- ~ 22 millions requests / day
- ~ 65 000 unique users / day
- 253 different applications used / day
- 12 reverse proxies
- 7 LDAP servers
- 4 portals
Top 10 connection's peak during 10 min
Top 10 event’s peak during 10 min

- lun. déc. 20
- 2019
- lun. mai 6
- lun. mai 13
- lun. mai 20

500 076
549 750
Top 10 unique user’s peak during 10 min
Unique users / month

- Janvier 2019: 104,432
- Février: 102,386
- Mars: 102,458
- Avril: 102,694
« good authentification » / month

- Février: 9,325,920
- Mars: 10,750,451
- Avril: 10,107,582
2019/2020 Evolution

- Upgrade all platform → LL::NG 2.0
- Connect Agent implementation
- 2FA implementation
- Cloud : SSO as a service (handler devops + scalability)
THANKS

Pour plus d’informations :

- info@worteks.com
- @worteks_com
- linkedin.com/company/worteks