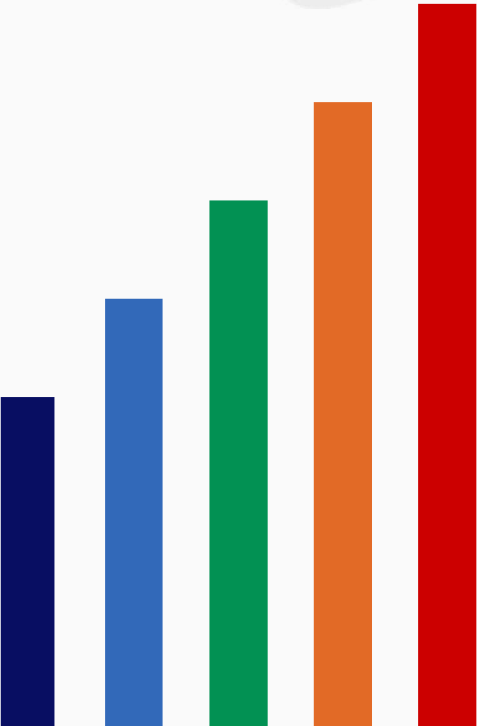




LDAP Tool Box, an Open Source project for OpenLDAP and Active Directory management

Table of contents



Packages and monitoring

CLI for OpenLDAP

Self Service Password

White Pages

Service Desk



LDAP Tool Box

Introduction

\$ ldapwhoami



Clément OUDOT
Identity Solutions Manager
Worteks

@clementoudot



LemonLDAP::NG
LDAP Tool Box
LDAP Synchronization Connector
FusionIAM



Creative Commons Music

Worteks

Open Source software experts and sovereign cloud providers
Training center

Actively contributing to numerous Open Source software like
LSC, LemonLDAP::NG, LDAP Tool Box, FusionIAM and OpenStack

Partners



Comprehensive offer

Heterogeneous and complex infrastructures, troubleshooting, cloud, mail, identity, authentication, security...

Worteks addresses a wide range of issues associated with your information system.



Audit and consulting



Technical expertise



Support and maintenance



Training



R&D and innovation

Customized solutions

Worteks publishes packaged solutions, entirely composed of Open Source bricks.

These solutions are available On Premise, SaaS or PaaS with our W'aaS offer.



Collaborative platform



Identity and access management solution



Complex infrastructure deployment solution



Ready to sing?

SCORPIONS



Password

WIND OF CHANGE

Scorpions – Password change

I follow the process
Down to login page
My account need a password change
It took me all the night
To be able to comply
To complexity rules of password change

Hackers brute force the login
Did you ever think
That they could be so close, in your browser
My password is in the air
I can see it everywhere
I know it really need to change

Take me to a simple application
Working day and night
That can connect to LDAP
Or AD, for a password change

You can breathe and relax
Here is LDAP Tool Box
An open source project, of course
OpenLDAP packages
Monitoring scripts
Web interfaces for password change



Packages and monitoring

OpenLDAP packages

- 2003: need to install OpenLDAP 2.1 on Red Hat server :
 - No recent packages available
 - Compilation required to set `OPENLDAP_FD_SETSIZE=4096` and choose overlays
- 2007: Creation of OpenLDAP 2.3 RPM packages for Red Hat Enterprise Linux 5
- 2013: Creation of OpenLDAP 2.4 packages for Debian

Current packages

- OpenLDAP 2.5, 2.6 and 2.7
- Debian Buster (10), Bullseye (11), Bookworm (12), Trixie (13)
- Ubuntu Jammy (22.04 LTS)
- RHEL 7, 8, 9 and 10

Catch 'em all

- Packages on <https://ltb-project.org/download.html>
- APT and DNF/YUM repositories
- Recipes :
 - <https://github.com/ltb-project/openldap-rpm>
 - <https://github.com/ltb-project/openldap-deb>

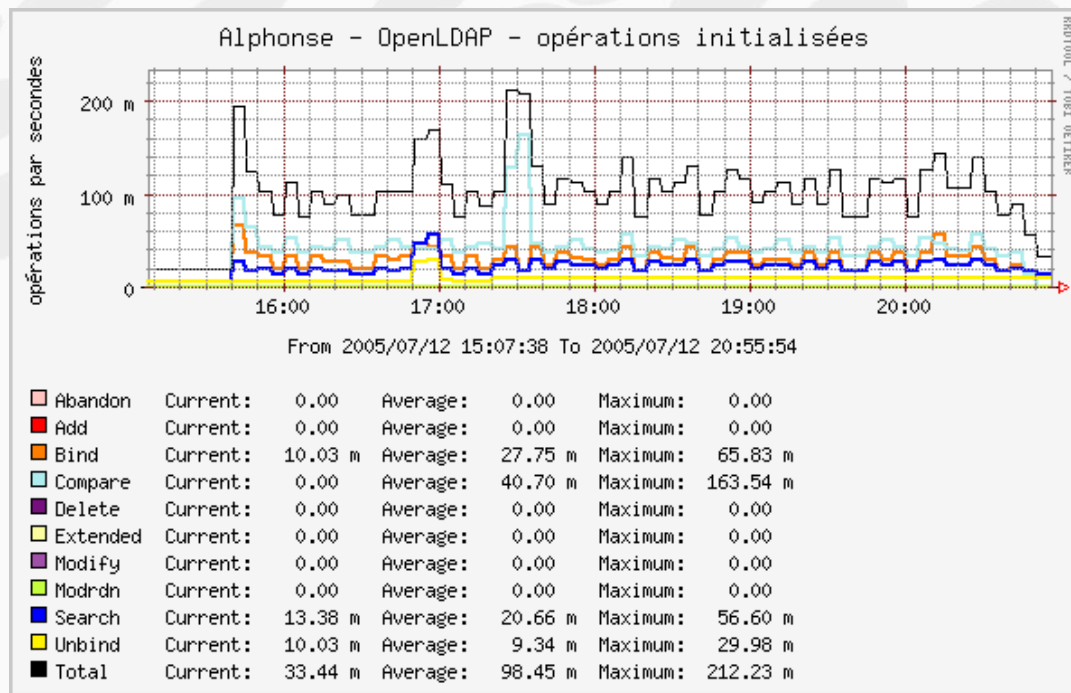
Monitoring

- 2003: Nagios default check_ldap was not suitable
 - Time precision in seconds
 - Request data suffix and not RootDSE, required to check LDAP proxies health
- Creation of several Nagios plugins:
 - check_ldap_time.pl
 - check_berkeleydb_locks.pl
 - check_ldap_slurpd_status.pl

More plugins

- Evolutions of plugins with OpenLDAP versions:
 - `check_ldap_monitor.pl`
 - `check_ldap_query.pl`
 - `check_ldap_syncrepl_status.pl`
 - `check_lmdb_usage.pl`

<https://github.com/ltb-project/nagios-plugins>



<https://github.com/ltb-project/cacti-plugins>

Not maintained any more

CLI for OpenLDAP

Stop, start and a lot more

- OpenLDAP does not provide any start/stop script
- First shell script for SysInit V: start, stop, restart, status
- Add actions to backup/restore data and config (slapd.conf and cn=config)
- Compatibility to SystemD
- Actions to check synchronization, import sample data and configuration
- Rename “OpenLDAP init script” to “slapd CLI”

Commands

- `slapd-cli start / slapd-cli stop / slapd-cli restart`
- `slapd-cli backup / slapd-cli restore`
- `slapd-cli backupconfig / slapd-cli restoreconfig`
- `slapd-cli debug`
- `slapd-cli status`
- `slapd-cli convertconfig /path/to/slapd.conf config.ldif`
- `slapd-cli configtest`
- `slapd-cli checksync`

Check synchronization

```
root@ltb:~# slapd-cli checksync
slapd-cli: [INFO] Using /usr/local/openldap/etc/openldap/slapd-cli.conf for configuration
slapd-cli: [INFO] Checking synchronization...
Suffix: dc=example,dc=com
detected providers:
rid="001" provider="ldaps://ldap2.example.com" type="refreshAndPersist" retry="5 5 300 +"
bindmethod="simple" binddn="cn=syncrepl,ou=dsa,dc=example,dc=com" credentials="secret"
searchbase="dc=example,dc=com"

Checking contextCSN for suffix dc=example,dc=com on remote host ldaps://ldap2.example.com
  Checking SID #001#
    INFO: remote (20240614155432.671536Z#000000#001#000000) and local
(20240614155432.671536Z#000000#001#000000) contextCSN found and synchronized
  Checking SID #002#
    INFO: remote (20240614155433.416314Z#000000#002#000000) and local
(20240614155433.416314Z#000000#002#000000) contextCSN found and synchronized
slapd-cli: [OK] Local directory synchronized to every declared provider
```



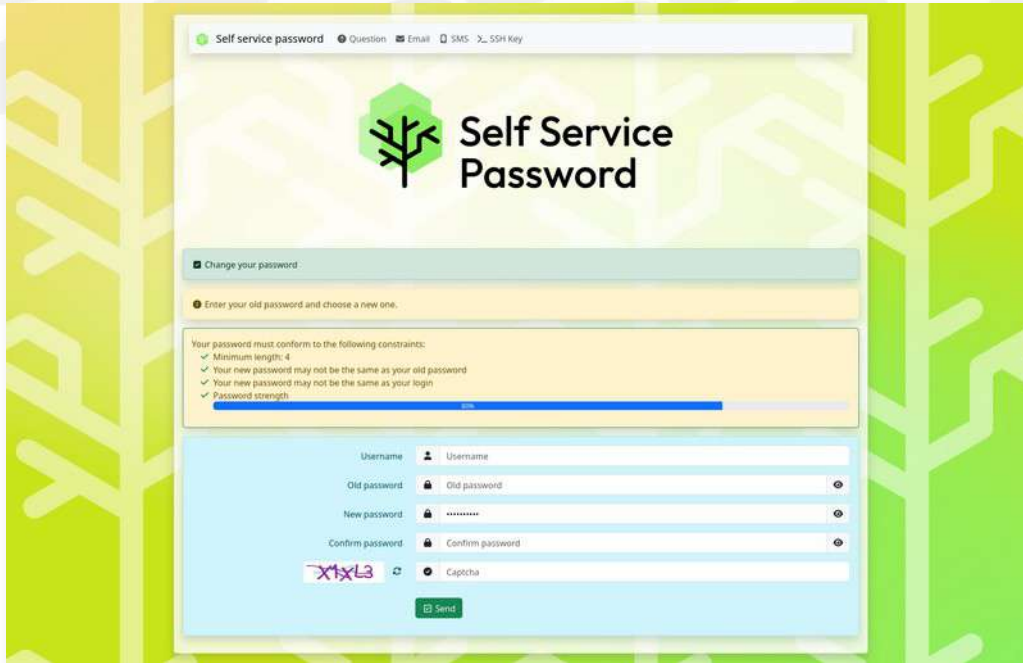


Self Service Password

Self Service Password

- **How it starts:** 2009, need a web form to change password on Active Directory, search on internet, nothing found...
- Creation of a PHP single page application with a configuration file and a design not too ugly
- Publication inside LDAP Tool Box project
- Password reset features and AD/OpenLDAP support
- **Now:** 1,3k stars on github, 29 languages

Features



The screenshot shows a web interface for 'Self Service Password'. At the top, there's a navigation bar with links: 'Self service password', 'Question', 'Email', 'SMS', and 'SSH Key'. The main heading is 'Self Service Password' with a green hexagonal logo containing a stylized tree. Below the heading, there's a section titled 'Change your password:' with a sub-instruction 'Enter your old password and choose a new one.' A yellow box lists password constraints: 'Your password must conform to the following constraints:' followed by a checklist: '✓ Minimum length: 4', '✓ Your new password may not be the same as your old password', '✓ Your new password may not be the same as your login', and '✓ Password strength'. A blue progress bar is shown below the checklist. The form fields include 'Username', 'Old password', 'New password', 'Confirm password', and a 'Captcha' field with a 'Send' button. A small 'X1xL3' logo is visible near the captcha.

- Change password
- Reset password by mail
- Reset password by questions
- Reset password by SMS
- Password policy
- Change SSH key
- Mail notifications
- REST API
- Audit file
- Hooks
- Mail/phone attributes update

Advanced LDAP

- LDAPS / StartTLS
- Pagination
- Password hash for OpenLDAP or AD
- Password policy control: know if account is locked or expired, get password complexity check result
- Password modify extended operation: because we can...

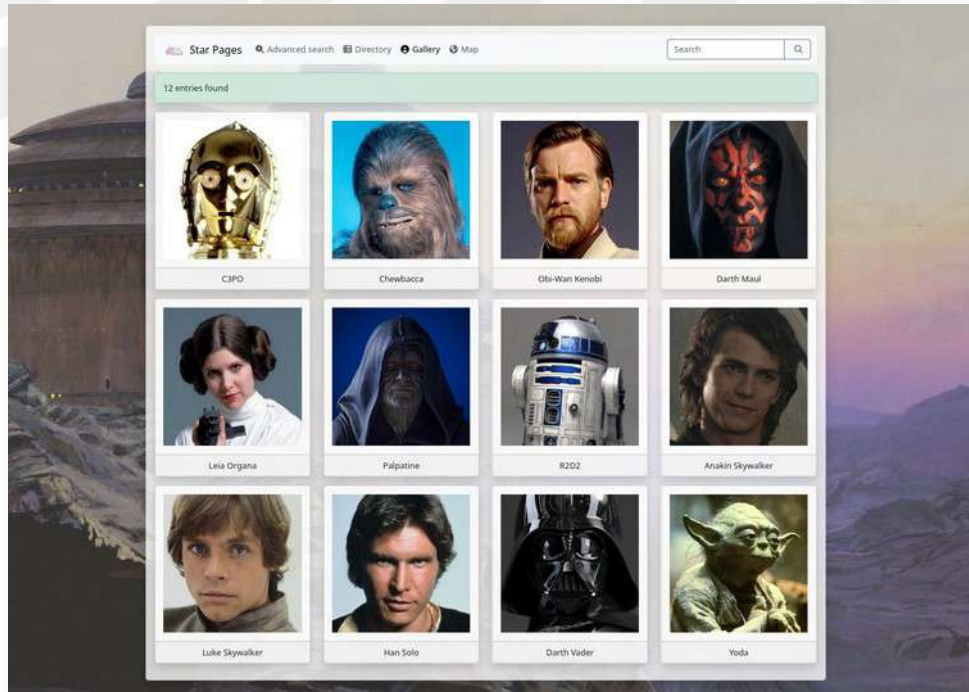


White Pages

White Pages

- OpenLDAP has no graphical interface (slapcat is not one...)
- Need a simple web application to search users and groups and display them, not an LDAP Browser (Apache Directory Studio is already here)
- Compatible with any LDAP directory, including AD
- First release in 2016

Features



- Quick and advanced search
- Directory
- Gallery
- Map (OpenStreetMap API)
- Export as vCard
- Export as CSV
- Anonymous/Authenticated access
- Edit own account

Edit own account

- Requires authentication (SSO or LDAP)
- Photo update in LDAP server (jpegPhoto) and/or on disk
- Configuration of allowed items for modification
- Direct link in menu to “your account”

The screenshot shows a web interface for editing a user account. At the top, there's a navigation bar with 'White Pages', 'Advanced search', 'Directory', 'Gallery', 'My account', and 'Logout'. A search bar is on the right. The main header shows the user's name 'Clément OUDOT'. Below this is a profile picture of a man with glasses and a beard. There are two buttons: 'Update photo' (green) and 'Delete photo' (grey). The form contains several fields: 'First name' (Clément), 'Last name' (OUDOT), 'Title' (Mr), 'Mail' (clem.oudot@example.com), 'Mail quota' (976,56 KB), 'Phone' (empty), 'Mobile' (+33 6 12 34 56 78), and 'Organization' (Worteks). Under 'Organization', there's a link 'Groupe avec deux espaces' and a list of groups: 'Les administrateurs', 'Group Test 1', 'Group Test 2', 'Group Test 3', 'Group Test 4', 'Group Test 5', and 'Les utilisateurs'. The 'Member of groups' section is empty. At the bottom, there are two buttons: 'Submit' (green) and 'Cancel and go back to entry' (grey).

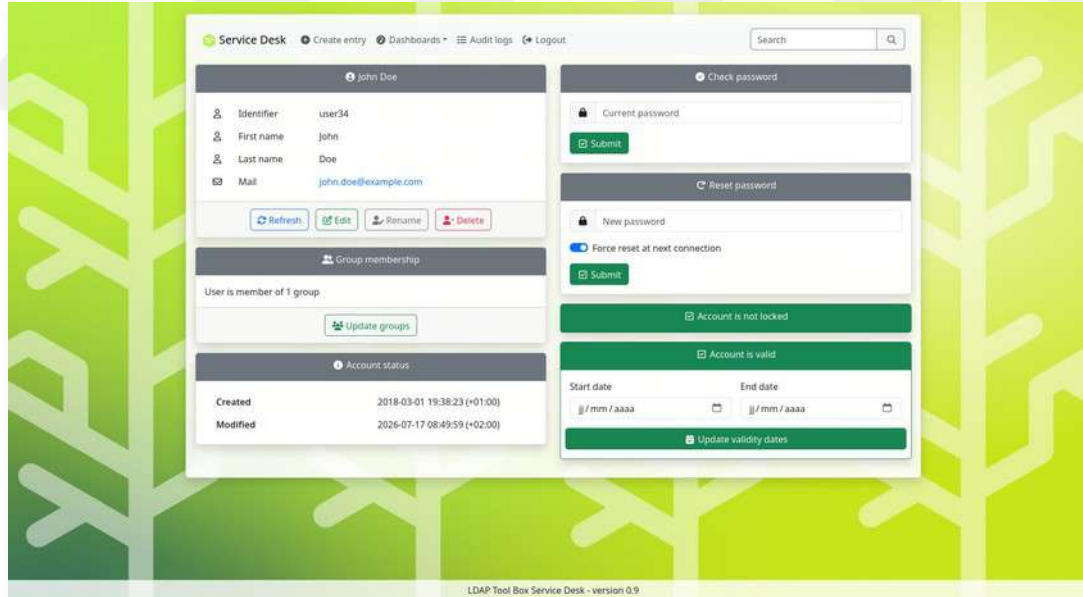


**Service
Desk**

Service Desk

- We deployed a mail SaaS solution for a big customer:
 - OpenLDAP as user database and LemonLDAP::NG as Authentication Portal (SSO/IDP)
 - Users could change their password
 - Most of them call support, and support need to reset passwords in the LDAP directory
- We created a first “Service Desk” application in a few days: quick search of a user in LDAP, display main attributes and account status, check password, reset password
- First release in 2020

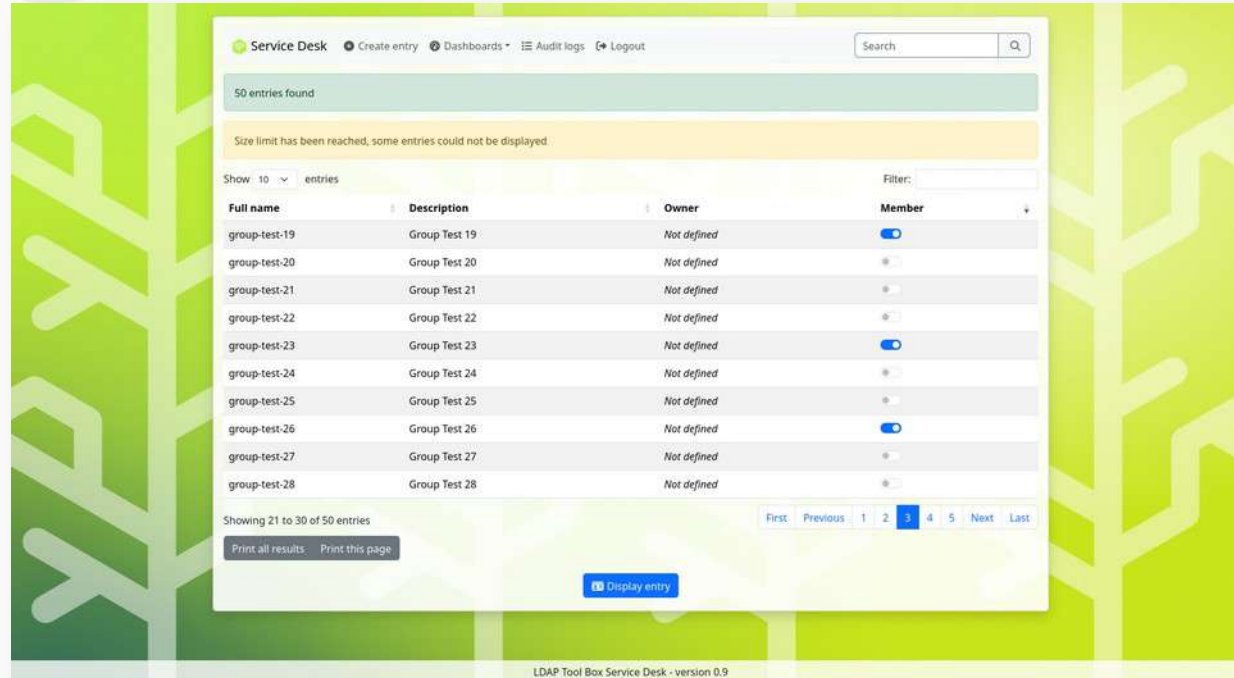
Features



- Check/reset password
- Lock/unlock account
- Enable/disable account
- Change validity dates
- Create/modify/rename/delete accounts
- Manage group membership
- Audit logs
- Comments
- Hooks
- Dashboards

Group membership

Display a list of groups, starting by ones the user is member of, and allow to add/remove user from these groups



The screenshot shows the 'Service Desk' interface of the LDAP Tool Box. At the top, there are navigation links: 'Create entry', 'Dashboards', 'Audit logs', and 'Logout'. A search bar is also present. Below the navigation, a message states '50 entries found' and 'Size limit has been reached, some entries could not be displayed'. The main content is a table with columns: 'Full name', 'Description', 'Owner', and 'Member'. The table lists 10 test groups, each with a 'Member' toggle switch. The 'Member' column is sorted in descending order, with the first three groups having their membership toggles turned on. At the bottom, there are pagination controls showing 'Showing 21 to 30 of 50 entries' and a 'Display entry' button.

Full name	Description	Owner	Member
group-test-19	Group Test 19	Not defined	☒
group-test-20	Group Test 20	Not defined	☐
group-test-21	Group Test 21	Not defined	☐
group-test-22	Group Test 22	Not defined	☐
group-test-23	Group Test 23	Not defined	☒
group-test-24	Group Test 24	Not defined	☐
group-test-25	Group Test 25	Not defined	☐
group-test-26	Group Test 26	Not defined	☒
group-test-27	Group Test 27	Not defined	☐
group-test-28	Group Test 28	Not defined	☐

Showing 21 to 30 of 50 entries

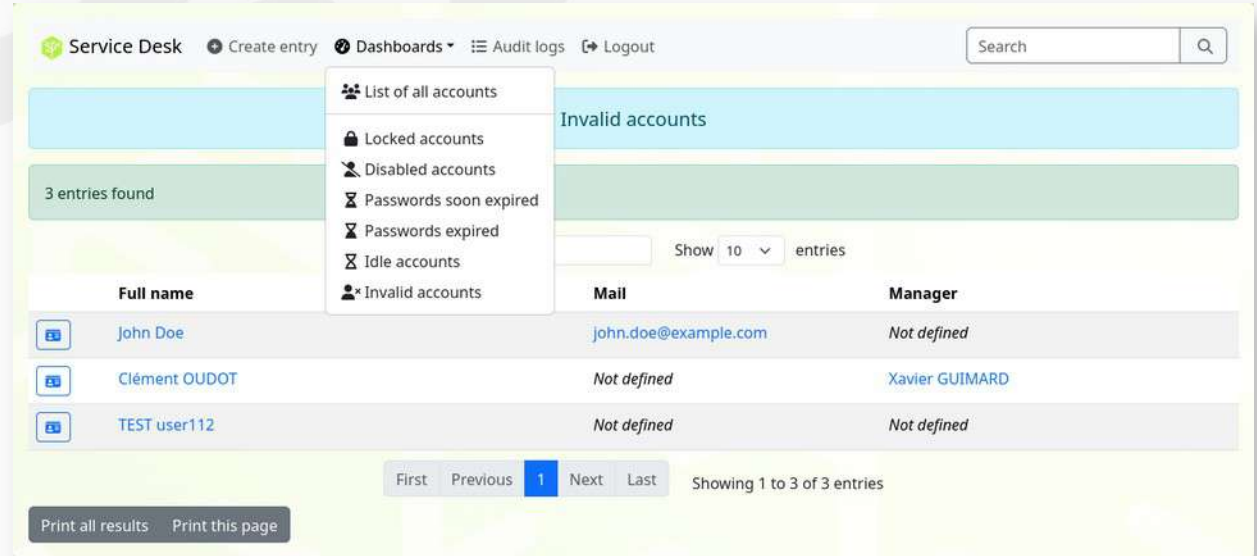
Print all results Print this page

Display entry

LDAP Tool Box Service Desk - version 0.9

Dashboards

- All accounts
- Accounts locked
- Accounts disabled
- Accounts with a password that will soon expire
- Accounts with an expired password
- Accounts idle
- Accounts invalid



The screenshot shows the 'Service Desk' interface with a 'Dashboards' dropdown menu open. The menu lists several filters: 'List of all accounts', 'Locked accounts', 'Disabled accounts', 'Passwords soon expired', 'Passwords expired', 'Idle accounts', and 'Invalid accounts'. The 'Invalid accounts' filter is selected, and the main content area displays a table of account details.

Invalid accounts

3 entries found

Show 10 entries

Full name	Mail	Manager
John Doe	john.doe@example.com	Not defined
Clément OUDOT	Not defined	Xavier GUIMARD
TEST user112	Not defined	Not defined

First Previous 1 Next Last Showing 1 to 3 of 3 entries

Print all results Print this page

Compatibility with AD

- OpenLDAP password management and AD password management are **totally different**
- On application side, we would like to avoid coding each function to adapt to OpenLDAP and AD
- Solution: creation of PHP ltb-common library and a “Directory” object interface (Ltb\Directory):
 - Ltb\Directory\OpenLDAP
 - Ltb\Directory\ActiveDirectory
- Easy to add another product, like 389DS

```
namespace Ltb;
use \DateTime;

interface Directory
{
    /**
     * Get specific operational attributes
     */
    public function getOperationalAttributes() : array;

    /**
     * Is account locked?
     */
    public function isLocked($entry, $pwdPolicyConfiguration) : bool;

    /**
     * Date when account has been locked
     */
    public function getLockDate($entry, $pwdPolicyConfiguration) : ?DateTime;

    /**
     * Date when account will be automatically unlocked
     */
    public function getUnlockDate($entry, $pwdPolicyConfiguration) : ?DateTime;

    /**
     * Lock account
     */
    public function lockAccount($ldap, $dn) : bool;

    /**
     * Unlock account
     */
    public function unlockAccount($ldap, $dn) : bool;

    /**
     * Is password expired?
     */
    public function isPasswordExpired($entry, $pwdPolicyConfiguration) : bool;

    /**
     * Date when password will be expired
     */
    public function getPasswordExpirationDate($entry, $pwdPolicyConfiguration) : ?DateTime;

    /**
```

Roadmap

Roadmap / Backlog

- Rewrite slapd-cli in C, add new actions
- Self Service Password:
 - Notifications script (password expiration, answers initialization, ...)
- White Pages:
 - Possibility to manage any object (user, group, organizations, ...)
 - Display organizational chart
 - Plugin system
- Service Desk:
 - Possibility to manage any object (user, group, organizations, ...)
 - Bulk import via CSV

Don't believe me...

Try it !



LDAP Tool Box

<https://ltb-project.org>

LDAP2026

TUEBINGEN

www.vorteks.com

 info@vorteks.com

 +33 1 84 20 86 47

 vorteks.com

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