

LDAP Account Manager - Manual

LDAP Account Manager - Manual

Table of Contents

| | |
|---|------|
| Overview | viii |
| 1. Big picture | 1 |
| Overview | 1 |
| Glossary | 3 |
| Architecture | 3 |
| 2. Installation | 5 |
| New installation | 5 |
| Requirements | 5 |
| Prepackaged releases | 5 |
| Installing the tar.bz2 | 7 |
| Docker | 8 |
| System configuration | 8 |
| Upgrading LAM or migrate from LAM to LAM Pro | 9 |
| Upgrade LAM | 9 |
| Version specific upgrade instructions | 10 |
| Uninstallation of LAM (Pro) | 14 |
| Migration to a new server | 14 |
| 3. Configuration | 16 |
| General settings | 17 |
| Configuration Database | 17 |
| License (LAM Pro only) | 17 |
| Security settings | 17 |
| Password policy | 18 |
| Logging | 19 |
| Mail options (LAM Pro) | 20 |
| WebAuthn/FIDO2 devices | 20 |
| Module settings and global cron job (LAM Pro) | 21 |
| Change master password | 21 |
| Server profiles | 21 |
| Manage server profiles | 21 |
| Editing a server profile | 23 |
| Cron jobs (LAM Pro) | 34 |
| Typical scenarios | 47 |
| Self Service (LAM Pro) | 48 |
| Import and export configuration | 48 |
| 4. Managing entries in your LDAP directory | 50 |
| Typical usage scenarios | 51 |
| Users | 53 |
| Personal | 55 |
| Unix | 59 |
| Group of names and group of members (LAM Pro) | 64 |
| Organizational roles (LAM Pro) | 65 |
| Shadow | 66 |
| NIS net groups | 66 |
| Password self reset (LAM Pro) | 67 |
| Hosts | 69 |
| Samba 3 | 69 |
| Windows (Samba 4/Active Directory) | 72 |
| AD LDS (formerly ADAM) (LAM Pro) | 77 |
| Filesystem quota (lamdaemon) | 81 |
| Filesystem quota (LDAP) | 82 |
| Kolab | 82 |
| Asterisk | 83 |
| EDU person | 83 |
| PyKota | 84 |

| | |
|--|-----|
| Password policy (LAM Pro) | 86 |
| Account locking for 389ds (LAM Pro) | 86 |
| FreeRadius | 87 |
| Heimdal Kerberos (LAM Pro) | 88 |
| MIT Kerberos (LAM Pro) | 89 |
| NIS mail aliases | 91 |
| Courier mail | 93 |
| Qmail (LAM Pro) | 94 |
| Mail routing | 95 |
| SSH public keys | 96 |
| SSH public keys (AD) | 97 |
| YubiKey | 98 |
| Authorized services | 100 |
| IMAP mailboxes | 100 |
| IP addresses (LAM Pro) | 102 |
| Account | 102 |
| OpenLDAP TOTP (LAM Pro) | 103 |
| Last login (LAM Pro) | 103 |
| Groups | 104 |
| Unix | 104 |
| Unix groups with rfc2307bis schema (LAM Pro) | 106 |
| Samba 3 | 108 |
| Windows (Samba 4) | 109 |
| AD LDS (formerly ADAM) (LAM Pro) | 110 |
| Kolab | 111 |
| Mail routing | 112 |
| Quota | 112 |
| Dynamic lists (LAM Pro) | 113 |
| PyKota | 115 |
| Hosts | 115 |
| Password policy (LAM Pro) | 116 |
| Hosts | 116 |
| Account | 116 |
| Device (LAM Pro) | 116 |
| Samba 3 | 116 |
| Windows (Samba 4) | 117 |
| IP addresses (LAM Pro) | 118 |
| MAC addresses | 118 |
| Puppet | 118 |
| NIS net groups | 119 |
| Password policy (LAM Pro) | 120 |
| Samba 3 domains | 120 |
| Group of (unique) names and group of members (LAM Pro) | 121 |
| Organizational roles (LAM Pro) | 123 |
| Simple Security Object (LAM Pro) | 125 |
| Asterisk | 125 |
| Kopano (LAM Pro) | 127 |
| Users | 127 |
| Contacts | 129 |
| Groups | 130 |
| Address lists | 131 |
| Dynamic groups | 132 |
| Servers | 133 |
| Kolab shared folders | 135 |
| DHCP | 136 |
| Bind dyndb-ldap (LAM Pro) | 139 |
| Configuration | 140 |
| DNS zones | 141 |

| | |
|--|-----|
| DNS entries | 142 |
| Bind DLZ (LAM Pro) | 145 |
| Configuration | 145 |
| DNS entries | 147 |
| XFR entries | 151 |
| PowerDNS (LAM Pro) | 152 |
| Aliases (LAM Pro) | 153 |
| Mail aliases | 154 |
| NIS mail aliases | 154 |
| Courier mail aliases | 155 |
| NIS net groups | 155 |
| NIS objects (LAM Pro) | 156 |
| Automount objects (LAM Pro) | 156 |
| Oracle databases (LAM Pro) | 157 |
| Password policies (LAM Pro) | 159 |
| MIT Kerberos policies (LAM Pro) | 160 |
| PyKota printers | 161 |
| PyKota billing codes | 162 |
| Custom types (LAM Pro) | 163 |
| Custom fields (LAM Pro) | 164 |
| Custom scripts (LAM Pro) | 173 |
| Sudo roles (LAM Pro) | 177 |
| LDAP views based on nsview (LAM Pro) | 178 |
| Apache Guacamole (LAM Pro) | 179 |
| Auto delete (LAM Pro) | 180 |
| General information | 181 |
| 5. Tools | 182 |
| Profile editor | 182 |
| PDF editor | 184 |
| File upload | 187 |
| Multi edit | 189 |
| LDAP import/export | 191 |
| Import | 191 |
| Export | 192 |
| OU editor | 193 |
| Tree view | 193 |
| Schema browser | 194 |
| Server information | 194 |
| WebAuthn devices | 195 |
| Tests | 196 |
| Lamdaemon test | 196 |
| Schema test | 196 |
| 6. Access levels and password reset page (LAM Pro) | 198 |
| Access levels | 198 |
| Password reset page | 198 |
| 7. Self service (LAM Pro) | 202 |
| Preparations | 202 |
| OpenLDAP ACLs | 202 |
| Other LDAP servers | 202 |
| Creating a self service profile | 202 |
| Edit your new profile | 204 |
| General settings | 204 |
| Page layout | 211 |
| Module settings | 214 |
| Samba 3 | 215 |
| Password self reset | 215 |
| User self registration | 219 |
| Request Access | 223 |

| | |
|---|-----|
| Custom fields | 228 |
| OpenLDAP TOTP | 235 |
| Adapt the self service to your corporate design | 236 |
| Custom header | 236 |
| CSS files | 236 |
| A. LDAP schema files | 237 |
| B. Security | 241 |
| LAM configuration passwords | 241 |
| Use of SSL | 241 |
| LDAP with SSL and TLS | 241 |
| Setup SSL certificates in LAM general settings | 241 |
| Setup SSL certificates on system level | 241 |
| SELinux | 242 |
| Chrooted servers | 243 |
| Protection of your LDAP password and directory contents | 243 |
| Apache configuration | 243 |
| Security headers | 243 |
| Sensitive directories | 243 |
| Use LDAP HTTP authentication for LAM | 244 |
| Self Service behind proxy in DMZ (LAM Pro) | 245 |
| Nginx configuration | 246 |
| Security headers | 246 |
| RPM based installations | 246 |
| DEB based installations | 246 |
| tar.bz2 based installations | 246 |
| WebAuthn/FIDO2 | 247 |
| C. Typical OpenLDAP settings | 248 |
| D. Setup for home directory and quota management | 249 |
| Installation | 249 |
| LDAP Account Manager configuration | 249 |
| Setup sudo | 250 |
| Setup Perl | 250 |
| Set up SSH | 251 |
| Troubleshooting | 251 |
| E. Setup password self reset schema (LAM Pro) | 252 |
| New installation | 252 |
| Schema update | 253 |
| F. Adapt LAM to your corporate design | 255 |
| G. Clustering LAM | 257 |
| H. Troubleshooting | 258 |
| Reset configuration password | 258 |
| Server profiles | 258 |
| Main configuration | 258 |
| Reset IP restriction | 258 |
| File system storage | 258 |
| Database storage | 259 |
| Functional issues | 259 |
| Performance issues | 260 |
| LDAP server | 260 |
| LAM web server | 261 |

List of Tables

| | |
|------------------------------------|-----|
| 1.1. Glossary | 3 |
| 2.1. Locales | 8 |
| 3.1. Options | 38 |
| 3.2. Options | 39 |
| 3.3. Options | 40 |
| 3.4. Options | 40 |
| 3.5. Options | 41 |
| 3.6. Options | 42 |
| 3.7. Options | 43 |
| 3.8. Options | 43 |
| 3.9. Options | 44 |
| 3.10. Options | 44 |
| 3.11. Options | 45 |
| 3.12. Options | 45 |
| 3.13. Options | 46 |
| 3.14. Options | 46 |
| 4.1. LDAP attribute mappings | 58 |
| 4.2. Zone file | 151 |
| 4.3. | 172 |
| 4.4. Action types | 174 |
| 5.1. | 190 |
| 7.1. General options | 205 |
| 7.2. Self service fields | 212 |
| 7.3. | 221 |
| 7.4. | 234 |
| A.1. LDAP schema files | 237 |

Overview

LDAP Account Manager (LAM) manages user, group and host accounts in an LDAP directory. LAM runs on any webserver with PHP8 support and connects to your LDAP server unencrypted or via SSL/TLS.

LAM supports Samba 3/4, Unix, Kopano, Kolab 3, address book entries, NIS mail aliases, MAC addresses and much more. There is a tree viewer included to allow access to the raw LDAP attributes. You can use templates for account creation and use multiple configuration profiles.

<https://www.ldap-account-manager.org/>

Copyright (C) 2003 - 2025 Roland Gruber <post@rolandgruber.de>

Key features:

- managing user/group/host/domain entries
- account profiles
- account creation via file upload
- multiple configuration profiles
- LDAP browser
- schema browser
- OU editor
- PDF export for all accounts
- manage user/group Quota and create home directories

Requirements:

- PHP (≥ 8.1)
- Any standard LDAP server (e.g. OpenLDAP, Active Directory, Samba 4, OpenDJ, 389 Directory Server, Apache DS, ...)
- A recent web browser that supports CSS2 and JavaScript, at minimum:
 - Firefox (max. 2 years old)
 - Chrome (max. 2 years old)
 - Edge (max. 2 years old)

License:

LAM is published under the GNU General Public License. The complete list of licenses can be found in the copyright file.

Have fun!

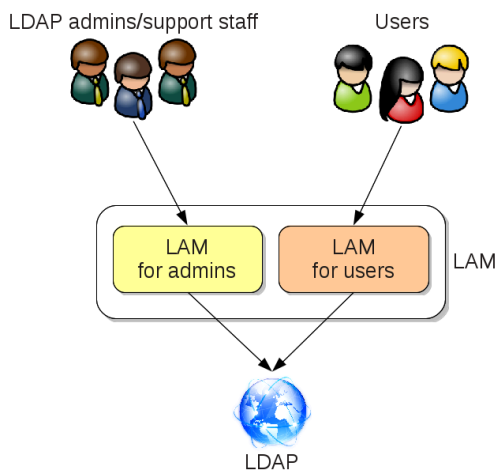
The LAM development team

Chapter 1. Big picture

Overview

LAM has two major areas:

- Admin interface to manage all sorts of different LDAP entries (e.g. users/groups/hosts)
- Self service (LAM Pro) where end users can edit their own data



Admin interface

This is the main part of the application. It allows to manage a large list of LDAP entries (e.g. users, groups, DNS entries, ...). This part is accessed by LDAP admins and support staff.

LDAP Account Manager Pro - 7.9.DEV

d_demo - admin

AccountsToolsHelp

123

Users

New userFile uploadDelete selected users

demo > People > test > de

User count: 125

| Actions | User name | First name | Last name | UID number | GID number | Account s |
|--------------------------|-----------|------------|-----------|------------|------------|-----------|
| Sort sequence | | | | | | |
| 7 Filter | | | | | | |
| <input type="checkbox"/> | cbach | Claudia | Bach | 15429 | 11819 | |
| <input type="checkbox"/> | ebaecker | Ernst | Bäcker | 15430 | 10815 | |
| <input type="checkbox"/> | fhuber | Franz | Huber | 26137 | 10816 | |
| <input type="checkbox"/> | hmeier | Helmut | Meier | 26139 | 10817 | |
| <input type="checkbox"/> | hschuster | Heinz | Schuster | 15427 | 10815 | |
| <input type="checkbox"/> | kmontag | Kerstin | Montag | 26141 | 11820 | |
| <input type="checkbox"/> | mfischer | Monika | Fischer | 15425 | 11820 | |
| <input type="checkbox"/> | rmontag | Ramona | Montag | 26140 | 11819 | |
| <input type="checkbox"/> | shuber | Sepp | Huber | 15419 | 10815 | |
| <input type="checkbox"/> | smiller | Steve | Miller | 26142 | 11820 | |
| <input type="checkbox"/> | thausen | Thomas | Hauser | 15423 | 10815 | |
| <input type="checkbox"/> | xmontag | Xaver | Montag | 26136 | 10816 | |

Functional areas:

1. Account types: Here you can switsch between different account types (e.g. user/groups)

2. Tools menu: Contains useful tools such as profile/PDF editor and tree view
3. Help: Link to manual
4. Logout: Logout of the application
5. List view: Lists all entries of the selected account type (e.g. users)
6. List configuration: Configuration settings for list view (e.g. number of entries per page)
7. Filter: Filter boxes allow to enter simple filters like "a*"

Self Service

The self service provides a simple interface for your users to edit their own data (e.g. telephone number). It also supports user self registration and password reset functionality.

You can fully customize the layout of the self service page.

LAM self service

Here you can change your personal settings.

Personal data

First name

Last name

User

Email address

Telephone number

Mobile telephone number

Street

Postal address

Business unit

test@ldap-account-manager.org

1234567891

123456789

Test 123

12345 City

Unit

Password

New password

Reenter password

Save

Logout

Configuration

Configuration is done on multiple levels:

Global

Effective for all parts of LAM (e.g. logging and password policy).

Configured via LAM admin login -> LAM configuration -> Edit general settings.

Server profile

All settings for an LDAP connection (e.g. server name, LDAP suffixes, account types/modules to activate) in admin interface. There may be multiple for one LDAP server (e.g. for multiple departments, different user groups, ...).

Configured via LAM admin login -> LAM configuration -> Edit server profile.

Self service

All settings for a self service interface (e.g. fields that can be edited, password reset functionality, ...).

Configured via LAM admin login -> LAM configuration -> Edit self service.

Profiles

Account profiles store default values for new LDAP entries.

PDF structures

PDF structures define the layout and list of data fields to include in PDF export.

Glossary

Here you can find a list of common terms used in LAM.

Table 1.1. Glossary

| Term | Description |
|----------------------|---|
| Account module | Plugin for a specific account type (e.g. Unix plugin for user type) |
| Account type | Type of an LDAP entry (e.g. user/group/host) |
| Admin interface | LAM webpages for admin user (e.g. to create new users) |
| Lamdaemon | Support script to manage user file system quotas and create home directories |
| PDF editor | Manages PDF structures |
| PDF export | Exports an entry to PDF by using a PDF structure |
| PDF structure | Defines the layout and list of data fields to include in PDF export |
| Profile | Template for creation of LDAP entries, contains default values |
| Profile editor | Manages profiles for all account types |
| Self Service | LAM webpages for normal users where they can edit their own data |
| Self service profile | Configuration for self service pages (multiple configurations can exist) |
| Tree view | LDAP browser that allows to modify LDAP entries on attribute/object class level |

Architecture

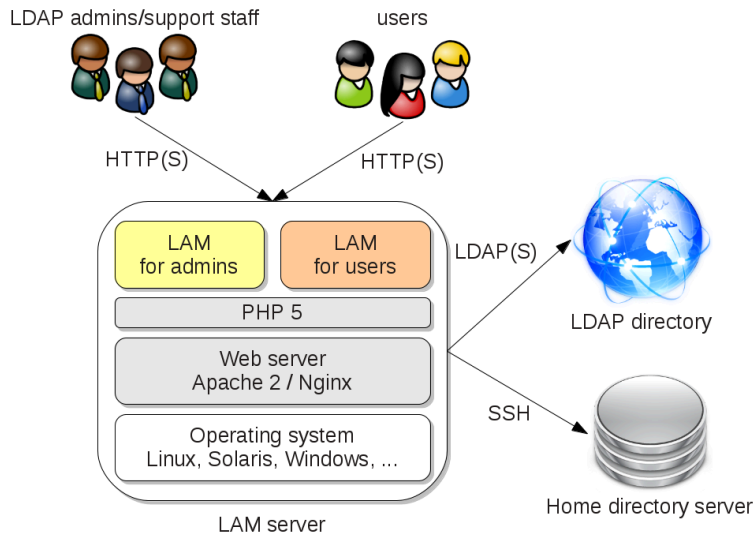
There are basically two groups of users for LAM:

- **LDAP administrators and support staff:**

These people administer LDAP entries like user accounts, groups, ...

- **Users:**

This includes all people who need to manage their own data inside the LDAP directory. E.g. these people edit their contact information with LAM self service (LAM Pro).



Therefore, LAM is split into two separate parts, LAM for admins and for users. LAM for admins allows to manage various types of LDAP entries (e.g. users, groups, hosts, ...). It also contains tools like batch upload, account profiles, LDAP schema viewer and an LDAP browser. LAM for users focuses on end users. It provides a self service for the users to edit their personal data (e.g. contact information). The LAM administrator is able to specify what data may be changed by the users. The design is also adaptable to your corporate design.

LAM for admins/users is accessible via HTTP(S) by all major web browsers (Firefox, IE, Opera, ...).

LAM runtime environment:

LAM runs on PHP. Therefore, it is independent of CPU architecture and operating system (OS). You can run LAM on any OS which supports Apache, Nginx or other PHP compatible web servers.

Home directory server:

You can manage user home directories and their quotas inside LAM. The home directories may reside on the server where LAM is installed or any remote server. The commands for home directory management are secured by SSH. LAM will use the user name and password of the logged in LAM administrator for authentication.

LDAP directory:

LAM connects to your LDAP server via standard LDAP protocol. It also supports encrypted connections with SSL and TLS.

Chapter 2. Installation

New installation

Requirements

LAM has the following requirements to run:

- Apache/Nginx webserver (SSL recommended) with PHP module (PHP (\geq 8.1) with ldap, gettext, xml, openssl and optional OpenSSL)
- Some LAM plugins may require additional PHP extensions (you will get a note on the login page if something is missing)
- Perl (optional, needed only for lamdaemon)
- Any standard LDAP server (e.g. OpenLDAP, Active Directory, Samba 4, OpenDJ, 389 Directory Server, Apache DS, ...)
- A recent web browser that supports CSS2 and JavaScript, at minimum:
 - Firefox (max. 2 years old)
 - Edge (max. 2 years old)
 - Opera (max. 2 years old)
 - Chrome (max. 2 years old)

OpenSSL will be used to store your LDAP password encrypted in the session file.

Please note that LAM does not ship with a SELinux policy. Please disable SELinux or create your own policy.

See LDAP schema files for information about used LDAP schema files.

Prepackaged releases

LAM is available as prepackaged version for various platforms.

Debian/Ubuntu



LAM is part of the official Debian/Ubuntu repository. New releases are uploaded to unstable and will be available automatically in testing and the stable releases. You can run

apt-get install ldap-account-manager

to install LAM on your server. Additionally, you may download the latest LAM Debian/Ubuntu packages from the LAM homepage [<http://www.ldap-account-manager.org/>] or the Debian package homepage [<http://packages.debian.org/search?keywords=ldap-account-manager>].

Installation of the latest packages on Debian/Ubuntu

1. Install the LAM package

```
dpkg -i ldap-account-manager_*.deb
```

If you get any messages about missing dependencies
run now: `apt-get -f install`

2. Install the lamdaemon package (optional)

```
dpkg -i ldap-account-manager-lamdaemon_*.deb
```

Suse/Fedora/CentOS



There are RPM packages available on the LAM home-page [<http://www.ldap-account-manager.org/>]. The packages can be installed with these commands:

```
rpm -e ldap-account-manager ldap-account-manager-lamdaemon (if an older version is installed)
```

```
rpm -i <path to LAM package>
```

Note: The RPM packages do not contain a dependency to PHP due to the various package names for it. Please make sure that you install Apache/Nginx with PHP.

Example installation for Apache + PHP 8 on OpenSuse 15:

- `zypper install apache2 php8 apache2-mod_php8 php8-ldap php8-zip php8-soap php8-gd php8-curl php8-gmp php8-mbstring php8-sqlite php8-mysql php8-gettext`
- `systemctl enable apache2`
- `systemctl start apache2`
- `firewall-cmd --add-service=http --permanent`
- `firewall-cmd --reload`

Other RPM based distributions

The RPM packages for Suse/Fedora are very generic and should be installable on other RPM-based distributions, too. The Fedora packages use `apache:apache` as file owner and the Suse ones use `wwwrun:www`.

FreeBSD



LAM is part of the official FreeBSD ports tree. For more details see these pages:

FreeBSD-SVN: <http://svnweb.freebsd.org/ports/head/sysutils/ldap-account-manager/>

FreshPorts: <http://www.freshports.org/sysutils/ldap-account-manager>

Installing the tar.bz2

Extract the archive

Please extract the archive with the following command:

```
tar xjf ldap-account-manager-<version>.tar.bz2
```

Install the files

Manual copy

Copy the files into the html-file scope of the web server. For example /apache/htdocs or /var/www/html.

Then set the appropriate file permissions inside the LAM directory:

- sess: write permission for apache/nginx user
- tmp: write permission for apache/nginx user
- tmp/internal: write permission for apache/nginx user
- config (with subdirectories): write permission for apache/nginx user
- lib/lamdaemon.pl: set executable

With configure script

Instead of manually copying files you can also use the included configure script to install LAM. Just run these commands in the extracted directory:

- ./configure
- make install

Options for "./configure":

- --with-httpd-user=USER USER is the name of your Apache/Nginx user account (default httpd)
- --with-httpd-group=GROUP GROUP is the name of your Apache/Nginx group (default httpd)
- --with-web-root=DIRECTORY DIRECTORY is the name where LAM should be installed (default /usr/local/lam)

Configuration files

Copy config/config.cfg.sample to config/config.cfg. Open the index.html in your web browser:

- Follow the link "LAM configuration" from the start page to configure LAM.
- Select "Edit general settings" to setup global settings and to change the master configuration password (default is "lam").
- Select "Edit server profiles" to setup a server profile.

Webserver configuration

Please see the Apache or Nginx chapter.

Docker

You can run LAM and LAM Pro inside Docker. See here [<https://github.com/LDAPAccountManager/docker/pkgs/container/lam>] for detailed instructions.

System configuration

PHP

LAM runs with PHP 8 (≥ 8.1). Needed changes in your `php.ini`:

`memory_limit = 128M`

For large installations (>10000 LDAP entries) you may need to increase the memory limit to 256M.

If you run PHP with activated Suhosin [<http://www.hardened-php.net/suhosin/index.html>] extension please check your logs for alerts. E.g. LAM requires that "`suhosin.post.max_name_length`" and "`suhosin.request.max_var_name_length`" are increased (e.g. to 256).

Locales for non-English translation

If you want to use a translated version of LAM be sure to install the needed locales. The following table shows the needed locales for the different languages.

Table 2.1. Locales

| Language | Locale |
|-------------------------|------------------------|
| Catalan | ca_ES.utf8 |
| Chinese (Simplified) | zh_CN.utf8 |
| Chinese (Traditional) | zh_TW.utf8 |
| Czech | cs_CZ.utf8 |
| Dutch | nl_NL.utf8 |
| English - Great Britain | no extra locale needed |
| English - USA | en_US.utf8 |
| French | fr_FR.utf8 |
| German | de_DE.utf8 |
| Hungarian | hu_HU.utf8 |
| Italian | it_IT.utf8 |
| Japanese | ja_JP.utf8 |
| Polish | pl_PL.utf8 |
| Portuguese | pt_BR.utf8 |
| Russian | ru_RU.utf8 |
| Slovak | sk_SK.utf8 |
| Spanish | es_ES.utf8 |
| Turkish | tr_TR.utf8 |
| Ukrainian | uk_UA.utf8 |

You can get a list of all installed locales on your system by executing:

`locale -a`

Debian/Ubuntu users can add locales with "dpkg-reconfigure locales".

Upgrading LAM or migrate from LAM to LAM Pro

Upgrading from LAM to LAM Pro is like installing a new LAM version. Simply install the LAM Pro packages/tar.bz2 instead of the LAM ones.

Upgrade LAM

Backup configuration files

Configuration files need only to be backed up for .tar.bz2 installations. DEB/RPM installations do not require this step.

LAM stores all configuration files in the "config" folder. Please backup the following files and copy them after the new version is installed.

```
config/*.conf
config/config.cfg
config/pdf/*.xml
config/profiles/*
```

LAM Pro only:

```
config/selfService/*.*
```

Uninstall current LAM (Pro) version

If you used the RPM installation packages then remove the ldap-account-manager and ldap-account-manager-lam-daemon packages by calling "rpm -e ldap-account-manager ldap-account-manager-lamdaemon".

Debian/Ubuntu needs no removal of old packages.

For tar.bz2 please remove the folder where you installed LAM via configure or by copying the files.

Install new LAM (Pro) version

Please install the new LAM (Pro) release. Skip the part about setting up LAM configuration files.

Restore configuration files

RPM:

Please check if there are any files ending with ".rpmsave" in /var/lib/ldap-account-manager/config. In this case you need to manually remove the .rpmsave extension by overwriting the package file. E.g. rename default.user.rpmsave to default.user.

DEB:

Nothing needs to be restored.

tar.bz2:

Please restore your configuration files from the backup. Copy all files from the backup folder to the config folder in your LAM Pro installation. Do not simply replace the folder because the new LAM (Pro) release might include additional files in this folder. Overwrite any existing files with your backup files.

Final steps

Now open your webbrowser and point it to the LAM login page. All your settings should be migrated.

Please check also the version specific instructions. They might include additional actions.

Version specific upgrade instructions

You need to follow all steps from your current version to the new version. Unless explicitly noticed there is no need to install an intermediate release.

9.0 -> 9.1

No actions required.

8.9 -> 9.0

Main configuration and server profiles: Both use a new file format (JSON). The configuration will be converted to the new JSON format if you save your settings. The old format is still supported when the configuration will be read. As the old format will be supported for a limited time, it is recommended to open LAM and save the main configuration and all server profiles after the upgrade. If you have any external processes to modify/generate these configurations please adapt them.

LAM Pro:

- Cron jobs of server profiles no longer use the job token parameter
- cron.sh and cronGlobal.sh are deprecated and will be removed in the next release. Use the new command "runCronJobs.sh". E.g. "runCronJobs.sh all" will run all global jobs and all server profile jobs. Execute "runCronJobs.sh" to get a list of possible options.

8.8 -> 8.9

No actions required.

8.7 -> 8.8

LAM Pro:

- Request access: please run the new global cron job to remove requests that are too old. The time limit can be configured in LAM's main configuration.

8.6 -> 8.7

LAM Pro:

- Self service profiles that were not saved with a LAM Pro version of the past 3 years must be saved with LAM Pro 8.6 before upgrading to LAM Pro 8.7.
- Self service profiles that have enabled "HTTP authentication" need to be reconfigured. Open the self service profile, select "HTTP authentication" as "Authentication method" (first tab, server settings) and save the self service profile.

8.1 -> 8.6

No actions required.

8.0 -> 8.1

Configuration settings in server profiles must be redone for group of unique names and group of members.

7.6 -> 8.0

No actions required.

7.5 -> 7.6

The tree view was rewritten from scratch. It moved to the tools menu. You need to reconfigure the tree suffix in your LAM server profile (tools section on first tab).

7.2 -> 7.5

No actions required.

7.1 -> 7.2

LAM Pro: All emails need a specified FROM address. This affects password email, self registration, password self reset and cron emails.

6.7 -> 7.1

No actions required.

6.6 -> 6.7

Self service: please verify the self service base URL in your self service profiles in case you have password self reset / user self registration enabled.

6.5 -> 6.6

No actions required.

6.4 -> 6.5

No actions required.

6.3 -> 6.4

No actions needed.

6.2 -> 6.3

Unix: Options in server profile for Unix users and groups need to be reconfigured. Several settings (e.g. id generation) are now specific to subaccount type.

Self Service: If you use a captcha for user self registration this needs to be reconfigured. On tab General settings please activate Google reCAPTCHA (the checkbox to secure login is optional). On tab Module settings please tick the captcha checkbox at self registration settings.

6.1 -> 6.2

No actions required.

6.0 -> 6.1

DEB+RPM configuration for nginx uses PHP 7 by default. Please see `/etc/ldap-account-manager/nginx.conf` if you use PHP 5.

5.7 -> 6.0

No actions needed.

5.6 -> 5.7

Windows: The department attribute was changed from "departmentNumber" to "department" to match Windows user manager. The attribute "departmentNumber" is no more supported by the Windows module. You will need to reactivate the department option in your server profile on module settings tab.

5.5 -> 5.6

Mail routing: No longer added by default. Use profile editor to activate by default for new users/groups.

Personal/Unix/Windows: no more replacement of e.g. \$user/\$group on user upload

5.4 -> 5.5

LAM Pro requires a license key. You can find it in your customer profile [<https://www.ldap-account-manager.org/lamcms/user/me>].

5.1 -> 5.4

No special actions needed.

5.0 -> 5.1

Self Service: There were large changes to provide a responsive design that works for desktop and mobile. If you use custom CSS to style Self Service then this must be updated.

4.9 -> 5.0

Samba 3: If you used logon hours then you need to set the correct time zone on tab "General settings" in server profile.

4.5 -> 4.9

No special actions needed.

4.4 -> 4.5

LAM will no longer follow referrals by default. This is ok for most installations. If you use LDAP referrals please activate referral following for your server profile (tab General settings -> Server settings -> Advanced options).

The self service pages now have an own option for allowed IPs. If your LAM installation uses IP restrictions please update the LAM main configuration.

Password self reset (LAM Pro) allows to set a backup email address. You need to update the LDAP schema if you want to use this feature.

4.3 -> 4.4

Apache configuration: LAM supports Apache 2.2 and 2.4. This requires that your Apache server has enabled the "version" module. For Debian/Ubuntu and Fedora this is the default setup. The Suse RPM will try to enable the version module during installation.

Kolab: User accounts get the object class "mailrecipient" by default. You can change this behaviour in the module settings section of your LAM server profile.

Windows: sAMAccountName is no longer set by default. Enable it in server profile if needed. The possible domains for the user name can also be set in server profile.

4.2.1 -> 4.3

LAM is no more shipped as tar.gz package but as tar.bz2 which allows smaller file sizes.

4.1 -> 4.2/4.2.1

Zarafa users: The default attribute for mail aliases is now "dn". If you use "uid" and did not change the server profile for a long time please check your LAM server profile for this setting and save it.

4.0 -> 4.1

Unix: The list of valid login shells is no longer configured in "config/shells" but in the server/self service profiles (Unix settings). LAM will use the following shells by default: /bin/bash, /bin/csh, /bin/dash, /bin/false, /bin/ksh, /bin/sh.

Please update your server/self service profile if you would like to change the list of valid login shells.

3.9 -> 4.0

The account profiles and PDF structures are now separated by server profile. This means that if you edit e.g. an account profile in server profile A then this change will not affect the account profiles in server profile B.

LAM will automatically migrate your existing files as soon as the login page is loaded.

Special install instructions:

- Debian: none, config files will be migrated when opening LAM's login page
- Suse/Fedora RPM:
 - Run "rpm -e ldap-account-manager ldap-account-manager-lamdaemon"
 - You may get warnings like "warning: /var/lib/ldap-account-manager/config/profiles/default.user saved as /var/lib/ldap-account-manager/config/profiles/default.user.rpmsave"
 - Please rename all files "*.rpmsave" and remove the file extension ".rpmsave". E.g. "default.user.rpmsave" needs to be renamed to "default.user".
 - Install the LAM packages with "rpm -i". E.g. "rpm -i ldap-account-manager-4.0-0.suse.1.noarch.rpm".
 - Open LAM's login page in your browser to complete the migration
- tar.gz: standard upgrade steps, config files will be migrated when opening LAM's login page

3.7 -> 3.9

No changes.

3.6 -> 3.7

Asterisk extensions: The extension entries are now grouped by extension name and account context. LAM will automatically assign priorities and set same owners for all entries.

3.5.0 -> 3.6

Debian users: LAM 3.6 requires to install FPDF 1.7. You can download the package here [<http://packages.debian.org/search?keywords=php-fpdf&searchon=names&suite=all§ion=all>]. If you use Debian Stable (Squeeze) please use the package from Testing (Wheezy).

3.4.0 -> 3.5.0

LAM Pro: The global config/passwordMailTemplate.txt is no longer supported. You can setup the mail settings now for each LAM server profile which provides more flexibility.

Suse/Fedora RPM installations: LAM is now installed to /usr/share/ldap-account-manager and /var/lib/ldap-account-manager.

Please note that configuration files are not migrated automatically. Please move the files from /srv/www/htdocs/lam/config (Suse) or /var/www/html/lam/config (Fedora) to /var/lib/ldap-account-manager/config.

3.3.0 -> 3.4.0

No changes.

3.2.0 -> 3.3.0

If you use custom images for the PDF export then these images need to be 5 times bigger than before (e.g. 250x250px instead of 50x50px). This allows to use images with higher resolution.

3.1.0 -> 3.2.0

No changes.

3.0.0 -> 3.1.0

LAM supported to set a list of valid workstations on the "Personal" page. This required to change the LDAP schema. Since 3.1.0 this is replaced by the new "Hosts" module for users.

Lamdaemon: The sudo entry needs to be changed to ".../lamdaemon.pl *".

2.3.0 -> 3.0.0

No changes.

2.2.0 -> 2.3.0

LAM Pro: There is now a separate account type for group of (unique) names. Please edit your server profiles to activate the new account type.

1.1.0 -> 2.2.0

No changes.

Uninstallation of LAM (Pro)

If you used the prepackaged installation packages then remove the ldap-account-manager and ldap-account-manager-lamdaemon packages.

Otherwise, remove the folder where you installed LAM via configure or by copying the files.

Migration to a new server

LAM provides configuration export and import. Use this to transport the configuration to your new server.

To manually move LAM (Pro) from one server to another please follow these steps:

1. Install LAM (Pro) on your new server
2. Copy the following files from the old server to the new one (base directory for RPM/DEB is /usr/share/ldap-account-manager/):

- config/*.conf
- config/config.cfg
- config/pdf/*
- config/profiles/*
- config/selfService/*.* (needed for LAM Pro only)

The files must be writable for the webserver user.

3. Open LAM (Pro) login page on new server and verify installation.
4. Uninstall LAM (Pro) on old server.

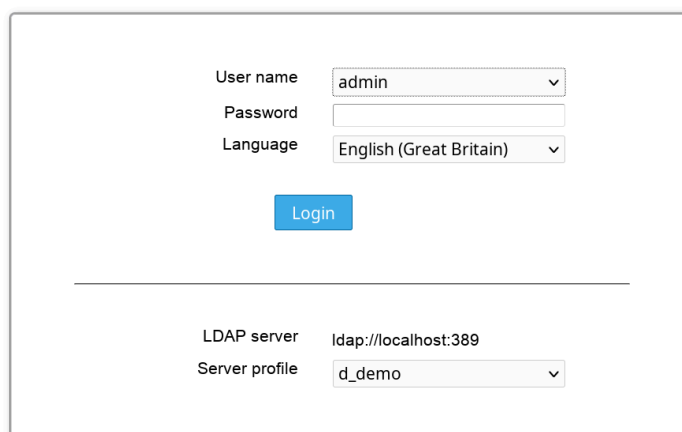
Chapter 3. Configuration

After you installed LAM you can configure it to fit your needs. The complete configuration can be done inside the application. There is no need to edit configuration files.

Please point your browser to the location where you installed LAM. E.g. for Debian/Ubuntu/RPM this is `http://yourServer/lam`. If you installed LAM via the tar.bz2 then this may vary. You should see the following page:

 LDAP Account Manager Pro - 7.9.DEV

LAM configuration

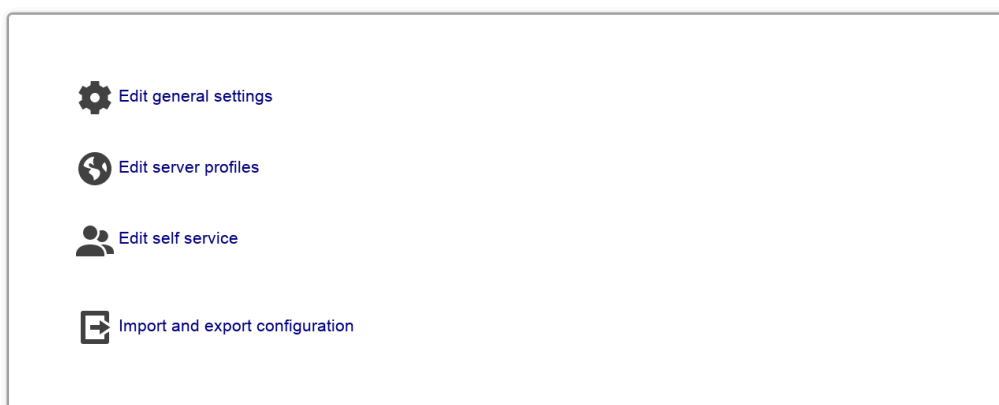


The screenshot shows the LAM login interface. It features a 'User name' dropdown menu with 'admin' selected, a 'Password' text input field, and a 'Language' dropdown menu with 'English (Great Britain)' selected. Below these fields is a blue 'Login' button. A horizontal line separates the login section from the configuration section below. The configuration section includes an 'LDAP server' text input field with 'ldap://localhost:389' and a 'Server profile' dropdown menu with 'd_demo' selected.

If you see an error message then you might need to install an additional PHP extension. Please follow the instructions and reload the page afterwards.

Now you are ready to configure LAM. Click on the "LAM configuration" link to proceed.

 LDAP Account Manager Pro - 7.9.DEV



The screenshot shows the LAM configuration menu. It contains four items, each with an icon and a text label: a gear icon for 'Edit general settings', a globe icon for 'Edit server profiles', a group of people icon for 'Edit self service', and a document with arrows icon for 'Import and export configuration'.

Here you can change LAM's general settings, setup server profiles for your LDAP server(s) and configure the self service (LAM Pro). You should start with the general settings and then setup a server profile.

General settings

Configuration Database

This defines where LAM should store the configuration settings. By default, local file system is used. If you have installed the PHP PDO extension incl. MySQL then you can also select MySQL here. This will then store all data (server profiles, account profiles, PDF structures, ...) in the database.

Exceptions:

- Configuration storage options
- LAM Pro license
- CA certificates

This is very useful when running LAM cloud native e.g. inside Docker.

General settings

Configuration storage

| | | |
|---------------------|-----------|---|
| Database type | MySQL | ? |
| Database host * | localhost | ? |
| Database port | | ? |
| Database name * | lam | ? |
| Database user * | lam | ? |
| Database password * | ... | ? |

License (LAM Pro only)

This is only required when you run LAM Pro. Please enter the license key from your customer profile [<https://www.ldap-account-manager.org/lamcms/user/me>]. In case you have purchased multiple licenses please only enter one license key block per installation.

When you entered the license key then the license details can be seen on LAM configuration overview page.

By default, LAM Pro will show a warning message on the login page 3 weeks before expiration. You can disable this here and/or send out an email instead.

Licence

Licence

Expiration warning

From address *

TO address *

Security settings

Here you can set a time period after which inactive sessions are automatically invalidated. The selected value represents minutes of inactivity.

If you do not want to expose why the login to LAM failed then activate "Hide LDAP details on failed logins". This way users will not see if their account was not found or is e.g. locked.

You may also set a list of IP addresses which are allowed to access LAM. The IPs can be specified as full IP (e.g. 123.123.123.123) or with the "*" wildcard (e.g. 123.123.123.*). Users which try to access LAM via an untrusted IP only get blank pages. There is a separate field for LAM Pro self service.

The screenshot shows the LAM configuration interface. It is divided into three main sections: General settings, Licence, and Security settings. Under General settings, there is a 'Configuration storage' section with a 'Database type' dropdown set to 'Local file system'. The 'Licence' section has a 'Licence' text area and an 'Expiration warning' dropdown set to 'Screen'. The 'Security settings' section includes a 'Session timeout' dropdown set to '90', a 'Hide LDAP details on failed login' checkbox (checked), and an 'Allowed hosts' text area containing '192.168.*' and '127.0.0.1'. There is also an 'Allowed hosts (self service)' text area.

SSL certificate setup:

By default, LAM uses the CA certificates that are preinstalled on your system. This will work if you connect via SSL/TLS to an LDAP server that uses a certificate signed by a well-known CA. In case you use your own CA (e.g. company internal CA) you can import the CA certificates here.

Please note that this can affect other web applications on the same server if they require different certificates. There seem to be problems on Debian/Ubuntu systems and you may also need to restart Apache. In case of any problems please delete the uploaded certificates and use the system setup.

You can either upload a DER/PEM formatted certificate file or import the certificates directly from an LDAP server that is available with LDAP+SSL (ldaps://). LAM will automatically override system certificates if at least one certificate is uploaded/imported.

The whole certificate list can be downloaded in PEM format. You can also delete single certificates from the list.

Please note that you might need to restart your webserver if you do any changes to this configuration.

The screenshot shows the LAM SSL certificates configuration interface. It has a header 'SSL certificates' and a sub-header 'use custom CA certificates' with three icons (a plus sign, a red X, and a question mark). Below this, there is a 'Browse...' button, a text field 'No file selected.', an 'Upload' button, and an 'Import from server' button. A text input field contains 'ldaps://'. Below these buttons is a table with four columns: 'Common name', 'Valid to', 'Serial number', and 'Delete'. The table contains two rows of certificates.

| Common name | Valid to | Serial number | Delete |
|-------------|------------|----------------------|--------|
| roland | 2021-08-16 | 10818998085225869741 | X |
| RG SE CA | 2039-04-06 | 10818998085225869735 | X |

Password policy

This allows you to specify a central password policy for LAM. The policy is valid for all password fields inside LAM admin (excluding tree view) and LAM self service. Configuration passwords do not need to follow this policy.

- Remote: sends log messages to a remote server that supports the Unix remote Syslogd [<https://www.rsyslog.com/>] protocol. Please enter destination as "server:port", e.g. "myserver:123".
- No logging: disabled logging

Logging

Log level

Debug

?

Log destination

File

?

File

/tmp/lam.log

PHP error reporting

all

?

Mail options (LAM Pro)

Here you can configure the mail server settings. If you do not set a mail server then LAM will try to use a locally installed one (e.g. postfix, exim, sendmail).

SMTP setup:

Mail server: enter name + port separated by ":". E.g. "server:25" will use "server" on port 25.

User name: enter the user name if your SMTP server requires authentication

Password: enter the password for the user above

Encryption protocol: Use TLS when unsure. SSL is only for older servers and deprecated. The no encryption setting should not be used for production installations.

Mail options

Mail server

?

User name

?

Password

.....

?

Encryption protocol

TLS

?

WebAuthn/FIDO2 devices

See the WebAuthn/FIDO2 appendix for an overview about WebAuthn/FIDO2 in LAM.

Here you can delete any webauthn device registrations. This section is only shown if at least one device is registered.

Enter a part of the user's DN in the input box and perform a search. LAM will show users and devices that match the search. You can then delete a device registration. If the user has no more registered devices then LAM will ask for registration on next login.

Note: You cannot add any device here. This can only be done by the user during login, webauthn tool or self service.

WebAuthn devices

User DN

?

Search

| User | Name | Registration | Last use | Delete |
|------|------|--------------|----------|--------|
| | | | | ✗ |

Module settings and global cron job (LAM Pro)

The global cron job is used to perform cleanup tasks.

Note: This is only needed when you use the "Request access" module. If you do not use this module you do not need to run the global cron job.

Cleanup actions

- Request access
 - Expiration of open requests (using "Request expiration period")
 - Cleanup request history (using "History retention period")

The screenshot shows two configuration sections. The 'Request access' section has two input fields: 'Request expiration period' with the value '31' and 'History retention period' with the value '3650'. Both fields have a blue question mark icon to their right. The 'Global cron job' section has a 'Cron command' field with the value '0 0 * * * /lib/cronGlobal.sh' and a blue question mark icon to its right.

Change master password

If you would like to change the master configuration password then enter a new password here.

The 'Change master password' dialog box contains two input fields: 'New master password' and 'Reenter password'. Both fields have a blue question mark icon to their right. At the bottom left, there are two buttons: 'Save' (blue) and 'Cancel' (white with a grey border).

Server profiles

The server profiles store information about your LDAP server (e.g. host name) and what kind of accounts (e.g. users and groups) you would like to manage. There is no limit on the number of server profiles. See the typical scenarios about how to structure your server profiles.

Manage server profiles

Select "Manage server profiles" to open the profile management page.

The dialog box titled 'Please enter your password to change the server preferences:' contains a 'Profile name' dropdown menu with 'd_demo' selected and a 'Password' input field with a blue question mark icon to its right. Below these fields is an 'Ok' button. At the bottom of the dialog, there is a link labeled 'Manage server profiles' which is highlighted with a red rectangular box.

Here you can create, rename and delete server profiles. The passwords of your server profiles can also be reset.

You may also specify the default server profile. This is the server profile which is preselected at the login page. It also specifies the language of the login and configuration pages.

Templates for new server profiles

You can create a new server profile based on one of the built-in templates or any existing profile. Of course, the account types and selected modules can be changed after you created your profile.

Built-in templates:

- addressbook: simple profile for user management with inetOrgPerson object class
- samba3: Samba 3 users, groups, hosts and domains
- unix: Unix users and groups (posixAccount/Group)
- windows_samba4: Active Directory user, group and host management

Profile management

Add profile

Profile name

Profile password

Reenter password

Template

unix

Add

Rename profile

Profile name

d_2factorDuo

New profile name

Rename

Delete profile

Profile name

d_2factorDuo

Delete

Set profile password

Profile name

d_2factorDuo

Profile password

Reenter password

Set profile password

Change default profile

Profile name

d_lam

Ok

All operations on the profile management page require that you authenticate yourself with the configuration master password.

Editing a server profile

Please select your server profile and enter its password to edit a server profile.

Each server profile contains the following information:

- **General settings:** general settings about your LDAP server (e.g. host name and security settings)
- **Account types:** list of account types (e.g. users and groups) that you would like to manage and type specific settings (e.g. LDAP suffix)
- **Modules:** list of modules which define what account aspects (e.g. Unix, Samba, Kolab) you would like to manage
- **Module settings:** settings which are specific for the selected account modules on the page before

General settings

Here you can specify the LDAP server and some security settings.

The server address of your LDAP server can be a DNS name or an IP address. Use ldap:// for unencrypted LDAP connections or TLS encrypted connections. LDAP+SSL (LDAPS) encrypted connections are specified with ldaps://. The port value is optional. TLS cannot be combined with ldaps://.

Hint: If you use a master/slave setup with referrals then point LAM to your master server. Due to bugs in the underlying LDAP libraries pointing to a slave might cause issues on write operations.

LAM includes an LDAP browser which allows direct modification of LDAP entries. If you would like to use it then enter the LDAP suffix at "Tree suffix".

The search limit is used to reduce the number of search results which are returned by your LDAP server.

The access level specifies if LAM should allow to modify LDAP entries. This feature is only available in LAM Pro. LAM non-Pro releases use write access. See this page for details on the different access levels.

Advanced options

Display name: Sometimes, you may not want to display the server address on the login page. In this case you can setup a display name here (e.g. "Production").

Follow referrals: By default LAM will not follow LDAP referrals. This is ok for most installations. If you use LDAP referrals please activate the referral option in advanced settings.

Paged results: Paged results should be activated only if you encounter any problems regarding size limits on Active Directory. LAM will then query LDAP to return results in chunks of 999 entries.

Show deleted entries: This is for Active Directory and Samba 4 only. It will unhide LDAP entries in "CN=Deleted Objects,DC=...". You can use this to browse these entries in tree view. To restore an entry run "Restore-ADObject -Identity GUID" in PowerShell where GUID is the value of the "objectGUID" attribute (you might need to base64 decode it).

Referential integrity overlay: Activate this checkbox if you have any server side extension for referential integrity in place. In this case the server will cleanup references to LDAP entries that are deleted.

The following actions are skipped in this case:

- Users: group of (unique) names: memberships are not deleted when user is deleted
- Users: organizational roles: role assignments are not deleted when user is deleted
- Groups: groupOf(Unique)Names: memberships are not deleted when group is deleted

Hide password prompt for expired password: Hides the password prompt when a user with expired password logs into LAM.

LAM is translated to many different languages. Here you can select the default language for this server profile. The language setting may be overridden at the LAM login page.

Please also set your time zone here.

| | |
|----------------------------|---------------------------|
| A Language settings | |
| Default language | English (Great Britain) ? |
| Time zone | Europe/Berlin ? |

LAM can manage user home directories and quotas with an external script. You can specify the home directory server and where the script is located. The default rights for new home directories can be set, too.

Note: This requires lamdaemon to be installed on the remote server. This comes as separate package for DEB/RPM. See here.

Script server format:


- "server": "server" is the DNS name of your script server
- "server:NAME": NAME is the display name of this server






- "server:NAME:/prefix": /prefix is the directory prefix for all operations. E.g. creating a home directory "/home/user" would create "/prefix/home/user" then.


You can provide a fixed user name. If you leave the field empty then LAM will use your current account (the account you used to login to LAM).

There are two possibilities to connect to your home directory/quota server:

- SSH key (recommended): Please generate a SSH key pair and provide the location to the **private** key file. If the key is protected by a password you can also specify it here.
- Password: If you do not set a SSH key then LAM will try to connect with your current account (the password you used to login to LAM).


 **Lamdaemon settings**





| | | |
|-------------------------|---|---|
| Server list | <input type="text" value="localhost"/> |  |
| Path to external script | <input type="text" value="/usr/share/ldap-account-manager/lib/lamdaemon.pl"/> |  |
| User name | <input type="text" value="admin"/> |  |
| SSH key file | <input type="text" value="/data/ssh/secret.key"/> |  |
| SSH key password | <input type="password" value="....."/> |  |

Rights for the home directory 

| | Read | Write | Execute |
|-------|-------------------------------------|-------------------------------------|-------------------------------------|
| Owner | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |
| Group | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input checked="" type="checkbox"/> |
| Other | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |


LAM Pro users may directly set passwords from list view. You can configure if it should be possible to set specific passwords and showing password on screen is allowed.







 **Password reset page settings**

| | |
|-------------------------------------|--|
| Allow setting specific passwords | <input checked="" type="checkbox"/>  |
| Allow to display password on screen | <input checked="" type="checkbox"/>  |
| Force password change by default | <input checked="" type="checkbox"/>  |
| Default password output | <input type="text" value="Send via mail"/>  |

LAM Pro users can send out changed passwords to their users. Here you can specify the options for these mails.

If you select "Allow alternate address" then password mails can be sent to any address (e.g. a secondary address if the user account is also bound to the mailbox).


 **Password mail settings**


| | | |
|-------------------------|---|---|
| From address * | <input type="text" value="admin@ldap-account-manager.org"/> |  |
| Reply-to address | <input type="text"/> |  |
| Subject | <input type="text" value="Password change"/> |  |
| HTML format | <input type="checkbox"/>  | |
| Allow alternate address | <input checked="" type="checkbox"/>  | |
| Text | <input type="text" value="Your password was set to: @@newPassword@@"/> |  |


LAM supports two methods for login:

- Fixed list

- LDAP search

 **Security settings**

Login method Fixed list 


List of valid users * cn=admin, 


The first one is to specify a fixed list of LDAP DN's that are allowed to login. Please enter one DN per line.


The second one is to let LAM search for the DN in your directory. E.g. if a user logs in with the user name "joe" then LAM will do an LDAP search for this user name. When it finds a matching DN then it will use this to authenticate the user. The wildcard "%USER%" will be replaced by "joe" in this example. This way you can provide login by user name, email address or other LDAP attributes.


Additionally, you can enable HTTP authentication when using "LDAP search". This way the web server is responsible to authenticate your users. LAM will use the given user name + password for the LDAP login. You can also configure this to setup advanced login restrictions (e.g. require group memberships for login). To setup HTTP authentication in Apache please see this link [<http://httpd.apache.org/docs/2.2/howto/auth.html>] and an example for LDAP authentication here.


Hint: LDAP search with group membership check can be done with either HTTP authentication or LDAP overlays like "memberOf" [<http://www.openldap.org/doc/admin24/overlays.html>] or "Dynamic lists" [<http://www.openldap.org/doc/admin24/overlays.html>]. Dynamic lists allow to insert virtual attributes to your user entries. These can then be used for the LDAP filter (e.g. "(&(uid=%USER%)(memberof=cn=admins,ou=groups,dc=company,dc=com))").


 **Security settings**


Login method LDAP search 


LDAP suffix * ou=people,o=test,c=de 


LDAP filter * uid=%USER% 


Bind user 


Bind password 


HTTP authentication ☐ 


 **Global password policy override**


Minimum password length 


Minimum lowercase characters 


Minimum uppercase characters 


Minimum numeric characters 

Minimum symbolic characters 

 **2-factor authentication**

Provider None 

 **Profile password**

New password 

Reenter password

Global password policy override

This allows you to override some password policy options of LAM's global password policy (LAM main configuration). You can increase and decrease the values of the global policy.


































Global password policy override

| | | |
|------------------------------|----|---|
| Minimum password length | 10 |  |
| Minimum lowercase characters | |  |
| Minimum uppercase characters | |  |
| Minimum numeric characters | |  |
| Minimum symbolic characters | |  |

2-factor authentication

LAM supports 2-factor authentication for your users. This means the user will not only authenticate by user+password but also with e.g. a token generated by a mobile device. This adds more security because the token is generated on a physically separated device (typically mobile phone).

2-factor authentication

| | | |
|---------------------------|---|---|
| Provider | privacyIDEA |  |
| User name attribute | uid |  |
| Base URL * | https://localhost |  |
| Label | |  |
| Optional | <input type="checkbox"/> |  |
| Disable certificate check | <input type="checkbox"/> |  |
| Caption |                            Stil Normal Schriftart Größe | |
| | <div> <p>Two Factor Authentication</p> <p>Please enter your PIN and token.</p> </div> | |
| | body p | |

The token is validated by a second application. LAM currently supports:

- privacyIdea [<https://www.privacyidea.org/>]
- YubiKey [<https://www.yubico.com/>]
- Duo [<https://duo.com/>]
- WebAuthn/FIDO2 [<https://webauthn.io/>]
- Okta [<https://www.okta.com/>]
- OpenID [<https://openid.net/>]

Configuration options:

privacyIDEA

- Base URL: please enter the URL of your privacyIDEA instance
- User name attribute: please enter the LDAP attribute name that contains the user ID (e.g. "uid").
- Optional: By default LAM will enforce to use a token and reject users that did not setup one. You can set this check to optional. But if a user has setup a token then this will always be required.

- **Disable certificate check:** This should be used on development instances only. It skips the certificate check when connecting to verification server.

Please note that LAM needs to authenticate to privacyIdea with the user's user name and password WITHOUT second factor. This is needed to get the list of tokens that are setup for the user. You can setup a separate policy (scope: authentication) for LAM inside privacyIdea that has IP restriction ("Client" setting) to LAM's server IP and an action "otppin" "none".

YubiKey

- **Base URLs:** please enter the URL(s) of your YubiKey verification server(s). If you run a custom verification API such as yubiserver then enter its URL (e.g. <http://www.example.com:8000/wsapi/2.0/verify>). The URL needs to end with "/wsapi/2.0/verify". For YubiKey cloud these are "<https://api.yubico.com/wsapi/2.0/verify>", "<https://api2.yubico.com/wsapi/2.0/verify>", "<https://api3.yubico.com/wsapi/2.0/verify>", "<https://api4.yubico.com/wsapi/2.0/verify>" and "<https://api5.yubico.com/wsapi/2.0/verify>". Enter one URL per line.
- **Client id:** this is only required for YubiKey cloud. You can register here: <https://upgrade.yubico.com/getapikey/>
- **Secret key:** this is only required for YubiKey cloud. You can register here: <https://upgrade.yubico.com/getapikey/>
- **Optional:** By default LAM will enforce to use a token and reject users that did not setup one. You can set this check to optional. But if a user has setup a token then this will always be required.
- **Disable certificate check:** This should be used on development instances only. It skips the certificate check when connecting to verification server.

Duo

This requires to register a new "Web SDK" application in your Duo admin panel.

- **User name attribute:** please enter the LDAP attribute name that contains the user ID (e.g. "uid").
- **Base URL:** please enter the API-URL of your Duo instance (e.g. api-12345.duosecurity.com).
- **Client id:** please enter your client id.
- **Secret key:** please enter your client secret.

WebAuthn/FIDO2

See the WebAuthn/FIDO2 appendix for an overview about WebAuthn/FIDO2 in LAM.

Users will be asked to register a device during login if no device is setup.

- **Domain:** Please enter the WebAuthn domain. This is the public domain of the web server (e.g. "example.com"). Do not include protocol or port. Browsers will reject authentication if the domain does not match the web server domain.
- **Optional:** By default LAM will enforce to use a 2FA device and reject users that do not setup one. You can set this check to optional. But if a user has setup a device then this will always be required.

Okta

This requires to register a new application of type "Web".

There, you will need to configure LAM's 2-factor URLs as "Login redirect URIs" in the new application. They are "<https://YOURDOMAIN/lam/templates/login2Factor.php>" for admin interface and "<https://YOURDOMAIN/lam/templates/selfService/selfService2Factor.php>" for self service. You will get an error message during login with the URL to configure in case it was wrong.


On "Sign On" tab you need to add a rule that prompts for the factor.


LAM options:

- **User name attribute:** please enter the LDAP attribute name that contains the user ID (e.g. "mail").

- Base URL: please enter the URL of your Okta domain (e.g. <https://mydomain.okta.com>)
- Client id: please enter your application client id.
- Secret key: please enter your application secret key.

← Back to Applications


 LAM

Active  [View Logs](#)

General Sign On Assignments Okta API Scopes



Client Credentials Edit

Client ID



Public identifier for the client that is required for all OAuth flows.


Client secret

Secret used by the client to exchange an authorization code for a token. This must be kept confidential! Do not include it in apps which cannot keep it secret, such as those running on a client.

General Settings Edit

Okta domain



APPLICATION

Application label

LAM

Application type

Web

Allowed grant types

Client acting on behalf of itself

☒ Client Credentials


Client acting on behalf of a user

☒ Authorization Code

☐ Refresh Token

☐ Implicit (Hybrid)

LOGIN

Login redirect URIs 

OpenID

This will use an OpenID server as 2nd factor for authentication.

LAM options:

- User name attribute: please enter the LDAP attribute name that contains the user ID (e.g. "uid").
- Base URL: please enter the URL of your OpenID client URL. The URL is the one before the `"/.well-known/openid-configuration"`.

- Client id: please enter your application client id.
- Secret key: please enter your application secret key.

KeyCloack example configuration:

Create a new client, select "OpenID Connect" client type and enter a client ID.

The screenshot shows the 'General Settings' tab for a new client in Keycloak. The 'Client type' is set to 'OpenID Connect'. The 'Client ID' is 'demo'. The 'Name' and 'Description' fields are empty. The 'Always display in UI' toggle is turned off.

Now enable "Client authentication" and enter the valid redirect URLs in the last step.

The screenshot shows the 'Capability config' tab for the client. 'Client authentication' is turned on. 'Authorization' is turned off. Under 'Authentication flow', 'Standard flow' and 'Direct access grants' are checked. 'Implicit flow', 'Service accounts roles', 'OAuth 2.0 Device Authorization Grant', and 'OIDC CIBA Grant' are unchecked.

They are "https://YOURDOMAIN/lam/templates/login2Factor.php" for admin interface and "https://YOURDOMAIN/lam/templates/selfService/selfService2Factor.php" for self service. You will get an error message during login in case it was wrong. Then save the configuration.

The screenshot shows the 'Login settings' tab for the client. The 'Root URL' and 'Home URL' fields are empty. The 'Valid redirect URIs' field contains two URLs: 'https://YOURDOMAIN/lam/templates/login2Factor.php' and 'https://YOURDOMAIN/lam/templates/selfService/selfService2Factor.php'. There are buttons to 'Add valid redirect URIs', 'Add valid post logout redirect URIs', and 'Add web origins'.

Next, switch to tab "Credentials" to get the client secret.


Example configuration values:







- User name: uid
- Base URL: http://openidserver/auth/realms/master
- Client id: demo
- Secret key: 59bdf504-b76e-4138-8421-ef662b2c6c83

Remember device

You can allow users to remember the 2FA device for privacyIDEA, WebAuthn and YubiKey. When a device is remembered then users can login for the specified time without presenting their 2nd factor.

The password for the device remembering is used to authenticate the device data. It can be any long passphrase (use > 30 characters). LAM auto-generates one for you. If you change the passphrase then all device data gets invalid and users need to represent their 2nd factor again (which then can be saved again).

 **2-factor authentication**

| | |
|------------------------------|---|
| Provider | WebAuthn  |
| Domain | example.com  |
| Optional | <input type="checkbox"/>  |
| Allow to remember device | <input checked="" type="checkbox"/>  |
| Duration to remember devices | 10h  |
| Password to remember devices |  |

Login

After logging in with user + password LAM will ask for the 2nd factor. If the user has setup multiple factors then he can choose one of them.

Two factor authentication

Please enter your PIN and token.

Serial number

cccccjclkg, vvgdggkkuhbl, vvfki bcvvhrv


Token


Submit

Cancel

Password











You may also change the password of this server profile. Please just enter the new password in both password fields.

 **Profile password**

| | |
|------------------|--|
| New password | <input type="password"/>  |
| Reenter password | <input type="password"/> |

Account types

LAM supports to manage various types of LDAP entries (e.g. users, groups, DHCP entries, ...). On this page you can select which types of entries you want to manage with LAM.

| General settings | Account types | Modules | Module settings | Jobs |
|---|---------------------|--------------------------------------|-----------------|------|
| Available account types | | | | |
|  | Aliases | Alias entries | | + |
|  | Asterisk extensions | Asterisk extensions entries | | + |
|  | Automount entries | Automount entries | | + |
|  | Billing codes | PyKota billing codes | | + |
|  | Bind DNS | Bind DNS entries | | + |
|  | Custom type | Custom entries | | + |
|  | DHCP | DHCP administration | | + |
|  | Groups | Group accounts (e.g. Unix and Samba) | | + |
|  | Groups of names | Group of names accounts | | + |
|  | Hosts | Host accounts (e.g. Samba) | | + |

The section at the top shows a list of possible types. You can activate them by simply clicking on the plus sign next to it.

Each account type has the following options:

- **LDAP suffix:** the LDAP suffix where entries of this type should be managed
- **List attributes:** a list of attributes which are shown in the account lists
- **Additional LDAP filter:** LAM will automatically detect the right LDAP entries for each account type. This can be used to further limit the number of visible entries (e.g. if you want to manage only some specific groups). You can use "@@LOGIN_DN@@" as wildcard (e.g. "(owner=@@LOGIN_DN@)"). It will be replaced by the DN of the user who is logged in.
- **Hidden:** This is used to hide account types that should not be displayed but are required by other account types. E.g. you can hide the Samba domains account type and still assign domains when you edit your users.
- **Read-only (LAM Pro only):** This allows to set a single account type to read-only mode. Please note that this is a restriction on functional level (e.g. group memberships can be changed on user page even if groups are read-only) and is no replacement for setting up proper ACLs on your LDAP server.
- **Custom label:** Here you can set a custom label for the account types. Use this if the standard label does not fit for you (e.g. enter "Servers" for hosts).
- **No new entries (LAM Pro only):** Use this if you want to prevent that new accounts of this type are created by your users. The GUI will hide buttons to create new entries and also disable file upload for this type.
- **Disallow delete (LAM Pro only):** Use this if you want to prevent that accounts of this type are deleted by your users.

Active account types

Users User accounts (e.g. Unix, Samba and Kolab) ↓ ×

LDAP suffix *

List attributes

Custom label

Additional LDAP filter

Read-only ☐

Hidden ☐

No new entries ☐

Disallow delete ☐

Groups Group accounts (e.g. Unix and Samba) ↑ ↓ ×

LDAP suffix *

List attributes

Custom label

Additional LDAP filter

Read-only ☐

Hidden ☐

No new entries ☐

Disallow delete ☐

On the next page you can specify in detail what extensions should be enabled for each account type.

Modules

The modules specify the active extensions for each account type. E.g. here you can setup if your user entries should be address book entries only or also support Unix or Samba.

General settings Account types **Modules** Module settings Jobs

Users

Selected modules

| | |
|--------------------------------|---|
| Personal (inetOrgPerson)(*) | × |
| Unix (posixAccount) | × |
| Password policy (ppolicyUser) | × |
| Kopano (kopanoUser) | × |
| Custom scripts (customScripts) | × |

Available modules

| | |
|---|---|
| Account (account)(*) | + |
| Account locking (locking389ds) | + |
| AD LDS (windowsLDSUser)(*) | + |
| Asterisk (asteriskAccount) | + |
| Asterisk voicemail (asteriskVoicemail) | + |
| Authorized Services (authorizedServiceObject) | + |

Each account type needs a so called "base module". This is the basement for all LDAP entries of this type. Usually, it provides the structural object class for the LDAP entries. There must be exactly one active base module for each account type.

Furthermore, there may be any number of additional active account modules. E.g. you may select "Personal" as base module and Unix + Samba as additional modules.

Module settings

Depending on the activated account modules there may be additional configuration options available. They can be found on the "Module settings" tab. E.g. the Personal account module allows to hide several input fields and the Unix module requires to specify ranges for UID numbers.

General settings
 Account types
 Modules
 Module settings
 Jobs

Personal

Hidden options ?

Description ☐
 Postal code ☐
 Postal address ☐
 Room number ☐
 Mobile number ☐
 Email address ☐
 Employee type ☐
 Manager ☐
 Employee number ☐
 User certificates ☐

Street ☐
 Location ☐
 Registered address ☐
 Telephone number ☐
 Fax number ☐
 Job title ☐
 Business category ☐
 Organisational unit ☐
 Initials ☐
 Photo ☐

Post office box ☐
 State ☐
 Office name ☐
 Home telephone number ☐
 Pager ☒
 Car license ☐
 Department ☐
 Organisation ☐
 Web site ☐
 Display name ☒

Advanced options

Unix

Users

UID generator

Fixed range

Minimum UID number *

10000

Maximum UID number *

20000

Cron jobs (LAM Pro)

LAM Pro can execute common tasks via cron job. This can be used to e.g. notify your users before their passwords expire.

LDAP and database configuration

Please add the LDAP bind user and password for all jobs. This LDAP account will be used to perform all LDAP read and write operations.

Next, select the database type where LAM should store job related data. Supported databases are SQLite and MySQL.

SQLite

This is a simple file based database. It needs no special database server. The database file will be located next to the server profile in config directory.

You will need to install the SQLite PDO module for PHP (pdo_sqlite.so). For Debian/Ubuntu this is located in package php-sqlite3.

34

General settings
Account types
Modules
Module settings
Jobs

LDAP

Bind user

Bind password

Database

Database type

SQLite

Test settings

Cron configuration

0 0 * * * /cron.sh

MySQL

This will store all job data in an external MySQL database.

You will need to install the MySQL PDO module for PHP (pdo_mysql.so). For Debian/Ubuntu this is located in package php-mysql.

Steps to create a MySQL database and user:

```
# login
mysql -u root -p
# create a database
mysql> create database lam_cron;
#
mysql> CREATE USER 'lam_cron'@'%' IDENTIFIED BY 'password';
mysql> CREATE USER 'lam_cron'@'localhost' IDENTIFIED BY 'password';
# grant access for new user
mysql> GRANT ALL PRIVILEGES ON lam_cron.* TO 'lam_cron'@'%';
mysql> GRANT ALL PRIVILEGES ON lam_cron.* TO 'lam_cron'@'localhost';
```

⚙️ General settings | 👤 Account types | 🧩 Modules | ⚙️ Module settings | 🕒 Jobs

LDAP

Bind user: ?

Bind password: ?

Database

Database type: MySQL ?

Database host*: ?

Database port: ?

Database name*: ?

Database user*: ?

Database password*: ?

Test settings

Cron configuration

0 0 * * * ?

Test your settings

After the LDAP and database settings are done you can test your settings.

Cron entry

LAM also prints the crontab line that you need to run the configured jobs on a daily basis. The command must be run as the same user as your webserver is running. You are free to change the starting time of the script or run it more often.

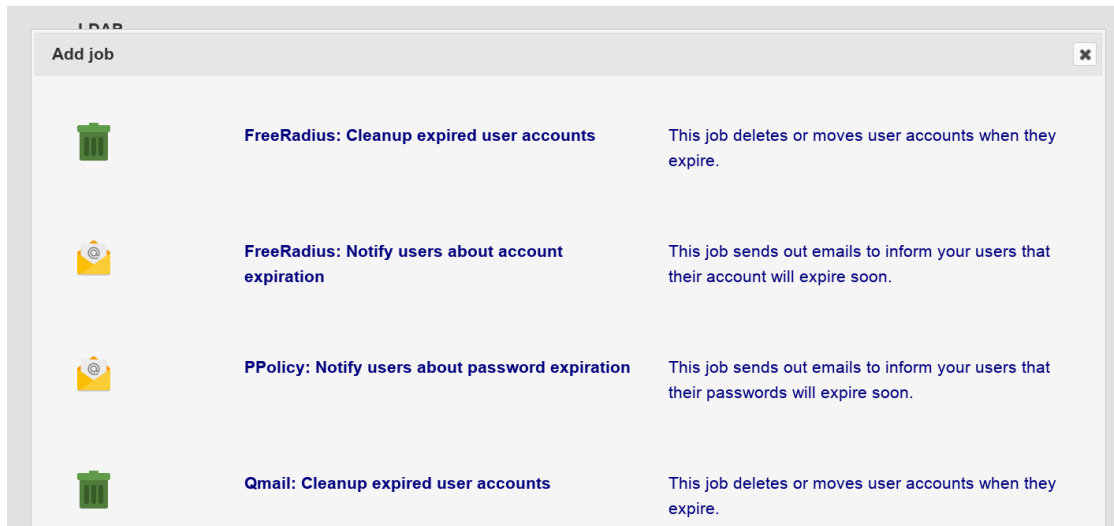
Dry-run: You can perform a dry-run of the job. This will not perform any actions but only print what would be done. For this please put "--dry-run" at the end of the command. E.g.:

```
/usr/share/ldap-account-manager/lib/runCronJobs.sh serverProfile lam --dry-run
```

Adding jobs

To add a new job just click on the "Add job" button and select the job type you need. The list of available jobs depends on your active account modules. E.g. the PPolicy job will only be available if you activated PPolicy user module.

Depending on the job type jobs may be added multiple times with different configurations. For descriptions about the available job types see next chapters.



Available jobs:

- PPolicy: Notify users about password expiration
- 389ds: Notify users about password expiration
- Shadow: Notify users about password expiration
- Shadow: Delete or move expired accounts
- Shadow: Notify users about account expiration
- Windows: Notify users about password expiration
- Windows: Notify users about account expiration
- Windows: Delete or move expired accounts
- Windows: Notify users about their managed groups
- FreeRadius: Delete or move expired accounts
- FreeRadius: Notify users about account expiration
- Qmail: Delete or move expired accounts
- Qmail: Notify users about account expiration
- OpenLDAP: Deactivate accounts based on last successful login

PPolicy: Notify users about password expiration

This will send your users an email reminder before their password expires.

You need to activate the PPolicy module for users to be able to add this job. The job can be added multiple times (e.g. to send a second warning at a later time).


LAM calculates the expiration date based on the last password change and the assigned password policy (or the default policy) using attributes `pwdMaxAge` and `pwdExpireWarning`. Negative values are possible to send mails when LDAP's warning time already started.

Examples:

Warning time (pwdExpireWarning) = 14 days, notification period = 10: LAM will send out the email 24 days before the password expires

Warning time (pwdExpireWarning) = 14 days, notification period = 0: LAM will send out the email 14 days before the password expires

No warning time (pwdExpireWarning), notification period = 10: LAM will send out the email 10 days before the password expires

 **PPolicy: Notify users about password expiration**

From address * ?

Reply-to address ?

CC address ?

BCC address ?

Subject ?

HTML format ☐ ?

Text ?

Notification period * ?

Default password policy * ?

[Delete this job](#)

Table 3.1. Options

| Option | Description |
|-------------------------|---|
| From address | The email address to set as FROM. |
| Reply-to address | Optional Reply-to address for email. |
| CC address | Optional CC mail address. |
| BCC address | Optional BCC mail address. |
| Subject | The email subject line. Supports wildcards, see below. |
| Text | The email body text. Supports wildcards, see below. |
| Notification period | Number of days to notify before password expires. |
| Default password policy | Default PPolicy password policy entry (object class "pwdPolicy"). |

Wildcards:

You can enter LDAP attributes as wildcards in the form @@ATTRIBUTE_NAME@@. E.g. to add the user's common name use "@@cn@@" . For the common name it would be "@@cn@@" .


There are also two special wildcards for the expiration date. @@EXPIRE_DATE_DDMMYYYY@@ will print the date as e.g. "31.12.2016". @@EXPIRE_DATE_YYYYMMDD@@ will print the date as e.g. "2016-12-31".

389ds: Notify users about password expiration

This will send your users an email reminder before their password expires.

You need to activate the Account Locking module for users to be able to add this job. The job can be added multiple times (e.g. to send a second warning at a later time).

LAM calculates the expiration date based on the attribute passwordExpirationTime.

 **389ds: Notify users about password expiration**

From address ^{*} ?

Reply-to address ?

CC address ?

BCC address ?

Subject ?

HTML format ☐ ?

Text ?

Notification period ^{*} ?

[Delete this job](#)

Table 3.2. Options

| Option | Description |
|---------------------|--|
| From address | The email address to set as FROM. |
| Reply-to address | Optional Reply-to address for email. |
| CC address | Optional CC mail address. |
| BCC address | Optional BCC mail address. |
| Subject | The email subject line. Supports wildcards, see below. |
| Text | The email body text. Supports wildcards, see below. |
| Notification period | Number of days to notify before password expires. |

Wildcards:

You can enter LDAP attributes as wildcards in the form @@ATTRIBUTE_NAME@@. E.g. to add the user's common name use "@@cn@@" . For the common name it would be "@@cn@@" .

There are also two special wildcards for the expiration date. @@EXPIRE_DATE_DDMMYYYY@@ will print the date as e.g. "31.12.2016". @@EXPIRE_DATE_YYYYMMDD@@ will print the date as e.g. "2016-12-31".

Shadow: Notify users about password expiration

This will send your users an email reminder before their password expires.


You need to activate the Shadow module for users to be able to add this job. The job can be added multiple times (e.g. to send a second warning at a later time).

LAM calculates the expiration date based on the last password change, the password warning time (attribute "shadowWarning") and the specified notification period. Negative values are possible to send mails when Shadow's warning time already started.

Examples:

Warning time = 14, notification period = 10: LAM will send out the email 24 days before the password expires

Warning time = 14, notification period = 0: LAM will send out the email 14 days before the password expires

 **Shadow: Notify users about password expiration**

From address * ?

Reply-to address ?

CC address ?

BCC address ?

Subject ?

HTML format ☐ ?

Text ?

Notification period * ?

[Delete this job](#)

Table 3.3. Options

| Option | Description |
|---------------------|--|
| From address | The email address to set as FROM. |
| Reply-to address | Optional Reply-to address for email. |
| CC address | Optional CC mail address. |
| BCC address | Optional BCC mail address. |
| Subject | The email subject line. Supports wildcards, see below. |
| Text | The email body text. Supports wildcards, see below. |
| Notification period | Number of days to notify before password expires. |


Wildcards:

You can enter LDAP attributes as wildcards in the form @@ATTRIBUTE_NAME@@. E.g. to add the user's common name use "@@cn@@". For the common name it would be "@@cn@@".

There are also two special wildcards for the expiration date. @@EXPIRE_DATE_DDMMYYYY@@ will print the date as e.g. "31.12.2016". @@EXPIRE_DATE_YYYYMMDD@@ will print the date as e.g. "2016-12-31".

Shadow: Delete or move expired accounts

You can automatically delete or move expired accounts. The job checks Shadow account expiration dates (not password expiration dates).

 **Shadow: Cleanup expired user accounts**

Delay ?

Action ?

[Delete this job](#)


Table 3.4. Options









| Option | Description |
|-----------|--|
| Delay | Number of days to wait after the account is expired. |
| Action | Delete or move accounts |
| Target DN | Move only: specifies the DN where accounts are moved |

Shadow: Notify users about account expiration

This will send your users an email reminder before their whole account expires.

You need to activate the Shadow module for users to be able to add this job. The job can be added multiple times (e.g. to send a second warning at a later time).

 **Shadow: Notify users about account expiration**

| | | |
|-----------------------|---|---|
| From address * | <input type="text" value="lampro@rg-se.de"/> |  |
| Reply-to address | <input type="text"/> |  |
| CC address | <input type="text"/> |  |
| BCC address | <input type="text"/> |  |
| Subject | <input type="text" value="Account expires soon"/> |  |
| HTML format | <input type="checkbox"/> |  |
| Text | <div><input type="text" value="Dear @@cn@@,"/> your account expires on @@EXPIRE_DATE_YYYYMMDD@@</div> |  |
| Notification period * | <input type="text" value="25"/> |  |

[Delete this job](#)

Table 3.5. Options

| Option | Description |
|---------------------|--|
| From address | The email address to set as FROM. |
| Reply-to address | Optional Reply-to address for email. |
| CC address | Optional CC mail address. |
| BCC address | Optional BCC mail address. |
| Subject | The email subject line. Supports wildcards, see below. |
| Text | The email body text. Supports wildcards, see below. |
| Notification period | Number of days to notify before account expires. |

Wildcards:

You can enter LDAP attributes as wildcards in the form @@ATTRIBUTE_NAME@@. E.g. to add the user's common name use "@@cn@@" . For the common name it would be "@@cn@@" .


There are also two special wildcards for the expiration date. @@EXPIRE_DATE_DDMMYYYY@@ will print the date as e.g. "31.12.2016". @@EXPIRE_DATE_YYYYMMDD@@ will print the date as e.g. "2016-12-31".

Windows: Notify users about password expiration

This will send your users an email reminder before their password expires.

You need to activate the Windows module for users to be able to add this job. The job can be added multiple times (e.g. to send a second warning at a later time).

LAM calculates the expiration date based on the last password change and the domain policy.

 **Windows: Notify users about password expiration**

From address ^{*} ?

Reply-to address ?

CC address ?

BCC address ?

Subject ?

HTML format ☐ ?

Text ?

Notification period ^{*} ?

[Delete this job](#)

Table 3.6. Options

| Option | Description |
|---------------------|--|
| From address | The email address to set as FROM. |
| Reply-to address | Optional Reply-to address for email. |
| CC address | Optional CC mail address. |
| BCC address | Optional BCC mail address. |
| Subject | The email subject line. Supports wildcards, see below. |
| Text | The email body text. Supports wildcards, see below. |
| Notification period | Number of days to notify before password expires. |

Wildcards:


You can enter LDAP attributes as wildcards in the form @@ATTRIBUTE_NAME@. E.g. to add the user's common name use "@@cn@". For the common name it would be "@@cn@".

There are also two special wildcards for the expiration date. @@EXPIRE_DATE_DDMMYYYY@@ will print the date as e.g. "31.12.2016". @@EXPIRE_DATE_YYYYMMDD@@ will print the date as e.g. "2016-12-31".

Windows: Notify users about account expiration

This will send your users an email reminder before their whole account expires.

You need to activate the Windows module for users to be able to add this job. The job can be added multiple times (e.g. to send a second warning at a later time).

 **Windows: Notify users about account expiration**

From address ^{*} ?

Reply-to address ?

CC address ?

BCC address ?

Subject ?

HTML format ☐ ?

Text ?

Notification period ^{*} ?

[Delete this job](#)

Table 3.7. Options

| Option | Description |
|---------------------|--|
| From address | The email address to set as FROM. |
| Reply-to address | Optional Reply-to address for email. |
| CC address | Optional CC mail address. |
| BCC address | Optional BCC mail address. |
| Subject | The email subject line. Supports wildcards, see below. |
| Text | The email body text. Supports wildcards, see below. |
| Notification period | Number of days to notify before account expires. |

Wildcards:

You can enter LDAP attributes as wildcards in the form @@ATTRIBUTE_NAME@. E.g. to add the user's common name use "@@cn@". For the common name it would be "@@cn@".

There are also two special wildcards for the expiration date. @@EXPIRE_DATE_DDMMYYYY@@ will print the date as e.g. "31.12.2016". @@EXPIRE_DATE_YYYYMMDD@@ will print the date as e.g. "2016-12-31".

Windows: Delete or move expired accounts

You can automatically delete or move expired accounts.


Windows: Cleanup expired user accounts

Delay
?

Action

Delete
▼
?

Delete this job


Table 3.8. Options

| Option | Description |
|-----------|--|
| Delay | Number of days to wait after the account is expired. |
| Action | Delete or move accounts |
| Target DN | Move only: specifies the DN where accounts are moved |

Windows: Notify users about their managed groups

This will send your users an email with the groups they manage. This also includes a list of users in these groups. The users and groups are searched using the user+group account types that are specified in server profile.

You need to activate the Windows module for users to be able to add this job. The job can be added multiple times.

 **Windows: Notify users about their managed groups**

From address * ?

Reply-to address ?

CC address ?

BCC address ?

Subject ?

HTML format ☐ ?

Text ?

Period ?

[Delete this job](#)

Table 3.9. Options

| Option | Description |
|------------------|--|
| From address | The email address to set as FROM. |
| Reply-to address | Optional Reply-to address for email. |
| CC address | Optional CC mail address. |
| BCC address | Optional BCC mail address. |
| Subject | The email subject line. Supports wildcards, see below. |
| HTML format | Send email as HTML instead of plain text. |
| Text | The email body text. Supports wildcards, see below. |
| Period | Defines how often the mail is sent (e.g. quarterly). |


Wildcards:

You can enter LDAP attributes as wildcards in the form @@ATTRIBUTE_NAME@@. E.g. to add the user's common name use "@@cn@@" . For the common name it would be "@@cn@@" .

Use the wildcard "@@LAM_MANAGED_GROUPS@@" to insert the group listing. This wildcard is mandatory.

FreeRadius: Delete or move expired accounts

You can automatically delete or move expired accounts.

 **FreeRadius: Cleanup expired user accounts**

Delay ?

Action ?

[Delete this job](#)


Table 3.10. Options


| Option | Description |
|-----------|--|
| Delay | Number of days to wait after the account is expired. |
| Action | Delete or move accounts |
| Target DN | Move only: specifies the DN where accounts are moved |


FreeRadius: Notify users about account expiration


This will send your users an email reminder before their FreeRadius account expires.


You need to activate the FreeRadius module for users to be able to add this job. The job can be added multiple times (e.g. to send a second warning at a later time).


 **FreeRadius: Notify users about account expiration**


From address 


Reply-to address 


CC address 

BCC address 

Subject 

HTML format ☐ 

Text 

Notification period 

[Delete this job](#)

Table 3.11. Options

| Option | Description |
|---------------------|--|
| From address | The email address to set as FROM. |
| Reply-to address | Optional Reply-to address for email. |
| CC address | Optional CC mail address. |
| BCC address | Optional BCC mail address. |
| Subject | The email subject line. Supports wildcards, see below. |
| Text | The email body text. Supports wildcards, see below. |
| Notification period | Number of days to notify before account expires. |


Wildcards:

You can enter LDAP attributes as wildcards in the form @@ATTRIBUTE_NAME@@. E.g. to add the user's common name use "@@cn@@" . For the common name it would be "@@cn@@" .

There are also two special wildcards for the expiration date. @@EXPIRE_DATE_DDMMYYYY@@ will print the date as e.g. "31.12.2016". @@EXPIRE_DATE_YYYYMMDD@@ will print the date as e.g. "2016-12-31".

Qmail: Delete or move expired accounts

You can automatically delete or move expired accounts. The job reads the qmail deletion date of user accounts.

 **Qmail: Cleanup expired user accounts**

Delay 

Action 

[Delete this job](#)


Table 3.12. Options

| Option | Description |
|-----------|--|
| Delay | Number of days to wait after the account is expired. |
| Action | Delete or move accounts |
| Target DN | Move only: specifies the DN where accounts are moved |

Qmail: Notify users about account expiration

This will send your users an email reminder before their Qmail account expires.

You need to activate the Qmail module for users to be able to add this job. The job can be added multiple times (e.g. to send a second warning at a later time).

 **Qmail: Notify users about account expiration**

From address * ?

Reply-to address ?

CC address ?

BCC address ?

Subject ?

HTML format ☐ ?

Text

Dear @@cn@@,

 your account expires on @@EXPIRE_DATE_YYYYMMDD@@

 ?

Notification period * ?

[Delete this job](#)

Table 3.13. Options

| Option | Description |
|---------------------|--|
| From address | The email address to set as FROM. |
| Reply-to address | Optional Reply-to address for email. |
| CC address | Optional CC mail address. |
| BCC address | Optional BCC mail address. |
| Subject | The email subject line. Supports wildcards, see below. |
| Text | The email body text. Supports wildcards, see below. |
| Notification period | Number of days to notify before account expires. |

Wildcards:


You can enter LDAP attributes as wildcards in the form @@ATTRIBUTE_NAME@@. E.g. to add the user's common name use "@@cn@@" . For the common name it would be "@@cn@@" .

There are also two special wildcards for the expiration date. @@EXPIRE_DATE_DDMMYYYY@@ will print the date as e.g. "31.12.2016". @@EXPIRE_DATE_YYYYMMDD@@ will print the date as e.g. "2016-12-31".

OpenLDAP: Deactivate accounts based on last successful login

This job deactivates all users that did not perform a successful login for a given time. It requires OpenLDAP with activated "lastBind" and "PPolicy" overlays.

You need to activate the Last login (lastBind) module for users to be able to add this job.

 **OpenLDAP: Deactivate accounts based on last successful login**

Delay ?

[Delete this job](#)

Table 3.14. Options

| Option | Description |
|--------|-------------|
|--------|-------------|

| | |
|-------|--|
| Delay | The number of days after the last successful login when to deactivate the account. |
|-------|--|

Job history

This will show the list of all executed job runs and their result.

General settings
Account types
Modules
Module settings
Jobs

Job history

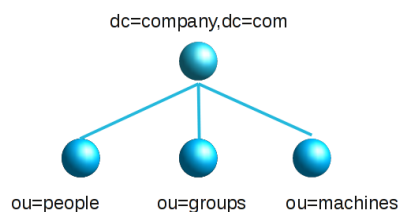
| Name | Time | Result | Messages |
|--|---------------------|--------|----------|
| Windows: Cleanup expired user accounts (1063595495311) | 2016-07-17 10:20:33 | Ok | |
| Windows: Cleanup expired user accounts (1063595495311) | 2016-07-17 10:20:14 | Ok | |
| Windows: Cleanup expired user accounts (1063595495311) | 2016-07-17 10:20:13 | Ok | |
| Windows: Cleanup expired user accounts (1063595495311) | 2016-07-17 10:19:38 | Ok | |
| Windows: Cleanup expired user accounts (1063595495311) | 2016-07-17 10:19:18 | Ok | |

Typical scenarios

This is a list of typical scenarios how your LDAP environment may look like and how to structure the server profiles for it.

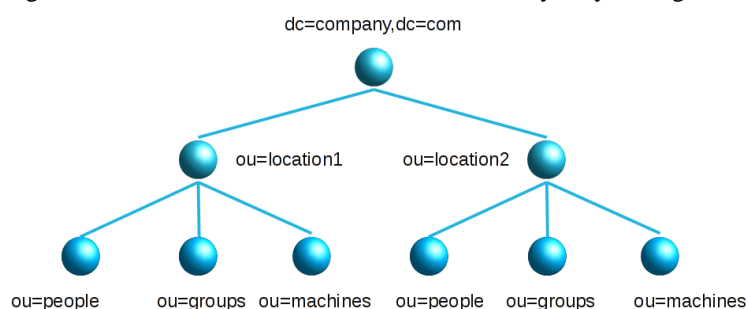
Simple: One LDAP directory managed by a small group of admins

This is the easiest and most common scenario. You want to manage a single LDAP server and there is only one or a few admins. In this case just create one server profile and you are done. The admins may be either specified as a fixed list or by using an LDAP search at login time.



Advanced: One LDAP server which is managed by different admin groups

Large organisations may have one big LDAP directory for all user/group accounts. But the users are managed by different groups of admins (e.g. departments, locations, subsidiaries, ...). The users are typically divided into organisational units in the LDAP tree. Admins may only manage the users in their part of the tree.

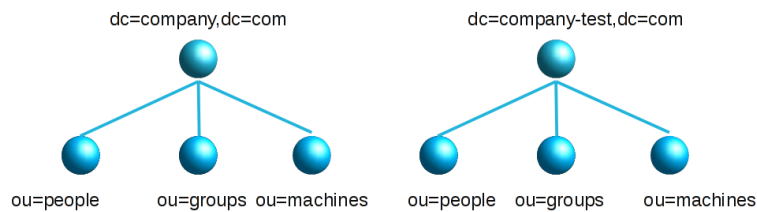


In this situation it is recommended to create one server profile for each admin group (e.g. department). Setup the LDAP suffixes in the server profiles to point to the needed organisational units. E.g. use `ou=people,ou=department1,dc=company,dc=com` or `ou=department1,ou=people,dc=company,dc=com` as LDAP suffix for users. Do the same for groups, hosts, ... This way each admin group will only see its own users. You may want to use LDAP search for the LAM login in this scenario. This will prevent that you need to update a server profile if the number of admins changes.

Attention: LAM's feature to automatically find free UIDs/GIDs for new users/groups will not work in this case. LAM uses the user/group suffix to search for already assigned UIDs/GIDs. As an alternative you can specify different UID/GID ranges for each department. Then the UIDs/GIDs will stay unique for the whole directory.

Multiple LDAP servers

You can manage as many LDAP servers with LAM as you wish. This scenario is similar to the advanced scenario above. Just create one server profile for each LDAP server.



Single LDAP directory with lots of users (>10 000)

LAM was tested to work with 10 000 users. If you have a lot more users then you have basically two options.

- Divide your LDAP tree in organisational units: This is usually the best performing option. Put your accounts in several organisational units and setup LAM as in the advanced scenario above.
- Increase memory limit: Increase the `memory_limit` parameter in your `php.ini`. This will allow LAM to read more entries. But this will slow down the response times of LAM.

Self Service (LAM Pro)

See Self Service chapter.

Import and export configuration

Here you can export and import LAM's whole configuration. You can use this to backup the configuration or migrate from one server to another.

You will need to login with the configuration master password to use this feature.

Export

Export

Import

Browse...

No file selected.

Submit

[Back to login](#)

Export

This will dump the whole configuration to one big single file. It is not possible to dump only parts of the configuration. During import you can select what exactly to import.

Import

Please select the import file first and submit. LAM will then present you possible import data. You can select what to import using the checkboxes.

Please note that LAM will not delete e.g. server profiles that are not in the import file.

Example: You have profile1+profile2 in your LAM installation and profile2+profile3 in your import file. When you select to import all server profiles then profile1 stays untouched, profile2 will be overwritten and profile3 will be added.

Export

Export

Import

Import steps

☒ General settings

☒ SSL certificates

☒ Server profiles

- ☒ 1. General settings
- ☒ 2. SSL certificates
- ☒ 3. Server profiles
- ☒ 4. Import profiles
- ☒ 5. Import profiles
- ☒ 6. Import profiles
- ☒ 7. Import profiles
- ☒ 8. Import profiles
- ☒ 9. Import profiles
- ☒ 10. Import profiles
- ☒ 11. Import profiles
- ☒ 12. Import profiles
- ☒ 13. Import profiles
- ☒ 14. Import profiles
- ☒ 15. Import profiles
- ☒ 16. Import profiles
- ☒ 17. Import profiles
- ☒ 18. Import profiles
- ☒ 19. Import profiles
- ☒ 20. Import profiles

Chapter 4. Managing entries in your LDAP directory

This chapter will give you instructions how to manage the different LDAP entries in your directory.

Please note that not all account types are manageable with the free LAM release. LAM Pro provides some more account types (e.g. group of names, aliases, ...) and modules (e.g. Kopano, custom scripts, ...) to support additional LDAP object classes. All LAM Pro features are marked in this manual.

Basic page layout:

After the login LAM will present you its main page. It consists of a header part which is equal for all pages and the content area which covers most the of the page.

The header part includes the links to manage all account types (e.g. users and groups). There is also the logout link and a tools entry.

When you login the you will see an account listing in the content area.

LDAP Account Manager Pro - 7.9.DEV

d_demo - admin





























































AccountsToolsHelp

Users

New userFile uploadDelete selected users

demo > People > test > de

User count: 12

| Actions | User name | First name | Last name | UID number | GID number | Account statu |
|--|-----------|------------|-----------|------------|------------|---|
| Sort sequence | | | | | | |
| <input type="checkbox"/> Filter | | | | | | |
| <input type="checkbox"/>     | cbach | Claudia | Bach | 15429 | 11819 |  |
| <input type="checkbox"/>     | ebaecker | Ernst | Bäcker | 15430 | 10815 |  |
| <input type="checkbox"/>     | fhuber | Franz | Huber | 26137 | 10816 |  |
| <input type="checkbox"/>     | hmeier | Helmut | Meier | 26139 | 10817 |  |
| <input type="checkbox"/>     | hschuster | Heinz | Schuster | 15427 | 10815 |  |
| <input type="checkbox"/>     | kmontag | Kerstin | Montag | 26141 | 11820 |  |
| <input type="checkbox"/>     | mfischer | Monika | Fischer | 15425 | 11820 |  |
| <input type="checkbox"/>     | rmontag | Ramona | Montag | 26140 | 11819 |  |
| <input type="checkbox"/>     | shuber | Sepp | Huber | 15419 | 10815 |  |
| <input type="checkbox"/>     | smiller | Steve | Miller | 26142 | 11820 |  |
| <input type="checkbox"/>     | thausser | Thomas | Hauser | 15423 | 10815 |  |
| <input type="checkbox"/>     | xmontag | Xaver | Montag | 26136 | 10816 |  |

Here you can create, delete and modify accounts. Use the action buttons at the left or double click on an entry to edit it.

The suffix selection box allows you to list only the accounts which are located in a subtree of your LDAP directory.

Change list settings

Maximum list entries

100

?

Translate GID number to group name

☐

Show account status

☒

Ok

Cancel

Managing entries in your LDAP directory

You can change the number of shown entries per page with "Change settings". Depending on the account type there may be additional settings. E.g. the user list can convert group numbers to group names.

When you select to edit an entry then LAM will show all its data on a tabbed view. There is one tab for each functional part of the account. You can set default values by loading an account profile.

SaveSet passwordDeleteReset changesBack to user listdefaultLoad profile

Claudia Bach

claudia.bach@ldap-account-manager.orgTelephone number 0123-4567-8900Mobile number 0123-4567-8922

Suffixdemo > People > test > deRDN identifieruid

Personal

Unix

Password policy

Custom scripts

First nameClaudia

Last name *Bach

Initials

DescriptionClaudia Bach

Address

StreetMyStreet 123

Post office box123456789

Postal code12345

Location

State

Postal address

Registered address

Office name

Room numberA 1.23

Contact data

Telephone number0123-4567-8900

Home telephone number0123-4567-8911

Mobile number0123-4567-8922

Fax number

Email addressclaudia.bach@ldap-account-mar

Web site

Delete photo

Typical usage scenarios

Here is a list of typical usage scenarios and what account types and modules you need to configure.

Address book entries:

Account types:

- Users (Personal)

Unix accounts:

Account types:

51

- Users (Personal + Unix)
- Groups (Unix (posixGroup))

Suse users may need to use Group (Group of names + Unix (rfc2307bisPosixGroup)) because of Suse's special LDAP schema.

Samba 3 accounts:

Account types:

- Users (Personal + User + Samba 3)
- Groups (Unix + Samba 3)
- Hosts (Account + Unix + Samba 3)
- Samba domains (Samba domain)

Samba 4/Active Directory:

Account types:

- Users (Windows)
- Groups (Windows)
- Hosts (Windows)

Please note that must change the attributes that are shown in the account lists. Otherwise, the account tables will show empty lines. See the documentation for the Windows user/group/host modules.

For Samba 4 with Kopano use the following modules:

- Users (Windows + Kopano (+ Kopano contact))
- Groups (Windows + Kopano)
- Hosts (Windows + Kopano)
- Kopano dynamic groups (Kopano dynamic group)
- Kopano address lists (Kopano address list)

See also the Kopano section for additional settings (e.g. using Kopano AD schema).

Asterisk:

Account types:

- Users (Personal + Asterisk)
- Asterisk extensions (Asterisk extension)

Kopano:

Account types:

- Users (Personal + Unix + Kopano (+ Kopano contact))
- Groups (Unix + Kopano)
- Kopano dynamic groups (Kopano dynamic group)
- Kopano address lists (Kopano address list)

- Hosts (Device + Kopano + IP Address)

PyKota:

Account types:

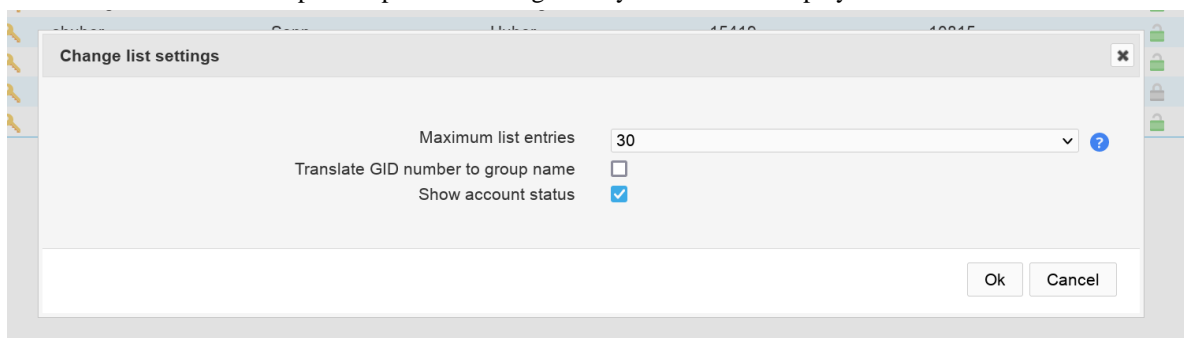
- Users (Personal + Unix + PyKota)
- Groups (Unix + PyKota)
- Printers (PyKota)
- Billing codes (PyKota)

Users

















































LAM manages various types of user accounts. This includes address book entries, Unix, Samba, Kopano and much more.

Account list settings:

The user list includes two special options to change how your users are displayed.

























































Translate GID number to group name: By default the user list can show the primary group IDs (GIDs) of your users. There are often cases where it is more suitable to show the group name instead. This can be done by activating this option. Please note that LAM will execute more LDAP queries which may result in decreased performance.

| Actions | User name | First name | Last name | UID number | GID number |
|--|----------------------|----------------------|----------------------|----------------------|----------------------|
| Sort sequence ▼ ▲ | ▼ ▲ | ▼ ▲ | ▼ ▲ | ▼ ▲ | ▼ ▲ |
| <input type="checkbox"/> Filter ▼ | <input type="text"/> | <input type="text"/> | <input type="text"/> | <input type="text"/> | <input type="text"/> |
| <input type="checkbox"/>     | cbach | Claudia | Bach | 15429 | admins |
| <input type="checkbox"/>     | ebaecker | Ernst | Bäcker | 15430 | project1 |
| <input type="checkbox"/>     | fhuber | Franz | Huber | 26137 | project2 |
| <input type="checkbox"/>     | hmeier | Helmut | Meier | 26139 | project3 |
| <input type="checkbox"/>     | hschuster | Heinz | Schuster | 15427 | project1 |
| <input type="checkbox"/>     | kmontag | Kerstin | Montag | 26141 | users |
| <input type="checkbox"/>     | mfischer | Monika | Fischer | 15425 | users |
| <input type="checkbox"/>     | rmontag | Ramona | Montag | 26140 | admins |
| <input type="checkbox"/>     | shuber | Sepp | Huber | 15419 | project1 |
| <input type="checkbox"/>     | smiller | Steve | Miller | 26142 | users |
| <input type="checkbox"/>     | thausser | Thomas | Hauser | 15423 | project1 |
| <input type="checkbox"/>     | xmontag | Xaver | Montag | 26136 | project2 |

Show account status: If you activate this option then there will be an additional column displayed that shows if the account is locked or expired. You can see more details when moving the mouse cursor over the lock icon. This function supports Unix, Samba, PPolicy, Windows and 389ds locking+deactivation.

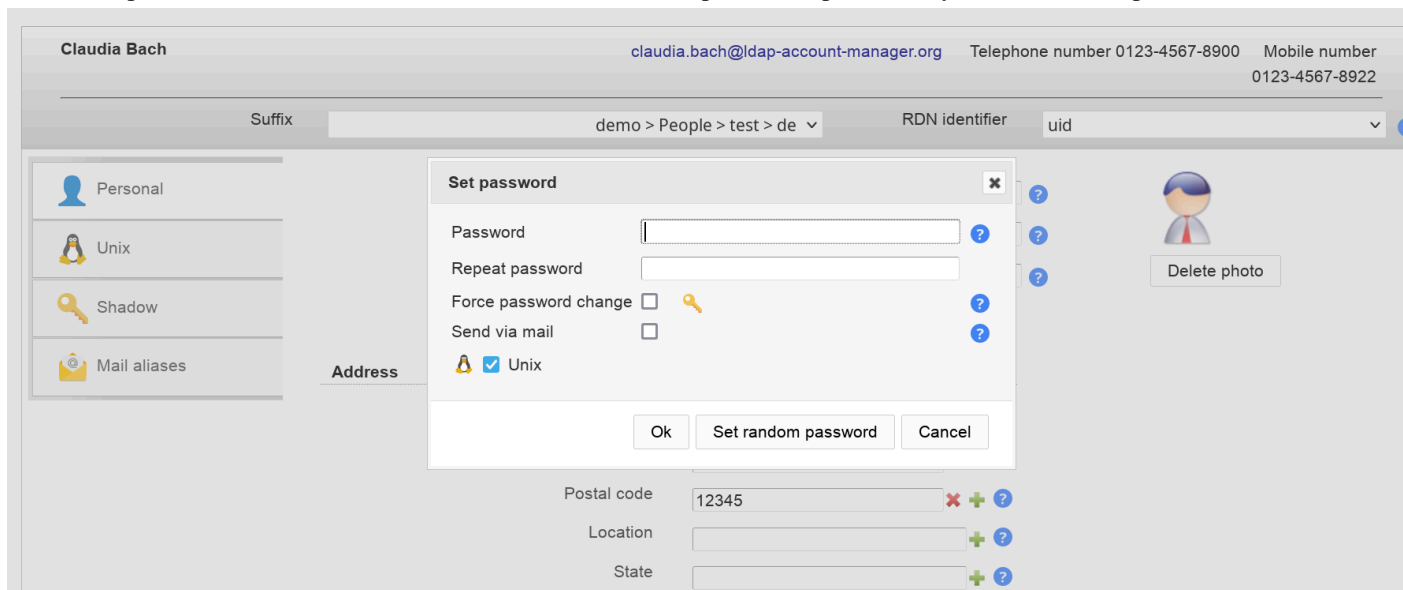
Managing entries in your LDAP directory

| Actions | User name | First name | Last name | UID number | GID number | Account status |
|--|----------------------|----------------------|----------------------|----------------------|----------------------|---|
| Sort sequence | ▼ ▲ | ▼ ▲ | ▼ ▲ | ▼ ▲ | ▼ ▲ | ▼ ▲ |
| <input type="checkbox"/> Filter ▼ | <input type="text"/> | <input type="text"/> | <input type="text"/> | <input type="text"/> | <input type="text"/> | <input type="text"/> |
| <input type="checkbox"/>     | cbach | Claudia | Bach | 15429 | 11819 |  |
| <input type="checkbox"/>     | ebaecker | Ernst | Bäcker | 15430 | 10815 |  |
| <input type="checkbox"/>     | fhuber | Franz | Huber | 26137 | 10816 |  |
| <input type="checkbox"/>     | hmeier | Helmut | Meier | 26139 | 10817 |  |
| <input type="checkbox"/>     | hschuster | Heinz | Schuster | 15427 | 10815 |  |
| <input type="checkbox"/>     | kmontag | Kerstin | Montag | 26141 | 11820 |  |
| <input type="checkbox"/>     | mfischer | Monika | Fischer | 15425 | 11820 |  |
| <input type="checkbox"/>     | rmontag | Ramona | Montag | 26140 | 11819 |  |
| <input type="checkbox"/>     | shuber | Sepp | Huber | 15419 | 10815 |  |
| <input type="checkbox"/>     | smiller | Steve | Miller | 26142 | 11820 |  |
| <input type="checkbox"/>     | thausen | Thomas | Hauser | 15423 | 10815 |  |
| <input type="checkbox"/>     | xmontag | Xaver | Montag | 26136 | 10816 |  |

Password:

Click the "Set password" button to change the user's password(s). Depending on the active account modules LAM will offer to change multiple passwords at the same time.

If a module supports to enforce a password change then you will see the appropriate checkbox. LAM Pro also offers to send the password via email after the account is saved. Email options are specified in your LAM server profile.



The screenshot shows the LAM user management interface for user Claudia Bach. The user's details are displayed at the top, including their email address (claudia.bach@ldap-account-manager.org), telephone number (0123-4567-8900), and mobile number (0123-4567-8922). The user's suffix is 'demo > People > test > de' and their RDN identifier is 'uid'. The user's address is '12345'. The user's location is 'State'. The user's postal code is '12345'. The user's account status is 'locked'.

The 'Set password' dialog is open, showing the following fields and options:

- Password:
- Repeat password:
- Force password change: ☐
- Send via mail: ☐
- Account modules: ☒ Unix

The dialog has three buttons: 'Ok', 'Set random password', and 'Cancel'.

Quick account (un)locking:

When you edit an user then LAM supports to quickly lock/unlock the whole account. This includes Unix, Samba and PPolicy. LAM can also remove group memberships if an account is locked.

You will see the current status of all account parts in the title area of the account.

If you click on the lock icon then a dialog will be opened to change these values. Depending on which parts are locked LAM will provide options to lock/unlock account parts.

Personal

This module is the most common basis for user accounts in LAM. You can use it stand-alone to manage address book entries or in combination with Unix, Samba or other modules.

The Personal module provides support for managing various personal data of your users including mail addresses and telephone numbers. You can also add photos of your users. If you do not need to manage all attributes then you can deactivate them in your server profile.


Configuration


Please activate the module "Personal (inetOrgPerson)" for users.


Managing entries in your LDAP directory

The module manages lots of fields. Probably, you will not need all of them. You can hide fields in module settings.

In advanced options you may also set fields to read-only (for existing accounts) and define limits for photo files. Additionally, you can add an "ou=addressbook" subentry to each user in case you manage user addressbooks.


 **Personal**

Password hash type SSHA 

Hidden options 

| | | | | | |
|-------------------|--------------------------|---------------------|--------------------------|-----------------------|-------------------------------------|
| Description | <input type="checkbox"/> | Street | <input type="checkbox"/> | Post office box | <input type="checkbox"/> |
| Postal code | <input type="checkbox"/> | Location | <input type="checkbox"/> | State | <input type="checkbox"/> |
| Postal address | <input type="checkbox"/> | Registered address | <input type="checkbox"/> | Office name | <input type="checkbox"/> |
| Room number | <input type="checkbox"/> | Telephone number | <input type="checkbox"/> | Home telephone number | <input type="checkbox"/> |
| Mobile number | <input type="checkbox"/> | Fax number | <input type="checkbox"/> | Pager | <input checked="" type="checkbox"/> |
| Email address | <input type="checkbox"/> | Job title | <input type="checkbox"/> | Car license | <input type="checkbox"/> |
| Employee type | <input type="checkbox"/> | Business category | <input type="checkbox"/> | Department | <input type="checkbox"/> |
| Manager | <input type="checkbox"/> | Organisational unit | <input type="checkbox"/> | Organisation | <input type="checkbox"/> |
| Employee number | <input type="checkbox"/> | Initials | <input type="checkbox"/> | Web site | <input type="checkbox"/> |
| User certificates | <input type="checkbox"/> | Photo | <input type="checkbox"/> | Display name | <input checked="" type="checkbox"/> |
| User name | <input type="checkbox"/> | | | | |


Advanced options


Add addressbook (ou=addressbook) ☐ 

Read-only fields

| | | | | | |
|-------------------|--------------------------|-----------------------|--------------------------|--------------------|--------------------------|
| Business category | <input type="checkbox"/> | Car license | <input type="checkbox"/> | Common name | <input type="checkbox"/> |
| Department | <input type="checkbox"/> | Description | <input type="checkbox"/> | Email address | <input type="checkbox"/> |
| Employee number | <input type="checkbox"/> | Employee type | <input type="checkbox"/> | Fax number | <input type="checkbox"/> |
| First name | <input type="checkbox"/> | Home telephone number | <input type="checkbox"/> | Initials | <input type="checkbox"/> |
| Job title | <input type="checkbox"/> | Last name | <input type="checkbox"/> | Location | <input type="checkbox"/> |
| Manager | <input type="checkbox"/> | Mobile number | <input type="checkbox"/> | Office name | <input type="checkbox"/> |
| Organisation | <input type="checkbox"/> | Organisational unit | <input type="checkbox"/> | Pager | <input type="checkbox"/> |
| Password | <input type="checkbox"/> | Photo | <input type="checkbox"/> | Post office box | <input type="checkbox"/> |
| Postal address | <input type="checkbox"/> | Postal code | <input type="checkbox"/> | Registered address | <input type="checkbox"/> |
| Room number | <input type="checkbox"/> | State | <input type="checkbox"/> | Street | <input type="checkbox"/> |
| Telephone number | <input type="checkbox"/> | User name | <input type="checkbox"/> | Web site | <input type="checkbox"/> |

Photo

Maximum width (px) 

Maximum height (px) 

Maximum file size (kB)

User management

Managing entries in your LDAP directory

Claudia Bachclaudia.bach@ldap-account-manager.orgTelephone number 0123-4567-8900Mobile number 0123-4567-8922

Suffixdemo > People > test > deRDN identifieruid

Personal

Roles

User namecbach?


First nameClaudia?

Last name *Bach?

Initials?

Common name *Claudia Bachx+?

DescriptionClaudia Bachx+?



Delete photo

Address

StreetMyStreet 123x+?

Post office box123456789x+?

Postal code12345x+?

Locationx+?

Statex+?

Postal address

Registered address

Office name

Room numberA 1.23?

Contact data

Telephone number0123-4567-8900x+?

Home telephone number0123-4567-8911x+?

Mobile number0123-4567-8922x+?

Fax numberx+?

Email addressclaudia.bach@ldap-account-marx+?

Web sitex+?

User certificates can be uploaded and downloaded. LAM will automatically convert PEM to DER format.

Claudia Bachclaudia.bach@ldap-account-manager.orgTelephone number 0123-4567-8900Mobile number 0123-4567-8922

Suffixdemo > People > test > deRDN identifieruid

Personal

Roles

14476788081586606336: /C=DE/ST=Bavaria/L=City/O=RGSE/CN=test

15038736106651474403: /C=DE/ST=Bavaria/L=City/O=RGSE/CN=test3

17839378481148738733: /C=DE/ST=Bavaria/L=City/O=RGSE/CN=test2

New user certificate

Browse...No file selected.

Upload

Back

Table 4.1. LDAP attribute mappings

| Attribute name | Name inside LAM |
|------------------------------|-----------------------|
| businessCategory | Business category |
| carLicense | Car license |
| cn/commonName | Common name |
| departmentNumber | Department(s) |
| description | Description |
| employeeNumber | Employee number |
| employeeType | Employee type |
| facsimileTelephoneNumber/fax | Fax number |
| givenName/gn | First name |
| homePhone | Home telephone number |
| initials | Initials |
| jpegPhoto | Photo |
| l | Location |
| labeledURI | Web site |
| mail/rfc822Mailbox | Email address |
| manager | Manager |
| mobile/mobileTelephoneNumber | Mobile number |
| organizationName/o | Organisation |
| ou | Organizational unit |
| pager | Pager number |
| physicalDeliveryOfficeName | Office name |
| postalAddress | Postal address |
| postalCode | Postal code |
| postOfficeBox | Post office box |
| registeredAddress | Registered address |
| roomNumber | Room number |
| sn/surname | Last name |
| st | State |
| street/streetAddress | Street |
| telephoneNumber | Telephone number |
| title | Job title |
| userCertificate | User certificates |
| uid/userid | User name |
| userPassword | Password |

Wildcards

This module provides the following wildcards (others may be provided by other modules). Add a "_" after the "\$" to get the value in lower-case (e.g. "\$_firstname").

- \$firstname: First name
- \$lastname: Last name

- \$user: User name
- \$commonname: Common name
- \$email: Email address

You can use them in the following input fields on user edit screen:

- Common name
- Description
- Mail
- Postal address
- Registered address
- Web site

Use this when some of your data always follows the same schema. E.g. using "\$firstname \$lastname" in common name field can be used like this to get "First Last". You can set the wildcards in profile editor so they are automatically applied for new users.

The 'New user' form is displayed with a sidebar on the left containing 'Personal' and 'Roles' tabs. The main area contains several input fields: 'User name', 'First name' (with 'First' entered), 'Last name' (with 'Last' entered), 'Initials', 'Common name' (with '\$firstname \$lastname' entered), and 'Description'. Above the fields, there are controls for 'Suffix', a dropdown menu showing 'People > test > de', and 'RDN identifier' set to 'cn'. Each input field has a blue question mark icon to its right. The 'Common name' and 'Description' fields also have a green plus icon to their right.

The 'First Last' form is displayed, showing the same sidebar and controls as the 'New user' form. The 'Common name' field now contains 'First Last' and has a red 'x' icon to its right, indicating an error. The 'Description' field remains empty. All other fields and their values are the same as in the previous screenshot.

Unix

The Unix module manages Unix user accounts including group memberships.

There are several configuration options for this module:

- UID generator: LAM will suggest UID numbers for your accounts. Please note that it may happen that there are duplicate IDs assigned if users create accounts at the same time. Use an overlay [<http://www.openldap.org/doc/>

admin24/overlays.html] like "Attribute Uniqueness" (example) if you have lots of LAM admins creating accounts.

- Fixed range: LAM searches for free numbers within the given limits. LAM always tries to use a free UID that is greater than the existing UIDs to prevent collisions with deleted accounts.
- Samba ID pool: This uses a special LDAP entry that includes attributes that store a counter for the last used UID/GID. Please note that this requires that you install the Samba schema and create an LDAP entry of object class "sambaUnixIdPool".
- Magic number: Use this if your LDAP server assigns the UID numbers automatically (e.g. DNA by 389 server). Enter the server's magic number setting.
- Password hash type: If possible use CRYPT-SHA512 or SSHA to protect your user's passwords. The option SASL will set the password to "{SASL}<user name>". If you want to use an LDAP EXOP password operation to update the password then select LDAP_EXOP.
- Login shells: List of valid login shells that can be selected when editing an account.
- Hidden options: Some input fields can be hidden to simplify the GUI if you do not need them.
- Set primary group as memberUid: By default primary group membership is not set on group objects but only on user (gidNumber). Activate this if you need to have the primary group membership in group object, too.
- Do not add object class: This is for Windows only. When the checkbox is activated then the posixAccount object class will not be added to a user.
- User name suggestion: The user name is automatically filled as specified in the configuration (default smiller for Steve Miller). Of course, the suggested value can be changed any time. Common name is also filled with first/last name by default.

Managing entries in your LDAP directory



Users

Users

UID generator: Fixed range ?

Minimum UID number *: 10000 ?

Maximum UID number *: 20000 ?

Suffix for UID/user name check: ?

User name suggestion: @givenname@%sn% ?

Hidden options ?

Gecos: ☐ Password: ☐ Groups of names: ☐

Create group with same name: ☐ Unix groups: ☐ Sync groups: ☐ ?

Exclude from group sync: ☐

Hosts

Hosts

UID generator: Fixed range ?

Minimum UID number *: 20000 ?

Maximum UID number *: 30000 ?

Suffix for UID/user name check: ?

Hidden options ?

Gecos: ☐

Options

Password hash type: SSHA ?

Login shells: /bin/bash ?
/bin/csh
/bin/dash
/bin/false
/bin/keh

Set primary group as memberUid: ☐ ?

Claudia Bach claudia.bach@ldap-account-manager.org Telephone number 0123-4567-8900 Mobile number 0123-4567-8922

Suffix: demo > People > test > de RDN identifier: uid

Personal

Unix

Shadow

Quota

User name *: cbach

Common name: Claudia Bach ✕ + ?

UID number: 15429

Gecos: Claudia Bach

Primary group: admins

Additional groups: Edit groups ?

Home directory *: /home/cbach

Check home directories

Login shell: /bin/bash

Password: Lock password Remove password

Managing entries in your LDAP directory

Group memberships can be changed when clicking on "Edit groups". Here you can select the Unix groups and group of names memberships.

To enable "Group of names" please either add the groups module "groupOfNames"/"groupOfUniqueNames" or add the account type "Group of names".

Claudia Bach

claudia.bach@ldap-account-manager.org

Telephone number 0123-4567-8900

Mobile number 0123-4567-8922

Suffix

demo > People > test > de

RDN identifier

uid

Personal

Unix

Shadow

Unix groups

Selected groups

Available groups

project1

project2

computers

pleaders

project3

users

←

→

?

Groups of names

Selected groups

Available groups

admins > demo > gon > test > de

demo > demo > gon > test > de

demosub > demo > gon > test > de

project1 > demo > gon > test > de

project2 > demo > gon > test > de

hr > demo > gon > test > de

it > demo > gon > test > de

managers > demo > gon > test > de

owners > demo > gon > test > de

project3 > demo > gon > test > de

←

→

?

Sync groups

Delete non-matching entries

☒

Sync Unix to group of names

Sync group of names to Unix

Back


You can also create home directories for your users if you setup lamdaemon. This allows you to create the directories on the local or remote servers.


It is also possible to check the status of the user's home directories. If needed the directories can be created or removed at any time.


Managing entries in your LDAP directory


Claudia Bachclaudia.bach@ldap-account-manager.orgTelephone number 0123-4567-8900Mobile number 0123-4567-8922

Suffixdemo > People > test > de ▼RDN identifieruid ▼

 Personal

 Unix

 Shadow

Home directory/home/cbach
localhost  Delete
Back

Wildcards

This module provides the following wildcards (others may be provided by other modules). Add a "_" after the "\$" to get the value in lower-case (e.g. "\$_user").

- \$user: User name
- \$group: Group name (not numeric number)


You can use them in the following input fields on user edit screen:

- Common name
- Gecos
- Home directory

Use this when some of your data always follows the same schema. E.g. using "/home/\$user" in home directory field can be used like this to get "/home/myuser". You can set the wildcards in profile editor so they are automatically applied for new users.

Claudia Bachclaudia.bach@ldap-account-manager.orgTelephone number 0123-4567-8900Mobile number 0123-4567-8922

Suffixdemo > People > test > de ▼RDN identifieruid ▼

 Personal

 Unix

 Shadow


User name *cbach


Common nameClaudia Bach   

UID number15429

GecosClaudia Bach

Primary groupadmins ▼

Additional groups  Edit groups

Home directory */home/\$user  Check home directories

Login shell/bin/bash ▼

Password Lock password Remove password

Claudia Bachclaudia.bach@ldap-account-manager.orgTelephone number 0123-4567-8900Mobile number 0123-4567-8922

Suffixdemo > People > test > de ▼RDN identifieruid ▼

Personal

Unix

Shadow

User name *cbach

Common nameClaudia Bach

UID number15429

GecosClaudia Bach

Primary groupadmins

Additional groupsEdit groups

Home directory */home/cbach

Check home directories

Login shell/bin/bash

PasswordLock passwordRemove password

Group of names and group of members (LAM Pro)

This module manages memberships in group of (unique) names and also group of members.

Please note that this module cannot be used if the Unix module is active. In this case group memberships may be managed with the Unix module.

Configuration

To activate this feature please add the user module "Group of names (groupOfNamesUser)" to your LAM server profile.

Users

Selected modules

Available modules

Personal (inetOrgPerson)(*)

Groups of names (groupOfNamesUser)

Account (account)(*)

Account locking (locking389ds)

AD LDS (windowsLDSUser)(*)

Asterisk (asteriskAccount)

Asterisk voicemail (asteriskVoicemail)

The module automatically detects if groups are based on "groupOfNames", "groupOfUniqueNames" or "groupOfMembers" and sets the correct attribute.

Claudia Bach

claudia.bach@ldap-account-manager.org

Telephone number 0123-4567-8900

Mobile number 0123-4567-8922

Suffix

demo > People > test > de

RDN identifier

uid

Personal

Groups of names

Selected groups

admins > demo > gon > test > de
demo > demo > gon > test > de
demo > gon > test > de
demosub > demo > gon > test > de
project1 > demo > gon > test > de
project2 > demo > gon > test > de

Filter

demo

Sync from other user

Available groups

hr > demo > gon > test > de
it > demo > gon > test > de
managers > demo > gon > test > de
owners > demo > gon > test > de
project3 > demo > gon > test > de

Filter

demo

Organizational roles (LAM Pro)

LAM can manage role memberships in `organizationalRole` objects. To activate this feature please add the user module "Roles (`organizationalRoleUser`)" to your LAM server profile.

Users

Selected modules

Personal (inetOrgPerson)*
Roles (organizationalRoleUser)

Available modules

Account (account)*
Account locking (locking389ds)
AD LDS (windowsLDSUser)*
Asterisk (asteriskAccount)
Asterisk voicemail (asteriskVoicemail)

User editing

Now, there will be a new tab "Roles" when you edit your user accounts. Here you can select the role memberships.

Claudia Bachclaudia.bach@ldap-account-manager.orgTelephone number 0123-4567-8900Mobile number 0123-4567-8922

Suffixdemo > People > test > de ▼RDN identifieruid ▼

Personal

Roles

Selected roles

Available roles

demo
role1
role2

role1
role2
role3
test
test2

←

→

?

Shadow

LAM supports the management of the LDAP substitution of /etc/shadow. Here you can setup password policies for your Unix accounts and also view the last password change of a user.

Claudia Bach

claudia.bach@ldap-account-manager.org

Telephone number 0123-4567-8900Mobile number 0123-4567-8922

Suffixdemo > People > test > de ▼RDN identifieruid ▼

Personal

Unix

Shadow

Samba 3

Password warning

Password expiration

Minimum password age

Maximum password age

Account expiration date

Last password change

10.12.2020

15.04.2021

?

?

Remove Shadow account extension

NIS net groups

Configuration

Please add the module "NIS net groups (nisNetGroupUser)" to the list of active user modules.

Managing entries in your LDAP directory

Users

Selected modules

Personal (inetOrgPerson)(*)

Unix (posixAccount)

Shadow (shadowAccount)

NIS net groups (nisNetGroupUser)

Available modules

Account (account)(*)

Account locking (locking389ds)

AD LDS (windowsLDSUser)(*)

Asterisk (asteriskAccount)

Asterisk voicemail (asteriskVoicemail)

Authorized Services (authorizedServiceObject)

User editing

You will now see a new tab when editing users. Here you can assign memberships in NIS net groups and also set host/domain.

Claudia Bach

claudia.bach@ldap-account-manager.org

Telephone number 0123-4567-8900

Mobile number 0123-4567-8922

Suffix

demo > People > test > de

RDN identifier

uid

Personal

Unix

Shadow

NIS net groups

Group

group01

Host name

host1

Domain name

Filter

group02

Password self reset (LAM Pro)

LAM Pro allows your users to reset their passwords by answering a security question. The reset link is displayed on the self service page. Additionally, you can set question + answer in the admin interface.

Please note that self service and LAM admin interface are separated functionalities. You need to specify the list of possible security questions in both self service profile(s) and server profile(s).

Schema installation

Please install the LDAP schema as described here.

Activate password self reset module

Please activate the password self reset module in your LAM Pro server profile.

Users

Selected modules

Personal (inetOrgPerson)*

Unix (posixAccount)

Shadow (shadowAccount)

Password self reset (passwordSelfReset)

Available modules

Account (account)*

Account locking (locking389ds)

AD LDS (windowsLDSUser)*

Asterisk (asteriskAccount)

Asterisk voicemail (asteriskVoicemail)

Authorized Services (authorizedServiceObject)

Now select the tab "Module settings" and specify the list of possible security questions. Only these questions will be selectable when you later edit accounts unless you explicitly allow to enter custom questions. LAM Pro supports to set up to three security questions per user.

If you do not want to set backup email addresses then you can hide this option.



Password self reset

| | |
|---------------------------------|---|
| Security questions | <div>What is the name of your favourite pet? What is the name of your favourite TV show? What is the brand of your first car?</div> |
| Number of questions | 3 |
| Allow custom security questions | <input type="checkbox"/> |
| Hidden options | <input type="checkbox"/> |
| Backup email | <input type="checkbox"/> |

Edit users

After everything is setup please login to LAM Pro and edit your users. You will see a new tab called "Password self reset". Here you can activate/remove the password self reset function for each user. You can also change the security question and answer.

If you set a backup email address then confirmation emails will also be sent to this address. This is useful if the user password grants access to the user's primary mailbox. So passwords can be unlocked with an external email address.

Hint: You can add the passwordSelfReset object class to all your users with the multi edit tool.

Samba 4 note: Due to a bug [https://bugzilla.samba.org/show_bug.cgi?id=10094] in Samba 4 you need to add the extension, save, and then select a question and set the answer. If you add the extension, set question/answer and then save all together this will cause an LDAP error and no changes will be saved.

Claudia Bach

claudia.bach@ldap-account-manager.org

Telephone number 0123-4567-8900

Mobile number 0123-4567-8922

Suffix

demo > People > test > de

RDN identifier

uid

Personal

Unix

Shadow

Password self reset

Question

What is the name of your favourite pet?

Answer

Change

Question (2)

What is the name of your favourite TV show?

Answer (2)

Change

Question (3)

What was the brand of your first car?

Answer (3)

Change

Backup email

cbach@rg-se.de

Remove password self reset extension

Hosts

You can specify a list of valid host names where the user may login. If you add the value "*" then the user may login to any host. This can be further restricted by adding explicit deny entries which are prefixed with "!" (e.g. "!hr_server").

Please note that your PAM settings need to support host restrictions. This feature is enabled by setting **pam_check_host_attr yes** in your **/etc/pam_ldap.conf**. When it is enabled then the account facility of pam_ldap will perform the checks and return an error when no proper host attribute is present. Please note that users without host attribute cannot login to such a configured server.

The screenshot shows the user profile for Claudia Bach. At the top, there's a header with the user's name, email (claudia.bach@ldap-account-manager.org), and phone numbers. Below this is a navigation bar with a suffix dropdown (demo > People > test > de) and an RDN identifier dropdown (uid). The main content area has a left sidebar with 'Personal', 'Unix', and 'Hosts' tabs. The 'Hosts' tab is active, showing a list of hosts: 'server01' and 'server02'. 'server01' has a red 'x' and a green '+', while 'server02' has a red 'x'. A 'Remove host extension' button is at the bottom right.

Samba 3

LAM supports full Samba 3 user management including logon hours and terminal server options.

The module is enabled by adding "Samba 3 (sambaSamAccount)" to your user modules.

The screenshot shows the 'Users' module selection page. It has a 'Selected modules' section on the left and an 'Available modules' section on the right. In the 'Selected modules' section, 'Personal (inetOrgPerson)*', 'Unix (posixAccount)', 'Shadow (shadowAccount)', and 'Samba 3 (sambaSamAccount)' are listed, each with a red 'x' icon. In the 'Available modules' section, 'Account (account)*', 'Account locking (locking389ds)', 'AD LDS (windowsLDSUser)*', 'Asterisk (asteriskAccount)', 'Asterisk voicemail (asteriskVoicemail)', and 'Authorized Services (authorizedServiceObject)' are listed, each with a green '+' icon.

In the configuration options you can enable password history checking. Depending on your LDAP server you might need ascending or descending order. Just switch the setting if the password history is not correctly updated.

In case you have no very old Windows clients (e.g. Windows 98) it is recommended to disable LM hashes. They are considered to be insecure.

You can also hide some input fields if you do not need them.

The screenshot shows the 'Samba 3' configuration page. It has a header with the 'Samba 3' title. Below this are two dropdown menus: 'Password history' set to 'yes - ordered ascending' and 'Disable LM hashes' set to 'yes'. At the bottom, there's a 'Hidden options' section with a question mark icon. It contains six checkboxes: 'Home drive', 'Logon script', 'Logon hours', 'Home path', 'Last password change', 'Terminal server options', 'Profile path', and 'Samba workstations'. All checkboxes are currently unchecked.

Managing entries in your LDAP directory

After configuring the module you will see the Samba 3 tab when you edit a user.

The screenshot shows the LDAP account manager interface for editing the user 'Claudia Bach'. The top header displays the user's name, email 'claudia.bach@ldap-account-manager.org', telephone number '0123-4567-8900', and mobile number '0123-4567-8922'. Below the header, there's a breadcrumb trail 'demo > People > test > de' and a dropdown for 'Suffix'. The 'RDN identifier' is set to 'uid'. On the left, a sidebar shows tabs for 'Personal', 'Unix', 'Shadow', and 'Samba 3', with 'Samba 3' being the active tab. The main area contains various configuration fields for the Samba 3 extension. Fields include 'Display name' (Claudia Bach), 'Use no password' (checkbox), 'Password does not expire' (checkbox, checked), 'Account is deactivated' (checkbox), 'Account is locked' (checkbox), 'Password change at next login' (checkbox, checked), 'Last password change' (date), 'User can change password' (checkbox), 'User must change password' (checkbox), 'Account expiration date' (date), 'Home drive' (dropdown, X:), 'Home path' (text), 'Profile path' (text), 'Logon script' (text), 'Samba workstations' (button 'Edit workstations'), 'Windows group' (dropdown, admins), 'Special user' (dropdown, -), 'Domain' (dropdown, MyCompany), 'Logon hours' (button 'Edit'), and 'Terminal server options' (button 'Edit'). A red button 'Remove Samba 3 extension' is at the bottom.

Wildcards


You can use wildcards in the following input fields on user edit screen:

- Display name
- Home path
- Profile path
- Logon script

Use this when some of your data always follows the same schema. E.g. using "\\server\%user" in home path field can be used like this to get "\\server\myuser". You can set the wildcards in profile editor so they are automatically applied for new users.


Logon hours


Managing entries in your LDAP directory


 **Claudia Bach**


claudia.bach@ldap-account-manager.org Telephone number 0123-4567-8900 Mobile number 0123-4567-8922

Suffix demo > People > test > de RDN identifier uid

 Personal

 Unix

 Shadow

 Samba 3

| Time | Sunday | Monday | Tuesday | Wednesday | Thursday | Friday | Saturday |
|---------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|
| 00:00 - 00:59 | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |
| 01:00 - 01:59 | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |
| 02:00 - 02:59 | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |
| 03:00 - 03:59 | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |
| 04:00 - 04:59 | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |
| 05:00 - 05:59 | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |
| 06:00 - 06:59 | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |
| 07:00 - 07:59 | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |
| 08:00 - 08:59 | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |
| 09:00 - 09:59 | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |
| 10:00 - 10:59 | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |
| 11:00 - 11:59 | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |
| 12:00 - 12:59 | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |
| 13:00 - 13:59 | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |
| 14:00 - 14:59 | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |
| 15:00 - 15:59 | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |
| 16:00 - 16:59 | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |
| 17:00 - 17:59 | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |
| 18:00 - 18:59 | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |
| 19:00 - 19:59 | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |
| 20:00 - 20:59 | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |
| 21:00 - 21:59 | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |
| 22:00 - 22:59 | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |
| 23:00 - 23:59 | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |

Ok Cancel

You can also setup terminal server settings.

Managing entries in your LDAP directory

Claudia Bach claudia.bach@ldap-account-manager.org Telephone number 0123-4567-8900 Mobile number 0123-4567-8922

Suffix: demo > People > test > de RDN identifier: uid

Personal **Unix** **Shadow** **Samba 3**

Allow terminal server login ☐ ?

Home directory: \\home\cbach

Home drive: D:

Profile path:

Inherit client startup configuration ☒ ?

Initial program: login.bat

Working directory:

Connection time limit: 0

Disconnection time limit: 0

Idle time limit: 0

Connect client drives ☒ ?

Connect client printers ☒ ?

Client printer is default ☒ ?

Shadowing: input off, notify off

On broken or timed out connection: reset

Reconnect if disconnected: from any client

Ok Cancel

Windows (Samba 4/Active Directory)

Please activate the account type "Users" in your LAM server profile and then add the user module "Windows (windowsUser)(*)".

Active account types

Users User accounts (e.g. Unix, Samba and Kolab) ↓ ×

LDAP suffix *: cn=users,dc=w2012,dc=test ?

List attributes: #cn;#givenName;#sn;#mail ?

Custom label: Users ?

Additional LDAP filter: ?

Read-only ☐ ?

Hidden ☐ ?

No new entries ☐ ?

Disallow delete ☐ ?

The default list attributes are for Unix and not suitable for Windows (blank lines in account table). Please use "#cn;#givenName;#sn;#mail" or select your own attributes to display in the account list.

Users

Selected modules

Windows (windowsUser)* ×

Available modules

- Account (account)* +
- Account locking (locking389ds) +
- AD LDS (windowsLDSUser)* +
- Asterisk (asteriskAccount) +

On tab "Module settings" you can specify the possible Windows domain names and if pre-Windows 2000 user names should be managed.

NIS support is deactivated by default. Enable it if needed.

You can also set maximum values for user photos in advanced options.



Windows

Hidden options ?

- | | |
|-------------------|--------------------------|
| Business category | <input type="checkbox"/> |
| Department | <input type="checkbox"/> |
| Email address | <input type="checkbox"/> |
| Employee type | <input type="checkbox"/> |
| Home drive | <input type="checkbox"/> |
| Last login | <input type="checkbox"/> |
| Logon script | <input type="checkbox"/> |
| NIS domain | <input type="checkbox"/> |
| Organisation | <input type="checkbox"/> |
| Other pagers | <input type="checkbox"/> |
| Pager | <input type="checkbox"/> |
| Postal code | <input type="checkbox"/> |
| Require smartcard | <input type="checkbox"/> |
| Telephone number | <input type="checkbox"/> |
| Workstations | <input type="checkbox"/> |

▼ Advanced options

Managing entries in your LDAP directory

Now you can manage your Windows users and e.g. assign groups. You might want to set the default domain name in the profile editor.

Attention:

- Password changes require a secure connection via ldaps://. Check your LAM server profile if password changes are refused by the server.
- Your server must run a 64bit operating system. Otherwise, the module might not work.

The screenshot shows the 'Hans Müller' profile page in the LDAP account manager. The interface includes a top navigation bar with the user's name, a breadcrumb trail 'Users > w2012 > test', and the RDN identifier 'cn'. A left sidebar shows the 'Windows' icon. The main content area is divided into 'General' and 'Address' sections. The 'General' section contains fields for 'User name', 'User name (pre W2K)', 'First name', 'Last name', 'Common name', 'Display name', 'Initials', and 'Description'. The 'Address' section contains fields for 'Street', 'Post office box', 'Postal code', 'Location', 'State', and 'Office name'. On the right, there is a blue silhouette placeholder for a photo with an 'Add photo' button, and a 'Groups' section with an 'Edit groups' button. The text 'demo' is visible at the bottom right of the profile area.

| Field | Value |
|---------------------|----------------|
| User name * | hmueller |
| User name (pre W2K) | hmueller |
| First name | Hans |
| Last name | Müller |
| Common name * | Hans Müller |
| Display name | Hans Müller |
| Initials | S.M. |
| Description | |
| Street | Some street 42 |
| Post office box | 12345 |
| Postal code | DE-12345 |
| Location | MyCity |
| State | My State |
| Office name | |

Contact data

Email address

hmueller@ldap-account-manager.org ?

Email alias

+ ?

Proxy-Addresses

+ ?

Telephone number

?

Other telephone numbers

+ ?

Mobile

?

Other mobiles

+ ?

Pager

?

Other pagers

+ ?

Fax number

?

Web site

?

Other web sites

+ ?

Work details

Job title

?

Car license

?

Employee number

123456 ?

Employee type

Temp ?

Business category

HR x + ?

Company

?

Department

?

Department number

+ ?

Organisational unit

+ ?

Organisation

+ ?

Manager

-

Change

 ?

Wildcards

This module provides the following wildcards (others may be provided by other modules). Add a "_" after the "\$" to get the value in lower-case (e.g. "\$_firstname").

- \$personaltitle: Personal title
- \$firstname: First name
- \$lastname: Last name
- \$user: User name
- \$commonname: Common name
- \$email: Email address

You can use them in the following input fields on user edit screen:

- Common name
- Display name
- Email

- Email alias
- Home directory
- Profile path
- Script path
- User name
- User name (pre W2K)

Use this when some of your data always follows the same schema. E.g. using "\$firstname \$lastname" in common name field can be used like this to get "First Last". You can set the wildcards in profile editor so they are automatically applied for new users.

The image shows two screenshots of a user profile editor's 'General' tab. Both screenshots have a 'Windows' logo in the top left corner. The top screenshot shows the following fields: 'User name' (myuser), 'User name (pre W2K)' (empty), 'First name' (First), 'Last name' (Last), and 'Common name' (\$firstname \$lastname). The 'Common name' field is highlighted with a red box. The bottom screenshot shows the same fields, but the 'Common name' field now contains 'First Last' and is also highlighted with a red box.

AD LDS (formerly ADAM) (LAM Pro)

Please activate the account type "Users" in your LAM server profile and then add the user module "AD LDS (windowsLDSUser)(*)".

Active account types

The screenshot shows the 'Active account types' section. Under the 'Users' account type, the 'User accounts (e.g. Unix, Samba and Kolab)' section is expanded. It contains the following fields: 'LDAP suffix' (cn=users,dc=w2012,dc=test), 'List attributes' (#cn;#givenName;#sn;#mail), 'Custom label' (Users), and 'Additional LDAP filter' (empty). Below these fields are four checkboxes: 'Read-only', 'Hidden', 'No new entries', and 'Disallow delete', all of which are currently unchecked.

The default list attributes are for Unix and not suitable for AD LDS (blank lines in account table). Please use "#cn;#givenName;#sn;#mail" or select your own attributes to display in the account list.

Managing entries in your LDAP directory

General settings

Account types

Modules

Module settings

Jobs

Users

Selected modules

AD LDS (windowsLDSUser)(*)

Available modules

Account (account)(*)

Account locking (locking389ds)

Asterisk (asteriskAccount)

Asterisk voicemail (asteriskVoicemail)

Authorized Services (authorizedServiceObject)


Auto delete (autoDelete)


Courier (courierMailAccount)


Custom fields (customFields)


On tab "Module settings" you can specify the possible Windows domain names.


You can also set maximum values for user photos in advanced options.


 General settings

 Account types

 Modules

 Module settings

 **AD LDS**

Hidden options 

Proxy-Addresses☐

Other mobiles☐

Last password change☐

Job title☐

Employee type☐

Department☐

Organisation☐

▼ Advanced options

Photo

Maximum width

Maximum height

Maximum file size

Now you can manage your AD LDS users and e.g. assign groups. You might want to set the default domain name in the profile editor.

Attention:


Password changes require a secure connection via ldaps://. Check your LAM server profile if password changes are refused by the server.

79

Managing entries in your LDAP directory

demo > users > instance1 > w10e

Suffixusers > instance1 > w10eRDN identifiercn ?

 AD LDS

General

User name *demo
w2012 ?

First nameDemo ?

Last nameUser ?

Common name *demo ?

Display nameDemo User ?

Initials ?

Description ?

Address

StreetDemo street 123 ?

Post office box ?

Postal code ?

LocationDomo Town ?

State ?

Office name ?

Contact data

Email addressdemo@ldap-account-manager.org ?

Work details

Job title ?

Car license ?

Employee number ?

Employee type ?

Business category ?

Company ?

Department ?

Department number ?

Organisational unit ?


Organisation ?

Manager - [Change](#) ?

Account

Last password change2020-02-19 16:13:12 ?

Last login2020-02-19 16:13:21 ?



Add photo

Groups

Edit groups

test11
test12
test13
testgroup

Wildcards

This module provides the following wildcards (others may be provided by other modules). Add a "_" after the "\$" to get the value in lower-case (e.g. "\$_firstname").

- \$firstname: First name

- \$lastname: Last name
- \$user: User name
- \$commonname: Common name
- \$email: Email address

You can use them in the following input fields on user edit screen:

- Common name
- Display name
- Email
- Email alias

Use this when some of your data always follows the same schema. E.g. using "\$firstname \$lastname" in common name field can be used like this to get "Demo User". You can set the wildcards in profile editor so they are automatically applied for new users.

demo > users > instance1 > w10e

Suffix users > instance1 > w10e RDN identifier cn ?

AD LDS

General

User name * demo w2012 ?

First name Demo ?

Last name User ?

Common name * demo ?

Display name \$firstname \$lastname ?

Add photo

demo > users > instance1 > w10e

Suffix users > instance1 > w10e RDN identifier cn ?

AD LDS

General

User name * demo w2012 ?

First name Demo ?

Last name User ?

Common name * demo ?

Display name Demo User ?

Add photo

Filesystem quota (lamdaemon)

You can manage file system quotas with LAM. This requires to setup lamdaemon. LAM connects to your server via SSH and manages the disk filesystem quotas. The quotas are stored directly on the filesystem. This is the default mechanism to store quotas for most systems.

Please add the module "Quota (quota)" for users to your LAM server profile to enable this feature.

If you store the quota information directly inside LDAP please see the next section.

| Mountpoint | Used blocks | Soft block limit | Hard block limit | Grace block period |
|---|-------------|------------------|------------------|--------------------|
| /daten/projekte/lam/quotaTest/xfsMount | 0 | 0 | 0 | |
| /daten/projekte/lam/quotaTest/userOnlyMount | 0 | 0 | 0 | |
| /daten/projekte/lam/quotaTest/userAndGroupMount | 0 | 0 | 0 | |
| /daten/projekte/lam/quotaTest/ext4Mount | 0 | 0 | 0 | |

Filesystem quota (LDAP)

You can store your filesystem quotas directly in LDAP. See Linux DiskQuota [<http://sourceforge.net/projects/linuxquota/>] for details since it requires quota tools that support LDAP. You will need to install the quota LDAP schema to manage the object class "systemQuotas".

Please add the module "Quota (systemQuotas)" for users to your LAM server profile to enable this feature.

If you store the quota information on the filesystem please see the previous section.

| Mountpoint | Soft block limit | Hard block limit | Soft inode limit | Hard inode limit | |
|------------|------------------|------------------|------------------|------------------|---|
| /home | 200000 | 250000 | 10000 | 15000 | ✗ |
| /share | 500000 | 700000 | 20000 | 25000 | ✗ |
| | 0 | 0 | 0 | 0 | ✚ |

Kolab

This module supports to manage Kolab accounts with LAM. E.g. you can set the user's mail quota and define invitation policies.

Please add the Kolab user module in your LAM server profile to activate Kolab support.

| Selected modules | Available modules |
|-------------------------------|--|
| Personal (inetOrgPerson)(*) ✗ | Account (account)(*) ✚ |
| Kolab (kolabUser) ✗ | Account locking (locking389ds) ✚ |
| | AD LDS (windowsLDSUser)(*) ✚ |
| | Asterisk (asteriskAccount) ✚ |
| | Asterisk voicemail (asteriskVoicemail) ✚ |

Please enter an email address at the Personal page and set a Unix password first. Both are required that Kolab accepts the accounts. The email address ("Personal" page) must match your Kolab domain, otherwise the account will not work.

The screenshot shows the 'Personal' page for a user named Claudia Bach. The interface has a top navigation bar with the user's name and email (claudia.bach@ldap-account-manager.org). Below this is a breadcrumb trail: Suffix > People > ldap-account-manager > org. On the right, there's a field for 'RDN identifier' with the value 'cn'. The main content area is divided into sections: 'Personal' (with a user icon), 'Kolab' (with a cloud icon), 'Mailbox quota' (with an input field and a help icon), 'Invitation policy' (with a dropdown menu set to 'Manual' and an 'Always accept' button), 'Email aliases' (with an input field and a plus icon), 'Delegates' (with a dropdown menu showing 'Hans Zimmer > People > ldap-account-manager > org' and a plus icon), and 'Options' (with 'Allowed recipients' and 'Allowed senders' input fields, each with a plus icon). The interface is clean and modern, with a light gray background and blue accents.

If you upgrade existing non-Kolab accounts please make sure that the account has an Unix password.

Asterisk

LAM supports Asterisk accounts, too. See the Asterisk section for details.

EDU person

EDU person accounts are mainly used in university networks. You can specify the principal name, nick names and much more.

Managing entries in your LDAP directory

Claudia Bachclaudia.bach@ldap-account-manager.orgTelephone number 0123-4567-8900Mobile number 0123-4567-8922

Suffixdemo > People > test > deRDN identifieruid

Personal

Unix

Shadow

EDU person

Principal namecbach

Primary affiliationemployee

Scoped affiliationsaffiliate @ cs.berkeley.edu

Affiliationslibrary-walk-in affiliate employee affiliate

Nick namesclaudia

Entitlementsurn:mace:washington.edu:confocalMicroscope

Organisationo=Hogwarts,dc=hsww,dc=wiz

Primary organisational unitou=Potions,o=Hogwarts,dc=hsww,dc=wiz

Organisational unitsou=Potions,o=Hogwarts,dc=hsww,dc=wiz

Assurance profileshttp://idm.example.org/LOA#sample urn:mace:incommon:IAQ:sample

Remove EDU person extension

PyKota

There are two LAM user modules depending if your user entries should be built on object class "pykotaObject" or a different structural object class (e.g. "inetOrgPerson"). For "pykotaObject" please select "PyKota (pykotaUserStructural(*))" and "PyKota (pykotaUser)" in all other cases.

Users

Selected modules

Available modules

Personal (inetOrgPerson)*

PyKota (pykotaUser)

Account (account)*

Account locking (locking389ds)

AD LDS (windowsLDSUser)*

Asterisk (asteriskAccount)

Asterisk voicemail (asteriskVoicemail)

To display the job history please setup the job DN on tab "Module settings":

PyKota

Job suffixou=jobs,ou=pykota,o=test,c=de


Now you can add the PyKota extension to your user accounts. Here you can setup the printing options and add payments for this user.


For LAM Pro there are also self service fields to allow users e.g. to view their current balance and job history.

Managing entries in your LDAP directory

Demo User

Suffixpeople > pykota > test > deRDN identifiercn

 Personal

 PyKota

Pykota user namedemo

Balance301 ?

Limit typeQuota

Overcharge factor1.0

Payment historyJob history ?

Payment

Amount

Comment


Add ?


Remove PyKota extension

You may also view the payment and job history.

Demo User

Suffixpeople > pykota > test > deRDN identifiercn

 Personal

 PyKota

Total paid301 ?

Payment history

| Date | Amount | Comment |
|------------------------|--------|-----------------|
| 2019-09-28 11:23:30,00 | 11.0 | |
| 2019-09-28 10:53:31,00 | 200.0 | |
| 2015-08-05 19:59:39,00 | 30.0 | |
| 2015-08-05 19:59:35,00 | 10.0 | |
| 2013-10-15 18:30:54,00 | 50.0 | initial payment |

Back

Demo User

Suffixpeople > pykota > test > deRDN identifiercn

 Personal

 PyKota

| Date | Printer | Price | Size | Title |
|---------------------|---------------------|-------|------|--|
| 06.08.2015 21:17:06 | Virtual_PDF_Printer | 9.5 | 90 | |
| 05.08.2015 22:00:33 | Virtual_PDF_Printer | 9.5 | 90 | |
| 05.08.2015 21:59:44 | Virtual_PDF_Printer | 9.5 | 90 | |
| 24.09.2013 20:55:28 | Virtual_PDF_Printer | 9.5 | 90 | LDAP Account Manager Pro (localhost:389) |

Back

Password policy (LAM Pro)

OpenLDAP supports the ppolicy [<http://linux.die.net/man/5/slapo-ppolicy>] overlay to manage password policies for LDAP entries. LAM Pro supports managing the policies and assigning them to user accounts.

Please add the account type "Password policies" to your LAM server profile and activate the "Password policy" module for the user/group/host type.

Users

Selected modules

Personal (inetOrgPerson)*

Unix (posixAccount)

Shadow (shadowAccount)

Password policy (ppolicyUser)

Available modules

Account (account)*

Account locking (locking389ds)

AD LDS (windowsLDSUser)*

Asterisk (asteriskAccount)

Asterisk voicemail (asteriskVoicemail)

You can select the password policy and force a password change on next login. Accounts can also be (un)locked.

Claudia Bach

claudia.bach@dap-account-manager.org

Telephone number 0123-4567-8900

Mobile number 0123-4567-8922

Suffix

demo > People > test > de

RDN identifier

uid

Personal

Unix

Shadow

Password policy

Password policy

default

Password change required

☐

Last password change

16.12.2021 08:53:38

Lock account

You can assign any password policy which is found in the LDAP suffix of the "Password policies" type. When you set the policy to "default" then OpenLDAP will use the default policy as defined in your slapd.conf file.

Attention: Locking and unlocking requires that you also activate the option "Lockout users" in the assigned password policy. Otherwise, it will have no effect.

Account locking for 389ds (LAM Pro)

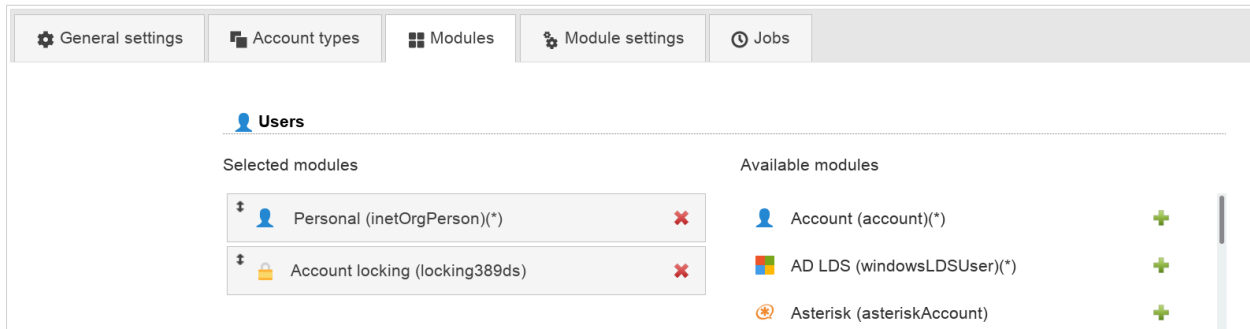
This module allows you to display if users are locked by 389ds server. You can (de)activate your users. The password expiration time can also be managed.

Requirements: 389ds LDAP server

Configuration

Please add the user module "Account locking (locking389ds)".

Managing entries in your LDAP directory



This will show the password expiration time. You can edit the value if needed.

If there are any failed login attempts then LAM displays their number and till when the user is locked by the system.

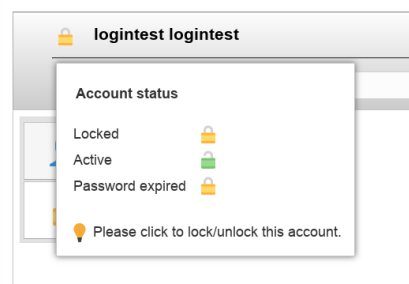
The limit of failed login attempts and lockout duration is configured on your LDAP server and not within LAM.



You can unlock the user by clicking on the lock icon.

Here you can also (de)activate the account.

Note: Accounts are only locked by the LDAP server due to failed password attempts. You cannot manually lock an account. Deactivate it in case you want to disable login for a user.



FreeRadius

FreeRadius is a software that implements the RADIUS authentication protocol. LAM allows you to manage several of the FreeRadius attributes.

To activate the FreeRadius plugin please activate the FreeRadius user module in your server profile:

Managing entries in your LDAP directory

The screenshot shows the 'Users' management interface. At the top, there are tabs: 'General settings', 'Account types', 'Modules', 'Module settings', and 'Jobs'. The 'Users' tab is active. Below the tabs, there are two columns: 'Selected modules' and 'Available modules'. The 'Selected modules' column contains four items: 'Personal (inetOrgPerson)(*)', 'Unix (posixAccount)', 'Shadow (shadowAccount)', and 'FreeRadius (freeRadius)'. The 'Available modules' column contains six items: 'Account (account)(*)', 'Account locking (locking389ds)', 'AD LDS (windowsLDSUser)(*)', 'Asterisk (asteriskAccount)', 'Asterisk voicemail (asteriskVoicemail)', and 'Authorized Services (authorizedServiceObject)'. Each item has a plus or minus icon to its right.

You can disable unneeded fields on the tab "Module settings". Here you can also set the DN where your Radius profile templates are stored if you use the option "Profile".

The screenshot shows the 'FreeRadius' module settings interface. At the top, there is a 'Profile DN' field with the value 'ou=radiusProfiles,o=test,c=de'. Below this, there is a 'Hidden options' section with a question mark icon. The 'Hidden options' section contains several checkboxes: 'IP address', 'Group names', 'Profile', 'Net mask', 'Expiration date', 'Realm', 'Idle timeout', and 'Enabled'. All checkboxes are currently unchecked.

Now you will see the tab "FreeRadius" when editing users. The extension can be (de)activated for each user. You can setup e.g. realm, IP and expiration date.

The screenshot shows the user profile editing interface for 'Claudia Bach'. At the top, there is a header bar with the user's name 'Claudia Bach', email 'claudia.bach@ldap-account-manager.org', telephone number '0123-4567-8900', and mobile number '0123-4567-8922'. Below the header bar, there is a navigation bar with 'Suffix' and 'RDN identifier' dropdowns. The 'Suffix' dropdown is set to 'demo > People > test > de' and the 'RDN identifier' dropdown is set to 'uid'. On the left side, there is a sidebar with four items: 'Personal', 'Unix', 'Shadow', and 'FreeRadius'. The 'FreeRadius' item is selected. On the right side, there are several fields: 'Realm' (ldap-account-manager.org), 'Group names' (admin, users), 'IP address' (123.123.123.123), 'Net mask' (255.255.255.0), 'Idle timeout' (3600), 'Expiration date' (01.01.2020 00:00), 'Profile' (-), and 'Enabled' (-). There is a 'Change' button next to the 'Expiration date' field. At the bottom right, there is a red button labeled 'Remove FreeRadius extension'.

Heimdal Kerberos (LAM Pro)

You can manage your Heimdal Kerberos accounts with LAM Pro. Please add the user module "Kerberos (heimdalKerberos)" to activate this feature.

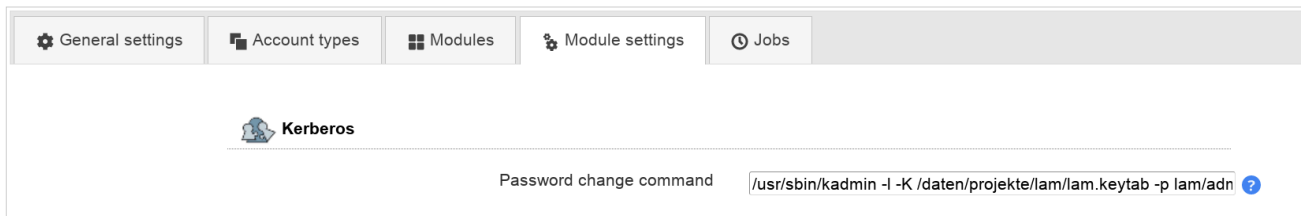
Setup password changing

LAM Pro cannot generate the password hashes itself because Heimdal uses a proprietary format for them. Therefore, LAM Pro needs to call e.g. kadmin to set the password.

The wildcards @@password@@ and @@principal@@ are replaced with password and principal name. Please use keytab authentication for this command since it must run without any interaction.

Example to create a keytab: ktutil -k /root/lam.keytab add -p lam@LAM.LOCAL -e aes256-cts-hmac-sha1-96 -V 1

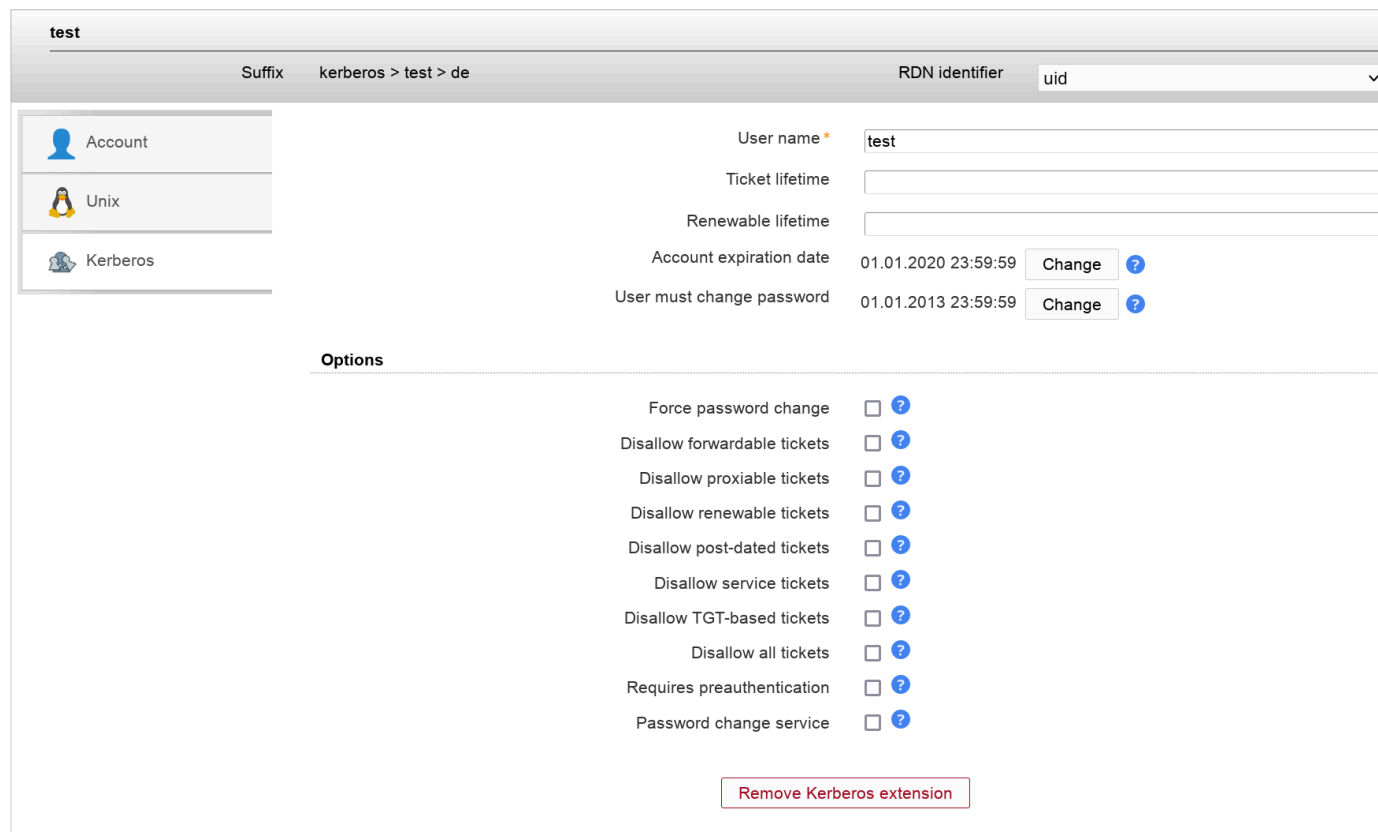
Security hint: Please secure your LAM Pro server since the new passwords will be visible for a short term in the process list during password change.



The screenshot shows the 'Kerberos' module settings in the LAM Pro web interface. The top navigation bar includes 'General settings', 'Account types', 'Modules', 'Module settings', and 'Jobs'. The 'Kerberos' module is selected, and the 'Password change command' field is populated with the command: `/usr/sbin/kadmin -l -K /daten/projekte/lam/lam.keytab -p lam/adn`.

User management

You can specify the principal/user name, ticket lifetimes and expiration dates. Additionally, you can set various account options.



The screenshot shows the 'test' user management page in the LAM Pro web interface. The page displays fields for 'User name', 'Ticket lifetime', 'Renewable lifetime', 'Account expiration date', and 'User must change password'. It also includes a section for 'Options' with checkboxes for various Kerberos settings.

| Field | Value | Action |
|---------------------------|---------------------|--------|
| User name | test | |
| Ticket lifetime | | |
| Renewable lifetime | | |
| Account expiration date | 01.01.2020 23:59:59 | Change |
| User must change password | 01.01.2013 23:59:59 | Change |

Options

- Force password change ☐
- Disallow forwardable tickets ☐
- Disallow proxiable tickets ☐
- Disallow renewable tickets ☐
- Disallow post-dated tickets ☐
- Disallow service tickets ☐
- Disallow TGT-based tickets ☐
- Disallow all tickets ☐
- Requires preauthentication ☐
- Password change service ☐

[Remove Kerberos extension](#)

MIT Kerberos (LAM Pro)

You can manage your MIT Kerberos accounts with LAM Pro. Please add the user module "Kerberos (mitKerberos)" to activate this feature. If you want to manage entries based on the structural object class "krbPrincipal" please use "Kerberos (mitKerberosStructural)" instead.

Setup password changing

LAM Pro cannot generate the password hashes itself because MIT uses a proprietary format for them. Therefore, LAM Pro needs to call `kadmin/kadmin.local` to set the password.

LAM will add `"-q 'cpw -pw PASSWORD PRINCIPAL'"` to the command to set the password. Please use keytab authentication for this command since it must run without any interaction.

Keytabs may be created with the `"ktutil"` application.

Security hint: Please secure your LAM Pro server since the new passwords will be visible for a short term in the process list during password change.

Please note that `kadmin/kadmin.local` often returns a successful command even if errors occurred (e.g. password policy violations). You need to test this before and if affected then write a wrapper script around `kadmin` that returns non-zero return codes for errors.

Example commands:

- `/usr/sbin/kadmin -k -t /home/www-data/apache.keytab -p realm/angepwd`
- `sudo /usr/sbin/kadmin.local`



Kerberos

Password change command

`/usr/sbin/kadmin -k -t /data/apache.keytab -p realm/angepwd` ?

User management

You can specify the principal/user name, ticket lifetimes and expiration dates. Additionally, you can set various account options.

test

Suffix

LAM.LOCAL > mitkerberos > test > de

RDN identifier

cn

Personal

Unix

Kerberos

User name *

test@LAM.LOCAL

Failed logins

3

Ticket lifetime

Renewable lifetime

User must change password

-

Change ?

Account expiration date

-

Change ?

Last password change

07.09.2021 10:49:45 ?

Last login

07.09.2021 10:59:26 ?

Last failed login

07.09.2021 11:00:02 ?

Options

Force password change

☐ ?

Disallow forwardable tickets

☐ ?

Disallow proxiable tickets

☐ ?

Disallow renewable tickets

☐ ?

Disallow post-dated tickets

☐ ?

Disallow service tickets

☐ ?

Disallow user-to-user authentication

☐ ?

Disallow all tickets

☐ ?

Requires preauthentication

☒ ?

Requires hardware authentication

☐ ?

Password change service

☐ ?

Password policy

demo

Remove Kerberos extension

NIS mail aliases

This module allows to add/remove the user in mail alias entries.

Note: You need to activate the mail alias type for this module.

To activate mail aliases for users please select the module "Mail aliases (nisMailAliasUser)":

Users

Selected modules

Available modules

Personal (inetOrgPerson)*

✖

Unix (posixAccount)

✖

Shadow (shadowAccount)

✖

Mail aliases (nisMailAliasUser)

✖

Account (account)*

+

Account locking (locking389ds)

+

AD LDS (windowsLDSUser)*

+

Asterisk (asteriskAccount)

+

Asterisk voicemail (asteriskVoicemail)

+

Authorized Services (authorizedServiceObject)

+

On tab Module settings you can select if you want to set the user name or email as recipient in alias entries.

Managing entries in your LDAP directory



Hidden options [?](#)
Aliases for user name ☐
Aliases for email ☐

Now you will see the mail aliases tab when editing an user.

The red cross will only remove the user from the alias entry. If you click the trash can button then the whole alias entry (which may contain other users) will be deleted.

Claudia Bach claudia.bach@ldap-account-manager.org Telephone number 0123-4567-8900 Mobile number 0123-4567-8922

Suffix demo > People > test > de RDN identifier uid

Personal

Unix

Shadow

Mail aliases

Aliases for user name

myAlias1 ✖ 🗑

Add

Aliases for email

claudia.bach.external ✖ 🗑
claudiabach ✖ 🗑

Add

You can add the user to existing alias entries or create completely new ones.

Claudia Bach
claudia.bach@ldap-account-manager.org Telephone number 0123-4567-8900 Mobile number 0123-4567-8922

Suffix demo > People > test > de RDN identifier uid

Personal

Unix

Shadow

Mail aliases

Recipient cbach

Create new alias

Suffix ou=mailaliases,o=test,c=de

Alias name

Create

Add to existing alias

Alias names

claudia.bach.external
claudiabach
testalias
testalias2

Add

Cancel

Courier mail

This module allows to add/remove the Courier extension for users.

Configuration:

Please activate the module Courier for users to enable this extension. The Unix module is optional.

Managing entries in your LDAP directory

Unix Users

Selected modules

- Personal (inetOrgPerson)(*)
- Unix (posixAccount)
- Courier (courierMailAccount)

Available modules

- Account (account)(*)
- Account locking (locking389ds)
- AD LDS (windowsLDSUser)(*)
- Asterisk (asteriskAccount)
- Asterisk voicemail (asteriskVoicemail)

Usage:

Your user tab will now show the Courier extension. This can be added/removed any time.

Here you can configure the home directory in case the Unix module is not activated. Additionally, mailbox folder, quota, server and feature flags can be configured.

Demo User demo@ldap-account-manager.org

Suffix: courier > test > de RDN identifier: cn

Personal Unix Courier

Mailbox folder: /mnt/mail/demo/

Mailbox host: mailserver

Mailbox quota: 500 GB

Disable IMAP access: ☐

Disable POP3 access: ☐

Disable webmail access: ☐

Disable shared folder access: ☐

Remove Courier mail extension

Qmail (LAM Pro)

LAM Pro manages all qmail attributes for users. This includes mail addresses, ID numbers and quota settings.

Please note that the main mail address is managed on tab "Personal" if this module is active. Otherwise, it will be on the qmail tab.

Managing entries in your LDAP directory

Claudia Bachclaudia.bach@ldap-account-manager.orgTelephone number 0123-4567-8900Mobile number 0123-4567-8922

Suffixdemo > People > test > deRDN identifieruid

Personal

Unix

Shadow

Qmail

Alternate addresscbach@ldap-account-manager.org

Forwarding addresscbach-backup@ldap-account-manager.org

UID number1234

GID number1111

Server addressqmail.ldap-account-manager.org

Message store/mail/cbach

Account statusActive

Configuration typeLDAP + .qmail

Delivery modeDefault

Autoreply textI am out of office.
Your mails will be answered soon.

Delivery program

Deletion date-
Change

Quota

Quota size1000000000

Message count limit10000

Message size limit100000000

Remove qmail extension

You can hide several qmail options if you do not want to manage them with LAM. This can be done on the module settings tab of your LAM server profile.



Hidden options

| | | | | | |
|----------------|--------------------------|---------------------|--------------------------|--------------------|--------------------------|
| Quota size | <input type="checkbox"/> | Message count limit | <input type="checkbox"/> | Message size limit | <input type="checkbox"/> |
| UID number | <input type="checkbox"/> | GID number | <input type="checkbox"/> | Autoreply text | <input type="checkbox"/> |
| Server address | <input type="checkbox"/> | Message store | <input type="checkbox"/> | Delivery program | <input type="checkbox"/> |
| Deletion date | <input type="checkbox"/> | Configuration type | <input type="checkbox"/> | | |

Mail routing

LAM supports to manage mail routing for user accounts.

Module activation:

This feature can be activated by adding the "Mail routing" module to the user account type in your server profile.

The screenshot shows the 'Users' module settings page. At the top, there is a navigation bar with tabs: 'General settings', 'Account types', 'Modules', 'Module settings', and 'Jobs'. The 'Modules' tab is selected. Below the navigation bar, the 'Users' section is active. It displays two columns: 'Selected modules' and 'Available modules'. The 'Selected modules' column lists four modules: 'Personal (inetOrgPerson)(*)', 'Unix (posixAccount)', 'Shadow (shadowAccount)', and 'Mail routing (inetLocalMailRecipient)'. Each module has a red 'X' icon to its right. The 'Available modules' column lists five modules: 'Account (account)(*)', 'Account locking (locking389ds)', 'AD LDS (windowsLDSUser)(*)', 'Asterisk (asteriskAccount)', and 'Asterisk voicemail (asteriskVoicemail)'. Each module has a green '+' icon to its right.

Usage

You can specify a routing address, the mail server and a number of local addresses to route.

In case you want to add this extension by default for new users there is an option in profile editor.

The screenshot shows the user profile editor for 'Claudia Bach'. At the top, the user's name 'Claudia Bach' is displayed, along with their email 'claudia.bach@ldap-account-manager.org', telephone number '0123-4567-8900', and mobile number '0123-4567-8922'. Below this, there is a 'Suffix' dropdown menu showing 'demo > People > test > de' and an 'RDN identifier' dropdown menu showing 'uid'. On the left side, there is a list of modules: 'Personal', 'Unix', 'Shadow', and 'Mail routing'. On the right side, there are three input fields: 'Routing address' with the value 'cbach@example.com', 'Mail server' with the value 'qmail.ldap-account-manager.org', and 'Local address' with the value 'claudia.bach@example.com'. Below these fields, there is a red button labeled 'Remove mail routing extension'.

Wildcards

The module supports wildcards in the following input fields:

- Routing address
- Local address

See the other modules that you activated what wildcards they provide (e.g. \$user).

SSH public keys

You can manage your public keys for SSH in LAM if you installed the LPK patch for SSH [<http://code.google.com/p/openssh-lpk/>] or setup AuthorizedKeysCommand (see below).

Activate the "SSH public key" module for users in the server profile and you can add keys to your user entries.

Managing entries in your LDAP directory

The screenshot displays the LDAP Account Manager (LAM) web interface. At the top, there's a navigation bar with tabs: General settings, Account types, Modules, Module settings, and Jobs. The 'Users' section is active, showing a list of 'Selected modules' (Personal, Unix, Shadow, SSH public key) and 'Available modules' (Account, Account locking, AD LDS, Asterisk, Asterisk voicemail). Below this, a user profile for 'Claudia Bach' is shown with contact information. The 'Suffix' is 'demo > People > test > de' and the 'RDN identifier' is 'uid'. On the left, a sidebar shows the selected modules. On the right, the 'SSH public key' field contains a key, and there is an 'Upload file' button with a 'Browse...' button and an 'Upload' button. A 'Remove SSH public key extension' button is also visible.

Example for AuthorizedKeysCommand

This will dynamically get the public key from LDAP. In this case there is no need to patch SSH sources.

Create the authentication script in e.g. /usr/bin/ldapAuthSSH.sh

```
#!/bin/bash
uid=$1
server=ldap.domain.com
baseDN=ou=people,dc=example,dc=com
port=389
ldapsearch -x -h $server -p $port -b $baseDN -s sub "(&(objectclass=posixAccount)(uid=$uid))" | sed -n '/^/{H;d};/sshPublicKey:'
```

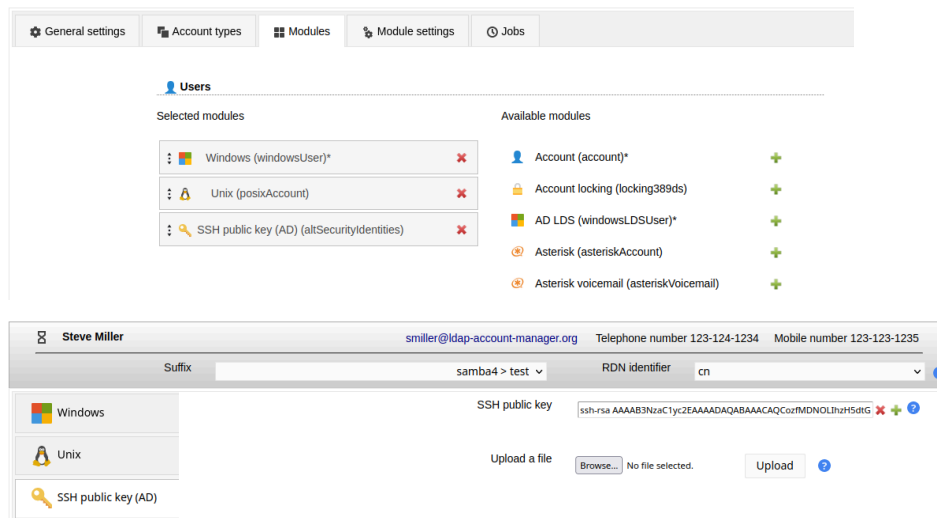
Now setup your sshd_config

```
AuthorizedKeysCommand /usr/bin/ldapAuthSSH.sh
AuthorizedKeysCommandUser root
```

SSH public keys (AD)

You can manage your public SSH keys in Active Directory/Samba 4. Activate the "SSH public key (AD)" module for users in the server profile and you can add keys to your user entries. This will use the attribute "altSecurityIdentities".

Managing entries in your LDAP directory



Example for AuthorizedKeysCommand

This will dynamically get the public key from LDAP.

Create the authentication script in e.g. /usr/bin/ldapAuthSSH.sh

```
#!/bin/bash
uid=$1
server=ldap.domain.com
baseDN=ou=people,dc=example,dc=com
port=389
ldapsearch -x -h $server -p $port -b $baseDN -s sub "(&(objectclass=posixAccount)(uid=$uid))" | sed -n '/^/{H;d};/altSecurityIdentities/'
```

Now setup your sshd_config

AuthorizedKeysCommand /usr/bin/ldapAuthSSH.sh

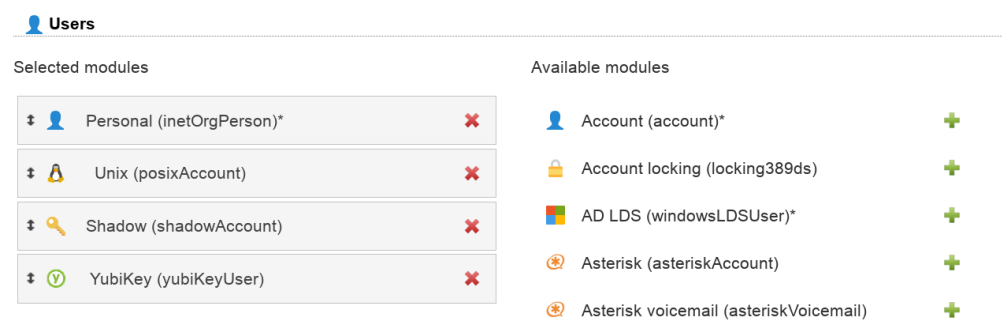
AuthorizedKeysCommandUser root

YubiKey

You can manage your YubiKey ids with LAM. It supports the yubiKeyUser schema [<https://github.com/mludvig/yubikey-ldap>] or any other attribute mapping.

Configuration

First, you need to activate the YubiKey module for users in your LAM server profile.



Second, you need to specify which object class and attribute name should be used.

Managing entries in your LDAP directory

Object class: If you have an object class just for the YubiKey ids then enter it here. LAM will then provide options to add and remove it. In case you reuse some existing attribute from e.g. inetOrgPerson please leave object class name blank.

Attribute name: please enter the attribute name that is used for the key ids.



| | | |
|------------------|--|--|
| Object class | <input type="text" value="yubiKeyUser"/> | |
| Attribute name * | <input type="text" value="yubiKeyId"/> | |

You will then be able to manage the key ids for your users.

Claudia Bach claudia.bach@ldap-account-manager.org Telephone number 0123-4567-8900 Mobile number 0123-4567-8922

Suffix RDN identifier

Personal

Unix

Shadow

YubiKey

YubiKey ids

[Remove YubiKey extension](#)

Self Service (LAM Pro)

This will allow your users to update their own keys.

You need to configure the object class and attribute name first. This is done on tab "Module settings" in self service profile.

Attention: Please note that both fields are mandatory here. Even if you reused an attribute from some existing object class you need to set it here. LAM needs this to detect if the user can add keys.



| | | |
|----------------|--|--|
| Object class | <input type="text" value="yubiKeyUser"/> | |
| Attribute name | <input type="text" value="yubiKeyId"/> | |

Then add the YubiKey ids field to your self service profile on tab "Page layout".

Add input field

| | | |
|---------------------|--|--|
| Input field | <input type="text" value="YubiKey ids"/> | |
| Group | <input type="text" value="Personal data"/> | |
| Add | | |

When a user with the specified object class logs in then the key input fields are shown.

YubiKey ids

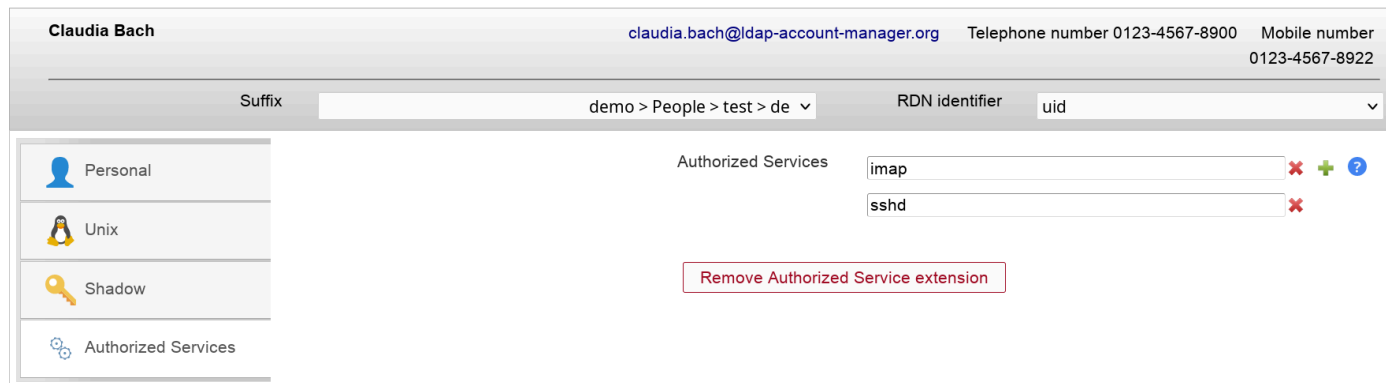
[+ Add](#)

Authorized services

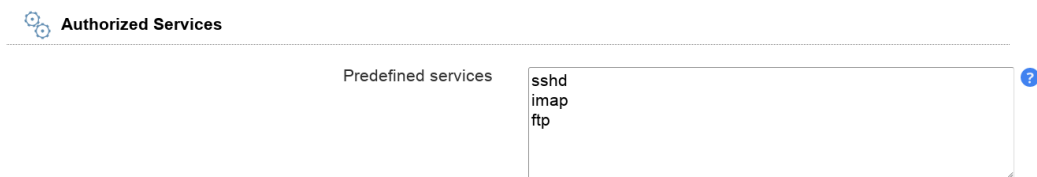
You can setup PAM to check if a user is allowed to run a specific service (e.g. sshd) by reading the LDAP attribute "authorizedService". This way you can manage all allowed services via LAM.

To activate this PAM feature please setup your **/etc/libnss-ldap.conf** and set "pam_check_service_attr" to "yes".

Inside LAM you can now set the allowed services. You may also setup default services in your account profiles.



You can define a list of services in your LAM server profile that is used for autocompletion.



The autocompletion will show all values that contains the entered text. To display the whole list you can press backspace in the empty input field. Of course, you can also insert a service name that is not in the list.



IMAP mailboxes

LAM may create and delete mailboxes on an IMAP server for your user accounts. You will need an IMAP server that supports either SSL or TLS for this feature.

To activate the mailbox management module please add the "Mailbox (imapAccess)" module for the type user in your LAM server profile:

Managing entries in your LDAP directory

| Selected modules | | Available modules | |
|-----------------------------|---|---|---|
| Personal (inetOrgPerson)(*) | ✖ | Account (account)(*) | + |
| Unix (posixAccount) | ✖ | Account locking (locking389ds) | + |
| Mailbox (imapAccess) | ✖ | AD LDS (windowsLDSUser)(*) | + |
| | | Asterisk (asteriskAccount) | + |
| | | Asterisk voicemail (asteriskVoicemail) | + |
| | | Authorized Services (authorizedServiceObject) | + |

Now configure the module on the tab "Module settings". Here you can specify the IMAP server name, encryption options, the authentication for the IMAP connection and the valid mail domains. LAM can use either your LAM login password for the IMAP connection or display a dialog where you need to enter the password. It is also possible to store the admin password in your server profile. This is not recommended for security reasons.

The user name can either be a fixed name (e.g. "admin") or it can be generated with LDAP attributes of the LAM admin user. E.g. \$uid\$ will be transformed to "myUser" if you login with "uid=myUser,ou=people,dc=example,dc=com".

The mail domains specify for which accounts mailboxes may be created/deleted. E.g. if you enter "lam-demo.org" then mailboxes can be managed for "user@lam-demo.org" but not for "user@example.com". Use "*" for any domain.

You need to install the SSL certificate of the CA that signed your server certificate. This is usually done by installing the certificate in /etc/ssl/certs. Different Linux distributions may offer different ways to do this. For Debian/Ubuntu please copy the certificate in "/usr/local/share/ca-certificates" and run "update-ca-certificates" as root.

It is not recommended to disable the validation of IMAP server certificates.

The prefix, user name attribute and path separator specifies how your mailboxes are named (e.g. "user.myUser@localhost" or "user/myUser"). Select the values depending on your IMAP server settings.

You can specify a list of initial folder names to create for new mailboxes. LAM will then create them with each new mailbox.

| | | |
|-----------------------------|-------------------------|---|
| Server address * | localhost | ? |
| Encryption protocol | TLS | ? |
| Validate server certificate | Yes | ? |
| IMAP admin user * | \$uid\$ | ? |
| IMAP password input | LAM user password | ? |
| Mail domains * | * | ? |
| Prefix for mailboxes | user | ? |
| Initial folders | Trash Sent Drafts | ? |
| User name attribute | uid | ? |
| Path separator | . | ? |

When you edit an user account then you will now see the tab "Mailbox". Here you can create/delete the mailbox for this user.

Managing entries in your LDAP directory

Please note that mailbox creation via file upload is not possible if you configured in LAM server profile to ask for the admin password.

Claudia Bach

claudia.bach@ldap-account-manager.orgTelephone number 0123-4567-8900Mobile number 0123-4567-8922

Suffixdemo > People > test > deRDN identifieruid

Personal

Unix

Mailbox

Email addressclaudia.bach@ldap-account-manager.org

Mailboxuser.cbach

Current usage (kB)0

Quota limit (kB)100000

Update quota

Delete mailbox

IP addresses (LAM Pro)

You can manage the IP addresses of user accounts (e.g. assigned by DHCP) with the ipHost module.

Configuration

General settingsAccount typesModulesModule settingsJobs

Users

Selected modules

Personal (inetOrgPerson)(*)

Unix (posixAccount)

IP address (ipHost)

Available modules

Account (account)(*)

Account locking (locking389ds)

AD LDS (windowsLDSUser)(*)

Asterisk (asteriskAccount)

Asterisk voicemail (asteriskVoicemail)

User editing

Claudia Bach

claudia.bach@ldap-account-manager.orgTelephone number 0123-4567-8900Mobile number 0123-4567-8922

Suffixdemo > People > test > deRDN identifieruid

Personal

Unix

IP address

IP address *192.168.0.22

Remove IP address extension

Account

This is a very simple module to manage accounts based on the object class "account". Usually, this is used for host accounts only. Please pay attention that users based on the "account" object class cannot have contact information (e.g. telephone number) as with "inetOrgPerson".

102

Managing entries in your LDAP directory

You can enter a user/host name and a description for your accounts.

The screenshot shows the 'demoUser' account edit form. At the top, there's a breadcrumb trail: 'demo > People > test > de'. Below this, there's a 'Suffix' field and an 'RDN identifier' dropdown set to 'uid'. On the left, there's a sidebar with 'Account' selected. The main form has two fields: 'User name' with the value 'demoUser' and 'Description' with the value 'This is a demo user'.

OpenLDAP TOTP (LAM Pro)

Use this module if you want to use OpenLDAP's builtin 2-factor-authentication with TOTP.

For admin interface add the OpenLDAP TOTP module:

The screenshot shows the 'Module settings' page for 'Users'. It has a top navigation bar with 'Account types', 'Modules', 'Module settings', and 'Jobs'. The 'Modules' section is active. It displays two columns: 'Selected modules' and 'Available modules'. The 'Selected modules' column lists: 'Personal (inetOrgPerson)(*)', 'Unix (posixAccount)', 'Shadow (shadowAccount)', and 'OpenLDAP TOTP (openldapTotp)'. The 'Available modules' column lists: 'Account (account)(*)', 'Account locking (locking389ds)', 'AD LDS (windowsLDSUser)(*)', 'Asterisk (asteriskAccount)', 'Asterisk voicemail (asteriskVoicemail)', and 'Authorized Services (authorizedServiceObject)'. Each module has a plus or minus icon to toggle its selection.

When one of your users activates TOTP then you can see the serial number and TOTP params in user edit screen.

Please note that the token can only be setup by the user in self service. Admins are not able to setup tokens. They can just delete them by removing the extension.

The screenshot shows the 'test' user edit screen. It has a breadcrumb trail: 'People > test > de'. The 'RDN identifier' dropdown is set to 'cn'. On the left, there's a sidebar with 'Personal', 'Unix', 'Shadow', and 'OpenLDAP TOTP' selected. The main form has two fields: 'Serial number' with the value '123456' and 'OTP parameters' with the value 'ou=People,o=test,c=de'. There is a 'Remove extension' button below the OTP parameters field.

Last login (LAM Pro)

This module shows the last successful login of the user. You can setup a cron job to deactivate inactive users.

Managing entries in your LDAP directory

Users

Selected modules

Personal (inetOrgPerson)*

Unix (posixAccount)

Last login (lastBind)

Available modules

Account (account)*

Account locking (locking389ds)

AD LDS (windowsLDSUser)*

Asterisk (asteriskAccount)

Asterisk voicemail (asteriskVoicemail)

Authorized Services (authorizedServiceObject)

Auto delete (autoDelete)

Steve Miller

Telephone number 123456789 Mobile number 123456789

Suffix People > test > de RDN identifier uid

Personal

Unix

Last login

Last login 07.01.2024 20:36:07

Groups

Unix

This module is used to manage Unix group entries. This is the default module to manage Unix groups and uses the nis.schema. Suse users who use the rfc2307bis.schema need to use LAM Pro.

Configuration

Special Please add the account type "Groups" and then select account module "Unix (posixGroup)".

Groups

Selected modules

Unix (posixGroup)*

Available modules

AD LDS (windowsLDSGroup)*

Auto delete (autoDelete)

Custom fields (customFields)

Custom scripts (customScripts)

Virtual list attributes:

Groups

Group accounts (e.g. Unix and Samba)

LDAP suffix *

List attributes

Custom label

Additional LDAP filter

Read-only

Hidden

No new entries

Disallow delete

ou=demo,ou=group,o=test,c=de

#cn;#gidNumber;#memberUID;#description

☐

☐

☐

☐

The following virtual attributes can be shown in the group list. These are no real LDAP attributes but extra data that can be shown by LAM.

- memberuid_count: number of entries in attribute "memberuid"

- member_count: number of entries in attribute "member"
- uniqueMember_count: number of entries in attribute "uniquemember"
- owner_count: number of entries in attribute "owner"
- roleOccupant_count: number of entries in attribute "roleOccupant"

Module settings:

GID generator: LAM will suggest GID numbers for your accounts. Please note that it may happen that there are duplicate IDs assigned if users create groups at the same time. Use an overlay [<http://www.openldap.org/doc/admin24/overlays.html>] like "Attribute Uniqueness" (example) if you have lots of LAM admins creating groups.

- Fixed range: LAM searches for free numbers within the given limits. LAM always tries to use a free GID that is greater than the existing GIDs to prevent collisions with deleted groups.
- Samba ID pool: This uses a special LDAP entry that includes attributes that store a counter for the last used UID/GID. Please note that this requires that you install the Samba schema and create an LDAP entry of object class "sambaUnixIdPool".
- Magic number: Use this if your LDAP server assigns the GID numbers automatically (e.g. DNA by 389 server). Enter the server's magic number setting.


Disable membership management: Disables group membership management. This is useful if memberships are e.g. managed via group of names.



Groups

| | | |
|---------------------------------|--------------------------|---|
| GID generator | Fixed range | ? |
| Minimum GID number * | 10000 | ? |
| Maximum GID number * | 20000 | ? |
| Suffix for GID/group name check | | ? |
| Disable membership management | <input type="checkbox"/> | ? |

Group management:

| admins | | Administrators |
|--|---|---------------------|
| Suffix | demo > group > test > de | RDN identifier cn ? |
|  Unix | | |
| Group name * | admins | |
| GID number | 11819 | |
| Description | Administrators | |
| Group members | <div>Edit members ?</div> <div>azpc01 azpc02 external shuber (shuber) smilleru1</div> | |

Group membership management:

admins Administrators

Suffix demo > group > test > de RDN identifier cn ?

Unix

Group members

Selected users

- azpc01
- azpc02
- external
- shuber (shuber)
- smilleru1

Filter

Back

Available users

- ebaecker (Ernst Bäcker)
- fhuber (Franz Huber)
- hmeier (Helmut Meier)
- hschuster (hschuster)
- kmontag (Kerstin Montag)
- mfischer (mfischer)
- smiller (Steve Miller)
- thauser (Thomas Hauser)
- xmontag (Xaver Montag)

Filter

Unix groups with rfc2307bis schema (LAM Pro)

Some applications (e.g. Suse Linux) use the rfc2307bis schema for Unix accounts instead of the nis schema. In this case group accounts are based on the object class groupOf(Unique)Names or namedObject. The object class posixGroup is auxiliary in this case.

LAM Pro supports these groups with a special account module: **rfc2307bisPosixGroup**

Use this module only if your system depends on the rfc2307bis schema. The module can be selected in the LAM configuration. Instead of using groupOfNames as basis for your groups you may also use namedObject.

Module activation:

Groups

Selected modules

- Group of names (groupOfNames)*
- Unix (rfc2307bisPosixGroup)

Available modules

- AD LDS (windowsLDSGroup)*
- Auto delete (autoDelete)
- Custom fields (customFields)
- Custom scripts (customScripts)

GID generator: LAM will suggest GID numbers for your accounts. Please note that it may happen that there are duplicate IDs assigned if users create groups at the same time. Use an overlay [<http://www.openldap.org/doc/admin24/overlays.html>] like "Attribute Uniqueness" (example) if you have lots of LAM admins creating groups.


- Fixed range: LAM searches for free numbers within the given limits. LAM always tries to use a free GID that is greater than the existing GIDs to prevent collisions with deleted groups.
- Samba ID pool: This uses a special LDAP entry that includes attributes that store a counter for the last used UID/GID. Please note that this requires that you install the Samba schema and create an LDAP entry of object class "sambaUnixIdPool".

Managing entries in your LDAP directory

- Magic number: Use this if your LDAP server assigns the GID numbers automatically (e.g. DNA by 389 server). Enter the server's magic number setting.


Disable membership management: Disables group membership management. This is useful if memberships are e.g. managed via group of names.

Force sync with group of names: This will automatically set the group memberships of the Unix part to the same members as set on group of names tab.


 **Unix**

Groups


GID generator

Fixed range 


Minimum GID number *

10000 


Maximum GID number *

20000 

Suffix for GID/group name check




Disable membership management

☐ 

Options

Force sync with group of names

☐ 


The GID number will be filled automatically based on the server profile configuration.


demo

Suffix

group > test > de


RDN identifier

cn 


 Unix

GID number

10001

 Group of names

Group members

Edit members 

demo_user (Demo User)

Group members can be edited and also synced with Group of (unique) names.

demo

Suffixgroup > test > deRDN identifiercn ?

Unix

Group of names

Group members

Selected users

demo_user (Demo User)

Filter

Available users

Filter

test

←

→

Sync from Group of names

Delete non-matching entries

☒

Back

Samba 3

LAM supports managing Samba 3 groups. You can set special group types and also create Windows predefined groups like "Domain admins".

Module activation:

Groups

Selected modules

Unix (posixGroup)*

Samba 3 (sambaGroupMapping)

Available modules

AD LDS (windowsLDSGroup)*

Auto delete (autoDelete)

Custom fields (customFields)

Custom scripts (customScripts)

Custom type (customBaseType)*

Group editing:

admins Administrators

Suffix demo > group > test > de RDN identifier cn ?

Unix

Samba 3

Display name Administrators

Windows group admins

Group type Domain group

Domain MyCompany

Local members + ?

Remove Samba 3 extension

Windows (Samba 4)

LAM can manage your Windows groups. Please enable the account type "Groups" in your LAM server profile and then add the group module "Windows (windowsGroup)(*)".

Groups

Group accounts (e.g. Unix and Samba) ↑ ↓ ×

LDAP suffix * cn=users,dc=w2012,dc=test ?

List attributes #cn;#description;#location ?

Custom label Groups ?

Additional LDAP filter ?

Read-only ☐ ?

Hidden ☐ ?

No new entries ☐ ?

Disallow delete ☐ ?

The default list attributes are for Unix and not suitable for Windows (blank lines in account table). Please use "#cn;#member;#description" or select your own attributes to display in the account list.

Groups

Selected modules

Windows (windowsGroup)*

Available modules

AD LDS (windowsLDSGroup)* +

Auto delete (autoDelete) +

Custom fields (customFields) +

Custom scripts (customScripts) +

Custom type (customBaseType)* +

NIS support is deactivated by default. Enable it if needed on tab "Module settings".

Windows

Hidden options ?

Email address ☐

NIS domain ☐

Managed by ☐

NIS name ☐

Now you can edit your groups inside LAM. You can manage the group name, description and its type. Of course, you can also set the group members.

Group scopes:

- Global: Use this for groups with frequent changes. Global groups are not replicated to other domains.

- Universal: Groups with universal scope are used to consolidate groups that span domains. They are globally replicated.
- Domain local: Groups with domain local scope can be used to set permissions inside one domain. They are not replicated to other domains.

Group type:

- Security: Use this group type to control permissions.
- Distribution: These groups are only used for email applications. They cannot be used to control permissions.

With "Show effective members" you can show a list of all members of this group including members of subgroups and their subgroups.

The screenshot shows the configuration page for a group named 'demo'. The page is titled 'demo' and 'Demo Group'. The breadcrumb trail is 'Users > w2012 > test'. The RDN identifier is 'cn'. The suffix is 'demo'. The group is managed by 'Hans Müller > Users > w2012 > test'. The group type is 'Security'. The group scope is 'Global'. The group description is 'Demo Group'. The group notes are 'This is a demo group'. The group members are listed as 'Hans Müller > Users > w2012 > test'. The group is a member of 'Hans Müller > Users > w2012 > test'.

AD LDS (formerly ADAM) (LAM Pro)

LAM can manage your AD LDS groups. Please enable the account type "Groups" in your LAM server profile and then add the group module "AD LDS (windowsLDSGroup)(*)".

The screenshot shows the configuration page for 'Groups'. The page is titled 'Groups'. The breadcrumb trail is 'Groups'. The group accounts are listed as 'cn=users,dc=w2012,dc=test'. The LDAP suffix is 'cn=users,dc=w2012,dc=test'. The list attributes are '#cn;#description;#location'. The custom label is 'Groups'. The additional LDAP filter is empty. The 'Read-only' checkbox is checked. The 'Hidden' checkbox is checked. The 'No new entries' checkbox is checked. The 'Disallow delete' checkbox is checked.

The default list attributes are for Unix and not suitable for AD LDS (blank lines in account table). Please use "#cn;#member;#description" or select your own attributes to display in the account list.

Managing entries in your LDAP directory

Groups

Selected modules

AD LDS (windowsLDSGroup)(*)

Available modules

Auto delete (autoDelete)

Custom fields (customFields)

Custom scripts (customScripts)

Custom type (customBaseType)(*)

Dynamic List (dynamicList)(*)

General information (generalInformation)

Now you can edit your groups inside LAM. You can manage the group name, description and its type. Of course, you can also set the group members.

With "Show effective members" you can show a list of all members of this group including members of subgroups and their subgroups.

demogroup > users > instance1 > w10e

Suffix

users > instance1 > w10e

RDN identifier

cn

AD LDS

Group name *

demogroup

Description

Managed by

Change

Group members

Edit

Show effective members

Member of

Edit

testgroup > users > instance1 > w10e

Kolab

Please activate the Kolab group module in your LAM server profile to activate Kolab support.

Groups

Selected modules

Group of unique names (groupOfUniqueNames)(*)

Kolab (kolabGroup)

Available modules

AD LDS (windowsLDSGroup)(*)



Auto delete (autoDelete)

Custom fields (customFields)

Custom scripts (customScripts)

Custom type (customBaseType)(*)

You can specify the email address and also set allowed sender and recipient addresses.







| QA Managers | | People who can manage QA entries | |
|---|--|----------------------------------|------|
| Suffix | Groups > ldap-account-manager > org | RDN identifier | cn ? |
|  Group of unique names | Email address * <input type="text" value="qa@ldap-account-manager.org"/> | | ? |
| | Allowed recipients <input type="text"/> | + | ? |
|  Kolab | Allowed senders <input type="text"/> | + | ? |

Mail routing

LAM supports to manage mail routing for group accounts.

Module activation:



This feature can be activated by adding the "Mail routing" module to the group account type in your server profile.

| Groups | |
|---|--|
| Selected modules | Available modules |
|  Unix (posixGroup)(*) |  AD LDS (windowsLDSGroup)(*) |
|  Mail routing (inetLocalMailRecipient) |  Auto delete (autoDelete) |
| |  Custom fields (customFields) |
| |  Custom scripts (customScripts) |

Usage:








You can specify a routing address, the mail server and a number of local addresses to route.

In case you want to add this extension by default for new groups there is an option in profile editor.

| project1 | | Project 1 | |
|--|---|----------------|------|
| Suffix | demo > group > test > de | RDN identifier | cn ? |
|  Unix | Routing address <input type="text" value="mail@example.com"/> | | |
| | Mail server <input type="text" value="mail.example.com"/> | | |
|  Mail routing | Local address <input type="text" value="mail1@example.com"/> | ✗ | + |
| <div>Remove mail routing extension</div> | | | |

Quota

You can manage file system quotas with LAM. This requires to setup lamdaemon. File system quotas are not stored inside LAM but managed directly on the specified servers.

| | | | | | |
|---|---|---|---|---|---|
| admins | | | | | |
| Suffix demo > group > test > de | | | | | |
| localhost | | | | | |
|  Unix | Mountpoint | Used blocks | Soft block limit | Hard block limit | Grace block period |
|  Quota |  |  |  |  |  |
| | /daten/projekte/lam/quotaTest/xfsMount | 0 | 0 | 0 | |
| | /daten/projekte/lam/quotaTest/userAndGroupMount | 0 | 0 | 0 | |
| | /daten/projekte/lam/quotaTest/groupOnlyMount | 0 | 20000 | 25000 | |
| | /daten/projekte/lam/quotaTest/ext4Mount | 0 | 0 | 0 | |









Dynamic lists (LAM Pro)

Dynamic lists [<http://www.openldap.org/doc/admin24/overlays.html#Dynamic%20Lists>] allow you to create LDAP entries that populate the value of an attribute via LDAP query. This is e.g. used to create groups that contain all users in a certain DN.










Please note that this functionality requires configuration on your LDAP server. E.g. on OpenLDAP you need to activate the "dynlist" overlay and need to specify attribute mappings.

Configuration

Add a new group account type and set a unique label for it.

| | | | | |
|---|---------------------|--------------------------------------|-----------------|------|
| General settings | Account types | Modules | Module settings | Jobs |
| Available account types | | | | |
|  | Aliases | Alias entries | | + |
|  | Asterisk extensions | Asterisk extensions entries | | + |
|  | Automount entries | Automount entries | | + |
|  | Billing codes | PyKota billing codes | | + |
|  | Bind DNS | Bind DNS entries | | + |
|  | Custom type | Custom entries | | + |
|  | DHCP | DHCP administration | | + |
|  | Groups | Group accounts (e.g. Unix and Samba) | | + |

Do not forget to set proper "List attributes" to be shown on the overview page of all dynamic lists.

| | | |
|---|--------------------------------------|---|
|  Dynamic Lists | Group accounts (e.g. Unix and Samba) | ↑ ↓ × |
| LDAP suffix * | ou=dynamiclists,o=test,c=de |  |
| List attributes | #cn;#memberURL |  |
| Custom label | Dynamic Lists |  |
| Additional LDAP filter | |  |
| Read-only | <input type="checkbox"/> |  |
| Hidden | <input type="checkbox"/> |  |
| No new entries | <input type="checkbox"/> |  |
| Disallow delete | <input type="checkbox"/> |  |

On tab "Modules" please add the dynamic lists module.

Dynamic Lists

Selected modules

Dynamic List (dynamicList)(*)

Available modules

AD LDS (windowsLDSGroup)(*)

Auto delete (autoDelete)

Custom fields (customFields)

Custom scripts (customScripts)

Custom type (customBaseType)(*)

On tab "Module settings" you can now configure your dynamic lists. Here you setup the used object class, RDN attribute, query attribute and list attribute (the one that is populated via query).

In case you have different types of dynamic lists you can simply redo the steps above to create more group types.

Dynamic List

Dynamic Lists

Object class *

groupOfURLs

RDN identifier *

cn

Query attribute *

memberURL

List attribute *

member

Usage

When you login to LAM you will see your new dynamic lists tab.

Dynamic Lists

New group

File upload

Delete selected groups

Group count: 1

| Actions | Group name | Entries |
|---------------------------------|------------|--|
| Sort sequence | | |
| <input type="checkbox"/> Filter | demo | |
| <input type="checkbox"/> | demo | ldap:///ou=demo,ou=People,o=test,c=de??one?(objectClass=inetOrgPerson) |

For each list you can manage the name and query string. LAM also displays which entries are auto-populated to the list.

demo > dynamiclists

Suffixdynamiclists

RDN identifiercn ?

Dynamic List

Name *

demo

Query *

ldap:///ou=demo,ou=People,o=test,c=de??one?(objectClass=inetOrg

Entries

cbach > demo > People
Ernst Bäcker > demo > People
fhuber > demo > People
hmeier > demo > People
hschuster > demo > People
k Montag > demo > People
mfischer > demo > People
r Montag > demo > People
shuber > demo > People
smiller > demo > People
thausen > demo > People
x Montag > demo > People

PyKota

There are two LAM group modules depending if your group entries should be built on object class "pykotaObject" or a different structural object class (e.g. "posixGroup"). For "pykotaObject" please select "PyKota (pykotaObjectStructural(*))" and "PyKota (pykotaGroup)" in all other cases.

Groups

Selected modules

Available modules

Unix (posixGroup)*

PyKota (pykotaGroup)

AD LDS (windowsLDSGroup)*

Auto delete (autoDelete)

Custom fields (customFields)

Custom scripts (customScripts)

Custom type (customBaseType)*

Now you can add the PyKota extension to your groups.

demo

Suffixgroups2 > pykota > test > de

RDN identifiercn ?

Unix

PyKota

Pykota group name

demo

Limit type

Quota

Remove PyKota extension

Hosts

You can specify a list of valid host names where the group's members may login. If you add the value "*" then the users may login to any host. This can be further restricted by adding explicit deny entries which are prefixed with "!" (e.g. "!hr_server").

Please note that your PAM settings need to support host restrictions. This feature is enabled by setting **pam_check_host_attr yes** in your **/etc/pam_ldap.conf**. When it is enabled then the account facility of pam_ldap

115

will perform the checks and return an error when no proper host attribute is present. Please note that users without host attribute cannot login to such a configured server.

The screenshot shows the 'demo2' configuration page. At the top, there's a 'Suffix' dropdown set to 'group > test > de' and an 'RDN identifier' dropdown set to 'cn'. Below this, there's a sidebar with icons for 'Unix', 'Samba 3', and 'Hosts'. The main area has a 'Host' field with a '+' icon and a list of hosts: 'server01' and 'server02', each with a red 'x' icon. A 'Remove host extension' button is at the bottom.

Password policy (LAM Pro)

See password policy for users.

Hosts

Account

Please see the description here.

Device (LAM Pro)

The device object class allows to manage general information about all sorts of devices (e.g. computers, network hardware, ...). You can enter the serial number, location and a describing text. It is also possible to specify the owner of the device.

The screenshot shows the 'server1' configuration page. At the top, there's a 'Suffix' dropdown set to 'kopano > test > de' and an 'RDN identifier' dropdown set to 'cn'. Below this, there's a sidebar with icons for 'Device', 'IP address', and 'Kopano'. The main area has fields for 'Name' (server1), 'Description' (Server 1), 'Serial number' (1234567890), 'Location' (Munich), and 'Owners' (Change button). The top right corner shows the ID '1234567890'.


Samba 3


You can manage Samba 3 host entries by adding the Unix and Samba 3 account modules.


The screenshot shows the 'pc01\$' configuration page. At the top, there's a 'Suffix' dropdown set to 'demo > machines > test > de' and an 'RDN identifier' dropdown set to 'uid'. Below this, there's a sidebar with icons for 'Account', 'Unix', and 'Samba 3'. The main area has fields for 'Host name' (pc01\$), 'Common name' (pc01), 'UID number' (25000), 'Gecos' (empty), 'Primary group' (admins), and 'Password' (Lock password / Remove password buttons). The top right corner shows the ID 'PC 01'.

pc01\$ PC 01

Suffix demo > machines > test > de RDN identifier uid

 Account

 Unix

 Samba 3

Display name PC 01

Domain MyCompany

Reset password

Windows (Samba 4)

LAM can manage your Windows servers and workstations. Please enable the account type "Hosts" in your LAM server profile and then add the host module "Windows (windowsHost)(*)".

■ Hosts

Host accounts (e.g. Samba) ↑ ↓ ✕

LDAP suffix *

List attributes

Custom label

Additional LDAP filter

Read-only ☐

Hidden ☐

No new entries ☐

Disallow delete ☐

cn=users,dc=w2012,dc=test

#cn;#description;#location

☐

☐

☐


☐


The default list attributes are for Unix and not suitable for Windows (blank lines in account table). Please use "#cn;#description;#location" or select your own attributes to display in the account list.


■ Hosts


Selected modules


Available modules

 Windows (windowsHost)*

 Account (account)*

 Auto delete (autoDelete)


 Custom fields (customFields)

 Custom scripts (customScripts)

Now you will see you computer accounts inside LAM. You can set e.g. the server's description and location information.

demoserver Demo server

Suffix Users > w2012 > test RDN identifier cn

 Windows

Host name * demoserver

Description Demo server

Location Munich

Last password change ?

Logon count 0

Managed by Hans Müller > Users > w2012 > test

IP addresses (LAM Pro)

You can manage the IP addresses of host accounts with the ipHost module. It manages the following information:

- IP addresses (IPv4/IPv6)
- location of the host
- manager: the person who is responsible for the host

You can activate this extension by adding the module ipHost to the list of active host modules.

The screenshot shows the 'demoserver' interface. On the left, there's a sidebar with 'Device' and 'IP address' options. The main area is titled 'ips' and contains fields for 'IP address' (10.20.30.40), 'Location' (Data center 3), and 'Manager' (cbach > demo > People). There are also buttons for 'Remove IP address extension' and a 'Device' icon.

MAC addresses

Hosts can have an unlimited number of MAC addresses. To enable this feature just add the "MAC address" module to the host account type.

The screenshot shows the 'pc01\$' interface. On the left, there's a sidebar with 'Account', 'IP address', and 'MAC address' options. The main area is titled 'demo > machines' and contains a 'MAC address' field (00:01:02:DE:EF:18). There are also buttons for 'Remove IP address extension' and a 'Device' icon.

Puppet

LAM supports to manage your Puppet [<http://puppetlabs.com/>] configuration. You can edit all attributes like environment, classes, variables and parent node.

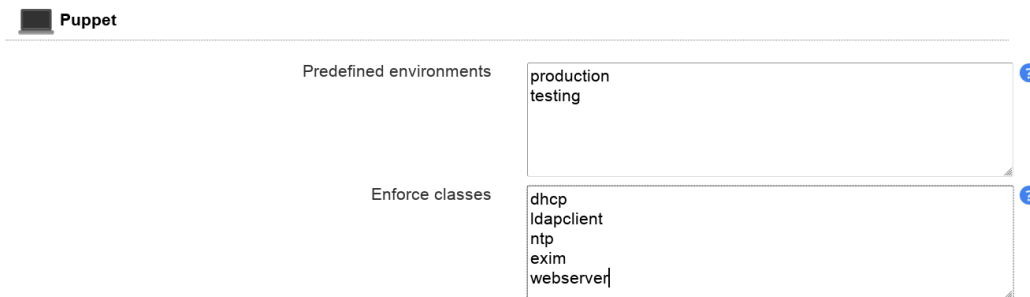
Configuration

To activate this feature please edit your LAM server profile and add the host module "Puppet (puppetClient)" on tab "Modules". This will add the Puppet tab to your host pages.

The screenshot shows the 'Hosts' configuration page. It has two columns: 'Selected modules' and 'Available modules'. The 'Selected modules' column contains 'Device (device)*' and 'Puppet (puppetClient)'. The 'Available modules' column contains 'Account (account)*', 'Auto delete (autoDelete)', 'Custom fields (customFields)', 'Custom scripts (customScripts)', and 'Custom type (customBaseType)*'. Each module has a plus or minus icon to toggle its selection.

On tab "Module settings" in your LAM server profile you may also setup some common environment names. LAM will use them to provide autocompletion hints when editing the environment for a node.

If you enter any value in "Enforce classes" then LAM will only accept this list of classes.



Puppet

Predefined environments

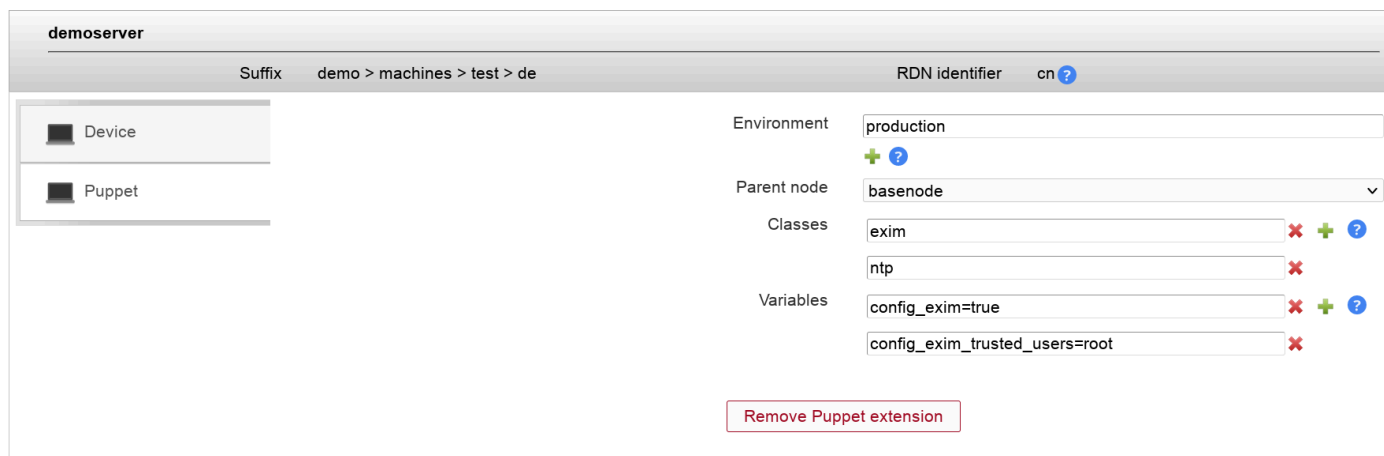
production
testing

Enforce classes

dhcp
ldapclient
ntp
exim
webserver

Editing nodes

When you edit a host entry then you will see the tab "Puppet". Here you can add/remove the Puppet extension and edit all attributes.



demoserver

Suffix demo > machines > test > de RDN identifier cn

Device

Puppet

Environment production

Parent node basenode

Classes

exim

ntp

Variables

config_exim=true

config_exim_trusted_users=root

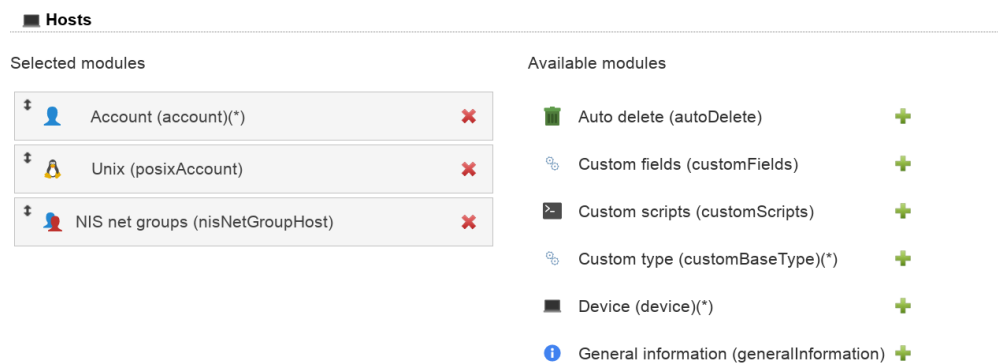
Remove Puppet extension

NIS net groups

NIS netgroups can be used to e.g. restrict SSH access to your machines.

Configuration

Please add the module "NIS net groups (nisNetGroupHost)" to the list of active host modules.



Hosts

Selected modules

Account (account)(*)

Unix (posixAccount)

NIS net groups (nisNetGroupHost)

Available modules

Auto delete (autoDelete)

Custom fields (customFields)

Custom scripts (customScripts)

Custom type (customBaseType)(*)

Device (device)(*)

General information (generalInformation)

Host editing

You will now see a new tab when editing hosts. Here you can assign memberships in NIS net groups and also set user/domain.

pc01\$ Sample host

Suffix: demo > machines > test > de RDN identifier: uid

| | Group | User name | Domain name |
|----------------|------------------------------|-----------|-------------|
| Account | group01 | user | |
| Unix | | | |
| NIS net groups | Filter: <input type="text"/> | | |
| | group02 | | |

Password policy (LAM Pro)

See password policy for users.

Samba 3 domains

Samba 3 stores information about its domain settings inside LDAP. This includes the domain name, its SID and some policies. You can manage all these attributes with LAM.

Please activate the account type "Samba domains" in your LAM server profile. Please notice that Samba by default uses the LDAP root for domain objects (e.g. dc=example,dc=com).

| | | |
|---------------|------------------------|---|
| Printers | PyKota printers | + |
| Samba domains | Samba 3 domain entries | + |
| Sudo roles | Sudo role management | + |


This will add a new tab to LAM where you can manage domain information.

The domain name, SID and RID base can only be specified for new domains and are not changeable via LAM at a later time. You may setup several password policies for your Samba domains and also some RID options that influence the creation of SIDs for users/groups/hosts.

MyCompany

S-1-2-33-1234-1234-1234

Suffixdemo > domains ▼RDN identifiersambaDomainName ?

 Samba domain

Domain nameMyCompany ?
Domain SIDS-1-2-33-1234-1234-1234 ?

Password policy

Minimal password length0 ▼

Password history length2 ▼

Logon for password changeOff ▼

Disconnect users outside logon hoursOn ▼

Allow machine password changes- ▼

Lockout users after bad logon attempts

Minimum password age

Maximum password age1209600

Lockout duration

Reset time after lockout

RID settings

Next RID

Next user RID

Next group RID

RID base1000 ?

Group of (unique) names and group of members (LAM Pro)

These classes can be used to represent group relations. Since they allow DN's as members you can also use them to represent nested groups.

Configuration:

Activate the account type "Group of names" in your LAM server profile to use these account modules. Alternatively, you can use the account type "Groups".

Groups of names

Group of names accounts

+

Groups of names

Group of names accounts

↑ ×

LDAP suffix *

?

List attributes#cn;#owner;#member;#uniqueMember?

Custom label?

Additional LDAP filter?

Read-only☐?

Hidden☐?

No new entries☐?



Disallow delete☐?

Then add the module "Group of names (groupOfNames)", "Group of unique names (groupOfUniqueNames)" or "Group of members (groupOfMembers)".



Managing entries in your LDAP directory



Groups of names



Selected modules



 Group of names (groupOfNames)(*) 



Available modules



 Auto delete (autoDelete) 

 Custom fields (customFields) 

 Custom scripts (customScripts) 



 General information (generalInformation) 

 Group of members (groupOfMembers)(*) 


 Group of unique names (groupOfUniqueNames)(*) 



Groups of names


Selected modules



 Group of members (groupOfMembers)(*) 



Available modules



 Auto delete (autoDelete) 


 Custom fields (customFields) 



 Custom scripts (customScripts) 

 General information (generalInformation) 

 Group of names (groupOfNames)(*) 



 Group of unique names (groupOfUniqueNames)(*) 


 Kopano (kopanoGroup) 


 Data (groupOfUniqueNames)(*) 

Virtual list attributes:


Groups of names

Group of names accounts  


LDAP suffix 

ou=gou,o=test,c=de 


List attributes


#cn,#owner,#member,#uniqueMember 


Custom label





Additional LDAP filter





Read-only 


☐ 


Hidden 

☐ 

No new entries 

☐ 

Disallow delete 


☐ 

The following virtual attributes can be shown in the group list. These are no real LDAP attributes but extra data that can be shown by LAM.

- member_count: number of entries in attribute "member"
- uniqueMember_count: number of entries in attribute "uniquemember"
- owner_count: number of entries in attribute "owner"
- roleOccupant_count: number of entries in attribute "roleOccupant"

Module settings:

On the module settings tab you set some options like the display format for members/owners and if fields like description should not be displayed.



Group of names

Members are optional ☐ ?

Display format ?

Hidden options ?

Owners ☐

Description ☐

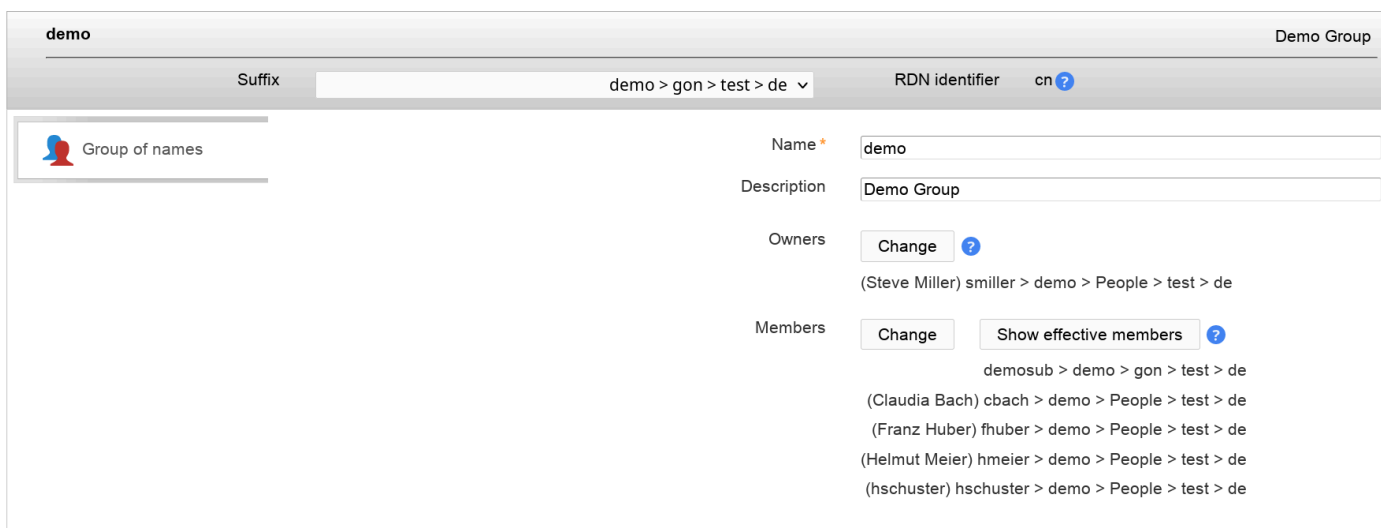
Group management:

Group of (unique) names have four basic attributes:

- Name: a unique name for the group
- Description: optional description
- Owner: the account which owns this group (optional)
- Members: the members of the group (at least one is required)

You can add any accounts as members. This includes other groups which leads to nested groups.

To show members of nested groups click on "Show effective members". Please note that for large groups this will run lots of queries against your LDAP server.



demo Demo Group

Suffix demo > gon > test > de RDN identifier cn ?

Group of names

Name * demo

Description Demo Group

Owners Change ?
(Steve Miller) smiller > demo > People > test > de

Members Change Show effective members ?
demosub > demo > gon > test > de
(Claudia Bach) cbach > demo > People > test > de
(Franz Huber) fhuber > demo > People > test > de
(Helmut Meier) hmeier > demo > People > test > de
(hschuster) hschuster > demo > People > test > de

Organizational roles (LAM Pro)

This module manages roles via the organizationalRole object class. There is also a user module to manage memberships on the user edit page.

Configuration:

Activate the account type "Groups" in your LAM server profile to use this account module. Alternatively, you can use the account type "Group of names".




Groups

Group accounts (e.g. Unix and Samba)



Managing entries in your LDAP directory

 **Roles**

Group accounts (e.g. Unix and Samba) ↑ ↓ ✕

LDAP suffix * ?

List attributes ?

Custom label ?

Additional LDAP filter ?


Read-only ☐ ?

Hidden ☐ ?


No new entries ☐ ?

Disallow delete ☐ ?






Then add the module "Role (organizationalRole)".

 **Roles**


Selected modules

 Role (organizationalRole)* ✕

Available modules

-  AD LDS (windowsLDSGroup)* +
-  Auto delete (autoDelete) +
-  Custom fields (customFields) +
-  Custom scripts (customScripts) +
-  Custom type (customBaseType)* +

On the module settings tab you set some options like the display format for members and if description should not be displayed.

 **Role**

Display format ?

Hidden options ?

Description ☐


Role management:

You can add any accounts as members. This includes other roles which leads to nested roles (needs to be supported by LDAP client applications).

To show members of nested roles click on "Show effective members". Please note that for large roles this will run lots of queries against your LDAP server.

demo Demo Role

Suffix RDN identifier ?

 **Role**

Name *

Description

Members Change Show effective members ?

- cbach
- fhuber
- hmeier
- role1
- role2

Simple Security Object (LAM Pro)

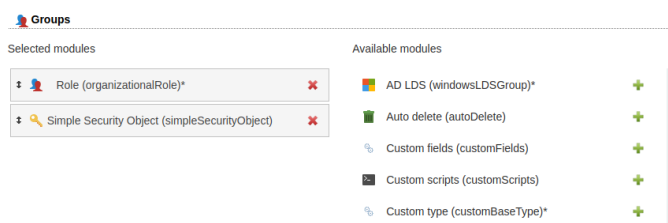
This allows to add passwords to LDAP entries which do not support passwords by other object classes. E.g. passwords can be added to organizational roles.

The simple security object module can be added to the following account types: users, groups, group of names and hosts

Attention: simple security objects require a password to be set. If you choose LDAP_EXOP as password hash then no new LDAP entries can be created. The reason is that EXOP requires to set the password on an already existing account (but simpleSecurityObject requires to set it in first place). So no password is set at the initial account creation which will then fail.

Configuration:

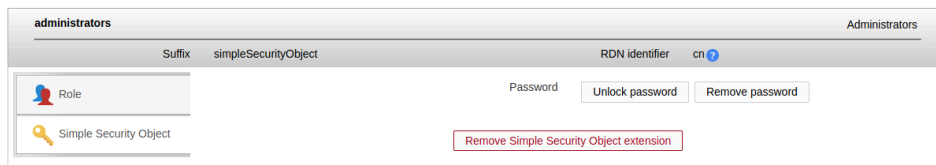
Add the Simple Security Object module to your account type.



Next configure the password hash type to use (module settings tab).



Now you can add a password to your entries by adding the extension to an entry.



Asterisk

LAM includes large support for Asterisk. You can add Asterisk extensions (including voicemail) to your users and also manage Asterisk extensions.

The Asterisk support for users can be added by selecting the Asterisk and Asterisk voicemail modules for users in your LAM server profile. This will add the following tabs to your user accounts.

Managing entries in your LDAP directory

Claudia Bach claudia.bach@ldap-account-manager.org Telephone number 0123-4567-8900 Mobile number 0123-4567-8922

Suffix: demo > People > test > de RDN identifier: uid

Personal
Unix
Asterisk voicemail
Asterisk

Caller ID * demo
Host * dynamic
Account context * default
Account type * friend
User agent
AMA flags -
Call groups
DTFM flags -

The Asterisk module allows to edit a large amount of attributes. Therefore, you can hide unused fields. Please edit your server profile (Module settings) to do so.

Asterisk

Asterisk realm: demo

Hidden options ?

| | | | | | |
|----------------------|--------------------------|---------------------------|--------------------------|------------------------|--------------------------|
| User agent | <input type="checkbox"/> | AMA flags | <input type="checkbox"/> | Call groups | <input type="checkbox"/> |
| DTFM flags | <input type="checkbox"/> | From user | <input type="checkbox"/> | From domain | <input type="checkbox"/> |
| Full contact | <input type="checkbox"/> | Insecure | <input type="checkbox"/> | Mailbox | <input type="checkbox"/> |
| NAT | <input type="checkbox"/> | Deny | <input type="checkbox"/> | Permit | <input type="checkbox"/> |
| Pickup group | <input type="checkbox"/> | Port | <input type="checkbox"/> | Qualify | <input type="checkbox"/> |
| Restrict caller ID | <input type="checkbox"/> | RTP timeout | <input type="checkbox"/> | RTP hold timeout | <input type="checkbox"/> |
| Disallowed codec | <input type="checkbox"/> | Allowed codec | <input type="checkbox"/> | Music on hold | <input type="checkbox"/> |
| Expiration timestamp | <input type="checkbox"/> | Registration context | <input type="checkbox"/> | Registration extension | <input type="checkbox"/> |
| Can call forward | <input type="checkbox"/> | IP address | <input type="checkbox"/> | Default user | <input type="checkbox"/> |
| Registration server | <input type="checkbox"/> | Last qualify milliseconds | <input type="checkbox"/> | | |

Of course, the voicemail part of Asterisk is also supported.

Claudia Bach claudia.bach@ldap-account-manager.org Telephone number 0123-4567-8900 Mobile number 0123-4567-8922

Suffix: demo > People > test > de RDN identifier: uid

Personal
Unix
Asterisk voicemail
Asterisk

Mailbox * demo
Account context * context
Full name
Email address
Pager
Options
Voicemail context

Remove Asterisk voicemail extension

If you also want to manage Asterisk extensions then simply add the account type "Asterisk extensions" and its module to your server profile.

LAM groups your Asterisk extension entries by extension name and account context. If you edit an extension then you will see the Asterisk entries as rules. LAM manages that all rule entries have the same owners and assigns the priorities.

The screenshot shows the LAM Pro interface for editing an Asterisk extension. The top bar has a 'demo' tab. Below it, a 'Suffix' dropdown is set to 'asteriskExt > test > de' and an 'RDN identifier' is set to 'cn'. On the left, a sidebar shows 'Asterisk extension' with an asterisk icon. The main area is titled 'Rules' and contains two rule entries. Each rule has an 'Application' field (app1 and app2) and an 'Application data' field (data1 and data2). Below each rule is a 'Delete rule' button and a directional arrow (down for app1, up for app2).

Kopano (LAM Pro)

Kopano is an OpenSource collaboration software. LAM Pro provides support to manage Kopano user entries, groups, address lists and servers. It covers all settings for these types including resource and quota settings.

Users

Configuration

To enable Kopano support for users please activate the Kopano module for the user account type in you server profile:


Users User accounts (e.g. Unix, Samba and Kolab) +

Adjust the suffix and list attributes to your needs.




The screenshot shows the configuration page for 'Users'. The left sidebar has a 'Users' tab with a user icon. The main area is titled 'User accounts (e.g. Unix, Samba and Kolab)' and has a dropdown arrow and a red 'X' icon. Below this, there are several configuration fields: 'LDAP suffix' (ou=kopano,o=test,c=de), 'List attributes' (#uid;#givenName;#sn;#mail), 'Custom label' (empty), and 'Additional LDAP filter' (empty). Each of these fields has a blue question mark icon to its right. Below these fields are four checkboxes: 'Read-only', 'Hidden', 'No new entries', and 'Disallow delete'. Each checkbox has a blue question mark icon to its right.




Then select the Kopano user module (tab Modules). You can combine it with Personal module, Unix or Windows.

Managing entries in your LDAP directory



 **Users**



Selected modules



  Personal (inetOrgPerson)(*) 



  Kopano (kopanoUser) 



Available modules

 Account (account)(*) 

 Account locking (locking389ds) 

 AD LDS (windowsLDSUser)(*) 

 Asterisk (asteriskAccount) 

 Asterisk voicemail (asteriskVoicemail) 

Next configure the module to your needs (tab Module settings).

Attention: LAM Pro uses the Kopano OpenLDAP schema by default. This schema fits for OpenLDAP, OpenDJ, Apache Directory server and other common LDAP servers. If you run Samba 4 or Active Directory then you need to switch the schema to "Active Directory" on the module settings tab.

You can hide options that you do not need. E.g. if you do not want to manage quotas per user then you can hide these options.

Examples for your Kopano ldap.cfg:

"Send as" attribute: dn


ldap_user_sendas_attribute_type = dn


"Send as" attribute: uid

ldap_user_sendas_attribute_type = text


ldap_user_sendas_relation_attribute = uid


Attention: If the Active Directory schema is used then LAM will always use dn and ignore this setting.


 **Kopano**

Kopano schema LDAP 

Users

"Send as" attribute dn 

Display format (cn) dn 

Hidden options 

Quota override ☐

Quota hard limit ☐

Type ☐

Admin ☐

Features ☐

Quota warning limit ☐

"Send as" privileges ☐

Capacity ☐

Archive servers ☐

Quota soft limit ☐

Shared store only ☐

Active ☐

User server ☐

Email aliases ☐

Usage

LAM Pro will now display the Kopano tab on your users. This includes email settings, quotas and some options (e.g. hide from address book). You can also set the resource type and capacity for meeting rooms and equipment. The Kopano extension can be added and removed at any time for every user.

Managing entries in your LDAP directory

Claudia Bach

cbach@ldap-account-manager.org

Suffixkopano > test > deRDN identifiercn

Personal

Kopano

Email aliases

"Send as" privileges

Change

Quota

Quota override

Quota warning limit

Quota soft limit

Quota hard limit

Resource settings

Type

Capacity

Archiving

Archive servers

Change

Options

Hidden

Shared store only

Active

Admin

User server

Features

IMAP

POP3

Remove Kopano extension

Contacts

Configuration

The configuration is similar to users. Instead of the Kopano user module please select the contact module.

Users

User accounts (e.g. Unix, Samba and Kolab)

Contacts

User accounts (e.g. Unix, Samba and Kolab)

LDAP suffix

List attributes

Custom label

Additional LDAP filter

Read-only

Hidden

No new entries

Disallow delete

ou=kopano2,o=test,c=de

#uid,#givenName,#sn,#mail

Contacts

☐

☐

☐

☐

?

?

?

?

?

?

?

?

Managing entries in your LDAP directory

Contacts

Selected modules

Personal (inetOrgPerson)(*)

Kopano contact (kopanoContact)

Available modules

Account (account)(*)

Account locking (locking389ds)

AD LDS (windowsLDSUser)(*)

Asterisk (asteriskAccount)

Asterisk voicemail (asteriskVoicemail)

Usage

LAM Pro will now display the Kopano contact tab on your users. The Kopano extension can be added and removed at any time for every user.

Franz Meier

fmeier@ldap-account-manager.org

Suffix

kopano2 > test > de

RDN identifier

cn

Personal

Kopano contact

UID number *

1001

Email aliases

"Send as" privileges

Change

Options

Hidden

Active

Remove Kopano extension

Groups

Configuration

To enable Kopano support for groups please activate the Kopano module for the group account type in you server profile:

Groups

Group accounts (e.g. Unix and Samba)

LDAP suffix *

List attributes

Custom label

Additional LDAP filter

Read-only

Hidden

No new entries

Disallow delete

ou=kopano,o=test,c=de

#cn,#description,#member

☐

☐

☐

☐

?

?

?

?

?

?

?

?

Then select the Kopano group module (tab Modules). You can combine it with groups of names module, Unix or Windows.

Managing entries in your LDAP directory

Groups

Selected modules

Group of names (groupOfNames)(*)

Kopano (kopanoGroup)

Available modules

AD LDS (windowsLDSGroup)(*)

Auto delete (autoDelete)

Custom fields (customFields)

Custom scripts (customScripts)

Next configure the module to your needs (tab Module settings).

Kopano

Groups

Display format

dn

Hidden options

?

"Send as" privileges

☐

Usage

LAM Pro will now display the Kopano tab on your groups. The Kopano extension can be added and removed at any time for every group.

project1

Project 1

Suffix

kopano > test > de

RDN identifier

cn

Group of names

Kopano

Email

Email

project1@ldap-account-manager.org

Email aliases

"Send as" privileges

Change

Options

Security group

☐

Hidden

☐

Active

☒

Remove Kopano extension

Address lists

Configuration

To enable Kopano support for address lists please activate the Kopano address list account type in you server profile (tab account types):

Kopano address lists

Kopano address lists

+

Adjust the suffix and list attributes to your needs.

Managing entries in your LDAP directory

Kopano address lists

Kopano address lists

↑ ↓ ✕

LDAP suffix *

ou=kopano,o=test,c=de

?

List attributes

#cn;#kopanoBase;#kopanoFilter

?

Custom label

?

Additional LDAP filter

?

Read-only

☐

?

Hidden

☐

?

No new entries

☐

?

Disallow delete

☐

?

Then select the Kopano address list module (tab Modules).

Kopano address lists

Selected modules

Available modules

✕ < Kopano address list (kopanoAddressList)(*) ✕

🗑️ Auto delete (autoDelete) +

🔗 Custom fields (customFields) +

📜 Custom scripts (customScripts) +

ℹ️ General information (generalInformation) +

Usage

LAM Pro will now display the Kopano address list tab.

Kopano address lists

New address list

File upload

Delete selected address lists

Address list count: 1

| Actions | List name | Base | Filter |
|-----------------------------------|-----------|--------------|---------------------------|
| Sort sequence | ▼ ▲ | ▼ ▲ | ▼ ▲ |
| <input type="checkbox"/> Filter ▾ | | | |
| <input type="checkbox"/> 🗑️ 📄 📄 📄 | all | o=test,c=dea | (objectclass=kopano-user) |

all

Suffix kopano > test > de

RDN identifier cn ?

Kopano address list

List name *

all

?

Base

o=test,c=dea

?

Filter

(objectclass=kopano-user)

?

Hidden

☐

?

Active

☒

?

Dynamic groups

Configuration

To enable Kopano support for dynamic groups please activate the Kopano dynamic group account type in your server profile (tab account types):

Kopano dynamic groups

Kopano dynamic groups

+

Adjust the suffix and list attributes to your needs.

132

Managing entries in your LDAP directory

Kopano dynamic groups

LDAP suffix *

List attributes

Custom label

Additional LDAP filter

Read-only

Hidden

No new entries

Disallow delete

Kopano dynamic groups

ou=kopano,o=test,c=de

#cn;#mail;#kopanoaliases;#kopanoBase;#kopanoFilter

☐

☐

☐

☐

Then select the Kopano dynamic group module (tab Modules).

Kopano dynamic groups

Selected modules

Available modules

Kopano dynamic group (kopanoDynamicGroup)(*)

Auto delete (autoDelete)

Custom fields (customFields)

Custom scripts (customScripts)

General information (generalInformation)

Usage

LAM Pro will now display the Kopano address list tab.

Kopano dynamic groups

New group

File upload

Delete selected groups

Group count: 5

| Actions | Group name | Email | Email aliases | Base | Filter |
|---------------------------------|------------|---------------------------------|---------------|-----------------------|----------|
| Sort sequence | | | | | |
| <input type="checkbox"/> Filter | | | | | |
| <input type="checkbox"/> | munich | munich@ldap-account-manager.org | | ou=kopano,o=test,c=de | l=Munich |

munich

munich@ldap-account-manager.org

Suffix

kopano > test > de

RDN identifier

cn

Kopano dynamic group

Group name *

Base

Filter

Email

Email

Email aliases

Options

Hidden

Active

Servers

Configuration

133

Managing entries in your LDAP directory

To enable Kopano support for servers please activate the Kopano server module for the hosts account type in you server profile (tab account types):

■ Hosts Host accounts (e.g. Samba) +

Adjust the suffix and list attributes to your needs.

■ Hosts Host accounts (e.g. Samba) ↑ ×

| | | |
|------------------------|---|---|
| LDAP suffix * | <input type="text" value="ou=kopano,o=test,c=de"/> | ? |
| List attributes | <input type="text" value="#cn,#description,#serialNumber"/> | ? |
| Custom label | <input type="text"/> | ? |
| Additional LDAP filter | <input type="text"/> | ? |
| Read-only | <input type="checkbox"/> | ? |
| Hidden | <input type="checkbox"/> | ? |
| No new entries | <input type="checkbox"/> | ? |
| Disallow delete | <input type="checkbox"/> | ? |

Then select the Kopano server module (tab Modules).

■ Hosts

| Selected modules | Available modules |
|------------------------------------|--|
| <div>Device (device)(*) ×</div> | <div>Account (account)(*) +</div> |
| <div>IP address (ipHost) ×</div> | <div>Auto delete (autoDelete) +</div> |
| <div>Kopano (kopanoServer) ×</div> | <div>Custom fields (customFields) +</div> |
| | <div>Custom scripts (customScripts) +</div> |
| | <div>Custom type (customBaseType)(*) +</div> |

Next configure the module to your needs (tab Module settings).



Servers

Hidden options ?
Proxy URL ☐

Usage

LAM Pro will now display the Kopano tab on your hosts. The Kopano extension can be added and removed at any time for every server.

server1 1234567890






Suffix kopano > test > de RDN identifier cn ?


| | |
|------------|---|
| Device | HTTP port <input type="text" value="80"/> |
| IP address | SSL port <input type="text" value="443"/> |
| Kopano | Proxy URL <input type="text"/> |
| | File path <input type="text"/> |
| | Public store <input type="checkbox"/> ? |

Remove Kopano extension

Kolab shared folders

Please add the account type "Kolab shared folders" in your LAM server profile and set the correct LDAP suffix.

| | | | |
|---|-----------------------|--|---|
|  | Groups of names | Group of names accounts | + |
|  | Hosts | Host accounts (e.g. Samba) | + |
|  | Kolab shared folders | Kolab shared folders (e.g. mail folders) | + |
|  | Kopano address lists | Kopano address lists | + |
|  | Kopano dynamic groups | Kopano dynamic groups | + |

 Kolab shared folders

Kolab shared folders (e.g. mail folders)

↑ ✖

LDAP suffix *

ou=Shared Folders,dc=ldap-account-manager,dc=org

?

List attributes

#cn,#kolabDelegate,#alias

?

Custom label

?

Additional LDAP filter

?

Read-only

☐

?

Hidden

☐

?

No new entries

☐


?

Disallow delete

☐


?

Then add the "Kolab shared folder" module on tab "Modules".

 Kolab shared folders


Selected modules

✚


 Kolab shared folder (kolabSharedFolder)(*)

✖


Available modules

 Auto delete (autoDelete)


+

 Custom fields (customFields)

+

 Custom scripts (customScripts)

+

 General information (generalInformation)

+

Now you can start to add shared folders inside LAM.


demo

Suffix

Shared Folders > ldap-account-manager > org

RDN identifier

cn?

 Kolab shared folder

Name *

demo

?

Email address *

demo@ldap-account-manager.org

?

Target IMAP folder *

shared/demo@ldap-account-manager.org

?

Type

Shared mail folder

?

Allowed recipients

+

?

Allowed senders

+

?

Email aliases

+

?

Delegates

cn=Claudia Bach,ou=People,dc=ldap-account-manager,dc=org

▼

+

?

DHCP

You can manage your DHCP server with LAM. It supports to manage subnets, fixed IP entries, IP ranges and DDNS.

Configuration

The DHCP management can be activated by adding the account type DHCP to your server profile. Please also add the DHCP modules.

LAM requires that you use an LDAP entry with the object class "dhcpService" or "dhcpServer" as suffix for this account type. If the "dhcpServer" entry points to a "dhcpService" entry via "dhcpServiceDN" then you need to use the DN of the "dhcpService" entry as LDAP suffix for DHCP.

Add account type:

| Available account types | | |
|-------------------------|-----------------------------|---|
| Aliases | Alias entries | + |
| Asterisk extensions | Asterisk extensions entries | + |
| Automount entries | Automount entries | + |
| Billing codes | PyKota billing codes | + |
| Bind DNS | Bind DNS entries | + |
| Custom type | Custom entries | + |
| DHCP | DHCP administration | + |

Set suffix:

DHCP

DHCP administration ↑ ↓ ✕

LDAP suffix *

List attributes

Custom label

Additional LDAP filter

Read-only ☐

Hidden ☐

No new entries ☐

Disallow delete ☐

Add modules:

DHCP

| Selected modules | Available modules |
|--------------------------------------|---|
| ↑ DHCP settings (dhcp_settings)(*) ✕ | 🗑️ Auto delete (autoDelete) + |
| ↑ Ranges (range) ✕ | 🔗 Custom fields (customFields) + |
| ↑ DDNS (ddns) ✕ | 📜 Custom scripts (customScripts) + |
| ↑ Hosts (fixed_ip) ✕ | ℹ️ General information (generalInformation) + |

Example server entry:

```
dn: cn=server,ou=dhcp,dc=ldap-account-manager,dc=org
objectclass: dhcpServer
objectclass: dhcpOptions
objectclass: top
cn: server
dhcpcomments: My DHCP server
dhcption: domain-name "ldap-account-manager.org"
dhcption: domain-name-servers 192.168.1.1
dhcption: routers 192.168.1.1
dhcption: netbios-name-servers 192.168.1.1
dhcption: subnet-mask 255.255.255.0
dhcption: netbios-node-type 8
dhcpstatements: default-lease-time 3600
dhcpstatements: max-lease-time 7200
dhcpstatements: include "mykey"
dhcpstatements: ddns-update-style interim
dhcpstatements: update-static-leases true
dhcpstatements: ignore client-updates
```

Example settings for dhcpd.conf:

```
ddns-update-style none;
deny unknown-clients;
ldap-server "server";
ldap-dhcp-server-cn "server";
ldap-port 389;
ldap-username "uid=dhcp,ou=people,dc=ldap-account-manager,dc=org";
ldap-password "{SSHA}XXXXXXXXXXXXX";
ldap-base-dn "ou=dhcp,dc=ldap-account-manager,dc=org";
ldap-method dynamic;
ldap-debug-file "/var/log/dhcp-ldap-startup.log";
```

slapd.conf changes:

```
include /etc/ldap/schema/dhcp.schema
```

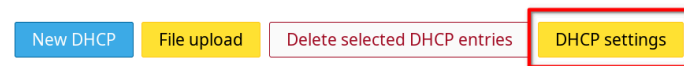
```
index dhcpHWAddress eq
```

```
index dhcpClassData eq
```

Run slapindex to rebuild the index.

You can manage the settings of your DHCP service/server entry:

DHCP



DHCP count: 22

You can easily create new subnet entries.

| Suffix | server | RDN identifier | cn ? |
|-------------------------|--------|----------------------|---------------|
| 192.168.1.0 Demo subnet | | | |
| DHCP settings | | Subnet * | 192.168.1.0 |
| Ranges | | Domain name | demo |
| DDNS | | Lease time | |
| Hosts | | Maximum lease time | |
| | | DNS | 192.168.1.1 |
| | | Search domains | |
| | | Default gateway | 192.168.1.1 |
| | | Netbios name servers | 192.168.1.1 |
| | | Netbios node type | H-Node (0x08) |
| | | Unknown clients | |
| | | Subnet mask * | 255.255.255.0 |
| | | Description | Demo subnet |
| | | Net mask | 24 |

It is also possible to specify a list of fixed IPs.

| IP address | PC name | MAC address | Description | Active |
|--------------|---------|-------------------|-------------|-------------------------------------|
| 192.168.1.11 | pc02 | 11:22:33:44:55:ab | | <input checked="" type="checkbox"/> |
| 192.168.1.12 | pc03 | 11:22:33:44:55:a2 | | <input checked="" type="checkbox"/> |
| 192.168.1.13 | pc04 | 11:22:33:44:55:a1 | | <input checked="" type="checkbox"/> |
| | | | | <input checked="" type="checkbox"/> |

Add existing host

IP ranges may be specified.

If you use failover pools for your IP ranges please use the pool options on the bottom. Here you can add DHCP pools (object class "dhcpPool") and specify the failover peer.

192.168.1.0

Demo subnet

SuffixserverRDN identifiercn?

DHCP settings

Ranges

DDNS

Hosts

Range from *192.168.1.1?

Range to *192.168.1.10?

Delete range?

Range from *192.168.1.20?

Range to *192.168.1.30?

Delete range?

Range from *192.168.1.40?

Range to *192.168.1.50?

Delete range?

New range?

Pools

Name *pool1?Delete pool

Failover peerpeer2?

Range from *192.168.1.80?

Range to *192.168.1.90?

Delete range?

New range?

New pool?

If you activated DDNS in the server entry then you may also specify the DDNS settings for this subnet.

192.168.1.0

Demo subnet

SuffixserverRDN identifiercn?

DHCP settings

Ranges

DDNS

Hosts

IP address of the DNS server192.168.1.1

Zone namezone

Reverse zone name1.168.192.in-addr.arpa

Bind dyndb-ldap (LAM Pro)

The bind-dyndb-ldap [<https://pagure.io/bind-dyndb-ldap>] plugin for Bind [<https://www.isc.org/bind/>] allows you to manage DNS entries in LDAP. Please install the bind-dyndb-ldap schema file on your LDAP server. It is part of the bind-dyndb-ldap download. LAM Pro can manage DNS zones and the following record types:

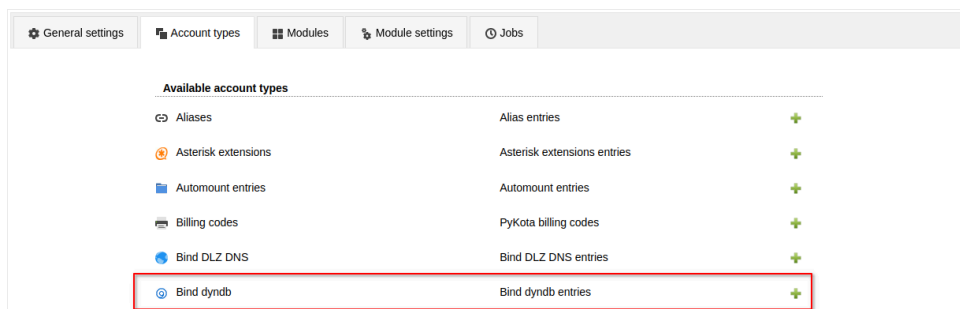
- A/AAAA: IP addresses
- CNAME: alias names

139

- DNAME: delegation name
- MX: mail servers
- NS: name servers
- PTR: reverse DNS entries
- SRV: service entries
- TXT: text records

Configuration

Please open your LAM server profile configuration and add two instances of the "Bind dyndb" account type. One for records and one for zones.



The recommended settings are as follows. Please adapt if needed.

DNS records:

- LDAP suffix: if you manage a single domain then use the DN of the zone entry. If you manage multiple domains then use the DN under which they are stored (e.g. the "nsContainer").
- List attributes: #idnsName;#aRecord;#aAAAREcord;#cNAMERecord;#dNameRecord;#tX-TRecord;#mxrecord;#srvrecord;#ptrrecord;#dnsttl
- Custom label: DNS records

DNS zones:

- LDAP suffix: use the DN under which the domains are stored (e.g. the "nsContainer").
- List attributes: #idnsName;#aRecord;#aAAAREcord;#cNAMERecord;#dNameRecord;#tX-TRecord;#idnssoaserial
- Custom label: DNS zones

Managing entries in your LDAP directory

Active account types

DNS records Bind dyndb entries ↓ ✕

LDAP suffix * ⓘ

List attributes ⓘ

Custom label ⓘ

Additional LDAP filter ⓘ

☐ Read-only ⓘ

☐ Hidden ⓘ

☐ No new entries ⓘ

☐ Disallow delete ⓘ

DNS zones Bind dyndb entries ↑ ✕

LDAP suffix * ⓘ

List attributes ⓘ

Custom label ⓘ

Additional LDAP filter ⓘ

☐ Read-only ⓘ

☐ Hidden ⓘ

☐ No new entries ⓘ

☐ Disallow delete ⓘ

Next, switch to the modules tab. Here, select DNS records for your record type and DNS zone for your zone type. Then you can save the server profile and login to LAM.

General settings Account types **Modules** Module settings Jobs

DNS records

Selected modules

Available modules

Auto delete (autoDelete) +

Custom fields (customFields) +

Custom scripts (customScripts) +

DNS records (bindDydbRecord)* +

DNS zone (bindDydbZone)* +

General information (generalInformation) +

DNS zones

Selected modules

Available modules

Auto delete (autoDelete) +

Custom fields (customFields) +

Custom scripts (customScripts) +

DNS records (bindDydbRecord)* +

DNS zone (bindDydbZone)* +

General information (generalInformation) +

DNS zones

This allows you to manage your DNS zones (SOA+NS records). You can e.g. specify timeouts and name servers.

Managing entries in your LDAP directory

demo.ldap-account-manager.org

Suffix dns > test > de v RDN identifier idnsname ?

DNS zone

Authoritative information ("SOA" record)

Name * ?

Expiration time * ?

Refresh time * ?

Minimum time * ?

Retry time * ?

Primary name server * ?

Admin email * ?

Serial number * ?

Default timeout ?

Active ☒ ?

Name servers ("NS" records)

Name server ✖ + ?

✖

Mail servers ("MX" records)

Mail server ? Preference ?

✖

✖

Add

IP addresses ("A/AAAA" records)

IP address + ?

IPv6 address + ?

Text ("TXT" records)

Text + ?

DNS entries

LAM supports the following DNS record types:

- A/AAAA: IP addresses
- CNAME: alias names
- DNAME: delegation name
- MX: mail servers
- PTR: reverse DNS entries
- SRV: service entries
- TXT: text records

IP addresses (A/AAAA)

Here you can enter IPv4 (A) or IPv6 (AAAA) addresses for a DNS name.

ns1.demo.ldap-account-manager.org

Suffix demo.ldap-account-manager.org > dns > test > de v RDN identifier idnsname ?

DNS records

Name * ?

Timeout ?

IP addresses ("A/AAAA" records)

IP address ✖ + ?

✖

IPv6 address ✖ + ?

✖

Alias names (CNAME)

Sometimes a DNS entry should simply point to a different DNS entry (e.g. for migrations). This can be done by adding an alias name.

The screenshot shows the configuration page for the domain `ns-master.demo.ldap-account-manager.org`. The breadcrumb trail is `Suffix demo.ldap-account-manager.org > dns > test > de v`. The RDN identifier is `idsname`. The left sidebar shows "DNS records" selected. The main form has the following fields:

- Name ***: `ns-master`
- Timeout**: (empty)
- Alias name ("CNAME" record)**: (empty)
- Target**: `ns1`

Alias names (DNAME)

You can delegate a DNS zone to a different server.

The screenshot shows the configuration page for the domain `sub.demo.ldap-account-manager.org`. The breadcrumb trail is `Suffix demo.ldap-account-manager.org > dns > test > de v`. The RDN identifier is `idsname`. The left sidebar shows "DNS records" selected. The main form has the following fields:

- Name ***: `sub`
- Timeout**: (empty)
- Text ("TXT" records)**: (empty)
- Text**: (empty)
- Alias name ("DNAME" record)**: (empty)
- Target**: `target.example.com.`

Mail servers (MX)

The mail server entries define where mails to a domain should be delivered. The server with the lowest preference has the highest priority.

The screenshot shows the configuration page for the domain `mail.demo.ldap-account-manager.org`. The breadcrumb trail is `Suffix demo.ldap-account-manager.org > dns > test > de v`. The RDN identifier is `idsname`. The left sidebar shows "DNS records" selected. The main form has the following sections and fields:

- Name ***: `mail`
- Timeout**: (empty)
- IP addresses ("A/AAAA" records)**:
 - IP address**: (empty)
 - IPv6 address**: (empty)
- Reverse DNS entries ("PTR" records)**:
 - PTR record**: (empty)
- Text ("TXT" records)**:
 - Text**: (empty)
- Mail servers ("MX" records)**:

| Mail server | Preference |
|---|-----------------|
| <code>mx1.ldap-account-manager.org</code> | <code>10</code> |
| <code>mx2.ldap-account-manager.org</code> | <code>20</code> |

Reverse DNS entries (PTR)

Reverse DNS entries are important when you need to find the DNS name that is associated with a given IP address. Reverse DNS entries are stored in a separate DNS zone.

Managing entries in your LDAP directory

The screenshot shows the 'DNS records' management interface for the domain '2.1.168.192.in-addr.arpa'. The interface includes a sidebar with a search icon and the text 'DNS records'. The main content area has a header with 'Suffix' (1.168.192.in-addr.arpa), 'dns', 'test', and 'de'. Below the header, there are sections for 'Reverse DNS entries ("PTR" records)' and 'Mail servers ("MX" records)'. The 'PTR record' section shows a record for 'test.idap-account-manager.org'. The 'MX records' section has an 'Add' button.

Services (SRV)

Service records can be used to specify which servers provide common services such as LDAP. Please note that the host name must be `_SERVICE._PROTOCOL` (e.g. `_ldap._tcp`).

Priority: The priority of the target host, lower value means more preferred.

Weight: A relative weight for records with the same priority. E.g. weights 20 and 80 for a service will result in 20% queries to the one server and 80% to the other.

Port: The port number that is used for your service.

Server: DNS name where service can be reached (relative without or absolute with dot at the end).

The screenshot shows the 'DNS records' management interface for the domain '_ldap._tcp.demo.idap-account-manager.org'. The interface includes a sidebar with a search icon and the text 'DNS records'. The main content area has a header with 'Suffix' (demo.idap-account-manager.org), 'dns', 'test', and 'de'. Below the header, there are sections for 'Text ("TXT" records)' and 'Services ("SRV" records)'. The 'SRV records' section shows two records for '_ldap1' and '_ldap2' with their respective priority, weight, and port. There are 'Delete' and 'Add' buttons.

Text records (TXT)

Text records can be added to store a description or other data (e.g. SPF information).

The screenshot shows the 'DNS records' management interface for the domain 'info.demo.idap-account-manager.org'. The interface includes a sidebar with a search icon and the text 'DNS records'. The main content area has a header with 'Suffix' (demo.idap-account-manager.org), 'dns', 'test', and 'de'. Below the header, there are sections for 'IP addresses ("A/AAAA" records)' and 'Text ("TXT" records)'. The 'IP addresses' section has fields for 'IP address' and 'IPv6 address'. The 'Text records' section shows two records for 'clientid=123456' and 'tenant=abc'. There are 'Delete' and 'Add' buttons.

Bind DLZ (LAM Pro)

Bind DLZ [<http://bind-dlz.sourceforge.net>] is an extension to the DNS server Bind [<http://www.isc.org/software/bind>] that allows to store DNS entries inside LDAP. Please install the Bind DLZ schema file on your LDAP server. It is part of the Bind download. You can also get it from Bind's git repository [<https://gitlab.isc.org/isc-projects/bind9/blob/master/contrib/dlz/modules/ldap/testing/dlz.schema>].

Configuration

First, you need to add the Bind DNS account type and the Bind DLZ module:

The screenshot shows the 'Available account types' section with a navigation bar at the top containing 'General settings', 'Account types', 'Modules', 'Module settings', and 'Jobs'. The 'Account types' tab is active. Below the tab, there is a table of available account types:

| Available account types | | |
|-------------------------|---------------------|-------------------------------|
| | Aliases | Alias entries + |
| | Asterisk extensions | Asterisk extensions entries + |
| | Automount entries | Automount entries + |
| | Billing codes | PyKota billing codes + |
| | Bind DNS | Bind DNS entries + |
| | Custom type | Custom entries + |

Please set the LDAP suffix either to an existing DNS zone (dlzZone) or an organizational unit that should include your DNS zones.

The screenshot shows the 'Active account types' section for 'Bind DNS'. The 'Bind DNS' tab is active. Below the tab, there is a form for configuring 'Bind DNS entries':

| | |
|------------------------|-----------------------------------|
| LDAP suffix * | ou=bind,o=test,c=de ? |
| List attributes | #dlzHostName;#zoneName;#records ? |
| Custom label | ? |
| Additional LDAP filter | ? |
| Read-only | <input type="checkbox"/> ? |
| Hidden | <input type="checkbox"/> ? |
| No new entries | <input type="checkbox"/> ? |
| Disallow delete | <input type="checkbox"/> ? |

For regular entry management use "DNS entry (bindDLZ)(*)" module.

The screenshot shows the 'Module settings' section for 'Bind DNS'. The 'Module settings' tab is active. Below the tab, there is a table of available modules:

| Selected modules | | Available modules | |
|------------------|------------------------|-------------------|--|
| | DNS entry (bindDLZ)(*) | | Auto delete (autoDelete) + |
| | | | Custom fields (customFields) + |
| | | | Custom scripts (customScripts) + |
| | | | General information (generalInformation) + |
| | | | XFR (bindDLZXfr)(*) |

XFR

If you want to edit XFR entries please add a second account type for XFR. Recommended list attributes are "#dlzipaddr;#dlzrecordid".

The screenshot shows the 'Bind XFR' configuration form. On the left, there are several checkboxes: 'Read-only', 'Hidden', 'No new entries', and 'Disallow delete', each with a question mark icon. The main form area is titled 'Bind DNS entries' and contains four text input fields: 'LDAP suffix' (value: 'ou=bind,o=test,c=de'), 'List attributes' (value: '#dlzipaddr;#dlzrecordid'), 'Custom label' (value: 'Bind XFR'), and 'Additional LDAP filter' (empty). Each input field has a question mark icon to its right. There are also up and down arrows and a red 'X' icon at the top right of the form area.

Now use the "XFR (bindDLZXfr)(*)" module for this account type.

The screenshot shows the 'Bind XFR' module selection interface. It is divided into two sections: 'Selected modules' and 'Available modules'. In the 'Selected modules' section, there is one module listed: 'XFR (bindDLZXfr)(*)' with a red 'X' icon to its right. In the 'Available modules' section, there are five modules listed, each with a green plus icon to its right: 'Auto delete (autoDelete)', 'Custom fields (customFields)', 'Custom scripts (customScripts)', 'DNS entry (bindDLZ)(*)', and 'General information (generalInformation)'.

Automatic PTR management

LAM can automatically create/delete PTR entries for the entered IPv4/6 records. You can enable this feature on the module settings tab.

PTR records will get the same TTL as IP records. Please note that you need to have matching reverse zones (".in-addr.arpa"/".ip6.arpa") under the same suffix as your other DNS entries.

The screenshot shows the 'DNS entry' module settings tab. At the top, there is a navigation bar with five tabs: 'General settings', 'Account types', 'Modules', 'Module settings', and 'Jobs'. The 'Module settings' tab is selected. Below the navigation bar, there is a section titled 'DNS entry' with a globe icon. At the bottom of this section, there is a checkbox labeled 'Automatic PTR changes' which is checked, and a question mark icon to its right.

Zone management













If you do not yet have a DNS zone then LAM can create one for you. In list view switch the suffix to an organizational unit DN. Now you will see a button "New zone".

This will create the zone container entry and a default DNS entry "@" for authoritative information. Now switch the suffix to your new zone and start adding DNS entries.

Bind DNS

New DNS entry File upload Delete selected DNS entries New zone

DNS entry count: 99

| Actions | Host name | Zone name | Records |
|--|----------------------|----------------------|----------------------|
| Sort sequence ▼ ▲ | ▼ ▲ | ▼ ▲ | ▼ ▲ |
| <input type="checkbox"/> Filter ▼ | <input type="text"/> | <input type="text"/> | <input type="text"/> |
| <input type="checkbox"/>     | 1.1 | 168.192.in-addr.arpa | IN PTR : |
| <input type="checkbox"/>     | 2.1 | 168.192.in-addr.arpa | IN PTR : |
| <input type="checkbox"/>     | 4.5 | 1.2.in-addr.arpa | IN PTR : |

DNS entries

LAM supports the following DNS record types:

- SOA: authoritative information
- NS: name servers
- A/AAAA: IP addresses
- PTR: reverse DNS entries
- CNAME: alias names
- MX: mail servers
- TXT: text records
- SRV: service entries

Authoritative (SOA) and name server (NS) records

Here you can manage general information about the zone like timeouts and name servers. Please note that name servers must be inserted in a special format (dot at the end).

Managing entries in your LDAP directory

@

Suffixexample.com > demo > bind > test > de

RDN identifierdlzHostName?

DNS entry

Host name@

IP addresses ("A/AAAA" records)

| IP address? | Timeout? | Description? | |
|-------------|----------|--------------|---|
| 1.1.1.1 | 2w | | ✖ |
| 2.2.2.2 | 2w | | ✖ |
| Add | | | |

Authoritative information ("SOA" record)

| | | | |
|-------------------|--------------------|-----------------------|-------------------|
| Expiration time * | 1w? | Refresh time * | 46m40s? |
| Minimum time * | 1d? | Retry time * | 2h? |
| Timeout * | 2w? | Primary name server * | ns1.example.com.? |
| Admin email * | root.example.com.? | Serial number * | 1↑? |
| Description | | | |
| Delete | | | |

Name servers ("NS" records)

| Name server? | Timeout? | Description? | |
|------------------|----------|--------------|---|
| ns1.example.com. | 2w | | ✖ |
| ns2.example.com. | 2w | | ✖ |
| Add | | | |

IP addresses (A/AAAA)

LAM will automatically set the correct type (A/AAAA) depending if you enter an IPv4 or IPv6 address.

www

Suffixexample.com > demo > bind > test > de

RDN identifierdlzHostName?

DNS entry

Host namewww

IP addresses ("A/AAAA" records)

| IP address? | Timeout? | Description? | |
|-----------------|----------|--------------|---|
| 123.123.123.123 | 2w | | ✖ |
| 1:2:3:4:5:6 | 2w | | ✖ |
| Add | | | |


Reverse DNS entries

Reverse DNS entries are important when you need to find the DNS name that is associated with a given IP address. Reverse DNS entries are stored in a separate DNS zone.

Managing entries in your LDAP directory

123.123

Suffix123.123.in-addr.arpa > demo > bind > test > de ▼RDN identifierdlzHostName ?

 DNS entryHost name123.123

Reverse DNS entries ("PTR" records)

Host name *www.demozone. ?Timeout *2w ?Description ? ?


Add

Alias names (CNAME)

Sometimes a DNS entry should simply point to a different DNS entry (e.g. for migrations). This can be done by adding an alias name.

www2

Suffixexample.com > demo > bind > test > de ▼RDN identifierdlzHostName ?

 DNS entryHost namewww2

Alias name ("CNAME" record)


Alias name *www ?Timeout *2w ?Description ? ?

Mail servers (MX)

The mail server entries define where mails to a domain should be delivered. The server with the lowest preference has the highest priority.

www

Suffixdemozone > demo > bind > test > de ▼RDN identifierdlzHostName ?

 DNS entryHost namewww

IP addresses ("A/AAAA" records)

IP address ?Timeout ?Description ?

123.123.123.1232m3s

1:2:3:4:5:62m3s

Add

Alias name ("DNAME" record)

Add

Mail servers ("MX" records)

Mail server ?Preference ?Timeout ?Description ?

123.123.123.123502w

Add

Text records (TXT)

Managing entries in your LDAP directory

Text records can be added to store a description or other data (e.g. SPF information).

server1

Suffixlam.de > bind > test > de ▼RDN identifierdlzHostName ?

DNS entry

Host nameserver1

Alias name ("DNAM" record)

Add

Text ("TXT" records)

Text ?

Timeout ?

Description ?

This is a test server2w

Managed by LAM Pro2w

Add

✖

✖

Services (SRV)

Service records can be used to specify which servers provide common services such as LDAP. Please note that the host name must be `_SERVICE._PROTOCOL` (e.g. `_ldap._tcp`).

Priority: The priority of the target host, lower value means more preferred.

Weight: A relative weight for records with the same priority. E.g. weights 20 and 80 for a service will result in 20% queries to the one server and 80% to the other.

Port: The port number that is used for your service.

Server: DNS name where service can be reached (with dot at the end).

_ldap._tcp

Suffixlam.de > bind > test > de ▼RDN identifierdlzHostName ?

DNS entry

Host name_ldap._tcp

Alias name ("DNAM" record)

Add

Services ("SRV" records)

Priority *

10 ?

Weight *

80 ?

Port *

389 ?

Server *

ldap.example.com. ?

Timeout *

2w ?

Description ?

Delete

Priority *

10 ?

Weight *

20 ?

Port *

389 ?

Server *

ldap2.example.com. ?

Timeout *

2w ?

Description ?

Delete

Add

File upload

You can upload complete DNS zones via LAM's file upload. Here is an example for a zone file and the corresponding CSV file.

Table 4.2. Zone file

| | | | |
|------|----|-------|---|
| @ | IN | SOA | ns1.example.com admin.n-s1.example.com (1 360000 3600 3600000 370000) |
| | IN | NS | ns1.example.com. |
| | IN | NS | ns2.example.com. |
| | IN | MX | 10 mail1.example.com |
| | IN | MX | 20 mail2.example.com |
| foo | IN | A | 123.123.123.100 |
| foo2 | IN | CNAME | foo.example.com |
| bar | IN | A | 123.123.123.101 |
| | IN | AAAA | 1:2:3:4:5 |

Please check that you have an existing zone entry that can be used for the file upload. See above to create a new zone.

Hint: If you use the function above to create a new zone then please skip the "@" entry in the CSV file below. LAM creates this entry with sample data.

In this example we assume that the following zone entry exists:

```
dn: dlzZoneName=example.com,ou=bind,dc=example,dc=com
dlzzonename: example.com
objectclass: dlzZone
objectclass: top
```

Here is the corresponding CSV file: bindUpload.csv [resources/bindUpload.csv]

XFR entries

You can manage the XFR entries in the second tab that you configured before.

Bind XFR

[New DNS entry](#) [File upload](#) [Delete selected DNS entries](#) [New zone](#) bind > test > de ▾

DNS entry count: 5

| Actions | IP address | Record ID |
|-----------------------------------|----------------------|----------------------|
| Sort sequence ▾ ▴ | | ▾ ▴ |
| <input type="checkbox"/> Filter ▾ | <input type="text"/> | <input type="text"/> |
| <input type="checkbox"/> | 1.1.1.1 | 2 |
| <input type="checkbox"/> | 1.1.2.2 | 2 |
| <input type="checkbox"/> | 2:3:4:56:33 | 3 |
| <input type="checkbox"/> | 123.123.123.123 | 1 |
| <input type="checkbox"/> | 123.123.123.126 | 4 |

For each XFR entry you can set a record ID and the IP address.

2 > bind > test > de

Suffixbind > test > deRDN identifierdlzipaddr

XFR

Record ID *2

IP address *1.1.1.1

PowerDNS (LAM Pro)

This module allows to manage DNS entries for the PowerDNS name server.

Configuration

First, add the PowerDNS account type to your server profile:

| | | |
|-------------------|-----------------------------|---|
| Password policies | Password policies (ppolicy) | + |
| PowerDNS | PowerDNS entries | + |
| Printers | PyKota printers | + |

Second, add the PowerDNS module to the new account type:

settingsAccount typesModulesModule settingsJobs

PowerDNS

Selected modules

DNS entry (powerDNS)*

Available modules

Auto delete (autoDelete)

Custom fields (customFields)

Custom scripts (customScripts)

Third, activate automatic generation of PTR entries if needed. This is only required if you did not configure PowerDNS itself to generate PTR entries dynamically.

tingsAccount typesModulesModule settingsJobs

DNS entry

Automatic PTR changes

Manage DNS entries

Now you can manage your DNS entries inside LAM.

LAM supports the following record types:

- A
- AAAA
- CNAME
- DNAME
- MX
- NS
- PTR
- SOA
- SRV
- TXT

PowerDNS

[New DNS entry](#) [File upload](#) [Delete selected DNS entries](#)

powerdns > powerdns

DNS entry count: 1

| Actions | Domain name | Records |
|---------------------------------|-----------------------------|--|
| Sort sequence | | |
| <input type="checkbox"/> Filter | aaaa | |
| <input type="checkbox"/> | aaaa.test.de; aaaa2.test.de | AAAA 2003:d8:9f28:5100:fa32:e4ff:fec0:8d98 AAAA fe80::fa32:e4ff:fec0:8d98 |

aaaa.test.de

Suffix powerdns > powerdns RDN identifier dc

DNS entry

Name * aaaa.test.de

Associated domains *
aaaa.test.de
aaaa2.test.de

Timeout

IP addresses ("A/AAAA" records)
IP address
IPv6 address
2003:d8:9f28:5100:fa32:e4ff:fec0:8d98
fe80::fa32:e4ff:fec0:8d98

Text ("TXT" records)
Text

Aliases (LAM Pro)

Some applications use the object class "alias" to link LDAP entries to other parts of the LDAP tree. Activate the account type "Aliases" in your LAM server profile to use this account type.

Currently, only user accounts can be aliased with the "uidObject" object class.

smiller

Suffix aliases RDN identifier uid ?

User name * smiller

Alias

smiller

Suffix aliases RDN identifier uid ?

Aliased entry smiller > People > company > com

Change ?

Mail aliases

You can manage mail aliases (e.g. for NIS) inside LAM. This can be used to replace local `/etc/aliases` files with LDAP.

To activate this type please add "Mail aliases" in your LAM server profile:

| | | |
|-----------------------|---|---|
| Kopano dynamic groups | Kopano dynamic groups | + |
| Mail aliases | Mailing aliases (e.g. NIS mail aliases) | + |
| MIT Kerberos policies | MIT Kerberos policies | + |

NIS mail aliases

Note: Use the mail alias user module to manage mail aliases on user pages.

All accounts of this type are based on the "nisMailAlias" object class and may have "cn" and "rfc822MailMember" attributes.

You need to select the Mail aliases module on the next tab.

Mail aliases

Selected modules

Available modules

Mail aliases (nisMailAlias)*

Auto delete (autoDelete)

Courier (courierMailAlias)

Custom fields (customFields)

Custom scripts (customScripts)

The mail aliases will then appear as separate tab inside LAM. You may then manage the aliases with their names and recipient addresses.

There are mail/user icons that allow to select a mail address/user name from the existing users.

The screenshot shows the 'claudiabach' entry in the LDAP directory. The 'Suffix' is 'mailaliases > test > de' and the 'RDN identifier' is 'cn'. On the left, there is a sidebar with 'Mail aliases' selected. On the right, there are input fields for 'Alias name' (claudiabach), 'Recipient' (claudia.bach@ldap-account-manager.org), and 'New recipient'. There are also icons for adding, deleting, and searching entries.

Courier mail aliases

Mail aliases for Courier SMTP can be used when activating NIS mail aliases and Courier modules:

The screenshot shows the 'Mail aliases' configuration page. It has two sections: 'Selected modules' and 'Available modules'. In the 'Selected modules' section, 'Mail aliases (nisMailAlias)(*)' and 'Courier (courierMailAlias)' are listed with red 'X' icons. In the 'Available modules' section, 'Auto delete (autoDelete)', 'Custom fields (customFields)', 'Custom scripts (customScripts)', and 'General information (generalInformation)' are listed with green '+' icons.

You will then get the Courier tab for your mail aliases.

The screenshot shows the 'demo' entry in the LDAP directory. The 'Suffix' is 'aliases' and the 'RDN identifier' is 'cn'. On the left, there is a sidebar with 'Mail aliases' and 'Courier' selected. On the right, there are input fields for 'Email address' (demo@ldap-account-manager.org), 'Recipient address' (project1@ldap-account-manager.org), 'Mail source' (empty), and 'Description' (Demo alias). There are also icons for adding, deleting, and searching entries.

NIS net groups

LAM supports to define NIS netgroups. You can use them e.g. to restrict SSH access to your machines.

Add the NIS net group account type and its module to your server profile. Then you can manage net groups in LAM. Net groups may contain other net groups as child groups. You can either insert the host/user names manually or print the search buttons next to the input fields to find existing entries in your directory.

The screenshot shows the LAM Pro interface for managing a group named 'demo'. The breadcrumb trail is 'netgroups > test > de'. The RDN identifier is 'cn'. On the left, there is a tab for 'NIS net group'. The main form contains the following fields:

- Group name: demo
- Description: Demo group
- Subgroups: administrators, group01, group02
- Edit subgroups button

Below the form is a 'Members' section with a table of users:

| Host | User | Domain |
|------|-------|----------|
| pc01 | user1 | mydomain |
| | user2 | |
| | | |

NIS objects (LAM Pro)

You can manage NIS objects with LAM Pro. This allows you define network mount points in LDAP.

Add the NIS objects type to your LAM configuration and then the NIS objects module. This will add the NIS objects tab to LAM.

The screenshot shows the LAM Pro interface for managing a NIS object named '/home'. The breadcrumb trail is 'nisObjects > test > de'. The RDN identifier is 'cn'. On the left, there is a tab for 'NIS object'. The main form contains the following fields:

- Name: /home
- Mapping name: auto.home
- Mapping entry: -fstype=nfs,rw homeserver:/home
- Description: Network home

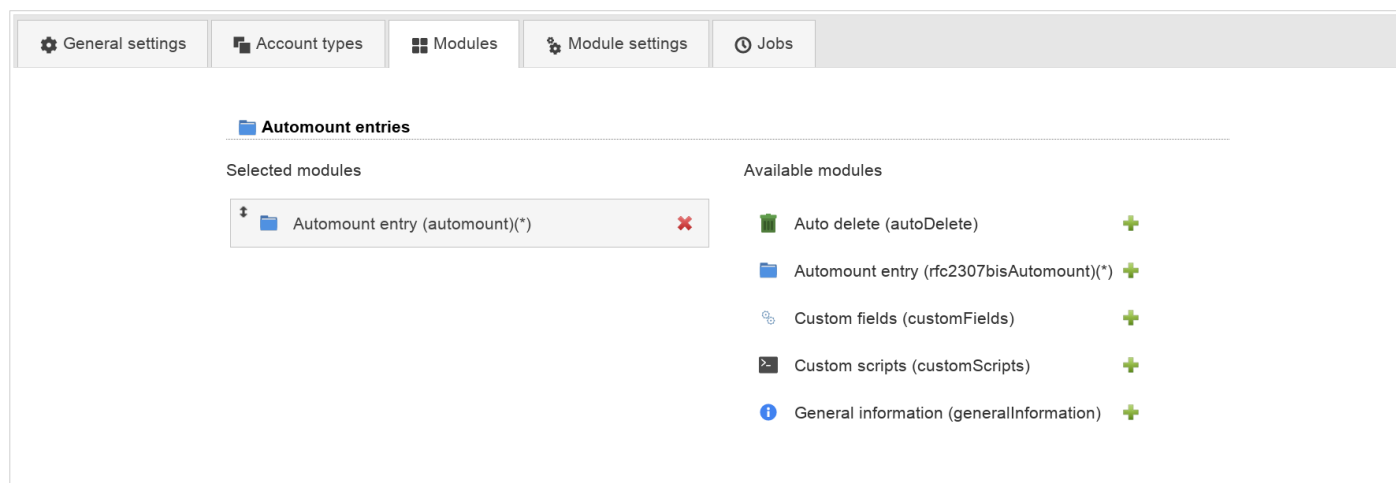
Automount objects (LAM Pro)

LAM Pro allows you to manage automount entries. Please activate the account type "Automount objects" in your LAM Pro server profile.

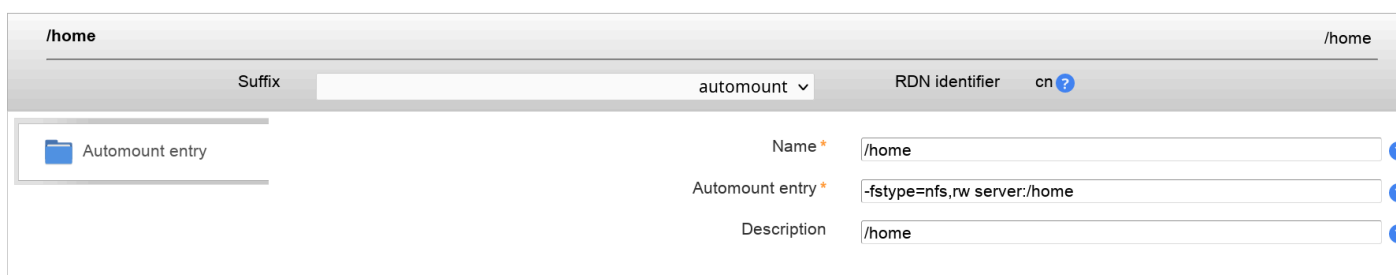
The screenshot shows the LAM Pro interface with the 'Account types' tab selected. The 'Available account types' section lists the following:

| Account type | Module | Action |
|--------------------------|-----------------------------|--------|
| Aliases | Alias entries | + |
| Asterisk extensions | Asterisk extensions entries | + |
| Automount entries | Automount entries | + |
| Billing codes | PyKota billing codes | + |
| Bind DNS | Bind DNS entries | + |
| Custom type | Custom entries | + |

Then add the correct automount module. Usually, this is "Automount entry (automount)". If you use Suse Linux with RFC2307bis schema please select "Automount entry (rfc2307bisAutomount)".



This will add a new tab to LAM Pro's main screen which includes a list of all automount entries. Here you can easily create new entries.



Please see the following external HowTos for more information on automounting and LDAP:

- AutofsLDAP [<https://help.ubuntu.com/community/AutofsLDAP>]
- Automount über LDAP (German) [<http://www.pro-linux.de/artikel/2/760/automount-ueber-ldap.html>]

Oracle databases (LAM Pro)

Oracle allows to manage connection data that is stored in tnsnames.ora to be stored in an LDAP directory.

Initial setup

LDAP server setup:

You will need to install the correct Oracle LDAP schema files on your LDAP server. If you run no Oracle LDAP server then you can get them (oidbase.schema, oidnet.schema, oidrdbms.schema, alias.schema) e.g. from here [http://www.idevelopment.info/data/Oracle/DBA_tips/LDAP/LDAP_8.shtml].

Next you need to create the root entry for Oracle. It should look like this:


```
dn: cn=OracleContext,dc=example,dc=com
objectclass: orclContext
cn: OracleContext
```

You can create it with LAM's tree view (tools menu). Please note that "cn" must be set to "OracleContext".

LAM setup:


Managing entries in your LDAP directory

Edit your LAM server profile and add the Oracle account type:

| | | |
|---|-----------------------------|---|
|  NIS objects | NIS object entries | + |
|  Oracle databases | Oracle database entries | + |
|  Password policies | Password policies (ppolicy) | + |

In case you manage a single Oracle context just enter the cn=OracleContext entry as LDAP suffix. If you manage multiple Oracle context entries then set the LDAP suffix to a parent entry of them.

Active account types

 Oracle databases

Oracle database entries

↓ ×

LDAP suffix *

ou=oracle,o=test,c=de

?

List attributes

#cn,#orclNetDescString,#description

?

Custom label

?

Additional LDAP filter

?

Read-only

☐

?

Hidden

☐

?

No new entries

☐

?

Disallow delete

☐

?

Next, add the Oracle module:

Settings

Account types

Modules

Module settings

Jobs

Oracle databases

Selected modules

↑ Oracle database (oracleService)* ×

Available modules

Auto delete (autoDelete)

+

Custom fields (customFields)

+

Custom scripts (customScripts)

+

General information (generalInformation)

+

Now you can login to LAM and start to add database entries.

Managing database entries

Each database has a service name, the connection string and an optional description.

mydb


This is a sample database

Suffix

OracleContext > ctx1 > oracle > test > de

RDN identifier

cn

 Oracle database

Name *

mydb

Description

This is a sample database

Connection string *

(DESCRIPTION=(ADDRESS=(PROTOCOL=TCP)(HOST=mydb.example.com)(PORT=1521))(CONNECT_DATA=(SERVICE_NAME=orcl)))

Database client setup for LDAP

You need to activate the LDAP adapter to make the database tools reading LDAP. Edit network/admin/sqlnet.ora like this:

```
NAMES.DIRECTORY_PATH= (TNSNAMES, LDAP)
```

Then add a file called ldap.ora next to your sqlnet.ora and set the LDAP server and DN suffix where cn=Oracle-Context is stored:

```
DIRECTORY_SERVERS= (ldap.example.com:389:636)
DEFAULT_ADMIN_CONTEXT = "ou=ctx1,ou=oracle,o=test,c=de"
DIRECTORY_SERVER_TYPE = OID
```

This will allow e.g. tnsping to get the connection data from LDAP:

```
[oracle@oracle bin]$ tnsping mydb
```

TNS Ping Utility for Linux: Version 12.1.0.1.0 - Production on 09-FEB-2014 18:06:54

Copyright (c) 1997, 2013, Oracle. All rights reserved.

Used parameter files:

```
/home/oracle/app/oracle/product/12.1.0/dbhome_1/network/admin/sqlnet.ora
```

Used **LDAP** adapter to resolve the alias

```
Attempting to contact (DESCRIPTION=(ADDRESS=(PROTOCOL=TCP)(HOST=mydb.example.com)(PORT=
OK (10 msec)
```

Password policies (LAM Pro)

OpenLDAP supports the ppolicy [<http://linux.die.net/man/5/slapo-ppolicy>] overlay to manage password policies for LDAP entries. This allows you to set password policies which are independent from your applications. The policies are managed internally by the LDAP server.

You can manage these policies with LAM Pro with the account type "Password policies".


The screenshot shows the LAM Pro web interface for managing a Password policy. The breadcrumb navigation is "demo > policies > test > de". The RDN identifier is "cn". On the left, there is a sidebar with a "Password policy" icon. The main area displays the configuration for a policy named "demo". The settings are as follows:

| Setting | Value |
|--|-------------------------------------|
| Name | demo |
| Minimum password age | 1d |
| Maximum password age | 1y |
| Expire warning | |
| Grace authentication limit | |
| Password history length | 10 |
| Password quality check | yes |
| Minimum password length | |
| Lockout users | <input type="checkbox"/> |
| Lockout duration | |
| Maximum failure count | |
| Failure count interval | |
| Require password change on first login | <input type="checkbox"/> |
| Allow password change | <input checked="" type="checkbox"/> |
| Password change requires old password | <input type="checkbox"/> |
| Password check module | |

You will need to add the ppolicy schema to your OpenLDAP configuration and activate the ppolicy [<http://linux.die.net/man/5/slapo-ppolicy>] overlay module in slapd.conf to use this feature.

MIT Kerberos policies (LAM Pro)


Please add the account type "MIT Kerberos policies" on tab "Account types" in your server profile and setup the LDAP suffix where printers are stored.

 MIT Kerberos policies

MIT Kerberos policies

MIT Kerberos policies

+

 MIT Kerberos policies

MIT Kerberos policies

MIT Kerberos policies

↑

×

LDAP suffix *

cn=LAM.LOCAL,cn=mitkerberos,o=test,c=de

?

List attributes

#cn;#krbMinPwdLife;#krbMaxPwdLife;#krbPwdMinLength;#krbP

?

Custom label

?

Additional LDAP filter

?

Read-only

☐

?

Hidden

☐

?

No new entries

☐


?

Disallow delete

☐

?


Then add the "Password policy (mitKerberosPolicy)" module on tab "Account modules".

 MIT Kerberos policies


Selected modules

Available modules


⌵

 Password policy (mitKerberosPolicy)(*)


×

 Auto delete (autoDelete)


+

 Custom fields (customFields)

+

 Custom scripts (customScripts)

+

 General information (generalInformation)

+

Now login to LAM and you will see the MIT Kerberos policies tab. Here you can manage the different policies.


demo

Suffix

LAM.LOCAL > mitkerberos > test > de

RDN identifier

cn?

 Password policy

Name *

demo

?

Minimum password age

?

Maximum password age

1y

?

Minimum password length

3

?

Password history length

1

?

Maximum failure count

3

?

Lockout duration

2h

?

Failure count interval

1h

?

Minimum character classes

1

?

Allowed key/salt types

?

PyKota printers

Please add the account type "Printers (PyKota printers)" on tab "Account types" in your server profile and setup the LDAP suffix where printers are stored.

Printers

PyKota printers

LDAP suffix *

List attributes

Custom label

Additional LDAP filter

Read-only ☐

Hidden ☐

No new entries ☐

Disallow delete ☐

Then add the PyKota printer module on tab "Account modules".

Printers

Selected modules

PyKota (pykotaPrinter)*

Available modules

Auto delete (autoDelete)

Custom fields (customFields)

Custom scripts (customScripts)

General information (generalInformation)

Next you can start managing printers inside LAM. Here you can setup the costs for a print job. LAM will also show if the printer is member of any printer groups.

printer3

Suffix printers > pykota > test > de

RDN identifier cn

Printer name * printer3

Maximum job size 0

Price per job 1.0

Price per page 0.5

Passthrough No

Description My printer

Printer groups printergroup5, printergroup7

Group members


You can also setup printer groups. Just add some members to your new group.

printergroup

My printer group

Suffixprinters > pykota > test > de

RDN identifiercn?

 PyKota

Printer name *printergroup

Maximum job size0

Price per job1.0

Price per page0.5

PassthroughNo

DescriptionMy printer group

Group membersprinter1 printer2

PyKota billing codes

Please add the account type "Billing codes" on tab "Account types" in your server profile and setup the LDAP suffix where billing codes are stored.

Billing codes

PyKota billing codes

Billing codes

PyKota billing codes

LDAP suffix *ou=billingcodes,ou=pykota,o=test,c=de

List attributes#cn,#description,#pykotaBalance,#pykotaPageCounter

Custom label

Additional LDAP filter

Read-only

Hidden

No new entries

Disallow delete

Then add the PyKota billing code module on tab "Account modules".

Billing codes

Selected modules

PyKota (pykotaBillingCode)*

Available modules

Auto delete (autoDelete)

Custom fields (customFields)

Custom scripts (customScripts)

Now login to LAM and you will see the billing code tab where you can manage your entries. If jobs were printed with a billing code then you will also see the balance and page count.

billingCode01

Suffix billingcodes > pykota > test > de RDN identifier cn

PyKota

Billing code * billingCode01

Balance 0.0

Page count 0

Description Some billing code

Reset

Custom types (LAM Pro)

This account type allows you to manage any type of LDAP entries. This is e.g. needed if you define your own structural object classes or LAM does not yet provide a module for a structural object class.

Always use this together with Custom fields to specify the LDAP attributes.

Configuration

Add a custom account type in your server profile (you can also add multiple if needed).

General settings Account types Modules Module settings Jobs

Available account types

| | | |
|---------------------|-----------------------------|---|
| Aliases | Alias entries | + |
| Asterisk extensions | Asterisk extensions entries | + |
| Automount entries | Automount entries | + |
| Billing codes | PyKota billing codes | + |
| Bind DNS | Bind DNS entries | + |
| Custom type | Custom entries | + |
| DHCP | DHCP administration | + |

Then specify the root DN where the entries should be stored. Also provide the attributes to show in list view and a unique label for your entries.

Custom entries

LDAP suffix * ou=custom1,o=test,c=de

List attributes #cn,ipserviceport:Port;ipserviceprotocol:Protocol

Custom label Custom entries

Additional LDAP filter

Read-only ☐

Hidden ☐

No new entries ☐

Disallow delete ☐

On tab modules add the custom type module. You will also need the Custom fields module to manage the attributes.

Managing entries in your LDAP directory

Custom entries

Selected modules

Custom type (customBaseType)(*)

Custom fields (customFields)

Available modules

Auto delete (autoDelete)

Custom scripts (customScripts)

General information (generalInformation)

Finally, switch to tab Module settings. Here you need to specify the structural object class. Also configure the Custom fields module to manage all your attributes.

Custom type

Custom entries

Object class * ipService

Manage your entries

You can now login to LAM and will see one tab for each configured custom type.

















Custom entries

New entry

File upload

Delete selected entries

Entry count: 4

| Actions | Common name | Port | Protocol |
|--|-------------|-------|----------|
| Sort sequence | | | |
| <input type="checkbox"/> Filter ▾ | | | |
| <input type="checkbox"/>     | service1 | 12345 | http |
| <input type="checkbox"/>     | service2 | 12345 | http |
| <input type="checkbox"/>     | service3 | 1236 | http |
| <input type="checkbox"/>     | test4 | 12 | tcp |

Custom fields (LAM Pro)

This module allows you to manage LDAP attributes that are not covered by the other LAM modules (e.g. if you use a custom LDAP schema). You can fully define how your input fields look like:

- Label
- LDAP attribute name
- Unique name for field
- Help text
- Read-only display
- Field type: text, password, text area, checkbox, radio buttons, select list, file upload, LDAP date (and time), constant
- Validation via regular expression
- Error message if validation fails

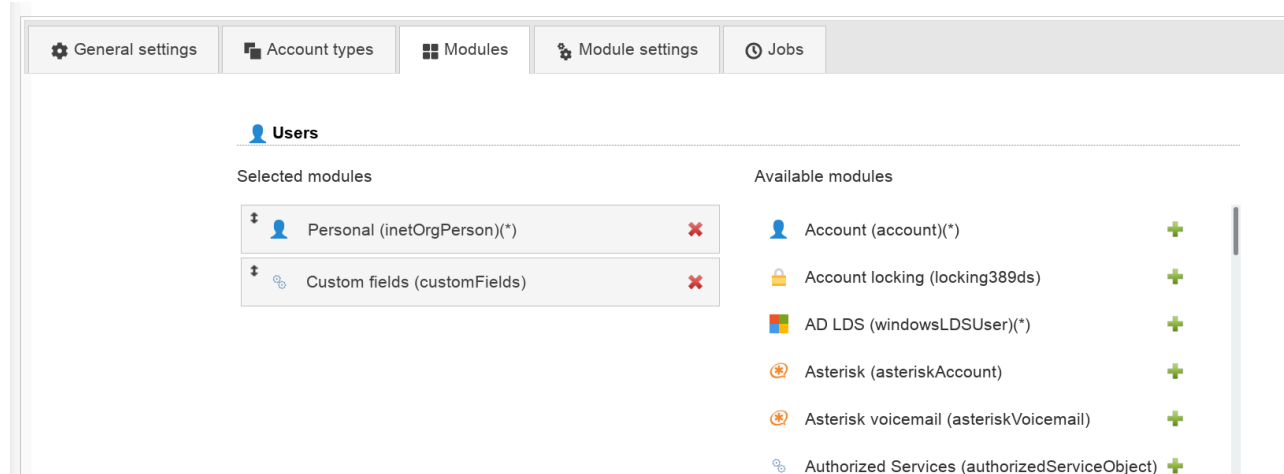
Limitations:

Custom fields cannot manage

- structural object classes (supported by Custom types)
- attributes that require validation rules across multiple attributes or cannot be described by a simple regular expression

Activating the custom fields module:

You may specify custom fields for all of your account types. Please enter tab "Modules" in your server profile. Now activate the "Custom fields (customFields)" module for all needed account types.

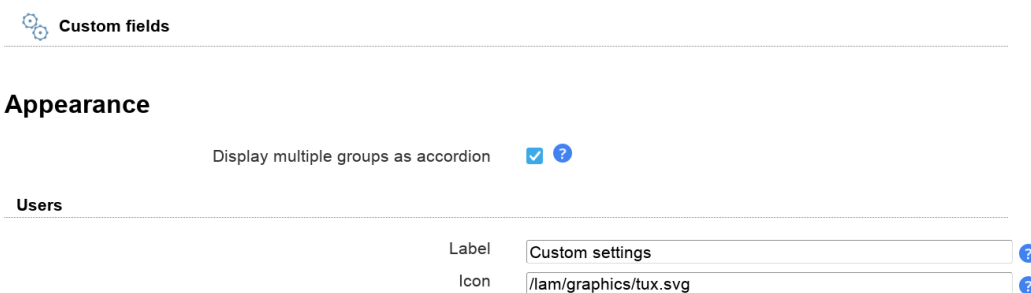


Setting label and icon:

You may set the label that is displayed e.g. on the tab when editing an account. It is also possible to specify an icon (must be a valid URL like "/images/icon.png" or "http://server/images/icon.png"). The icon size should be 32x32 pixels.

LAM will display a default icon and "Custom fields" as label if you do not enter any values.

You may also specify how LAM displays custom fields when there are multiple field groups. The default is accordion view where you can switch field groups by clicking on the title. You may also deactivate this mode. Then all field groups are displayed one below the other.



Defining groups:

All input fields are divided into groups. A group may contain one or more object classes and allows you to add/remove a certain set of input fields.

E.g. you may define two groups - "My application A" and "My application B" - that manage different LDAP attributes and object classes. This way you will be able to control both attribute sets independently.

To create a group please edit your server profile and switch to tab "Module settings". You will see the section "Custom fields" which allows you to add new groups. Now select your account type (e.g. Users) and specify an alias for your group. This alias will be printed as group header when you later edit an account in the admin interface.

Create new group

Account type

Alias *

?

After you created your new group you can setup the managed object classes. If you specify any object classes then you will later be able to add/remove a complete set of attributes including their object classes.

Skipping the object classes field is only useful if you want to manage some attributes that are not yet supported by LAM but there is already a LAM module that manages the object class.

Create new group

Account type

Alias *

?

Personal

Account type

Alias *

Object classes

Add new field

Move

Delete group

The group may look like when you edit a user.

Claudia Bach claudia.bach@ldap-account-manager.org Telephone number 0123-4567-8900 Mobile number 0123-4567-8922

Suffix RDN identifier

Claudia Bach claudia.bach@ldap-account-manager.org Telephone number 0123-4567-8900 Mobile number 0123-4567-8922

Suffix RDN identifier

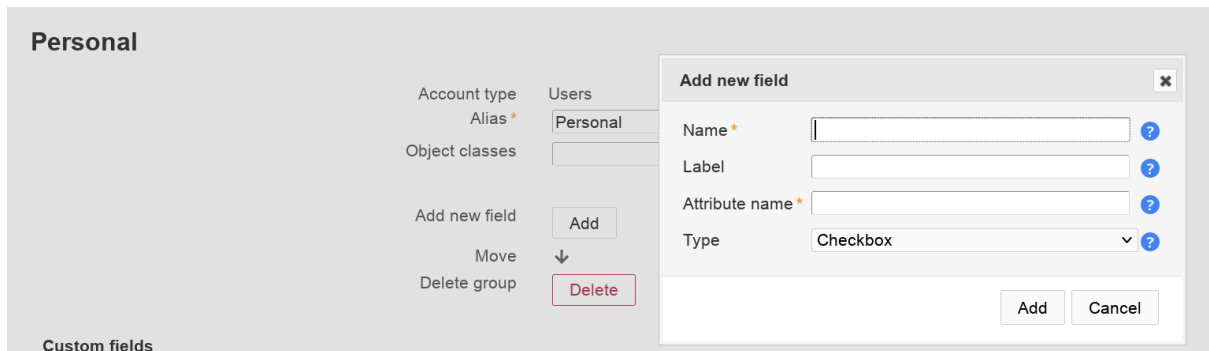
Routing address

Active ☐

Adding fields:

Now you can add a new field that manages an LDAP attribute. Simply fill the fields and press on "Add".

Please note that the field name cannot be changed later. It is the unique ID for this field.



Examples for fields and their representation:

Text field:

Text fields allow to specify a validation expression and error message.

You can also enable auto-completion. In this case LAM will search all accounts for the given attribute and provide auto-completion hints when the user edits this field. This should only be used if there is a limited number of different values for this attribute.

In case your field is a date value you can show a calendar for easy editing.

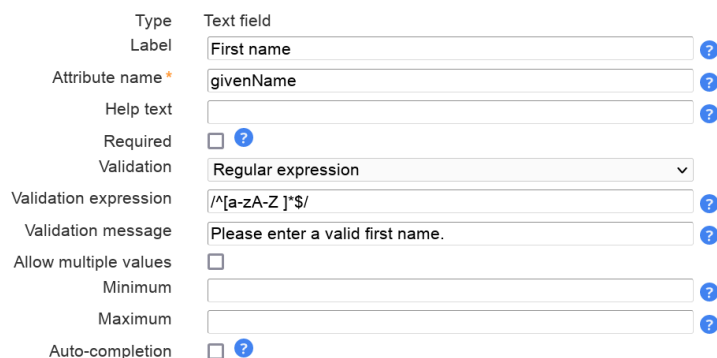
Example calendar formats:

- d.m.Y: 31.12.2025
- Y-m-d: 2025-12-31
- d M, y: 31 Dec, 25
- d MM, Y: 31 December, 2025

You can escape wildcards with "\". E.g. "d.m.Y \d" will result in "31.12.2025 d".

Profile editor: For multi-value fields you can separate multiple values by semicolon in profile editor (e.g. "value1; value2"). LAM will split the text when loading the profile.

givenName ✖



Presentation:

First name

Password field:

You can also manage custom password fields. LAM Pro will display two fields where the user must enter the same password. You can hash the password if needed.

customPassword 

| | |
|-----------------------|--|
| Type | Password |
| Label | <input type="text" value="Custom Password"/> ? |
| Attribute name * | <input type="text" value="userPassword"/> ? |
| Help text | <input type="text"/> ? |
| Validation | Regular expression |
| Validation expression | <input type="text"/> ? |
| Validation message | <input type="text"/> ? |
| Password hash type | <input type="text" value="ARGON2ID"/> ? |

Presentation:

Custom Password

Text area:

This adds a multi-line field. The options are similar to text fields. Additionally, you can set the size with the number of columns and rows.

Please note that the validation expression should be set to multi-line. This is done by adding "m" at the end.

postalAddress 

| | |
|-----------------------|---|
| Type | Text area |
| Label | <input type="text" value="Postal address"/> ? |
| Attribute name * | <input type="text" value="postalAddress"/> ? |
| Help text | <input type="text"/> ? |
| Required | <input checked="" type="checkbox"/> ? |
| Validation | Regular expression |
| Validation expression | <input type="text" value="/[0-9a-zA-Z]*\$/m"/> ? |
| Validation message | <input type="text" value="Invalid postal address"/> ? |
| Columns | <input type="text" value="25"/> ? |
| Rows | <input type="text" value="4"/> ? |

Presentation:

Postal address *

Checkbox:

Sometimes you may want to allow only yes/no values for your LDAP attributes. This can be represented by a checkbox. You can specify the values for checked and unchecked. The default value is set if the LDAP attribute has no value.

carLicense 

| | |
|-------------------------|--|
| Type | Checkbox |
| Label | <input type="text" value="Car license"/> ? |
| Attribute name * | <input type="text" value="carLicense"/> ? |
| Help text | <input type="text"/> ? |
| Value for "checked" * | <input type="text" value="yes"/> ? |
| Value for "unchecked" * | <input type="text" value="no"/> ? |
| Default value | <input type="checkbox"/> ? |

Presentation:

Car license ☒

Radio buttons:

This displays a list of radio buttons where the user can select one value.

You can specify a mapping of LDAP attribute values and their display (label) on the Self Service page. To add more mapping fields please press "Add more mapping fields".

businessCategory ✖

| | |
|------------------|--|
| Type | Radio buttons |
| Label | <input type="text" value="Business category"/> |
| Attribute name * | <input type="text" value="businessCategory"/> |
| Help text | <input type="text"/> |
| Value mapping ? | |

| Value | Label |
|----------------------------------|--|
| <input type="text" value="-"/> | <input type="text" value="-"/> |
| <input type="text" value="hr"/> | <input type="text" value="Human Resources"/> |
| <input type="text" value="it"/> | <input type="text" value="IT"/> |
| <input type="text" value="man"/> | <input type="text" value="Management"/> |
| <input type="text" value="org"/> | <input type="text" value="Organisation"/> |

Presentation:

Business category

☐ -

☐ Human Resources

☐ IT

☐ Management

☒ Organisation

Select list:

Select lists allow the user to select a value in a large list of options. The definition of the possible values and their display is similar to radio buttons.

You can also allow multiple values.

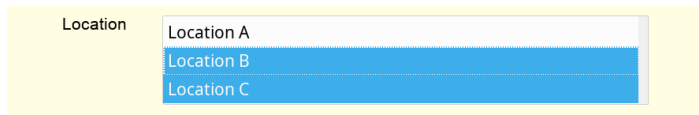
departmentNumber ✖

| | |
|-----------------------|---|
| Type | Select list |
| Label | <input type="text" value="Department"/> |
| Attribute name * | <input type="text" value="departmentNumber"/> |
| Help text | <input type="text"/> |
| Allow multiple values | <input type="checkbox"/> |
| Minimum | <input type="text" value="2"/> |
| Maximum | <input type="text" value="3"/> |
| Value mapping ? | |

| Value | Label |
|--|---|
| <input type="text" value="car"/> | <input type="text" value="Automotive"/> |
| <input type="text" value="it"/> | <input type="text" value="IT Consulting"/> |
| <input type="text" value="bank"/> | <input type="text" value="Financial Services"/> |
| <input type="text" value="insurance"/> | <input type="text" value="Insurance"/> |

Presentation:

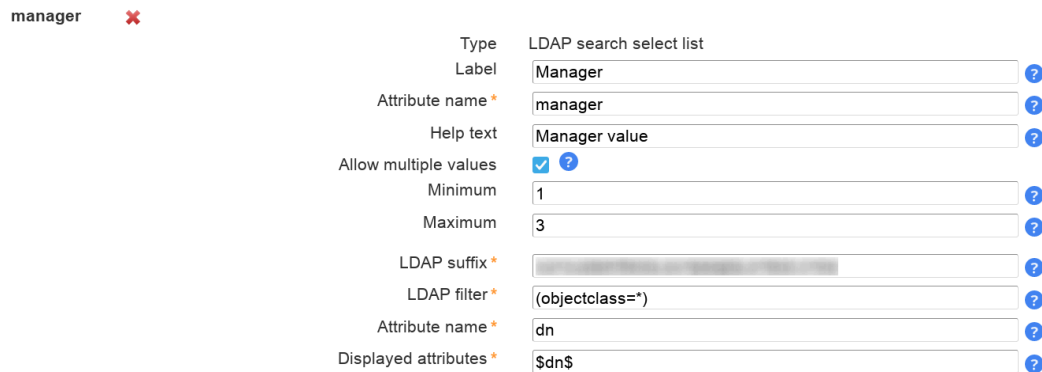
Department



A screenshot of a web form showing a dropdown menu for 'Location'. The menu is open, displaying three options: 'Location A', 'Location B', and 'Location C'. 'Location B' is currently selected and highlighted in blue.

LDAP search select list

This is similar to "Select list" but the options are read from LDAP. You can use this to define e.g. a DN selection list. Multiple values are supported.



A screenshot of the configuration form for an 'LDAP search select list'. The form includes fields for 'Label' (Manager), 'Attribute name' (manager), 'Help text' (Manager value), 'Allow multiple values' (checked), 'Minimum' (1), 'Maximum' (3), 'LDAP suffix' (empty), 'LDAP filter' ((objectclass=*)), 'Attribute name' (dn), and 'Displayed attributes' (\$dn\$). Each field has a help icon (question mark) to its right.

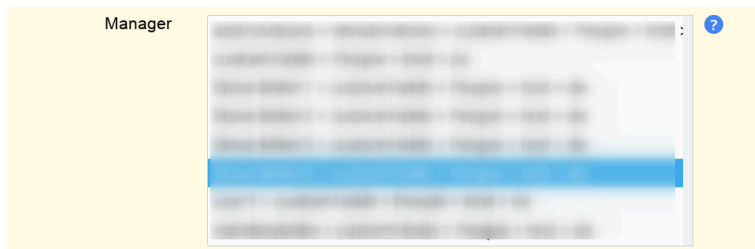
LDAP suffix: The LDAP DN that is used as starting point to search for LDAP entries.

LDAP filter: Only LDAP entries that match this filter will be used. If all entries should be used then use "(objectclass=*)".

Attribute name: The values of this attribute will be used to build the selection list.

Display attributes: List of attributes to show as label for the options in select box. Attribute wildcards are surrounded by "\$", e.g. "\$cn\$" will be replaced by "cn" attribute. Default is "\$dn\$".

Presentation:

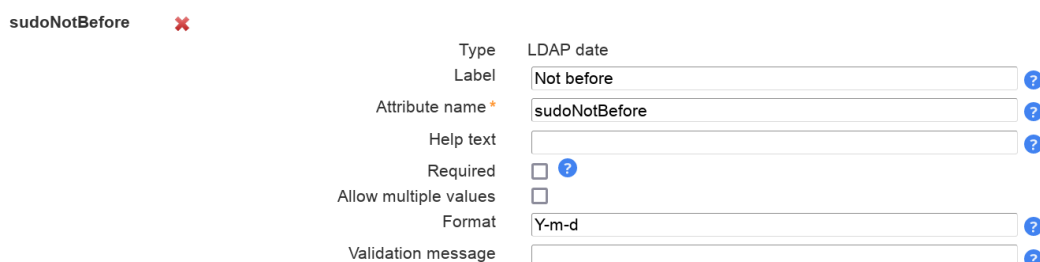


A screenshot showing the presentation of the LDAP search select list. It displays a dropdown menu with the label 'Manager' and a list of LDAP entries. One entry is selected and highlighted in blue.

LDAP date

Use this for LDAP attributes with syntax "Generalized Time" (1.3.6.1.4.1.1466.115.121.1.24).

LAM will automatically set hour/minute/second to "0". If this is not intended please use type "LDAP date and time".



A screenshot of the configuration form for an 'LDAP date'. The form includes fields for 'Label' (Not before), 'Attribute name' (sudoNotBefore), 'Help text' (empty), 'Required' (unchecked), 'Allow multiple values' (unchecked), 'Format' (Y-m-d), and 'Validation message' (empty). Each field has a help icon (question mark) to its right.

Presentation:

LAM will display a calendar to select the date.

The screenshot shows a web form with a calendar overlay. The calendar is for January 2022, with the 25th selected. Below the calendar, the text 'Sudo' is visible. To the right, there is a 'Not before' field with the value '2022-01-01'.

LDAP date and time

Use this for LDAP attributes with syntax "Generalized Time" (1.3.6.1.4.1.1466.115.121.1.24).

LAM can convert the displayed value to the configured time zone of your server/self service profile. In this case, please activate "Display in local time".

sudoNotAfter ✖

| | |
|-----------------------|---------------------------------------|
| Type | LDAP date and time |
| Label | Not after ? |
| Attribute name * | sudoNotAfter ? |
| Help text | ? ? |
| Required | <input type="checkbox"/> ? |
| Allow multiple values | <input type="checkbox"/> |
| Format | Y-m-d H:i:s ? |
| Validation message | ? ? |
| Display in local time | <input checked="" type="checkbox"/> ? |

Presentation:

LAM will display a calendar to select the date and time.

The screenshot shows a web form with a calendar overlay. The calendar is for January 2022, with the 25th selected. Below the calendar, the text 'Not after' is visible. To the right, there is a field showing the value '2022-01-01 12:25:10'.

Constant value

This will set the attribute to a constant value. You can also specify wildcards to inject other attribute's values.

employeeType ✖

| | |
|------------------|-----------------|
| Type | Constant |
| Label | Employee Type ? |
| Attribute name * | employeeType ? |
| Help text | help test ? |
| Value * | !!cn!! ? |

Wildcards:

- %attribute%: attribute value
- @attribute@: first character of attribute
- ?attribute?: first character of attribute in lower case
- !attribute!: first character of attribute in upper case
- ??attribute??: attribute in lower case
- !!attribute!!: attribute in upper case
- ((attribute)): space if attribute is set
- §attribute|§; attribute values separated by ";" (you can set other separators if you want)

Examples for attributes gn="Steve", sn="Miller" and memberUid=("user1", "user2") (specified value -> resulting LDAP value):

Table 4.3.

| Constant value | Resulting LDAP value |
|----------------|---|
| my constant | my constant |
| %gn% | Steve |
| %gn%((gn))%sn% | Steve Miller (would be "Miller" if gn is empty) |
| §memberUid , § | user1, user2 |

Presentation:

The LDAP value will be shown as text.

Employee Type [text input] ?

File upload:

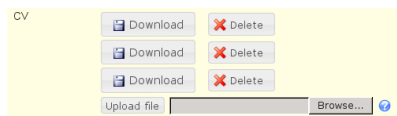
This is used for binary data. You can restrict uploaded data to a given file extension and set the maximum file size.

Name cv ✖

| | |
|-------------------|---------------------------------------|
| Type | File upload |
| Label | CV ? |
| Attribute name * | userCV ? |
| Read-only | <input type="checkbox"/> ? |
| File extension | .pdf ? |
| Maximum file size | 100000 ? |
| Multi value | <input checked="" type="checkbox"/> ? |

Presentation:

The uploaded data may also be downloaded via LAM.



Validation expressions:

The validation expressions follow the standard of Perl regular expressions [<http://perldoc.perl.org/perlre.html>]. They start and end with a "/". The beginning of a line is specified by "^" and the end by "\$".

Examples:

`/^[a-z0-9]+$` allows small letters and numbers. The value must not be empty ("").

`/^[a-z0-9]+$/i` allows small and capital letters ("i" at the end means ignore case) and numbers. The value must not be empty ("").

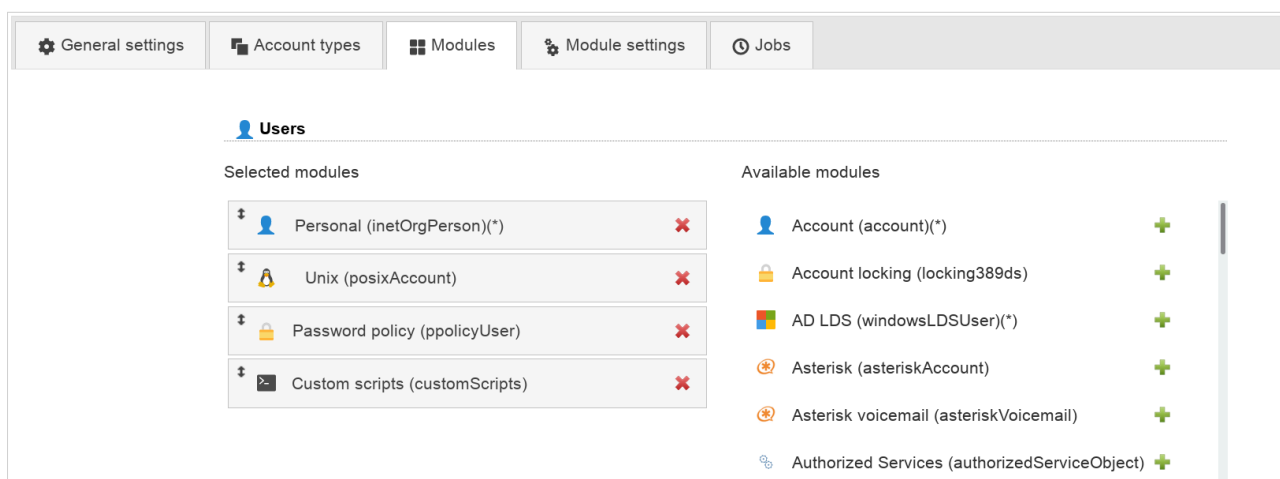
Special characters that must be escaped with "\": "\", ".", "(", ")"

E.g. `/^[a-z0-9\\.]+$`

Custom scripts (LAM Pro)

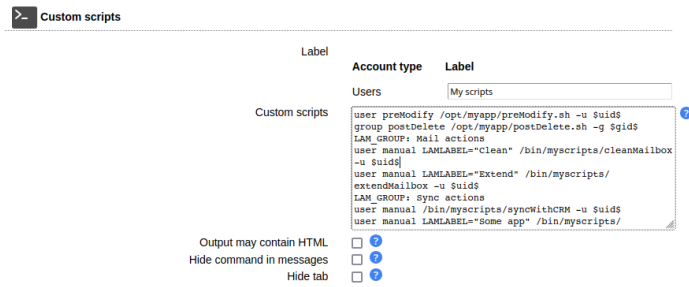
LAM Pro allows you to execute scripts whenever an account is created, modified or deleted. This can be useful to automate processes which needed manual work afterwards (e.g. sending your user a welcome mail or register a mailbox). Additionally, you can specify manual scripts that can be executed from within LAM Pro.

To activate this feature please add the "Custom scripts" module to all needed account types on the configuration pages.



In "Module settings" you can specify multiple scripts for each action type (e.g. modify) and account type (e.g. user). The scripts need to be located on the filesystem of your webserver and will be executed in its user environment. E.g. if you webserver runs as user www-data with the group www-data then the custom scripts will be run under this user with his rights. The output of the scripts will be shown in LAM.

You can specify the scripts on the LAM configuration pages.



Label:

Here you can enter a descriptive label for the module tab inside LAM.

Syntax:

Please enter one script per line. Each line has the following format: <account type> <action> <script>

E.g.: user preModify /usr/bin/myCustomScript -u \$uid\$

Account types:

You can setup scripts for all available account types (e.g. user, group, host, ...). Please see the help on the configuration page about your current active account types.

Actions:

Table 4.4. Action types

| Action name | Description |
|-------------|--|
| preCreate | Executed before creating a new account (cancels operation if a script returns an exit code > 0, not available for file upload) |
| postCreate | Executed after creating a new account (does not run if preCreate or LDAP operations fail) |
| preModify | Executed before an account is modified (cancels operation if a script returns an exit code > 0) |
| postModify | Executed after an account was modified (does not run if preModify or LDAP operations fail) |
| preDelete | Executed before an account is modified (cancels operation if a script returns an exit code > 0) |
| postDelete | Executed after an account was modified (does not run if preDelete or LDAP operations fail) |
| manual | Can be run manually on account page. If you add LAM-LABEL="text" before the command then LAM will use the text as label for the button in account edit screen. |

Script:

You can execute any script which is located on the filesystem of your webserver. The path may be absolute or relative to the PATH-variable of the environment of your webserver process. It is also possible to add commandline arguments to your scripts. Additionally, LAM will resolve wildcards to LDAP attributes. If your script includes an wildcard in the format \$ATTRIBUTE\$ then LAM will replace it with the attribute value of the current LDAP entry. The values of multi-value attributes are separated by commas. E.g. if you create an account with the attribute "uid" and value "steve" then LAM will resolve "\$uid\$" to "steve".

Please note that manual scripts can only use the current LDAP attribute values of the account. Any modifications done that are not saved will not be available. Manual scripts are also not available for new accounts that are not yet saved to LDAP.

You can switch LAM's logging to debug mode if you are unsure which attributes with which values are available.

The following special wildcards are available for automatic scripts:

- **\$INFO.lamLoginDn\$**: the DN of the user that is logged in to LAM.
- **\$INFO.lamProfileName\$**: the current server or self service profile name
- **\$INFO.debug\$**: list of all possible wildcards and their values (e.g. "\$objectClass\$:posixAccount,inetOrgPerson; \$loginShell\$:/bin/bash; \$gidNumber\$:12345; \$uid\$:userid...")
- **\$INFO.userPasswordClearText\$**: cleartext password when Unix/Windows password is changed (e.g. useful for external password synchronisation) for new/modified accounts
- **\$INFO.userPasswordStatusChange\$**: provides additional information if the Personal/Unix password locking status was changed, possible values: locked, unlocked, unchanged
- **\$INFO.passwordSelfResetAnswerClearText\$**: cleartext answer to security question
- **\$INFO.389lockingStatusChange\$**: for 389ds account locking, provides information if account was unlocked. Possible values: unchanged, unlocked
- **\$INFO.389deactivationStatusChange\$**: for 389ds account locking, provides information if account was deactivated. Possible values: unchanged, activated, deactivated
- **\$INFO.isNewAccount\$**: specifies if the account already exists or is newly created (yes|no)
- **\$INFO.passwordUpdated\$**: specifies if the user password was changed (yes|no)
- **\$INFO.passwordChangeType\$**: password type (manual|random|none) where "none" means no password change
- **\$INFO.passwordChangeModules\$**: module names of password change operation (e.g. "posixAccount")
- **\$INFO.forcePasswordChange\$**: a password change was forced (yes|no)
- **\$INFO.sendPasswordViaEmail\$**: send password via email (yes|no)
- **\$INFO.sendPasswordAlternateAddress\$**: alternate email address for password email if set (e.g. "test@example.com")
- **\$NEW.<attribute>\$**: the value of a new attribute (e.g. \$NEW.telephoneNumber\$) for modified accounts
- **\$DEL.<attribute>\$**: the value of a deleted attribute (e.g. \$DEL.telephoneNumber\$) for modified accounts
- **\$MOD.<attribute>\$**: the new value of a modified attribute (e.g. \$MOD.telephoneNumber\$) for modified accounts
- **\$ORIG.<attribute>\$**: the original value of an attribute (e.g. \$ORIG.telephoneNumber\$) for modified accounts

Grouping of manual scripts:

If you have a larger number of manual scripts then you can divide them into groups. Add a line "LAM_GROUP: My group description" when you want to start a new group.

Example:

```
user preModify /opt/myapp/preModify.sh -u $uid$
group postDelete /opt/myapp/postDelete.sh -g $gid$
LAM_GROUP: Mail actions
user manual LAMLABEL="Clean" /bin/myscripts/cleanMailbox -u $uid$
user manual LAMLABEL="Extend" /bin/myscripts/extendMailbox -u $uid$
```

LAM_GROUP: Sync actions

user manual /bin/myscripts/syncWithCRM -u \$uid\$

user manual LAMLABEL="Some app" /bin/myscripts/syncWithSomeApp -u \$uid\$

Interactive parameters for manual scripts

You can define parameters that are specified by the user on the script execution page. E.g., this can be used to specify a target environment (dev/qa/prod).

Interactive parameters allow the user to select the right value instead of having the need to duplicate script entries.

Format: LAM_{TYPE}_{NAME}: {label}={value(s)}

Possible input types:

- Selection
 - Parameter name needs to start with "LAM_SELECTION_", e.g. "LAM_SELECTION_ENV".
 - Values must be separated by semicolons (e.g. "dev;qa;prod")
- Text input
 - Parameter name needs to start with "LAM_TEXT_", e.g. "LAM_TEXT_COMMENT".
 - Value is optional, will be used as default if present.

The parameters can then be used as wildcards in the commands similar to attribute values.

Example:

LAM_SELECTION_ENV: Environment=dev;qa;prod

LAM_SELECTION_TENANT: Tenant=foo;bar

LAM_TEXT_COMMENT: Comment=no comment

LAM_TEXT_AMOUNT: Amount

user manual LAMLABEL="Clean" /bin/myscripts/cleanMailbox -u \$uid\$ -e \$LAM_SELECTION_ENV\$

user manual LAMLABEL="Extend" /bin/myscripts/extendMailbox -u \$uid\$ -e \$LAM_SELECTION_TENANT\$

user manual /bin/myscripts/syncWithCRM -u \$uid\$ -c \$LAM_TEXT_COMMENT\$

user manual LAMLABEL="Some app" /bin/myscripts/syncWithSomeApp -u \$uid\$ -a \$LAM_TEXT_AMOUNT\$

Manual scripts

| | |
|-------------|------------|
| Environment | dev |
| Tenant | foo |
| Comment | no comment |
| Amount | |

Mail actions

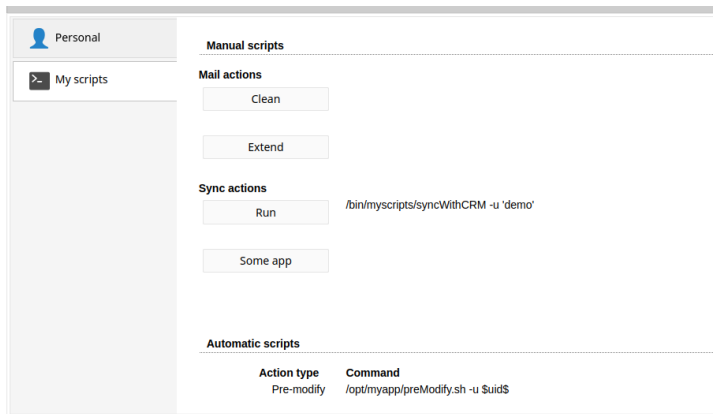
Clean

Extend

Output may contain HTML: If your scripts generate HTML output then activate this option.

Hide command in messages: You may want to prevent that your users see the executed commands. In this case activating this option will only show the command output but not the command itself.

You can see a preview of the commands which will be automatically executed on the "Custom scripts" tab. Here you can also run the manual scripts.



Sudo roles (LAM Pro)

You can manage your sudo roles in LDAP if you have installed the sudo-ldap package or compiled sudo with LDAP support [http://www.sudo.ws/sudo/readme_ldap.html].

To activate sudo management in LAM Pro edit your server profile and add the type "Sudo roles".

| | | |
|---------------|--|---|
| Samba domains | Samba 3 domain entries | + |
| Sudo roles | Sudo role management | + |
| Users | User accounts (e.g. Unix, Samba and Kolab) | + |

Sudo roles

Selected modules

Sudo role (sudoRole)*

✖

Available modules

Auto delete (autoDelete)

+

Custom fields (customFields)

+

Custom scripts (customScripts)

+

General information (generalInformation)

+

Now you can create sudo commands.

backupRootFileSystem

Backup script

SuffixsudoRoles ▼RDN identifiercn ?

>- Sudo role

Role name *

backupRootFileSystem

Description

Backup script

Users

user1

user2

Hosts

host1

host2

Commands

/etc/init.d/apache restart

/etc/init.d/exim restart

Run users

root

www-data

Run groups

group1

group2

Options

!authenticate

setenv

Not before

Not after

Order

The sudo roles in LDAP work similar to those in /etc/sudoers. You can specify who may run which commands as which user. It is also possible to specify options like NOPASSWD.

LDAP views based on nsview (LAM Pro)

LAM Pro supports LDAP views based on the "nsview" object class. These views allow to create an organizational unit that shows a subset of your LDAP content. The subset is determined by an LDAP filter.

Configuration:

To activate view management in LAM Pro edit your server profile and add the type "LDAP views".

Views

LDAP views based on nsview

Views

Selected modules

View (nsview)(*)

Available modules

Auto delete (autoDelete)

Custom fields (customFields)

Custom scripts (customScripts)

General information (generalInformation)













Now you are ready to create your views. Each view has a name, LDAP filter and an optional description.

Views

New viewFile uploadDelete selected views

dirsrv > de ▾

View count: 3

| Actions | Name | Filter | Description |
|--|-----------|---------------|------------------------------|
| Sort sequence <input type="checkbox"/> Filter ▾ | | | |
| <input type="checkbox"/>     | barcelona | (l=Barcelona) | Employees based in Barcelona |
| <input type="checkbox"/>     | munich | (l=Munich) | Employees based in Munich |
| <input type="checkbox"/>     | tokyo | (l=Tokyo) | Employees based in Tokyo |

munich

Suffix views

Employees based in Munich

RDN identifier ou ?

Name *munich

Filter * (l=Munich)

Description Employees based in Munich

Apache Guacamole (LAM Pro)


Apache Guacamole offers remote desktop connections based on RDP/VNC.


Configuration


Please create a new group or group of names type on tab "Account types".


General settingsAccount typesModulesModule settingsJobs


Available account types


 AliasesAlias entries+


 Asterisk extensionsAsterisk extensions entries+


 Automount entriesAutomount entries+


 Billing codesPyKota billing codes+

 Bind DNSBind DNS entries+

 Custom typeCustom entries+

 DHCPDHCP administration+


 GroupsGroup accounts (e.g. Unix and Samba)+

 Groups of namesGroup of names accounts+


Then add the Guacamole module on tab "Modules".


Apache Guacamole


Selected modules


 Apache Guacamole (guacamole)*


Available modules


 Auto delete (autoDelete)+

 Custom fields (customFields)+

 Custom scripts (customScripts)+

 General information (generalInformation)+

 Group of members (groupOfMembers)*+

 Group of names (groupOfNames)*+

Now you can manage the Guacamole entries with protocol and parameters.

The screenshot shows the Apache Guacamole configuration interface. At the top, there's a breadcrumb 'demo > guacamole'. Below it, a sidebar shows the 'Apache Guacamole' logo. The main area is titled 'Suffix guacamole' and 'RDN identifier cn'. It contains several fields: 'Name' with value 'demo', 'Description' with value 'Demo configuration', 'Configuration protocol' set to 'VNC', and 'Configuration parameters' with two entries: 'test=1' and 'test=2'. There are 'Owners' and 'Members' sections, each with a 'Change' button. At the bottom, it shows the path '(Claudia Bach) cbach > demo > People'.

Auto delete (LAM Pro)

This module allows to mark any new entry to be marked for auto deletion. The cleanup is done by the LDAP server itself. Please note that this will not delete any relations etc. in other entries (e.g. group memberships).

Requirements

- LDAP server with DDS (Dynamic Directory Services) support: your LDAP server needs to be configured to allow auto deletion of entries. See e.g. OpenLDAP configuration [<http://www.openldap.org/doc/admin24/overlays.html>].
- Your user has the right to set a deletion date. This is configured on your LDAP server via ACLs. E.g. OpenLDAP requires manage rights to attribute "entryTtl".

Restrictions

The maximum time for auto deletion is one year and six days. This is a restriction by the DDS standard itself. The deletion date can be extended for existing accounts but always by a maximum of one year and six days.

You should configure the maximum TTL value on your LDAP server as default is often much less than a year.

A deletion date on an existing entry cannot be removed but only be extended.

Configuration

You can add the auto delete module to any account type.

The screenshot shows the 'Users' configuration page in Apache Guacamole. It has a top navigation bar with tabs: 'General settings', 'Account types', 'Modules', 'Module settings', and 'Jobs'. The 'Modules' tab is selected. Below the tabs, there's a section titled 'Users'. It contains two columns: 'Selected modules' and 'Available modules'. The 'Selected modules' column lists four modules: 'Personal (inetOrgPerson)(*)', 'Unix (posixAccount)', 'Shadow (shadowAccount)', and 'Auto delete (autoDelete)'. Each has a red 'X' icon. The 'Available modules' column lists five modules: 'Account (account)(*)', 'Account locking (locking389ds)', 'AD LDS (windowsLDSUser)(*)', 'Asterisk (asteriskAccount)', and 'Asterisk voicemail (asteriskVoicemail)'. Each has a green '+' icon.

Usage

You can set a deletion time for any new account. Please note the restrictions above. If you get an error about invalid TTL then you might have exceeded the maximum TTL.

Existing accounts cannot be marked for deletion. But you may update the deletion date on existing accounts that are already marked for deletion.

Profile editor can be used to setup a default deletion time.

New user

Suffixdemo > People > test > deRDN identifiercn

Personal

Unix

Shadow

Auto delete

Deletion time
2023-02-02 16:00:51
Change?

General information

This module is available for all account types. It shows some internal information about the LDAP entries like the creation time and who modified the entry.

If you use the "memberOf" overlay in OpenLDAP then this will also show group memberships done by the overlay.

Claudia Bach

claudia.bach@ldap-account-manager.orgTelephone number 0123-4567-8900Mobile number 0123-4567-8922

Suffixdemo > People > test > deRDN identifieruid

Personal

Unix

Shadow

General information

Created by
Creation timeadmin > test > de
21.03.2007 18:03:30

Modified by
Modification timeadmin > test > de
02.02.2022 15:55:31

Has subentries
yes

Groups
222-1 > asteriskExt > test > de
xx_4-1 > asteriskExt > test > de
project1 > demo > gon > test > de
base > gon > test > de
sub12 > gon > test > de
demosub > demo > gon > test > de
demo > demo > gon > test > de
xx_3-1 > asteriskExt > test > de
xx_3-2 > asteriskExt > test > de
xx_3-3 > asteriskExt > test > de
demo > gon > test > de
testers > gon > test > de
business > gon > test > de
admins > demo > gon > test > de

181

Chapter 5. Tools

Profile editor

The account profiles are templates for your accounts. Here you can specify default values which can then be loaded when you create accounts. You may also load a template for an existing account to reset it to default values. When you create a new account then LAM will always load the profile named **"default"**. This account profile can include default values for all your accounts.
















Profile editor

Create a new profile

Groups


Create

Manage existing profiles

| | | |
|---|---------|--|
|  Groups | default |     |
|  Password policies | default |     |
|  Users | default |     |

You can enter the LDAP suffix, RDN identifier and various other attributes depending on account type and activated modules.

Profile editor

 **General settings**

Profile name *


LDAP suffix


RDN identifier


default


-

cn







 **Personal**

Initials

Description


Street


Post office box


Postal code


Location


State

















Import/export:

Profiles can be exported to and imported from other server profiles.

Profile editor

Create a new profile

Groups

Manage existing profiles






| | | |
|---|--------------------------------------|--|
|  Groups | <input type="text" value="default"/> |     |
|  Password policies | <input type="text" value="default"/> |     |
|  Users | <input type="text" value="default"/> |     |

Profile editor

Create a new profile

Groups

Manage existing profiles

| | | |
|--|--------------------------------------|--|
|  Groups | <input type="text" value="default"/> |     |
|--|--------------------------------------|--|

Import profiles

Profiles

- a_w10_las**
 - Groups: default
- d_w2012**
 - Groups 2: default
 - Groups: default
- d_zarafa**
 - Groups: a
 - Groups: aaa
 - Groups: default
 - Groups: test
 - Gruppen2: default
- d_zendServer**
 - Groups: a
 - Groups: aaa
 - Groups: default
 - Groups: test

Master password

There is a special export target called "*Global templates". All profiles exported here will be copied to all other server profiles (incl. new ones). But existing profiles with the same name are not overwritten. So a profile in global templates is treated as default profile for all server profiles.
















Use this if you would like to setup default profiles that are valid for all server profiles.

Profile editor

Create a new profile

Groups ▼ Create

Manage existing profiles

| | | |
|---|------------------------|---|
|  Groups | default ▼ |     |
|  Password policies | default |     |
|  Users | default ▼ |     |

Export profile ✕

Target server profile

Users

d_w2012

Users

Users 2

d_zarafa

Benutzer 1

Benutzer2

d_zendServer

Users

***Global templates**

Global templates

Master password

?

Ok Cancel

PDF editor

All accounts in LAM may be exported as PDF files. You can specify the page structure and displayed information by editing the PDF profiles.

PDF editor

Create a new PDF structure




Groups ▼

Create

Manage existing PDF structures

| | | |
|--|------------------------|--|
|  Groups | default ▼ |     |
|  Users | default ▼ |     |

Manage logos

printLogo.jpg (240 x 255)   

Browse...

No file selected.

Upload

Global template logos ?

Delete

printLogo.jpg












Master password * ?

Delete

When you export accounts to PDF then each account will get its own page inside the PDF. There is a headline on each page where you can show a page title. You may also add a logo to each page. To add more logos please use the logo management on the PDF editor main page.

PDF editor

| | |
|-------------------------------|--|
| Structure name * | default ? |
| Headline | User information |
| Logo | printLogo.jpg (240 x 255) ▼ |
| Folding marks | No ▼ |

| | |
|----------------------------|---|
| Personal user information | ↓  |
| Personal: Job title | ↓  |
| Personal: First name | ↑ ↓  |
| Personal: Last name | ↑ ↓  |
| Personal: Street | ↑ ↓  |
| Personal: Postal code | ↑ ↓  |
| Personal: Postal address | ↑ ↓  |
| Personal: Email address | ↑ ↓  |
| Personal: Telephone number | ↑ ↓  |
| Personal: Mobile number | ↑ ↓  |
| Personal: Fax number | ↑ ↓  |

The main part is structured into sections of information. Each section has a title. This can either be static text or the value of an attribute. You may also insert a static text block as section. Sections can be moved by using the arrows next to the section title.

Each section can contain multiple fields which usually represent LDAP attributes. You can simply add new fields by selecting the field name and its position. Then use the arrows to move the field inside the section.

Import/export:

PDF structures can be exported to and imported from other server profiles.

PDF editor

Create a new PDF structure

Groups

Manage existing PDF structures






| | | |
|--|--------------------------------------|--|
|  Groups | <input type="text" value="default"/> |     |
|  Users | <input type="text" value="default"/> |     |

PDF editor

Create a new PDF structure

Groups

Manage existing PDF structures

| | | |
|--|--------------------------------------|--|
|  Groups | <input type="text" value="default"/> |     |
|--|--------------------------------------|--|

Import PDF structures

PDF structures

u_waviz

Groups 2: default

Groups: default

d_zarafa

Groups: default

Groups: groupOfNames

Groups: groupOfUniqueNames

Groups: rfc2307

Groups: zarafa

Gruppen2: default

d_zendServer

Groups: default

Groups: groupOfNames

Groups: groupOfUniqueNames

Groups: rfc2307

Groups: zarafa

Master password

There is a special export target called "***Global templates**". All PDF structures exported here will be copied to all other server profiles (incl. new ones). But existing PDF structures with the same name are not overwritten. So a PDF structure in global templates is treated as default structure for all server profiles.



Use this if you would like to setup default PDF structures that are valid for all server profiles.

The screenshot shows the 'PDF editor' interface. At the top, there's a section 'Create a new PDF structure' with a 'Groups' dropdown and a 'Create' button. Below that is 'Manage existing PDF structures' with two rows: 'Groups' and 'Users', each with a 'default' dropdown and edit/delete icons. A modal dialog titled 'Export PDF structure' is open. It has a 'Target server profile' list with items like 'Users', 'd_w2012', 'd_zarafa', 'd_zendServer', and '*Global templates'. Below the list is a 'Master password' field. At the bottom right of the dialog are 'Ok' and 'Cancel' buttons.

Logo management:

You can upload image files to put a custom logo on the PDF files. The image file name must end with .png or .jpg.

Manage logos

printLogo.jpg (240 x 255)  

No file selected.

File upload

When you need to create lots of accounts then you can use LAM's file upload to create them. In contrast to LDAP import/export this operates on account type level.

LAM will read a CSV formatted file and create the related LDAP entries. Please check the data in you CSV file carefully. LAM will do less checks for the file upload than for single account creation.


At the first page please select the account type and what extensions should be activated.


Account creation via file upload


Here you can create multiple accounts by providing a CSV file.


Account type Users

Selected modules

 ☐ Personal

 ☒ Unix

 ☒ Password policy

 ☒ Custom scripts

Ok

The next page shows all available options for the file upload. You will also find a sample CSV file which can be used as template for your CSV file. All red options are required columns in the file. You need to specify a value for each account.

When you upload the CSV file then LAM first does some checks on this file. This includes syntax checks and if all required data was entered. No changes in the LDAP directory are done at this time.

If the checks were successful then LAM will ask again if you want to create the accounts. You will also have the chance to check the upload by viewing the changes in LDIF format.

File upload

Please provide a CSV formatted file with your account data. The cells in the first row must be filled with the column identifiers. The following rows represent one account for each row. Check your input carefully. LAM will only do some basic checks on the upload data.

Hint: Format all cells as text in your spreadsheet program and turn off auto correction.

Download sample CSV file



CSV file

Browse...

No file selected.

Create PDF files



PDF structure

default

Font

DejaVu

Upload file and create accounts

Columns

DN settings

| Name | Identifier | Example value | Default value | Possible values |
|--------------------|------------|-------------------------------|-------------------------------|-----------------|
| ? DN suffix | dn_suffix | ou=demo,ou=People,o=test,c=de | ou=demo,ou=People,o=test,c=de | |
| ? RDN identifier * | dn_rdn | uid | | uid, cn |
| ? Overwrite | overwrite | false | false | true, false |

Personal

| Name | Identifier | Example value | Default value | Possible values |
|---------------|---------------------------|------------------------------|---------------|-----------------|
| ? First name | inetOrgPerson_firstName | Steve | | |
| ? Last name * | inetOrgPerson_lastName | Miller | | |
| ? Initials | inetOrgPerson_initials | A.B. | | |
| ? Description | inetOrgPerson_description | Temp, contract till December | | |
| ? Job title | inetOrgPerson_title | President | | |

Multi edit

This tool allows you to modify a large list of LDAP entries in batch mode. You can add new attributes/object classes, remove attributes and set attributes to a specific value.

At the beginning, you need to specify where the entries are stored that should be changed. You can select an account suffix, the tree suffix or enter your own DN by selecting "Other".

Next, enter an additional LDAP filter to limit the entries that should be changed. E.g. use "(objectclass=inetOrgPerson)" to filter for users. You may also enter e.g. "(!objectClass=passwordSelfReset)" to match all accounts that do not yet have the password self reset feature.

Now, it is time to define the changes that should be done. The following operations are possible:

- **Add:** Adds an attribute value if not yet existing. Please do not use for single-value attributes that already have a value.
- **Modify:** Sets an attribute to the given value. If the attribute does not yet exist then it is added. If the attribute has multiple values then all other values are removed.
- **Delete:** Deletes the specified value from this attribute. If you leave the value field blank then all attribute values are removed.

Please note that all actions are run as separate LDAP commands. You cannot add an object class and a required attribute at the same time.

You can use the following wildcards to use existing attribute data of the entries:

- %attribute%: attribute value
- @attribute@: first character of attribute
- ?attribute?: first character of attribute in lower case
- !attribute!: first character of attribute in upper case
- ??attribute??: attribute in lower case
- !!attribute!!: attribute in upper case
- ((attribute)): space if attribute is set
- \$attribute|\$; attribute values separated by ";" (you can set other separators if you want)

Examples for attributes `gn="Steve"`, `sn="Miller"` and `memberUid=("user1", "user2")` (specified value -> resulting LDAP value):

Table 5.1.

| Value | Resulting LDAP value |
|------------------|---|
| my value | my value |
| %gn% | Steve |
| %gn%((gn))%sn% | Steve Miller (would be "Miller" if gn is empty) |
| \$memberUid , \$ | user1, user2 |

Multi edit

LDAP suffix

Users ?

LDAP filter

(objectClass=inetOrgPerson) ?

Operations ?

| Type | Attribute name | Value |
|-------|----------------|---------------|
| Add ▾ | street | My Street 123 |
| Add ▾ | | |
| Add ▾ | | |

Add more fields

Apply changes

Dry run

Dry run

You should always start with a dry run. It will not do any changes to your LDAP directory but print out all modifications that will be done. You will also be able to download the changes in LDIF format to use with `ldapmodify`. This is useful if you want to adjust some actions manually.

Progress

Dry run finished.

LDIF file

[ldif953431121372.ldif](#)

Log output

```
uid=shuber,ou=demo,ou=People,o=test,c=de
+street=My Street 123

uid=thausser,ou=demo,ou=People,o=test,c=de
+street=My Street 123
```

Apply changes

This will run the actions against your LDAP directory. You will see which accounts are edited in the progress area and also if any errors occurred.

Progress

uid=shuber,ou=demo,ou=People,o=test,c=de

Finished all operations.

LDAP import/export

Here you can import and export plain LDAP data. In contrast to file upload this operates on plain LDAP attribute level.

Import

The LDAP import supports input data in LDIF [https://en.wikipedia.org/wiki/LDAP_Data_Interchange_Format] format. You can provide plain text or upload an LDIF file.

The "Don't stop on errors" option will cause the import to continue even if entries could not be created.

Import

Export

Import

Source

☒ Text input

☐ File

LDIF data

☐ Don't stop on errors

Submit

Export

Here you can export your plain LDAP data as LDIF or CSV file.

Import

Export

Export

Base DN *

ou=demo,ou=group,o=test,c=de

Search scope

Sub (entire subtree)

Search filter

(objectClass=*)

Attributes

*

☐ Include system attributes

☐ Save as file

Export format

LDIF

End of line

Unix

Submit

Base DN: this is the starting point of the export. Enter a DN or press the magnifying glass icon to open the DN selection dialog.

Search scope: You can export just the base DN, base DN + its direct children or the whole subtree.

Search filter: this can be used to filter the entries by specifying a standard LDAP filter. The preselected filter "(objectclass=*)" matches all entries.

Attributes: the list of attributes that should be part of export. "*" matches all standard attributes (excluding system attributes).

Include system attributes: this will also include system attributes like the entry creation time and creator's DN.

Save as file: will save to file instead of printing the data on the web page.

Export format: you can select LDIF or CSV (e.g. for usage in spreadsheet applications).

End of line: use the one appropriate for your operating system.

OU editor

This is a simple editor to add/delete organisational units in your LDAP tree. This way you can structure the accounts.

OU editor

New organisational unit

Parent DN

demo > People > test > de ?

Name

Ok

Delete organisational unit

Organisational unit


demo > People > test > de ?

Ok

Tree view

The tree view provides a raw view on your LDAP directory. This feature is for people who are experienced with LDAP and need special functionality which the LAM account modules not provide. E.g. if you want to add a special object class to an account or edit attributes ignoring LAM's syntax checks.

To use this tool you will need to configure its suffix in your LAM server profile on first tab. You can also specify multiple suffixes separated by semicolon.

 **Tool settings**

Hidden tools

Server information

PDF editor

LDAP import/export

Tests

File upload

OU editor

WebAuthn devices

Schema browser

Multi edit

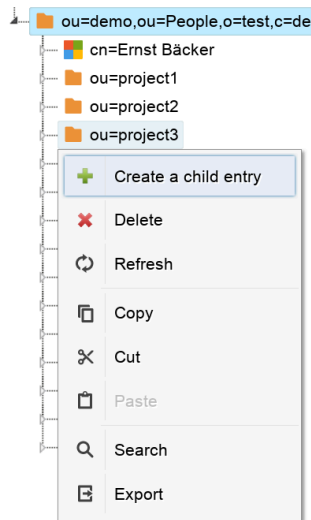
Profile editor

Tree view

Tree view

Tree suffix

ou=demo,ou=People,o=test,c=de ?



ou=demo,ou=People,o=test,c=de

Attributes

objectClass * organizationalUnit + -

ou * demo + -

Add new attribute

Attribute

Save

Internal attributes

[Show internal attributes](#)

Schema browser

Here you browse the schema of your LDAP server. You can view what object classes, attributes, syntaxes and matching rules are available. This is useful if you need to check if a certain object class is available.

Schema browser

| Object classes | Attribute types | Syntaxes | Matching rules |
|--|--|----------|----------------|
| Jump to an object class <input type="text" value="inetOrgPerson"/> | | | |
| inetorgperson | | | |
| OID | 2.16.840.1.113730.3.2.2 | | |
| Description | RFC2798: Internet Organizational Person | | |
| Type | structural | | |
| Inherits from | organizationalPerson | | |
| Optional attributes | audio businessCategory carLicense departmentNumber displayName employeeNumber employeeType givenName homePhone homePostalAddress initials jpegPhoto | | |

Server information

This shows information and statistics about your LDAP server. This includes the suffixes, used overlays, connection data and operation statistics. You will need "cn=monitor" setup to see all details. Some data may not be available depending on your LDAP server software.

Please see the following links how to setup "cn=monitor":

- OpenLDAP [<http://www.openldap.org/doc/admin24/monitoringslapd.html>]

- 389 server [http://directory.fedoraproject.org/wiki/Howto:CN%3DMonitor_LDAP_Monitoring]

Server information

| | |
|------------------------------|--|
| Managed suffixes | o=test,c=de |
| LDAP version | 3 |
| Config suffix | cn=config |
| Schema suffix | cn=Subschema |
| Dynamic subtrees | o=test,c=de |
| SASL mechanisms | DIGEST-MD5, NTLM, CRAM-MD5 |
| Name | OpenLDAP: slapd 2.4.57+dfsg-3 (May 15 2021 23:03:34) |
| Listeners | IP=0.0.0.0:389, IP=[::]:389, IP=0.0.0.0:636, IP=[::]:636, PATH=/var/run/slapd/ldapi |
| Backends | config, ldif, bdb, monitor |
| Overlays | dynlist, unique, memberof, dds, ppolicy, glue |
| Max. file descriptors | 1024 |

Server statistics

| | |
|---------------------|---------------------|
| LDAP entries | 4433 |
| Referrals | 0 |
| Start time | 04.03.2022 07:31:05 |
| Server time | 04.03.2022 08:02:37 |
| Uptime | 0:0:31 |

Connection statistics

| | |
|----------------------------|--------|
| Current connections | 8 |
| Total connections | 1070 |
| Bytes sent | 2.01MB |
| PDUs sent | 4680 |

Operation statistics

| | Initiated | Completed |
|-------------------|-----------|-----------|
| Bind | 70 | 70 |
| Unbind | 62 | 62 |
| Search | 179 | 178 |
| Add | 0 | 0 |
| Modify | 0 | 0 |
| Delete | 0 | 0 |
| Modify RDN | 0 | 0 |
| Compare | 0 | 0 |
| Abandon | 0 | 0 |
| Extended | 0 | 0 |
| Total | 311 | 310 |

WebAuthn devices

See the WebAuthn/FIDO2 appendix for an overview about WebAuthn/FIDO2 in LAM.

Here you can manage your webauthn/FIDO2 devices.

You can register additional security devices and remove old ones. In addition, you can set a name for your devices. This helps if you need to remove a device at a later point.

If no more device is registered then LAM will ask you for registration on next login.

WebAuthn devices

Register new device

| Name | Save | Registration | Last use | Delete |
|-------|---|---------------------|---------------------|---|
| key 1 |  | 2022-01-15 10:59:01 | 2022-03-04 20:04:54 |  |
| key 2 |  | 2022-03-04 20:05:12 | 2022-03-04 20:05:12 |  |
| key 3 |  | 2022-03-04 20:05:21 | 2022-03-04 20:05:21 |  |

Tests

This allows you to check if your LDAP schema is compatible with LAM and to find possible problems.








Lamdaemon test

LAM provides an external script to manage home directories and quotas. You can test here if everything is setup correctly.

If you get an error like "no tty present and no askpass program specified" then the path to the lamdaemon.pl may be wrong. Please see the lamdaemon installation instructions for setup details.

Lamdaemon test

LOCAL (localhost)

| | | |
|-----------------------------------|---|---|
| Lamdaemon server and path |  | Using localhost as lamdaemon remote server. |
| SSH connection |  | SSH connection established. |
| Execute lamdaemon |  | Lamdaemon successfully run. |
| Lamdaemon version |  | Lamdaemon successfully run. |
| Lamdaemon: check NSS LDAP |  | Lamdaemon successfully run. |
| Lamdaemon: Quota module installed |  | Lamdaemon successfully run. |
| Lamdaemon: read quotas |  | Lamdaemon successfully run. |

Lamdaemon test finished.

Schema test

This will test if your LDAP schema supports all object classes and attributes of the active LAM modules. If you get a message that something is missing please check that you installed all required schemas.

If you get error messages about object class violations then this test can tell you what is missing.

Schema test**Users**

| | | |
|-----------------|---|--------------------|
| Personal | ✓ | No problems found. |
| Unix | ✓ | No problems found. |
| Shadow | ✓ | No problems found. |
| Password policy | ✓ | No problems found. |

Groups

| | | |
|------|---|--------------------|
| Unix | ✓ | No problems found. |
|------|---|--------------------|

Password policies

| | | |
|-----------------|---|--------------------|
| Password policy | ✓ | No problems found. |
|-----------------|---|--------------------|

Chapter 6. Access levels and password reset page (LAM Pro)

You can define different access levels for each profile to allow or disallow write access. The password reset page helps your desktide support staff to reset user passwords.

Access levels

There are three access levels:

- **Write access (default)**

There are no restrictions. LAM admin users can manage account, create profiles and set passwords.

- **Change passwords**

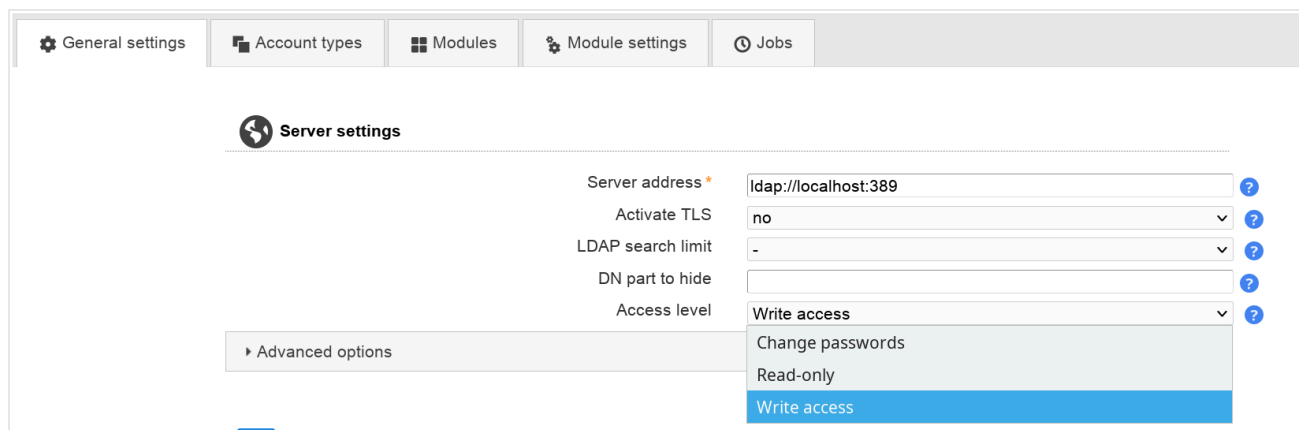
Similar to "Read only" except that the password reset page is available.

- **Read only**

No write access to the LDAP database is allowed. It is also impossible to manage account and PDF profiles.

Accounts may be viewed but no changes can be saved.

The access level can be set on the server configuration page:



Password reset page





































This special page allows your desktide support staff to reset the Unix and Samba passwords of your users. Account may also be (un)locked. If you set the access level to "Change passwords" then LAM will not allow any changes to the LDAP database except password changes via this page. The account pages will be still available in read-only mode.

You can open the password reset page by clicking on the key symbol on each user account:

Users

[New user](#) [File upload](#) [Delete selected users](#)

User count: 12

| Actions | User name | First name |
|--|----------------------|----------------------|
| Sort sequence | ▼ ▲ | ▼ ▲ |
| <input type="checkbox"/> Filter ▼ | <input type="text"/> | <input type="text"/> |
| <input type="checkbox"/>    | cbach | Claudia |
| <input type="checkbox"/>    | ebaecker | Ernst |
| <input type="checkbox"/>    | fhuber | Franz |
| <input type="checkbox"/>    | hmeier | Helmut |
| <input type="checkbox"/>    | hschuster | Heinz |
| <input type="checkbox"/>    | kmontag | Kerstin |
| <input type="checkbox"/>    | mfischer | Monika |
| <input type="checkbox"/>    | rmontag | Ramona |
| <input type="checkbox"/>    | shuber | Sepp |
| <input type="checkbox"/>    | smiller | Steve |
| <input type="checkbox"/>    | thausen | Thomas |
| <input type="checkbox"/>    | xmontag | Xaver |

There are three different options to set a new password. You can further restrict these options in server profile settings.

- **set random password and display it on screen**

This will set the user's password to a random value. The password will be 11 characters long with a random combination of letters, digits and "-_".

You may want to use this method to tell users their new passwords via phone.

- **set random password and mail it to user**

If the user account has set the mail attribute then LAM can send your user a mail with the new password. You can change the mail template to fit your needs. Please configure your LAM server profile to setup the sender address, subject and mail body. See here for setting up your SMTP server.

Using this method will prevent that your support staff knows the new password.

- **set specific password**

Here you can specify your own password.

Change password

Account details

| | |
|------------------|---------------------------------------|
| Full name | Claudia Bach |
| Email address | claudia.bach@ldap-account-manager.org |
| Telephone number | 0123-4567-8900 |
| User name | cbach |

Password change options

| | |
|----------------------------|-------------------------------------|
| Change Unix password | <input checked="" type="checkbox"/> |
| Force Unix password change | <input checked="" type="checkbox"/> |

Generate random password

This will set a random password and display it on the screen or send it to the user via mail.

☐ Display on screen ?
☒ Send via mail
☐ Both

Alternate address

cbach@rg-se.de ?

Change password

Set specific password

Here you can specify the new password yourself.

Password

Repeat password

Send via mail

☐

Change password

LAM will display contact information about the user like the user's name, email address and telephone number. This will help your desktide support to easily contact your users.

Options:

Depending on the account there may be additional options available.

- **Sync Samba NT/LM password with Unix password:** If a user account has Samba passwords set then LAM will offer to synchronize the passwords.
- **Unlock Samba account:** Locked Samba accounts can be unlocked with the password change.
- **Update Samba password timestamps:** This will set the timestamps when the password was changed (sambaPwdLastSet). Only existing attributes are updated. No new attributes are added.
- **Sync Kerberos password with Unix password:** This will also update the Heimdal Kerberos password.
- **Sync Asterisk (voicemail) password with Unix password:** Changes also the Asterisk passwords.
- **Force password change:** This will force the user to change his password at next login. This option supports Shadow, Samba 3 and PPolicy (automatically detected).

Account (un)locking:

Depending if the account includes a Unix/Samba extension and PPolicy is activated the page will show options to (un)lock the account. E.g. if the account is fully unlocked then there will be no unlocking options printed.

Lock account

Samba ☒

Lock account

Chapter 7. Self service (LAM Pro)

Preparations

OpenLDAP ACLs

By default only a few administrative users have write access to the LDAP database. Before your users may change their settings you must allow them to change their LDAP data.

Hint: The ACLs below are not required if you decide to run all operations as the LDAP bind user (option "Use for all operations").

This can be done by adding ACLs to your slapd.conf or slapd.d/cn=config/olcDatabase={1}bdb.ldif which look similar to these:

access to

attrs=userPassword

by self write

by anonymous auth

by * none

access to

attrs=mail,sn,givenName,telephoneNumber,mobile,facsimileTelephoneNumber,street,postalAddress,postOfficeBox,postalCode,roomNumber,shadowLastChange,passwordSelfResetAnswer,passwordSelfResetQuestion,passwordSelfResetBackupMail

by self write

by * read

If you do not want them to change all attributes then reduce the list to fit your needs. Some modules may require additional LDAP attributes. You can use the tree view to get the technical attribute names e.g. by selecting an user account.

Usually, the slapd.conf file is located in /etc/ldap or /etc/openldap.

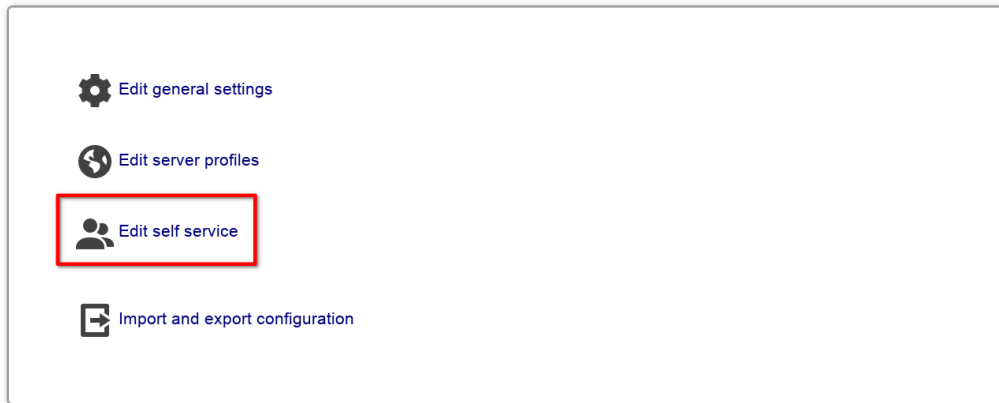
Other LDAP servers

There exist many LDAP implementations. If you do not use OpenLDAP you need to write your own ACLs. Please check the manual of your LDAP server for instructions.

Creating a self service profile

A self service profile defines what input fields your users see and some other general settings like the login caption.

When you go to the LAM configuration page you will see the self service link at the bottom. This will lead you to the self service configuration pages



Now we need to create a new self service profile. Click on the link to manage the self service profiles.

A screenshot of a dialog box titled "Please enter your master configuration password to change the self service profile:". The dialog contains two input fields: "Profile name" with a dropdown menu showing "d_demo", and "Password" with a text input field and a blue question mark icon. Below the fields is a blue "Ok" button. At the bottom of the dialog, there is a link "Manage self service profiles" highlighted with a red rectangle.

Specify a name for the new profile and enter your master configuration password (default is "lam") to save the profile.

Profile management

Add profile

Profile name

Type

Rename profile

Profile name

New profile name

Delete profile

Profile name

Now go back to the profile login and enter your master configuration password to edit your new profile.

Edit your new profile

General settings

On top of the page you see the link to the user login page. Copy this link address and give it to your users.

Below the link you can specify several options.

Self service configuration editor

Link to self service login page for your users: [Self service login](#)

General settings Page layout Module settings

Server settings

Server address

LDAP suffix

Activate TLS ☐

Follow referrals ☐

LDAP search attribute

LDAP user

LDAP password

Use for all operations ☐

Additional LDAP filter

Authentication method

Default language

Enforce language ☐

Time zone

Base URL

2-factor authentication

Provider

Table 7.1. General options

| | |
|------------------------|---|
| Server address | The address of your LDAP server. For LDAP+SSL use "ldaps://myserver" |
| Activate TLS | Activates TLS encryption. Please note that this cannot be combined with LDAP+SSL ("ldaps://"). |
| LDAP suffix | The part of the LDAP tree where LAM should search for users |
| LDAP search attribute | Here you can specify if your users can login with user name + password, email + password or other attributes. |
| Follow referrals | By default LAM will not follow LDAP referrals. This is ok for most installations. If you use LDAP referrals please activate the referral option in advanced settings. |
| LDAP user + password | The DN and password which is used to search for users in the LDAP database. It is sufficient if this DN has only read rights. If you leave these fields empty LAM will try to connect anonymously. |
| Use for all operations | By default LAM will use the credentials of the user that logged in to self service for read/modify operations. If you select this box then the connection user specified before will be used instead. Please note that this can be a security risk because the user requires write access to all users. You need to make sure that your LAM server is well protected. |
| Additional LDAP filter | Use this to enter an additional LDAP filter (e.g. "(objectClass=passwordSelfReset)") to reduce the number of accounts who may use self service. |
| Authentication method | The default method is user and password login. You can also enable HTTP authentication for your users. This way the web server is responsible to authenticate your users. LAM will use the given user name + password for the LDAP login. To setup HTTP authentication in Apache please see this link [http://httpd.apache.org/docs/2.2/howto/auth.html]. If you use Okta or OpenID for 2FA then you can also select to trust the 2FA provider. In this case the user does not need to enter any password in LAM itself (SSO). |
| Default language | This language is preselected on login. |
| Enforce language | Disables language selection and uses default language. |
| Time zone | Please provide your time zone. |
| Base URL | Please enter the base URL of your webserver (e.g. https://www.example.com). This is used to generate links in emails for password self reset and user self registration. |
| Login attribute label | This is the description for the LDAP search attribute. Set it to something which your users are familiar with. |
| Password field label | This text is placed as label for the password field on the login page. LAM will use "Password" if you do not enter any text. |
| Login caption | This text is displayed on the login page inside the login mask. |

| | |
|----------------------|--|
| Login footer | This text is displayed on the login page below the login mask. |
| Main page caption | This text is displayed on the self service main page where your users change their data. |
| Main page footer | This text is displayed as footer on the self service main page where your users change their data. |
| Page header | This HTML code will be placed on top of all self service pages. E.g. you can use this to place your custom logo. Any HTML code is permitted. |
| Base color | Here you can change the background color for the user pages. |
| Additional CSS links | Here you can specify additional CSS links to change the layout of the self service pages. This is useful to adapt them to your corporate design. Please enter one link per line. |

2-factor authentication

LAM supports 2-factor authentication for your users. This means the user will not only authenticate by user+password but also with e.g. a token generated by a mobile device. This adds more security because the token is generated on a physically separated device (typically mobile phone).

2-factor authentication

Provider
User name attribute
Base URL *
Label
Optional
Disable certificate check
Caption

privacyIDEA
uid
https://myserver
Optional
Disable certificate check

Quellcode

Two factor authentication

Please provide your PIN and token.

The token is validated by a second application. LAM currently supports:

- privacyIdea [<https://www.privacyidea.org/>]
- YubiKey [<https://www.yubico.com/>]
- Duo [<https://duo.com/>]
- WebAuthn/FIDO2 [<https://en.wikipedia.org/wiki/WebAuthn>]
- Okta [<https://www.okta.com/>]
- OpenID [<https://openid.net/>]

privacyIDEA

- Base URL: please enter the URL of your privacyIDEA instance
- User name attribute: please enter the LDAP attribute name that contains the user ID (e.g. "uid")
- Optional: By default LAM will enforce to use a token and reject users that did not setup one. You can set this check to optional. But if a user has setup a token then this will always be required.
- Disable certificate check: This should be used on development instances only. It skips the certificate check when connecting to verification server.

Please note that LAM needs to authenticate to privacyIDEA with the user's user name and password **WITHOUT** second factor. This is needed to get the list of tokens that are setup for the user. You can setup a separate policy (scope: authentication) for LAM inside privacyIDEA that has IP restriction ("Client" setting) to LAM's server IP and an action "otppin" "none".

YubiKey

- Base URLs: please enter the URL(s) of your YubiKey verification server(s). If you run a custom verification API such as yubiserver then enter its URL (e.g. <http://www.example.com:8000/wsapi/2.0/verify>). The URL needs to end with "/wsapi/2.0/verify". For YubiKey cloud these are "<https://api.yubico.com/wsapi/2.0/verify>", "<https://api2.yubico.com/wsapi/2.0/verify>", "<https://api3.yubico.com/wsapi/2.0/verify>", "<https://api4.yubico.com/wsapi/2.0/verify>" and "<https://api5.yubico.com/wsapi/2.0/verify>". Enter one URL per line.
- Client id: this is only required for YubiKey cloud. You can register here: <https://upgrade.yubico.com/getapikey/>
- Secret key: this is only required for YubiKey cloud. You can register here: <https://upgrade.yubico.com/getapikey/>
- Optional: By default LAM will enforce to use a token and reject users that did not setup one. You can set this check to optional. But if a user has setup a token then this will always be required.
- Disable certificate check: This should be used on development instances only. It skips the certificate check when connecting to verification server.

Duo

This requires to register a new "Web SDK" application in your Duo admin panel.

- User name attribute: please enter the LDAP attribute name that contains the user ID (e.g. "uid").
- Base URL: please enter the API-URL of your Duo instance (e.g. api-12345.duosecurity.com).
- Client id: please enter your client id.
- Secret key: please enter your client secret.

WebAuthn/FIDO2

See the WebAuthn/FIDO2 appendix for an overview about WebAuthn/FIDO2 in LAM.

Users will be asked to register a device during login if no device is setup.

- Domain: Please enter the WebAuthn domain. This is the public domain of the web server (e.g. "example.com"). Do not include protocol or port. Browsers will reject authentication if the domain does not match the web server domain.
- Optional: By default LAM will enforce to use a 2FA device and reject users that do not setup one. You can set this check to optional. But if a user has setup a device then this will always be required.

Okta

This requires to register a new application of type "Web".



There, you will need to configure LAM's 2-factor URLs as "Login redirect URIs" in the new application. They are "https://YOURDOMAIN/lam/templates/login2Factor.php" for admin interface and "https://YOURDOMAIN/lam/templates/selfService/selfService2Factor.php?scope=user&name=YOUR_PROFILE" for self service. You will get an error message during login with the URL to configure in case it was wrong.

On "Sign On" tab you need to add a rule that prompts for the factor.

LAM options:

- User name attribute: please enter the LDAP attribute name that contains the user ID (e.g. "mail").
- Base URL: please enter the URL of your Okta domain (e.g. https://mydomain.okta.com)
- Client id: please enter your application client id.
- Secret key: please enter your application secret key.


[← Back to Applications](#)

 **LAM** Active ▾  [View Logs](#)

[General](#) [Sign On](#) [Assignments](#) [Okta API Scopes](#)


Client Credentials Edit

Client ID



Public identifier for the client that is required for all OAuth flows.


Client secret



Secret used by the client to exchange an authorization code for a token. This must be kept confidential! Do not include it in apps which cannot keep it secret, such as those running on a client.

General Settings Edit

Okta domain



APPLICATION

Application label

LAM

Application type

Web

Allowed grant types

Client acting on behalf of itself

☒ Client Credentials


Client acting on behalf of a user

☒ Authorization Code

☐ Refresh Token

☐ Implicit (Hybrid)

LOGIN

Login redirect URIs 

OpenID

This will use an OpenID server as 2nd factor for authentication.

LAM options:

- User name attribute: please enter the LDAP attribute name that contains the user ID (e.g. "uid").
- Base URL: please enter the URL of your OpenID client URL. The URL is the one before the `"/.well-known/openid-configuration"`.
- Client id: please enter your application client id.
- Secret key: please enter your application secret key.

KeyCloack example configuration:

Create a new client, select "OpenID Connect" client type and enter a client ID.

The screenshot shows the 'General Settings' tab for a new client in Keycloak. The 'Client type' is set to 'OpenID Connect'. The 'Client ID' is 'demo'. The 'Name' and 'Description' fields are empty. The 'Always display in UI' toggle is turned off.

Now enable "Client authentication" and enter the valid redirect URLs in the last step.

The screenshot shows the 'Capability config' tab for the client. 'Client authentication' is turned on. 'Authorization' is turned off. Under 'Authentication flow', 'Standard flow' and 'Direct access grants' are checked. 'Implicit flow', 'Service accounts roles', 'OAuth 2.0 Device Authorization Grant', and 'OIDC CIBA Grant' are unchecked.

They are `"https://YOURDOMAIN/lam/templates/login2Factor.php"` for admin interface and `"https://YOURDOMAIN/lam/templates/selfService/selfService2Factor.php"` for self service. You will get an error message during login in case it was wrong. Then save the configuration.

The screenshot shows the 'Login settings' tab for the client. The 'Root URL' and 'Home URL' fields are empty. The 'Valid redirect URIs' field contains two URLs: `https://YOURDOMAIN/lam/templates/login2Factor.php` and `https://YOURDOMAIN/lam/templates/selfService/selfService2Factor.php`. There is a link to 'Add valid redirect URIs'. The 'Valid post logout redirect URIs' field is empty with a link to 'Add valid post logout redirect URIs'. The 'Web origins' field is empty with a link to 'Add web origins'.

Next, switch to tab "Credentials" to get the client secret.

Example configuration values:

- User name: uid
- Base URL: `http://openidserver/auth/realms/master`

- Client id: demo
- Secret key: 59bdf504-b76e-4138-8421-ef662b2c6c83

Remember device

You can allow users to remember the 2FA device for privacyIDEA, WebAuthn and YubiKey. When a device is remembered then users can login for the specified time without presenting their 2nd factor.

The password for the device remembering is used to authenticate the device data. It can be any long passphrase (use > 30 characters). LAM auto-generates one for you. If you change the passphrase then all device data gets invalid and users need to represent their 2nd factor again (which then can be saved again).

2-factor authentication

| | | |
|------------------------------|-------------------------------------|---|
| Provider | WebAuthn | ? |
| Domain | example.com | ? |
| Optional | <input type="checkbox"/> | ? |
| Allow to remember device | <input checked="" type="checkbox"/> | ? |
| Duration to remember devices | 10m | ? |
| Password to remember devices | | ? |

Login

After logging in with user + password LAM will ask for the 2nd factor. If the user has setup multiple factors then he can choose one of them.

Two factor verification

Please **provide** your code.

Serial number

ccccccjclkg, vvgdggkkuhbl, vvfkibcvvhrv

YubiKey

Submit

Cancel

Captcha

LAM Pro can optionally display a captcha to verify that logins are not from robots. Captchas will be displayed when you tick the checkbox to secure login with a captcha. The supported captcha providers are:

Google reCAPTCHA

You will need the site and secret key for your domain. They can be retrieved from here: <https://www.google.com/recaptcha>

Please note that your web server must be able to access "<https://www.google.com/recaptcha/api/siteverify>" to verify the captchas.

Friendly Captcha

Please enter your site (see applications) and API key. The web server must be able to contact "<https://api.friendlycaptcha.com>" for verification.

hCaptcha

Please enter your site and secret key (not API key). The web server must be able to contact "https://hcaptcha.com" for verification.

Captcha

| | | |
|----------------------|-------------------------------------|---|
| Captcha | Google reCAPTCHA | |
| reCAPTCHA site key | | ? |
| reCAPTCHA secret key | | ? |
| Secure login | <input checked="" type="checkbox"/> | ? |

Lamdaemon

This section is only required if you want to display file system quotas or create home directories via lamdaemon.

Server list format options:

- "server": "server" is the DNS name of your script server
- "server:NAME": NAME is the display name of this server
- "server:NAME:/prefix": /prefix is the directory prefix for all operations. E.g. creating a home directory "/home/user" would create "/prefix/home/user" then.

You need to provide a fixed user name.

Self service requires a SSH connection with SSH key. Please generate a SSH key pair and provide the location to the **private** key file. If the key is protected by a password you can also specify it here.

In case you want to create home directories during user self registration please provide the rights for it (e.g. 750).

Lamdaemon settings

| | | |
|-------------------------------|-------|---|
| Server list | | ? |
| Path to external script | | ? |
| User name | | ? |
| SSH key file | | ? |
| SSH key password | | ? |
| Rights for the home directory | 750 | ? |

Page layout

Here you can specify what input fields your users can see. It is also possible to group several input fields.

Please use the arrow signs to change the order of the fields/groups.

You may also set some fields as read-only for your users. This can be done by clicking on the lock symbol. Read-only fields can be used to show your users additional data on the self service page that must not be changed by themselves (e.g. first/last name).

Sometimes, you may want to set a custom label for an input field. Click on the edit icon to set your own label text (Personal: Department is relabeled as "Business unit" here).

Self service configuration editor

Link to self service login page for your users: [Self service login](#)

General settings
Page layout
Module settings

Input fields

Personal data

Change ↓ ×

Personal: First name

↓ × 🔒 ✎

Personal: Last name

↑ ↓ × 🔒 ✎

Personal: Email address

↑ ↓ × 🔒 ✎

Personal: Telephone number

↑ ↓ × 🔒 ✎

Personal: Mobile number

↑ ↓ × 🔒 ✎

Personal: Street

↑ ↓ × 🔒 ✎

Personal: Postal address

↑ ↓ × 🔒 ✎

Personal: Department

↑ × 🔒









Business unit





↻







Possible input fields

This is a list of input fields you may add to the self service page.

Table 7.2. Self service fields

| Account type | Option | Description |
|--|---|--|
|  Account locking | Password expiration | Read only value of password expiration date |
|  Asterisk (voicemail) | Sync Asterisk password with Unix password | This is a hidden field. It will update the Asterisk password each time the Unix password is changed. |
|  Group of names | Group memberships (read-only) | |
|  Kerberos | Sync Kerberos password with Unix password | This is a hidden field. It will update the Kerberos password each time the Unix password is changed. |
|  Kolab | Delegates | Allows to manage delegate permissions |
| | Invitation policy | Invitation policy management |
|  Password policy | Last password change | read-only |
|  Password self reset | Question | Security question selection |
| | Answer | Security answer |
| | Backup email | (External) backup email address that has no relation to user password. |
|  Personal | Business category | |
| | Car license | |
| | Department | |
| | Description | |
| | Email address | |
| | Fax number | |

| | | |
|---|--|--|
| | First name | |
| | Home telephone number | |
| | Initials | |
| | Job title | |
| | Last name | |
| | Location | |
| | Mobile number | |
| | Office name | |
| | Organisation | |
| | Organisational unit | |
| | Photo | Shows the user photo if set. The user may also remove the photo or upload a new one. |
| | Postal address | |
| | Postal code | |
| | Post office box | |
| | Registered address | |
| | Room number | |
| | State | |
| | Street | |
| | Telephone number | |
| | User certificates | Upload of user certificates in PEM or DER format |
| | User name | |
| | Web site | |
|  Mail routing | Local address (read-only) | |
| | Mail routing address (read-only) | |
|  OpenLDAP TOTP | OpenLDAP TOTP token + serial number | See OpenLDAP TOTP |
|  Quota | Quota (read-only) | Displays the user's system quote. Requires lamdaemon configuration. |
|  Samba 3 | Password | Input field to set a new NT/LM password. The attribute "sambaPwd-LastSet" is updated if it existed before. |
| | Sync Samba LM password with Unix password | This is a hidden field. It will update the Samba LM password each time the Unix password is changed. |
| | Sync Samba NT password with Unix password | This is a hidden field. It will update the Samba NT password each time the Unix password is changed. |
| | Update attribute "sambaPwd-LastSet" on password change | Updates the password timestamp when password is synchronized with Unix. |
| | Last password change (read-only) | Displays the date and time of the user's last password change. |

| | | |
|---|--|---|
|  Shadow | Account expiration date (read-only) | |
| | Last password change (read-only) | Displays the date and time of the user's last password change (Unix). |
|  Windows (AD, AD LDS, Samba 4) | Password | Change the user's password |
| | Location | |
| | Mail alias (read-only) | |
| | Office name | |
| | Postal code | |
| | Post office box | |
| | Proxy-Addresses (read-only) | |
| | State | |
| | Street | |
| | Telephone number | |
| | Web site | |
|  Unix | Common name | |
| | Group memberships (read-only) | |
| | Login shell | |
| | Password | This is also the source for several password synchronization options. |
| | Sync Unix password with Windows password | This is a hidden field. It will update the Unix password each time the Windows password is changed. |
|  WebAuthn | WebAuthn devices | Allows the user to manage his webauthn/FIDO2 security keys. |
|  Kopano | "Send as" privileges | Define user who may send mails as this user |
| | Email aliases | Email aliases |
|  PyKota | Balance (read-only) | Current balance for printing |
| | Total paid (read-only) | Total money paid |
| | Payment history | History of user payments |
| | Job history | History of printed jobs |

Module settings

This allows to configure some module specific options (e.g. custom scripts or password hash type).

Self service configuration editor

Link to self service login page for your users: [Self service login](#)

General settings
 Page layout
 Module settings

Custom scripts

Custom scripts

Output may contain HTML

☐

Hide command in messages

☐

Kerberos

Samba 3

LAM Pro can check the password history and minimum age for Samba 3 password changes. In this case please provide the LDAP suffix where your Samba 3 domain(s) are stored.

If you leave the field empty then no history and age checks will be done.

Password history: depending on your LDAP server you might need ascending or descending order. Just switch the setting if the password history is not correctly updated.

Samba 3

Domain suffix

o=test,c=de

Password history

yes - ordered ascending

Password self reset

Schema installation

Please install the LDAP schema as described [here](#).

Settings

You can allow your users to reset their passwords themselves. This will reduce your administrative costs for cases where users forget their passwords.

To enable this feature please activate the checkbox "Enable password self reset link".

Hint: Please note that LAM Pro uses security questions by default. Activate confirmation mails and then deactivate security questions if you want to use only email validation.

The password reset must be finished by the user within 24h or the process must be restarted.

The screenshot shows the top toolbar of the LibreOffice Writer application. The 'Quellcode' (Source Code) button is highlighted. The toolbar includes icons for text formatting: bold (B), italic (I), underline (U), strikethrough (ABC), subscript (x₂), and superscript (x²). It also features icons for text alignment (left, center, right, justified), bulleted and numbered lists, indentation, link and unlink, and a flag icon. Below the toolbar, the 'Stil' (Style) dropdown is set to 'Format', and the 'Schriftart' (Font) dropdown is set to 'Größe' (Size).

Send confirmation mail

Identification method, used LDAP attributes:

- Email: mail
- Employee number: employeeNumber
- Self service login attribute: same as configured on first tab of self service profile
- User name: uid
- User name and email address: uid and mail
- User name or email address: uid and mail

You can now configure the minimum answer length for password reset answers. This is checked when you allow you users to specify their answers via the self service. Additionally, you can specify the text of the password reset link (default: "Forgot password?"). The link is displayed below the password field on the self service login page.

Next, please enter the DN and password of an LDAP entry that is allowed to reset the passwords. This entry needs write access to the attributes `shadowLastChange`, `pwdAccountLockedTime` and `userPassword`. It also needs read

access to uid, mail, passwordSelfResetQuestion and passwordSelfResetAnswer. Please note that LAM Pro saves the password on your server file system. Therefore, it is required to protect your server against unauthorised access.

Please also specify the list of password reset questions that the user can choose.

Please note that self service and LAM admin interface are separated functionalities. You need to specify the list of possible security questions in both self service profile(s) and server profile(s).

You can inform your users via mail about their password change. The mail can include the new password by using the special wildcard "@@newPassword@@" . Additionally, you may want to insert other wildcards that are replaced by the corresponding LDAP attributes. E.g. "@@uid@@" will be replaced by the user name. See [here](#) for setting up your SMTP server.

LAM Pro can send your users an email with a confirmation link to validate their email address. Of course, this should only be used if the email account is independent from the user password (e.g. at external provider) or you use the backup email address feature. The mail body must include the confirmation link by using the special wildcard "@@resetLink@@" . Additionally, you may want to insert other wildcards that are replaced by the corresponding LDAP attributes. E.g. "@@uid@@" will be replaced by the user name.

There is also an option to skip the security question at all if email verification is enabled. In this case the password can be reset directly after clicking on the confirmation link. Please handle with care since anybody with access to the user's mail account can reset the password.

Captcha support

LAM Pro can optionally display a captcha to verify that password resets are not from robots. The captcha provider is configured on "General settings" tab.

Captchas will be displayed when you tick the checkbox to use a captcha.

Captcha

Use captcha ☒ ?

Troubleshooting:

1. You get messages like "Unable to find user account."

This can have multiple reasons:

- security questions enabled but no security question and/or answer set for this user
- user name + email combination does not exist
- no connection to LDAP server

Turn on logging in LAM's main configuration settings. The exact reason is logged on notice level.

2. You do not see security question and answer fields when logged into self service.

Probably, the user does not have the object class "passwordSelfReset" set. You can do this in admin interface. If you have multiple users to change then use the Multi Edit Tool to add the object class.

New fields for self service page

There are special fields that you may put on the self service page for your users. These fields allow them to change the reset questions and its answers. It is also possible to set a backup email address to reset passwords with an external email address.

| | | |
|------------------------|-------------|---------------|
| Add new group | | |
| | Group | |
| Add input field | | |
| | Input field | Answer |
| | Group | Personal data |
| | | Add ? |

This is an example how can be presented to your users on the self service page:

Password reset

| | |
|--------------|---|
| Question | What is the name of your favourite pet? |
| Answer | <input type="text"/> ✓ |
| Question | <input type="text"/> |
| Answer | <input type="text"/> ✓ |
| Question | <input type="text"/> |
| Answer | <input type="text"/> ✓ |
| Backup email | roland.gruber@rg-se.de |

Password reset link

After activating the password self reset feature there will be a new link on the self service login page. The text can be configured as described above (default: "Forgot password?").

Welcome to LAM self service. Please enter your user name and password.

User name

Password

Language

[Forgot password?](#)
[Register new account](#)

When a user clicks on the link then he will be asked for identification with his user name and email address.

Password self reset

User name *

LAM Pro will use this information to find the correct LDAP entry of this user. It then displays the user's security questions and input fields for his new password. If the answer is correct then the new password will be set. Additionally, pwdAccountLockedTime will be removed and shadowLastChange updated to the current time if existing.

Password self reset

| | |
|-----------------------------------|---|
| User name | roland2 |
| Question | What is the name of your favourite pet? |
| Answer * | <input type="text"/> |
| New password * | <input type="text"/> |
| Repeat password * | <input type="text"/> |
| <input type="button" value="Ok"/> | |

Prefilling the input fields

You might want to provide personalized URLs to your users that already prefill the fields in first step of password self reset. This can be done by adding an additional URL parameter with the attribute name in lower case.

LAM will not generate these URLs for you. This needs to be done by the system that provides the URL to your user.

Examples:

- `/lam/templates/selfService/selfServiceSP.php?scope=user&name=myProfile&page=passwordSelfReset&language=en_GB.utf8&uid=yourUserId`
- `/lam/templates/selfService/selfServiceSP.php?scope=user&name=myProfile&page=passwordSelfReset&language=en_GB.utf8&mail=yourUserId@company.com`
- `/lam/templates/selfService/selfServiceSP.php?scope=user&name=myProfile&page=passwordSelfReset&language=en_GB.utf8&uidmail=yourUserId` (for "user or email" method)
- `/lam/templates/selfService/selfServiceSP.php?scope=user&name=myProfile&page=passwordSelfReset&language=en_GB.utf8&customattribute=yourUserId`

User self registration

With LAM Pro your users can create their own accounts if you like. LAM Pro will display an additional link on the self service login page that allows you users to create a new account including email validation (see here for setting up your SMTP server).

You enable this feature in your self service profile. Just activate the checkbox "Enable self registration link".

Attributes: This is a list of additional attributes that the user can enter. Please note that user name, password and email address (attribute "mail") are mandatory anyway and need not be specified. Just in case you use the legacy attribute "email" for account it needs to be specified (attribute "mail" will then not be shown).

Each line represents one LDAP attribute. The settings are separated by "::". The first setting specifies the field type. The second setting is the LDAP attribute name (add ";binary" to attribute names for file upload). Depending on the field type you can enter additional options:

Table 7.3.

| Description | Type | Attribute name | First option | Second option | Third option |
|--|-----------|--|---|--|---|
| An optional input field that is displayed on the registration page. | optional | e.g. "givenName" or "jpegPhoto;binary" | Label that is displayed on page | Optional regular expression for validation (e.g. "[0-9a-zA-Z]+\$"). For binary fields the file name will be checked. | Validation message if value does not match validation expression. |
| A required input field that is displayed on the registration page. Self registration cannot be done if such a field is left empty by the user. | required | e.g. "sn" or "jpegPhoto;binary" | Label that is displayed on page | Optional regular expression for validation (e.g. "[0-9a-zA-Z]+\$"). For binary fields the file name will be checked. | Validation message if value does not match validation expression. |
| Constant attribute value, not visible for the user. Can be used to set some initial values or data that must not be edited by the user. | constant | e.g. "homeDirectory" | attribute value, supports wildcards to insert other attribute values (e.g. "@@uid@@") | | |
| Auto-numbering for attributes such as uidNumber. Will do a search for attribute values in the given range and use highest value + 1. | autorange | e.g. uidNumber | LDAP search base, e.g. ou=people,dc=company,dc=com | Minimum value, e.g. 1000 | Maximum value, e.g. 2000 |

For a syntax description of validation expressions see here [<http://perldoc.perl.org/perlre.html>]. Validation is optional, you can leave these options blank.

Examples:

Unix account:

optional::givenName::First name::/^[:alnum:]]+\$/:Please enter a valid first name.

required::sn::Last name::/^[:alnum:]]+\$/:Please enter a valid last name.

constant::homeDirectory::/home/@@uid@@

autorange::uidNumber::ou=people,dc=company,dc=com::10000::20000

If you use the object class "inetOrgPerson" and do not provide the "cn" attribute then LAM will set it to the user name value.

Active Directory/Samba4:

required::cn::Common Name::^[[:alnum:]]+\$/:u::Enter common name.

constant::userPrincipalName::@ @uid@ @ @samba4.test

constant::sAMAccountName::@ @uid@ @

constant::userAccountControl::512

Binary file:

required::jpegPhoto;binary::Photo::/.jp(e)?g\$/i::Please select a JPG file

Please note that only simple input boxes are supported for account registration. The user may log in to self service when his account was created to manage all his attributes.

Create home directory: This will create the home directory via lamdaemon. The user must have the following attributes: uid, uidNumber, gidNumber, homeDirectory

Approval

You can send the account request to an administrator for approval. The email will include links for approval/reject. Please use the wildcards @ @approveLink@ @ and @ @rejectLink@ @ for this.

If the request was rejected then no email will be sent to the user.

Approval settings

| | |
|-------------------|--|
| Approval required | <input checked="" type="checkbox"/> ? |
| From address * | <input type="text" value="lampro@rg-se.de"/> ? |
| To address * | <input type="text" value="approvers@ldap-account-manager.org"/> ? |
| Subject * | <input type="text" value="Account creation approval"/> ? |
| HTML format | <input type="checkbox"/> ? |
| Text * | <div><p>Hi,</p><p>a new user registered an account:</p><p>First name: @ @givenName@ @</p><p>Last name: @ @sn@ @</p><p>Email: @ @mail@ @</p><p>User name: @ @uid@ @</p><p>Approve: @ @approveLink@ @</p><p>Reject: @ @rejectLink@ @</p></div> ? |

Captcha support

LAM Pro can optionally display a captcha to verify that registrations are not from robots. The captcha provider is configured on "General settings" tab.

Captchas will be displayed when you tick the checkbox to use a captcha.

Captcha

Use captcha ☒ ?

User view:

The user can register by clicking on a link on the self service login page:

Here he can insert the data that you specified in the self service profile:

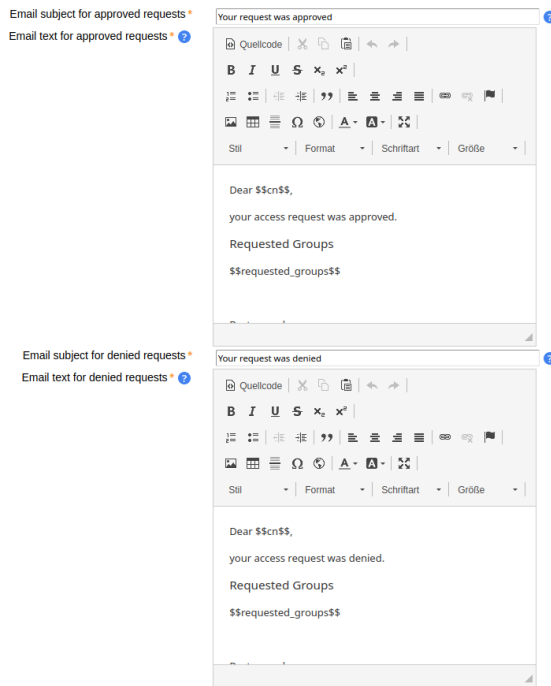
LAM will then send him an email with a validation link that is valid for 24 hours. When he clicks on this link then the account will be created in the self service user suffix. The DN will look like this: *uid=<user name>,...*

Request Access

Use this feature to allow your users to request access for group memberships/ownerships. Requests will require the approval by the group owners/managers and optionally a special approver group (leave empty for owner/manager approval only).

Setup cleanup

Please use the global cron job to clean any outdated requests or history entries. Here you can configure how long requests should be kept open and when to clean the history.



The email body texts support wildcards. You can use group owner/approver LDAP attributes in the form @@attribute@@ (e.g. @@uid@@ for the user name).

The requester's LDAP attributes can be used in the form \$\$attribute\$\$ (e.g. \$\$uid\$\$ for the user name). This is supported for mails to the group owners/managers and the approval/deny mails to the requester.

The wildcard \$\$requested_groups\$\$ will resolve to the requested groups. This is available for all mails.

In addition, \$\$requested_groups_member\$\$ and \$\$requested_groups_owner\$\$ can be used to inject the groups for member or owner requests (only emails for approved/denied requests).

Use the wildcard \$\$requested_type\$\$ in owner emails to get the request type (Member/Owner). The request type label is replaced in the language of the requester's self service session.

The wildcard \$\$requester_notes\$\$ resolves to the requester's optional notes. This is available for the mails to the group owners/managers.

Use \$\$request_comment\$\$ to inject the owner's or approver's comment. This can be used in mails to approvers and requesters.

The wildcards \$\$approveLink\$\$ and \$\$rejectLink\$\$ resolve to an URL that allows to approve/deny all requests listed in \$\$requested_groups\$\$\$. This is available for the mails to the group owners/managers and approvers. Use it as target URL for a link inside the email body.

The wildcard \$\$membershipRevocationTime\$\$ resolves to the revocation date of the membership if set. It is available for the mails to the approvers.

Example for owner email:

Dear @@cn@@,

a new access request was created by \$\$cn\$\$:

Requested groups: \$\$requested_groups\$\$

Reason: \$\$requester_notes\$\$

Approve all: \$\$approveLink\$\$
Deny all: \$\$rejectLink\$\$

Please check here (link to self service) for details.

Best regards,
IT team

Example for approver email:

Dear @ @cn@ @,

there are new access requests waiting for approval:

\$\$requested_groups\$\$

Comment: \$\$request_comment\$\$

Approve all: \$\$approveLink\$\$
Deny all: \$\$rejectLink\$\$

Please check here (link to self service) for details.

Best regards,
IT team

Example for approved/denied request email:

Dear \$\$cn\$\$,

your access request was approved/denied.
Requested groups: \$\$requested_groups\$\$
Comment: \$\$request_comment\$\$

Best regards,
IT team

Membership Revocation

You can select to revoke memberships after a given time. LAM will then remove them using global cron job once the time is reached. Please configure the following settings. If you use multiple self-service profiles for requester/owner/approver views then you need to configure this in the one that group owners use.

If you do not specify a revocation time then memberships/ownerships will not expire unless a custom revocation time is used. Allowing custom revocation times enables group owners to enter a custom date of revocation or no revocation time. The admin DN and password are used to perform the LDAP operation to remove the memberships.

| | | |
|------------------------------|---|--|
| Membership revocation time | <input type="text" value="365"/> | |
| Allow custom expiration time | <input type="checkbox"/> | |
| Admin DN | <input type="text" value="cn=admin,o=test,c=de"/> | |
| Admin password | <input type="password" value="...."/> | |

Field Configuration

Next, the fields need to be added to the "Page layout" tab. There are three fields:

- Request Access: Request access - User view that allows to initiate the process.
- Request Access: Owner view - Owner view for group owners.
- Request Access: Approver view - Approver view for approver group
- Request Access: History of own requests - History of the current user's requests
- Request Access: History of requests - History of all requests
 - Users that have no approver role see only requests for their managed groups
 - Users that are neither approver nor managing groups will not see anything
- Request access: Revocation information - Displays when roles will be revoked by the system
 - Users that have no approver role see only their managed groups
 - Users that are neither approver nor managing groups will not see anything

You can set custom labels using the pencil icon.

Request view

The user sees a button to open the new request dialog. Here the groups can be selected and an optional note can be provided.

Owner/approver view

Once the request is created, all owners of the respective groups get an email notification. They can then enter self service and view their open requests.

If an approver group is configured then its members will get an email notification after owner approval. In case no approver group is configured, the permissions are directly granted when the owner approves the request.

Owner approval

| Requester | Requested group | Note | Approve or deny |
|-----------|-----------------|---|--------------------------|
| thuber | project-xyz | Hi, i joined the company this month and would like to support on XYZ. | <input type="checkbox"/> |
| | | | <input type="checkbox"/> |

Approve selected Deny selected

Own request history

History of own requests

| Creation d... | Group | Request ty... | Note | Approvers | Archived at | Status |
|---------------|---------------|---------------|------|------------------|-------------|----------------------|
| 2024-05-01 | project-alpha | Owner | add | thuber, thuber@2 | 2024-05-01 | Approved by approver |
| 2024-05-01 | project-alpha | Member | add | thuber, thuber@2 | 2024-05-01 | Approved by approver |
| 2024-05-01 | project-alpha | Owner | add | thuber, thuber@2 | 2024-05-01 | Approved by approver |
| 2024-05-01 | project-alpha | Member | add | thuber, thuber@2 | 2024-05-01 | Approved by approver |

50 1

Request history

History of requests

| Requester | Creation... | Group | Request... | Note | Approvers | Archive... | Status |
|-----------|-------------|---------------|------------|------|-----------|------------|-------------------|
| thuber | 2024-05-01 | project-alpha | Member | add | thuber | 2024-05-01 | Denied by owner |
| thuber | 2024-05-01 | project-alpha | Owner | add | thuber | 2024-05-01 | Denied by owner |
| thuber | 2024-05-01 | project-alpha | Member | add | thuber | 2024-05-01 | Denied by owner |
| thuber | 2024-05-01 | project-alpha | Owner | add | thuber | 2024-05-01 | Approved by owner |

50 1

Custom fields

This module allows you to manage LDAP attributes that are not covered by the other LAM modules (e.g. if you use custom LDAP schemas). You can fully define how your input fields look like:

- Label
- LDAP attribute name
- Unique name for field
- Help text
- Read-only display
- Field type: text, password, text area, checkbox, radio buttons, select list, file upload, LDAP date (and time), constant
- Validation via regular expression
- Error message if validation fails

To create custom fields for the Self Service please edit your Self Service profile and switch to tab "Module settings". Here you can add a new field. Simply fill the fields and press on "Add".

Please note that the field name cannot be changed later. It is the unique ID for this field.

After you created your fields please press on "Sync fields with page layout". Now you can switch to tab "Page layout" and add your new fields like any other standard field.

Examples for fields and their representation in Self Service:

Text field:

Text fields allow to specify a validation expression and error message.

You can also enable auto-completion. In this case LAM will search all accounts for the given attribute and provide auto-completion hints when the user edits this field. This should only be used if there is a limited number of different values for this attribute.

In case your field is a date value you can show a calendar for easy editing.

Example calendar formats:

- d.m.Y: 31.12.2025
- Y-m-d: 2025-12-31
- d M, y: 31 Dec, 25
- d MM, Y: 31 December, 2025

You can escape wildcards with "\". E.g. "d.m.Y \d" will result in "31.12.2025 d".

Presentation in Self Service:

Password field:

You can also manage custom password fields. LAM Pro will display two fields where the user must enter the same password. You can hash the password if needed.

customPassword ✖

| | | |
|-----------------------|--------------------|---|
| Type | Password | |
| Label | Custom Password | ? |
| Attribute name * | userPassword | ? |
| Help text | | ? |
| Validation | Regular expression | |
| Validation expression | | ? |
| Validation message | | ? |
| Password hash type | ARGON2ID | ? |

Presentation in Self Service:

| | |
|-----------------|--------------------------|
| Custom Password | <input type="password"/> |
| | <input type="password"/> |

Text area:

This adds a multi-line field. The options are similar to text fields. Additionally, you can set the size with the number of columns and rows.

Please note that the validation expression should be set to multi-line. This is done by adding "m" at the end.

postalAddress ✖

| | | |
|-----------------------|---------------------------------------|---|
| Type | Text area | |
| Label | Postal address | ? |
| Attribute name * | postalAddress | ? |
| Help text | | ? |
| Required | <input checked="" type="checkbox"/> ? | |
| Validation | Regular expression | |
| Validation expression | /[0-9a-zA-Z]*\$/m | ? |
| Validation message | Invalid postal address | ? |
| Columns | 25 | ? |
| Rows | 4 | ? |

Presentation in Self Service:

| | |
|------------------|---|
| Postal address * | <input type="text" value="12345 City"/> |
|------------------|---|

Checkbox:

Sometimes you may want to allow only yes/no values for your LDAP attributes. This can be represented by a checkbox. You can specify the values for checked and unchecked. The default value is set if the LDAP attribute has no value.

carLicense ✖

| | | |
|-------------------------|----------------------------|---|
| Type | Checkbox | |
| Label | Car license | ? |
| Attribute name * | carLicense | ? |
| Help text | | ? |
| Value for "checked" * | yes | ? |
| Value for "unchecked" * | no | ? |
| Default value | <input type="checkbox"/> ? | |

Presentation in Self Service:

| | |
|-------------|-------------------------------------|
| Car license | <input checked="" type="checkbox"/> |
|-------------|-------------------------------------|

Radio buttons:

This displays a list of radio buttons where the user can select one value.

You can specify a mapping of LDAP attribute values and their display (label) on the Self Service page. To add more mapping fields please press "Add more mapping fields".

businessCategory ✖

Type: Radio buttons

Label: ?

Attribute name *: ?

Help text: ?

Value mapping ?

| Value | Label |
|----------------------------------|--|
| <input type="text" value=""/> | <input type="text" value="-"/> |
| <input type="text" value="hr"/> | <input type="text" value="Human Resources"/> |
| <input type="text" value="it"/> | <input type="text" value="IT"/> |
| <input type="text" value="man"/> | <input type="text" value="Management"/> |
| <input type="text" value="org"/> | <input type="text" value="Organisation"/> |

Presentation in Self Service:

Business category

☐ -
☐ Human Resources
☐ IT
☐ Management
☒ Organisation

Select list:

Select lists allow the user to select a value in a large list of options. The definition of the possible values and their display is similar to radio buttons.

You can also allow multiple values.

departmentNumber ✖

Type: Select list

Label: ?

Attribute name *: ?

Help text: ?

Allow multiple values: ☐ ?

Minimum: ?

Maximum: ?

Value mapping ?

| Value | Label |
|--|---|
| <input type="text" value="car"/> | <input type="text" value="Automotive"/> |
| <input type="text" value="it"/> | <input type="text" value="IT Consulting"/> |
| <input type="text" value="bank"/> | <input type="text" value="Financial Services"/> |
| <input type="text" value="insurance"/> | <input type="text" value="Insurance"/> |

Presentation in Self Service:

Department: ▼

Location:

LDAP search select list

This is similar to "Select list" but the options are read from LDAP. You can use this to define e.g. a DN selection list. Multiple values are supported.

manager ✖

| | |
|------------------------|---------------------------------------|
| Type | LDAP search select list |
| Label | Manager ? |
| Attribute name * | manager ? |
| Help text | Manager value ? |
| Allow multiple values | <input checked="" type="checkbox"/> ? |
| Minimum | 1 ? |
| Maximum | 3 ? |
| LDAP suffix * | |
| LDAP filter * | (objectclass=*) ? |
| Attribute name * | dn ? |
| Displayed attributes * | \$dn\$? |

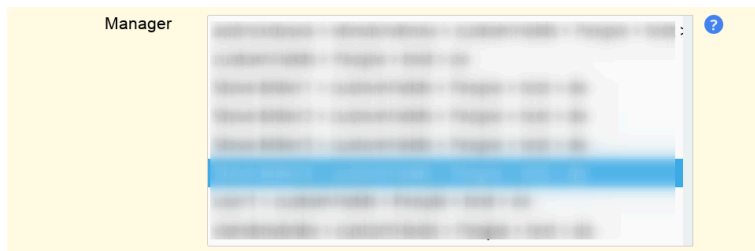
LDAP suffix: The LDAP DN that is used as starting point to search for LDAP entries.

LDAP filter: Only LDAP entries that match this filter will be used. If all entries should be used then use "(objectclass=*)".

Attribute name: The values of this attribute will be used to build the selection list.

Display attributes: List of attributes to show as label for the options in select box. Attribute wildcards are surrounded by "\$", e.g. "\$cn\$" will be replaced by "cn" attribute. Default is "\$dn\$".

Presentation:



LDAP date

Use this for LDAP attributes with syntax "Generalized Time" (1.3.6.1.4.1.1466.115.121.1.24).

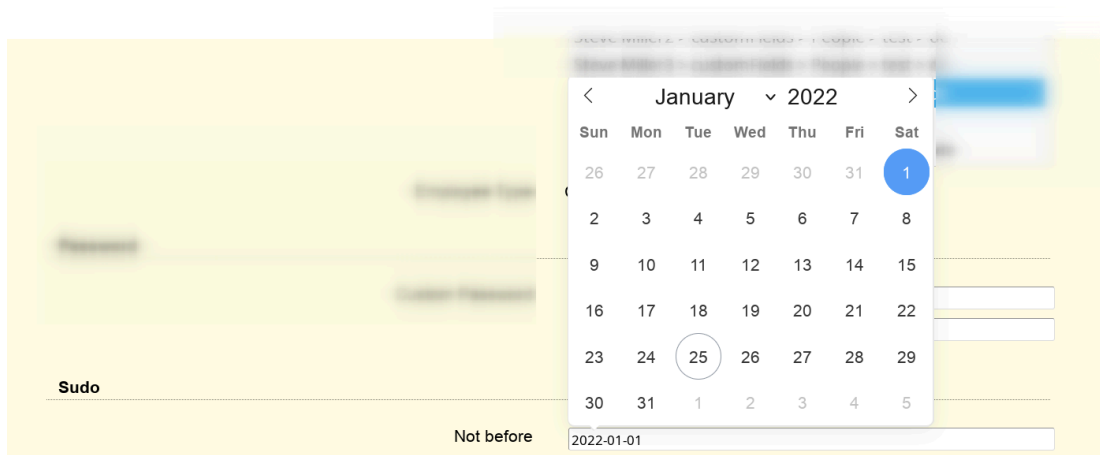
LAM will automatically set hour/minute/second to "0". If this is not intended please use type "LDAP date and time".

sudoNotBefore ✖

| | |
|-----------------------|----------------------------|
| Type | LDAP date |
| Label | Not before ? |
| Attribute name * | sudoNotBefore ? |
| Help text | |
| Required | <input type="checkbox"/> ? |
| Allow multiple values | <input type="checkbox"/> |
| Format | Y-m-d ? |
| Validation message | |

Presentation:

LAM will display a calendar to select the date.



LDAP date and time

Use this for LDAP attributes with syntax "Generalized Time" (1.3.6.1.4.1.1466.115.121.1.24).

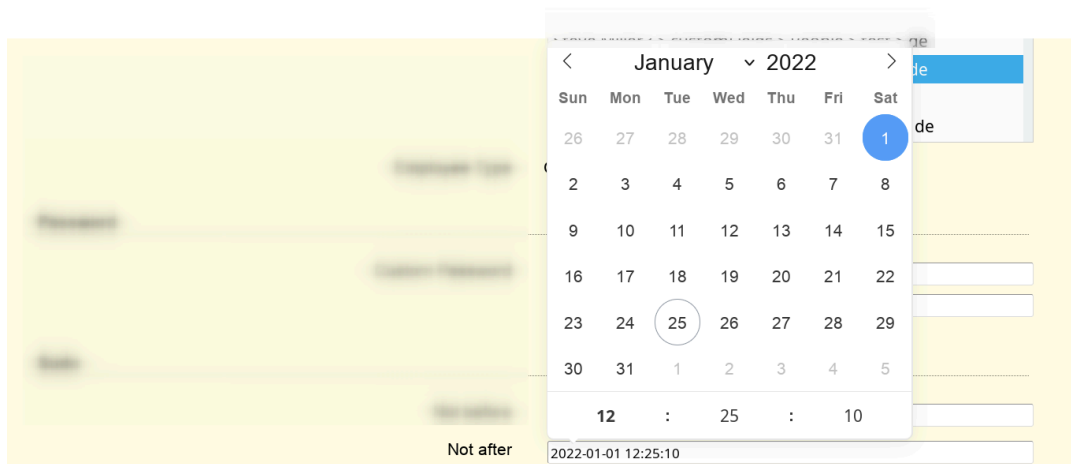
LAM can convert the displayed value to the configured time zone of your server/self service profile. In this case, please activate "Display in local time".

sudoNotAfter ✖

| | | |
|-----------------------|---------------------------------------|---|
| Type | LDAP date and time | |
| Label | Not after | ? |
| Attribute name * | sudoNotAfter | ? |
| Help text | | ? |
| Required | <input type="checkbox"/> ? | |
| Allow multiple values | <input type="checkbox"/> | |
| Format | Y-m-d H:i:s | ? |
| Validation message | | ? |
| Display in local time | <input checked="" type="checkbox"/> ? | |

Presentation:

LAM will display a calendar to select the date and time.



Constant value

This will set the attribute to a constant value. You can also specify wildcards to inject other attribute's values.

employeeType ✖

| | | |
|------------------|---------------|---|
| Type | Constant | |
| Label | Employee Type | ? |
| Attribute name * | employeeType | ? |
| Help text | help test | ? |
| Value * | !!cn!! | ? |

Wildcards:

- %attribute%: attribute value
- @attribute@: first character of attribute
- ?attribute?: first character of attribute in lower case
- !attribute!: first character of attribute in upper case
- ??attribute??: attribute in lower case
- !!attribute!!: attribute in upper case
- ((attribute)): space if attribute is set
- \$attribute|;\$: attribute values separated by ";" (you can set other separators if you want)

Examples for attributes gn="Steve", sn="Miller" and memberUid=("user1", "user2") (specified value -> resulting LDAP value):

Table 7.4.

| Constant value | Resulting LDAP value |
|------------------|---|
| my constant | my constant |
| %gn% | Steve |
| %gn%((gn))%sn% | Steve Miller (would be "Miller" if gn is empty) |
| \$memberUid , \$ | user1, user2 |

Presentation:

The LDAP value will be shown as text.

Employee Type ?

File upload:

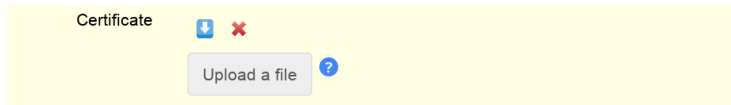
This is used for binary data. You can restrict uploaded data to a given file extension and set the maximum file size.

userCertificate ✖

| | | |
|-------------------|---------------------------------------|---|
| Type | File upload | |
| Label | Certificate | ? |
| Attribute name * | userCertificate;binary | ? |
| Help text | | ? |
| File extension | .crt | ? |
| Maximum file size | 100000 | ? |
| Multi value | <input checked="" type="checkbox"/> ? | |

Presentation:

The uploaded data may also be downloaded via LAM.



Validation expressions:

The validation expressions follow the standard of Perl regular expressions [<http://perldoc.perl.org/perlre.html>]. They start and end with a "/>". The beginning of a line is specified by "^" and the end by "\$".

Examples:

/^[a-z0-9]+\$/ allows small letters and numbers. The value must not be empty ("").

/^[a-z0-9]+\$/i allows small and capital letters ("i" at the end means ignore case) and numbers. The value must not be empty ("").

Special characters that must be escaped with "\": "\", ".", "(", ")"

E.g. /^[a-z0-9\\.]+\$/i

OpenLDAP TOTP

This allows your users to setup OpenLDAP TOTP tokens.

Please note that this requires to use a bind user that is also used for all operations. This user needs to be able to add/remove the TOTP object classes and attributes.

Server settings

| | | |
|------------------------|-------------------------------------|---|
| Server address * | 192.168.0.54 | ? |
| LDAP suffix * | ou=people,o=test,c=de | ? |
| Activate TLS | <input type="checkbox"/> | ? |
| Follow referrals | <input type="checkbox"/> | ? |
| LDAP search attribute | uid | ? |
| LDAP user | cn=admin,o=test,c=de | ? |
| LDAP password | | ? |
| Use for all operations | <input checked="" type="checkbox"/> | ? |
| Additional LDAP filter | | ? |
| HTTP authentication | <input type="checkbox"/> | ? |
| Default language | English (Great Britain) | ? |
| Enforce language | <input checked="" type="checkbox"/> | ? |
| Time zone | Europe/London | ? |
| Base URL | http://localhost | ? |

On page layout tab you can then add the fields for serial number (optional) and the token. Users will then be able to manage their token via self service.

TOTP

Change ↑ ×

OpenLDAP TOTP: Serial number ↓ × ✎

OpenLDAP TOTP: Register new token ↑ × ✎

On module settings tab please provide the DN of your TOTP settings entry (object class "oathTOTPParams").

OpenLDAP TOTP

OTP parameters

ou=People

Adapt the self service to your corporate design

LAM Pro allows you to integrate custom CSS style definitions and design the header of all self service pages. This way you can integrate your own logo and use your company's colors.

Custom header

The default LAM Pro header includes a logo and a horizontal line. You can enter any HTML code here. It will be included in the self services pages after the body tag.

Page header ?

CSS files

Usually, companies have regulations about their corporate design and use common CSS files. This assures a common appearance of all intranet pages (e.g. colors and fonts). To include additional CSS files just use the following setting for this task. The additional CSS links will be added after LAM Pro's default CSS link. This way you can overwrite LAM Pro's style.






Base color

Additional CSS links

Appendix A. LDAP schema files




Here is a list of needed LDAP schema files for the different LAM modules. For OpenLDAP we also provide a source where you can get the files.

Table A.1. LDAP schema files

| | Account type | Object class(es) | Schema name | Source | Notes |
|---|--|--|---|--|--|
|  | Unix accounts | posixAccount, shadowAccount, hostObject, posixGroup | nis.schema, rfc2307bis.schema, ldapns.schema (hostObject) | Part of OpenLDAP installation, part of libpam-ldap (ldapns.schema) | The rfc2307bis.schema is only supported by LAM Pro. Use the nis.schema if you do not want to upgrade to LAM Pro. |
|  | Address book entries | inetOrgPerson | inetorgperson.schema | Part of OpenLDAP installation | |
|  | Samba 3 accounts | sambaSamAccount, sambaGroupMapping, sambaDomain | samba.schema | Part of Samba tarball (examples/LDAP/samba.schema) | |
|  | Windows AD (Samba 4) | user, group, computer | | Samba 4 built-in | |
|  | AD LDS | user, group | | AD LDS built-in | |
|  | Kolab 2/3 users | kolabUser | kolab2/3.schema, rfc2739.schema | Part of Kolab 2/3 installation | |
|  | Asterisk (extension) | AsteriskSIPUser, AsteriskExtension | asterisk.schema | Part of Asterisk installation | |
|  | PyKota users, groups, printers and billing codes | pykotaObject, pykotaAccount, pykotaAccountBalance, pykotaGroup, pykotaPrinter, pykotaBilling | pykota.schema | Part of PyKota installation | |
|  | Mail routing | inetLocalMailRecipient | misc.schema | Part of OpenLDAP installation | |
|  | Hosts | hostObject, device | ldapns.schema | Part of libpam-ldap installation | The device object class is only available in LAM Pro. |
|  | Authorized services | authorizedServiceObject | ldapns.schema | Part of libpam-ldap installation | |
|  | Mail aliases | nisMailAlias | misc.schema | Part of OpenLDAP installation | |
|  | Qmail user | qmailUser | qmail.schema | Part of qmail_ldap [http:// | LAM Pro only |

| | Account type | Object class(es) | Schema name | Source | Notes |
|---|-------------------------|---|--------------------|---|---|
| | | | | www.nrg4u.com/ | |
|  | MAC addresses | ieee802device | nis.schema | Part of OpenLDAP installation | |
|  | IP addresses | ipHost | nis.schema | Part of OpenLDAP installation | LAM Pro only |
|  | Puppet | puppetClient | puppet.schema | Puppet on GitHub [https://github.com/puppetlabs/puppet/blob/master/ext/ldap/puppet.schema] | |
|  | EDU person | eduPerson | eduperson.schema | http://middleware.internet2.edu [http://middleware.internet2.edu/eduperson/] | |
|  | Simple Accounts | account | cosine.schema | Part of OpenLDAP installation | |
|  | SSH public keys | ldapPublicKey | openssh-lpk.schema | Included in patch from http://code.google.com/p/openssh-lpk/ | |
|  | SSH public keys (AD) | - | built-in | AD/Samba 4 built-in | |
|  | Filesystem quotas | systemQuotas | quota.schema | Linux DiskQuota [http://sourceforge.net/projects/linuxquota/] | |
|  | Group of (unique) names | groupOfNames, groupOfUniqueNames, groupOfMembers | core.schema | Part of OpenLDAP installation | LAM Pro only |
|  | Groups | organizationalRole | core.schema | Part of OpenLDAP installation | LAM Pro only |
|  | DHCP | dhcpOptions, dhcpSubnet, dhcpServer | dhcp.schema | docs/schema/dhcp.schema | The LDAP suffix should be set to your dhcpServer entry. |
|  | Bind dyndb-ldap | idnsZone, idnsRecord | schema.ldif | part of bind-dyn-db-ldap | LAM Pro only |
|  | Bind DLZ DNS | dlzZone, dlzHost, dlzSOARecord, dlzNSRecord, dlzARecord, dlzMXRecord, dlzCNameRe- | dlz.schema | part of Bind DLZ patch [http://bind-dlz.sourceforge.net/] | LAM Pro only |

| | Account type | Object class(es) | Schema name | Source | Notes |
|---|------------------------|---|---|---|------------------------------|
| | | cord, dlzPTR-Record | | | |
|  | Aliases | alias, uidObject | core.schema | Part of OpenLDAP installation | LAM Pro only |
|  | NIS netgroups | nisNetgroup | nis.schema | Part of OpenLDAP installation | |
|  | NIS objects | nisObject | nis.schema | Part of OpenLDAP installation | LAM Pro only |
|  | Automount objects | automount | autofs.schema, rfc2307bis.schema | Autofs LDAP | LAM Pro only |
|  | Oracle databases | orclNetService | oidbase.schema, oidnet.schema, oidrdbm-s.schema, alias.schema | Preinstalled on Oracle directory server, OpenLDAP schemas can be downloaded e.g. here [http://www.idevelopment.info/data/Oracle/DBA_tips/LDAP/LDAP_8.shtml] | LAM Pro only |
|  | Password policies | pwdPolicy, device | ppolicy.schema, core.schema | Part of OpenLDAP installation | LAM Pro only |
|  | PowerDNS | dNSDomain2, domainRelatedObject | dnsdomain2.schema | Part of OpenLDAP installation | LAM Pro only |
|  | FreeRadius users | radiusprofile | openldap.schema | Part of FreeRadius installation | |
|  | Heimdal Kerberos | krb5KDCEntry | hdb.schema | Part of Heimdal Kerberos installation | LAM Pro only |
|  | MIT Kerberos | krbPrincipal, krbPrincipalAux, krbTicketPolicyAux | kerberos.schema | Part of MIT Kerberos installation | LAM Pro only |
|  | Simple Security Object | simpleSecurityObject | core.schema | Part of OpenLDAP installation | LAM Pro only |
|  | Sudo roles | sudoRole | sudo.schema | Part of sudo-ldap installation | LAM Pro only |
|  | Kopano | kopano-user, kopano-contact, kopano-group, kopano-dynamicgroup, kopano-addresslist, kopano-server | kopano.ldif | Part of Kopano installation | LAM Pro only |
|  | IMAP mailboxes | - | - | - | Does not require any schema. |

| | Account type | Object class(es) | Schema name | Source | Notes |
|---|------------------|----------------------------|--------------------------|--|--|
|  | LDAP views | nsview, organizationalunit | built-in | Part of LDAP server installation (e.g. 389 server) | LAM Pro only |
|  | Apache Guacamole | guacConfig-Group | guacConfig-Group.ldif | Part of Guacamole Auth LDAP installation | LAM Pro only |
|  | All | dynamicObject | built-in with DDS module | Part of LDAP server installation | LAM Pro only, requires DDS extension on LDAP server side |

Appendix B. Security

LAM configuration passwords

LAM supports a two level authorization system for its configuration. Therefore, there are two types of configuration passwords:

- **master configuration password:** needed to change general settings, create/delete server profiles and self service profiles
- **server profile password:** used to change the settings of a server profile (e.g. LDAP server and account types to manage)

The master configuration password can be used to reset a server profile password. Each server profile has its own profile password.

Both password types are stored as hash values in the configuration files for enhanced security.

Use of SSL

The data which is transferred between you and LAM is very sensitive. Please always use SSL encrypted connections between LAM and your browser to protect yourself against network sniffers.

LDAP with SSL and TLS

SSL will be used if you use `ldaps://servername` in your configuration profile. TLS can be activated with the "Activate TLS" option.

If your LDAP server uses a SSL certificate of a well-know certificate authority (CA) then you probably need no changes. If you use a custom CA in your company then there are two ways to setup the CA certificates.

Setup SSL certificates in LAM general settings

This is much easier than system level setup and will only affect LAM. There might be some cases where other web applications on the same web server are influenced.

See [here](#) for details.

Setup SSL certificates on system level

This will make the CA certificates available also to other applications on your system (e.g. other web applications).

You will need to setup `ldap.conf` to trust your server certificate. Some installations use `/etc/ldap.conf` and some use `/etc/ldap/ldap.conf`. It is a good idea to symlink `/etc/ldap.conf` to `/etc/ldap/ldap.conf`. Specify the server CA certificate with the following option:

```
TLS_CACERT /etc/ldap/ca/myCA/cacert.pem
```

This needs to be the public part of the signing certificate authority. See "man ldap.conf" for additional options.

You may also need to specify the CA certificate in your Apache configuration by using the option "LDAPTrustedGlobalCert":

```
LDAPTrustedGlobalCert CA_BASE64 /etc/ldap/ca/myCA/cacert.pem
```

SELinux

In case your server has SELinux installed you might need to extend the SELinux ruleset. E.g. your webserver might not be allowed to write in /var/lib.

Read SELinux status

The following command will tell you if SELinux is running in Enforcing or Permissive mode.

Enforcing: access that does not match rules is denied

Permissive: access that does not match rules is granted but logged to audit.log

```
getenforce
```

Set SELinux to Permissive mode

This will just log any access violations. You will need this to get a list of missing rights.

```
setenforce Permissive
```

Now do any actions inside LAM that you need for your daily work (e.g. edit server profiles, manage LDAP entries, ...).

Extend SELinux rules

SELinux now has logged any violations to audit.log. You can use this now to extend your ruleset and enable enforcing later.

The following example is for httpd. You can also adapt it to e.g. nginx.

```
# build additional SELinux rules from audit.log
grep httpd /var/log/audit/audit.log | audit2allow -m httpdlocal -o httpdlocal.te
```

The httpdlocal.te might look like this:

```
module httpdlocal 1.0;
```

```
require {
    type httpd_t;
    type var_lib_t;
    class file { setattr write };
}
```

```
#===== httpd_t =====
```

```
##### WARNING 'httpd_t' is not allowed to write or create to var_lib_t.  Change the lab
##### $ semanage fcontext -a -t httpd_var_lib_t /var/lib/ldap-account-manager/config/la
##### $ restorecon -R -v /var/lib/ldap-account-manager/config/lam.conf
allow httpd_t var_lib_t:file { setattr write };
```

Now we can compile and install this rule:

```
# build module
checkmodule -M -m -o httpdlocal.mod httpdlocal.te
# package module
```

```
semodule_package -o httpdlocal.pp -m httpdlocal.mod
# install module
semodule -i httpdlocal.pp
```

Now you can switch back to Enforcing mode:

```
setenforce Enforcing
```

LAM should now work as expected with active SELinux.

Chrooted servers

If your server is chrooted and you have no access to `/dev/random` or `/dev/urandom` this can be a security risk. LAM stores your LDAP password encrypted in the session. LAM uses `rand()` to generate the key if `/dev/random` and `/dev/urandom` are not accessible. Therefore the key can be easily guessed. An attacker needs read access to the session file (e.g. by another Apache instance) to exploit this.

Protection of your LDAP password and directory contents

You have to install the OpenSSL extension for PHP to enable encryption.

Your LDAP password is stored encrypted in the session file. The key and IV to decrypt it are stored in two cookies. We use OpenSSL/AES to encrypt the password. All data that was read from LDAP and needs to be stored in the session file is also encrypted.

Apache configuration

Security headers

LAM already sets several security headers by default. For production machines it is recommended to run LAM with `"https://"` enabled. In this case the HSTS header should be set, e.g. like this:

```
Header always set Strict-Transport-Security "max-age=31536000"
```

This will enforce browsers to connect via `"https://"`. Please note that you need to make sure that your installation has a valid certificate now and in the future. The configuration requires `mod_headers` to be active.

Sensitive directories

LAM includes several `.htaccess` files to protect your configuration files and temporary data. Apache is often configured to not use `.htaccess` files by default. Therefore, please check your Apache configuration and change the override setting to:

```
AllowOverride All
```

If you are experienced in configuring Apache then you can also copy the security settings from the `.htaccess` files to your main Apache configuration.

If possible, you should not rely on `.htaccess` files but also move the `config` and `sess` directory to a place outside of your WWW root. You can put a symbolic link in the LAM directory so that LAM finds the configuration/session files.

Security sensitive directories:

config: Contains your LAM configuration and account profiles

- LAM configuration passwords (SSHA hashed)
- default values for new accounts
- directory must be accessible by Apache but needs not to be accessible by the browser

sess: PHP session files

- LAM admin password in clear text or OpenSSL encrypted
- cached LDAP entries in clear text or OpenSSL encrypted
- directory must be accessible by Apache but needs not to be accessible by the browser

tmp: temporary files

- PDF documents which may also include passwords
- images of your users
- directory contents must be accessible by browser but directory itself needs not to be browsable

Use LDAP HTTP authentication for LAM

With HTTP authentication Apache will be responsible to ask for the user name and password. Both will then be forwarded to LAM which will use it to access LDAP. This approach gives you more flexibility to restrict the number of users that may access LAM (e.g. by requiring group memberships).

First of all you need to load additional Apache modules. These are "mod_ldap [http://httpd.apache.org/docs/2.2/mod/mod_ldap.html]" and "mod_authnz_ldap [http://httpd.apache.org/docs/2.2/mod/mod_authnz_ldap.html]".

Next you can add a file called "lam_auth_ldap" to /etc/apache/conf.d. This simple example restricts access to all URLs beginning with "lam" to LDAP authentication.

```
<location /lam>
  AuthType Basic
  AuthBasicProvider ldap
  AuthName "LAM"
  AuthLDAPURL "ldap://localhost:389/ou=People,dc=company,dc=com?uid"
  Require valid-user
</location>
```

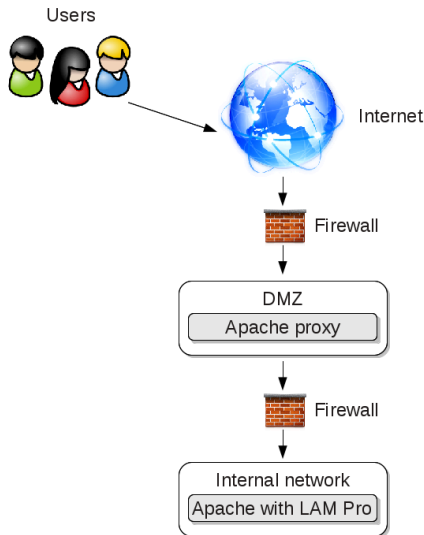
You can also require that your users belong to a certain Unix group in LDAP:

```
<location /lam>
  AuthType Basic
  AuthBasicProvider ldap
  AuthName "LAM"
  AuthLDAPURL "ldap://localhost:389/ou=People,dc=company,dc=com?uid"
  Require valid-user
  # force membership of lam-admins
  AuthLDAPGroupAttribute memberUid
  AuthLDAPGroupAttributeIsDN off
  Require ldap-group cn=lam-admins,ou=group,dc=company,dc=com
</location>
```

Please see the Apache documentation [http://httpd.apache.org/docs/2.2/mod/mod_authnz_ldap.html] for more details.

Self Service behind proxy in DMZ (LAM Pro)

In some cases you might want to make the self service accessible via the internet. Here is an Apache config to forward only the required URLs via a proxy server (lamproxy.company.com) in your DMZ to the internal LAM server (lam.company.com).



This configuration allows your users to open <https://lamproxy.company.com> which will then proxy the self service on the internal server.

```

<VirtualHost lamproxy.company.com:443>
    ServerName lamproxy.company.com
    ErrorLog /var/log/apache2/lam-proxy-error.log
    CustomLog /var/log/apache2/lam-proxy-access.log combined
    DocumentRoot /var/www/lam-proxy
    <Proxy *>
        Require all granted
    </Proxy>
    SSLProxyEngine on
    SSLEngine on
    SSLCertificateFile /etc/apache2/ssl/apache.pem
    ProxyPreserveHost On
    ProxyRequests off
    loglevel info

    # redirect front page to self service login page
    RewriteEngine on
    RedirectMatch ^/$ /templates/selfService/selfServiceLogin.php?scope=user\&name=

    # proxy required URLs
    ProxyPass /tmp https://lam.company.com/lam/tmp
    ProxyPass /sess https://lam.company.com/lam/sess
    ProxyPass /templates/lib https://lam.company.com/lam/templates/lib
    ProxyPass /templates/selfService https://lam.company.com/lam/templates/selfServ
    ProxyPass /templates/misc https://lam.company.com/lam/templates/misc
    ProxyPass /style https://lam.company.com/lam/style
    ProxyPass /graphics https://lam.company.com/lam/graphics

    ProxyPassReverse /tmp https://lam.company.com/lam/tmp
    ProxyPassReverse /sess https://lam.company.com/lam/sess
    ProxyPassReverse /templates/lib https://lam.company.com/lam/templates/lib
  
```

```
ProxyPassReverse /templates/selfService https://lam.company.com/lam/templates/s
ProxyPassReverse /templates/misc https://lam.company.com/lam/templates/misc
ProxyPassReverse /style https://lam.company.com/lam/style
ProxyPassReverse /graphics https://lam.company.com/lam/graphics
</VirtualHost>
```

Nginx configuration

There is no fully automatic setup of Nginx but LAM provides a ready-to-use configuration file.

Security headers

LAM already sets several security headers by default. For production machines it is recommended to run LAM with "https://" enabled. In this case the HSTS header should be set.

This will enforce browsers to connect via "https://". Please note that you need to make sure that your installation has a valid certificate now and in the future.

The example configurations below already include a commented example for "Strict-Transport-Security" (HSTS). You can activate it if needed.

RPM based installations

The RPM package has dependencies on Apache. Therefore, Nginx is not officially supported with this installation mode. Use tar.bz2 if you are unsure.

However, the package also includes an Nginx configuration file. Please include it in your server directive like this:

```
server {
    ...

    include /etc/ldap-account-manager/lam.nginx.conf;

    ...
}
```

The included config file uses "127.0.0.1:9000" for PHP. In case you run PHP with a socket please update the parameter "fastcgi_pass" to e.g. "/var/run/php8-fpm.sock".

DEB based installations

The LAM installation package ships with an Nginx configuration file. Please include it in your server directive like this:

```
server {
    ...

    include /etc/ldap-account-manager/nginx.conf;

    ...
}
```

The included config file uses PHP 8.2. In case you run with a different PHP version please update the parameter "fastcgi_pass" to e.g. "/var/run/php/php8.3-fpm.sock".

tar.bz2 based installations

Please add the following configuration snippet to your server directive.

You will need to change the alias location ("/usr/share/ldap-account-manager") and fastcgi_pass (e.g. "/var/run/php/php-fpm.sock" or "/var/run/php8-fpm.sock") to match your installation.

```
location /lam {
    index index.html;
    alias /usr/share/ldap-account-manager;
    autoindex off;
    # HSTS header to enforce https:// connections
    # add_header Strict-Transport-Security "max-age=31536000";

    location ~ /\.php$ {
        fastcgi_split_path_info ^(.+\.php)(/.+)$;
        fastcgi_pass unix:/var/run/php8-fpm.sock;
        fastcgi_index index.php;
        fastcgi_param SCRIPT_FILENAME $request_filename;
        include fastcgi_params;
    }

    location ~ /lam/(tmp/internal|sess|config|lib|help|locale) {
        deny all;
        return 403;
    }
}
```

WebAuthn/FIDO2

LAM allows to secure logins via WebAuthn/FIDO2 [<https://en.wikipedia.org/wiki/WebAuthn>]. This means your users login with their LDAP password and an additional hardware token (e.g. Yubico Security Key, Windows Hello and many more).

WebAuthn/FIDO2 is a very strong 2-factor-authentication method as it also checks the website domain. This prevents attacks via web proxies.

To use this feature you need to activate the 2-factor authentication in LAM.

LAM admin interface

Please activate WebAuthn/FIDO2 in your LAM server profile. Then users will be asked to authenticate via WebAuthn/FIDO2 on each login.

If no device is registered for a user then LAM will ask for this during login. Afterwards, users can manage their devices with the WebAuthn tool.

LAM Self Service

Please activate WebAuthn/FIDO2 in your LAM self service profile. Then users will be asked to authenticate via WebAuthn/FIDO2 on each login.

If no device is registered for a user then LAM will ask for this during login. Afterwards, users can manage their devices with the WebAuthn field.

Global device management

This is for cases where one of your users has no more access to his device and cannot login anymore. In this case you can delete his device(s) in the LAM main configuration.

Note that devices can only be deleted. Registration of devices can only be done by the user during login or on the management pages listed above.

Appendix C. Typical OpenLDAP settings

Some basic hints to configure the OpenLDAP server:

Size limit:

You will get a message like "LDAP sizelimit exceeded, not all entries are shown." when you hit the LDAP search limit.

OpenLDAP allows by default 500 return values per search, if you have more users/groups/hosts please change this:

slapd.conf:

e.g. "sizelimit 10000" or "sizelimit -1" for unlimited return values

slapd.d:

e.g. "olcSizeLimit: 10000" or "olcSizeLimit: -1" for unlimited return values in /etc/ldap/slapd.d/cn=config.ldif

Unique attributes:

There are cases where you do not want that same attribute values exist multiple times in your database. A good example are UID/GID numbers.

OpenLDAP provides the attribute uniqueness overlay [<http://www.openldap.org/doc/admin24/overlays.html>] for this task.

Example to force unique UID numbers:

In `/etc/ldap/slapd.d/cn=config/cn=module{0}.ldif` add "olcModuleLoad: {3}unique" (replace "3" with the highest existing number plus one).

Now in `/etc/ldap/slapd.d/cn=config/olcDatabase={1}bdb.ldif` add e.g. "olcUniqueURI: ldap:///uidNumber?sub"

Indices:

Indices will improve the performance when searching for entries in the LDAP directory. The following indices are recommended:

```
index objectClass eq
index default sub
index uidNumber eq
index gidNumber eq
index memberUid eq
index cn,sn,uid,displayName pres,sub,eq
# Samba 3.x
index sambaSID eq
index sambaPrimaryGroupSID eq
index sambaDomainName eq
```

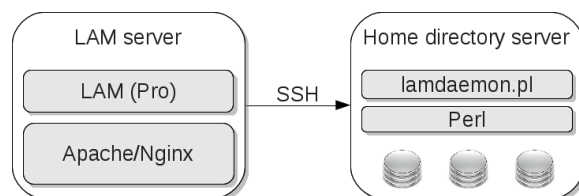
Appendix D. Setup for home directory and quota management

Lamdaemon.pl is used to modify quota and home directories on a remote or local host via SSH (even if homedirs are located on localhost).

If you want to use it you have to set up the following things to get it to work:

Installation

First of all, you need to install lamdaemon.pl on your remote server where LAM should manage homedirs and/or quota. This is usually a different server than the one where LAM is installed. But there is no problem if it is the same.



Debian based (e.g. also Ubuntu)

Please install the lamdaemon DEB package on your quota/homedir server.

RPM based (Fedora, CentOS, Suse, ...)


Please install the lamdaemon RPM package on your quota/homedir server.

Other

Please copy lib/lamdaemon.pl from the LAM tar.bz2 package to your quota/homedir server. The location may be anywhere (e.g. use /opt/lamdaemon). Please make the lamdaemon.pl script executable.

LDAP Account Manager configuration

- Set the remote or local host in the configuration (e.g. 127.0.0.1)
- Path to lamdaemon.pl, e.g. /srv/www/htdocs/lam/lib/lamdaemon.pl If you installed a DEB or RPM package then the script will be located at /usr/share/ldap-account-manager/lib/lamdaemon.pl.
- Your LAM admin user must be a valid Unix account. It needs to have the object class "posixAccount" and an attribute "uid". This account must be accepted by the SSH daemon of your home directory server. Do not create a second local account but change your system to accept LDAP users. You can use LAM to add the Unix account part to your admin user or create a new account. Please do not forget to setup LDAP write access (ACLs [<http://www.openldap.org/doc/admin24/access-control.html>]) if you create a new account.


 **Lamdaemon settings**

| | | |
|-------------------------|-------------------|---|
| Server list | localhost:LOCAL | ? |
| Path to external script | /lib/lamdaemon.pl | ? |
| User name | | ? |
| SSH key file | .key | ? |
| SSH key password | ***** | ? |

Rights for the home directory ?

| | Read | Write | Execute |
|-------|-------------------------------------|-------------------------------------|-------------------------------------|
| Owner | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |
| Group | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input checked="" type="checkbox"/> |
| Other | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |

Note that the builtin admin/manager entries do not work for lamdaemon. You need to login with a Unix account.

 **Security settings**

| | | |
|-----------------------|----------------------|---|
| Login method | Fixed list | ? |
| List of valid users * | cn=admin,o=test,c=de | ? |

OpenLDAP ACL location:

The access rights for OpenLDAP are configured in `/etc/ldap/slapd.conf` or `/etc/ldap/slapd.d/cn=config/olcDatabase={1}bdb.ldif`.

Setup sudo

The perl script has to run as root. Therefore we need a wrapper, sudo. Edit `/etc/sudoers` on host where homedirs or quotas should be used and add the following line:

```
$admin All= NOPASSWD: $path_to_lamdaemon *
```

\$admin is the admin user from LAM (must be a valid Unix account) and *\$path_to_lamdaemon* is the path to lamdaemon.pl.

Example:

```
myAdmin ALL= NOPASSWD: /srv/www/htdocs/lam/lib/lamdaemon.pl *
```

You might need to run the sudo command once manually to init sudo. The command "sudo -l" will show all possible sudo commands of the current user.

Attention: Please do not use the options "Defaults requiretty" and "Defaults env_reset" in `/etc/sudoers`. Otherwise you might get errors like "you must have a tty to run sudo" or "no tty present and no askpass program specified".

Setup Perl

We need an extra Perl module - Quota. To install it, run:

```
perl -MCPAN -e shell
install Quota
```

If your Perl executable is not located in `/usr/bin/perl` you will have to edit the path in the first line of lamdaemon.pl. If you have problems compiling the Perl modules try installing a newer release of your GCC compiler and the "make" application.

Several Linux distributions already include a quota package for Perl.

Set up SSH

Your SSH daemon must offer the password authentication method. To activate it just use this configuration option in `/etc/ssh/sshd_config`:

```
PasswordAuthentication yes
```

Troubleshooting

If you have problems managing quotas and home directories then these points might help:

- There is a test page for lamdaemon: Login to LAM and open Tools -> Tests -> Lamdaemon test
- Check `/var/log/auth.log` or its equivalent on your system. This file contains messages about all logins. If the ssh login failed then you will find a description about the reason here.
- Set sshd in debug mode. In `/etc/ssh/sshd_config` add these lines:

```
SyslogFacility AUTH  
LogLevel DEBUG3
```

Now check `/var/log/syslog` for messages from sshd.

Error message **"Your LAM admin user (...) must be a valid Unix account to work with lamdaemon!"**: This happens if you use the default LDAP admin/manager user to login to LAM. Please see [here](#) and setup a Unix account.

Appendix E. Setup password self reset schema (LAM Pro)

New installation

Please see [here](#) if you want to upgrade an existing schema version.

Schema installation

Please install the schema that comes with LAM Pro. The schema files are located in:

- tar.bz2: docs/schema
- DEB: /usr/share/doc/ldap-account-manager/docs/schema
- RPM: /usr/share/doc/ldap-account-manager-{VERSION}/schema

OpenLDAP with slapd.conf configuration

For a configuration with slapd.conf-file copy passwordSelfReset.schema to /etc/ldap/schema/ and add this line to slapd.conf:

```
include      /etc/ldap/schema/passwordSelfReset.schema
```

OpenLDAP with slapd.d configuration

For slapd.d configurations you need to upload the schema file passwordSelfReset.ldif via ldapadd command:

```
ldapadd -x -W -H ldap://localhost -D "cn=admin,o=test,c=de" -f passwordSelfReset.ldif
```

Please replace "localhost" with your LDAP server and "cn=admin,o=test,c=de" with your LDAP admin user (usually starts with cn=admin or cn=manager).

In some cases you might need to import directly on the OpenLDAP server as root:

```
ldapadd -Y EXTERNAL -H ldapi:/// -f passwordSelfReset.ldif
```

389 server

Please replace INSTANCE with installation ID, e.g. slapd-389ds.

```
cp passwordSelfReset-389server.ldif /etc/dirsrv/INSTANCE/schema/70pwdreset.ldif
systemctl restart dirsrv.target
```

Samba 4

The schema files are passwordSelfReset-Samba4-attributes.ldif and passwordSelfReset-Samba4-objectClass.ldif.

First, you need to edit them and replace "DOMAIN_TOP_DN" with your LDAP suffix (e.g. dc=samba4,dc=test).

Then install the attribute and afterwards the object class schema file:

```
ldbmodify -H /var/lib/samba/private/sam.ldb passwordSelfReset-Samba4-attributes.ldif --option="dsdb:schema update allowed"
```



```
ldbmodify -H /var/lib/samba/private/sam.ldb passwordSelfReset-Samba4-objectClass.ldif --option="dsdb:schema update allowed"
```

Windows

The schema file is passwordSelfReset-Windows.ldif.

First, you need to edit it and replace "DOMAIN_TOP_DN" with your LDAP suffix (e.g. dc=windows,dc=test).

Then install the schema file as administrator on a command line:

```
ldifde -v -i -f passwordSelfReset-Windows.ldif
```

This allows to set a security question + answer for each account.

Schema update

The schema files are located in:

- tar.bz2: docs/schema/updates
- DEB: /usr/share/doc/ldap-account-manager/docs/schema/updates
- RPM: /usr/share/doc/ldap-account-manager-{VERSION}/schema/updates

Schema versions:

1. Initial version (LAM Pro 3.6 - 4.4)
2. Added passwordSelfResetBackupMail (LAM Pro 4.5 - 5.5)
3. Multiple security questions (LAM Pro 5.6)

OpenLDAP with slapd.conf configuration

Install the schema file like a new install (skip modification of slapd.conf file).

OpenLDAP with slapd.d configuration

The upgrade requires to stop the LDAP server.

Steps:

1. Stop OpenLDAP with e.g. "/etc/init.d/slapd stop"
2. Delete the old schema file. It is located in e.g. "/etc/ldap/slapd.d/cn=config/cn=schema" and called "cn={XX}passwordselfreset.ldif" (XX can be any number)
3. Start OpenLDAP with e.g. "/etc/init.d/slapd start"
4. Install the schema file like a new install

Samba 4

Install the these update files by following the install instructions in the file. In case you you upgrade with a version difference of 2 or more you will need to apply all intermediate update scripts.

- samba4_version_1_to_2_attributes.ldif (upgrade from version 1 only)
- samba4_version_1_to_2_objectClass.ldif (upgrade from version 1 only)
- samba4_version_2_to_3_attributes.ldif (upgrade from version 2)
- samba4_version_2_to_3_objectClass.ldif (upgrade from version 2)

Please note that attributes file needs to be installed first.

Windows

Install the file(s) by following the install instructions in the file. In case you you upgrade with a version difference of 2 or more you will need to apply all intermediate update scripts.

- windows_version_1_to_2.ldif (upgrade from version 1 only)
- windows_version_2_to_3.ldif (upgrade from version 2)

Appendix F. Adapt LAM to your corporate design

There are cases where you might want to change LAM's default look'n'feel to better integrate it in your company network. Changes can be done like this:

Change colors, fonts and other parts with custom CSS

You can integrate custom CSS files in LAM. It is recommended to write a separate CSS file instead of modifying LAM's default files.

The CSS files are located in

DEB/RPM: /usr/share/ldap-account-manager/style
tar.bz2: style

LAM will automatically integrate all CSS files in alphabetical order. E.g. you can create a file called "900_my-Company.css" which will be added as last file.

In many cases it can be sufficient to overwrite some CSS variables. See top of 500_layout.css [https://github.com/LDAPAccountManager/lam/blob/develop/lam/style/500_layout.css] for defined variables.

Example:

This will change the background color of all pages to grey.

```
:root {  
    --lam-background-color-default: #E7E7E7;  
}
```

Change LAM logo:

```
div.lam-header-left img {  
    background: url("../graphics/key.svg") center no-repeat;  
    box-sizing: border-box;  
    width: 32px;  
    height: 32px;  
    padding-left: 32px;  
}
```

You can use the same way to change font/button colors and more.

Change header bar to mark different environments

```
.lam-header {  
    box-shadow: 0px 3px 2px -2px red;  
}
```

Other images

All images are located in

DEB/RPM: /usr/share/ldap-account-manager/graphics
tar.bz2: graphics

Please note that if you replace images then you need to reapply your changes every time you upgrade LAM.

Special changes with custom JavaScript

In rare cases it might not be sufficient to write custom CSS or replace some image files. E.g. you might want to add custom content to all pages.

For these cases you can add a custom JavaScript file that contains your code.

The JavaScript files are located in

DEB/RPM: /usr/share/ldap-account-manager/templates/lib
tar.bz2: templates/lib

LAM will automatically integrate all .js files in alphabetical order. E.g. you can create a file called "900_my-Company.js" which will be added as last file.

Self service

See [here](#) for self service customisations.

Appendix G. Clustering LAM

LAM is a web application based on PHP. Therefore, clustering is not directly a part of the application.

But here are some hints to run LAM in a clustered environment.

Application parts:

LAM can be divided into three parts

- Software
- Configuration files
- Session files and temporary data

Software:

This is the simplest part. Just install LAM on each cluster node. Please note that if you run LAM Pro you will need either one license for each active cluster node or a company license.

Configuration files:

These files include the LAM server profiles, account profiles, PDF structures, ... Usually, they do not change frequently and can be put on a shared file system (e.g. NFS, AFS, ...).

Please link "config" or "/var/lib/ldap-account-manager/config" to a directory on your shared file system.

Session data and temporary files:

These are critical because the files may change on every page load. There are basically two options:

- load balancer with session stickiness: In this case your load balancer will forward all requests of a user to the same cluster node. In this case you can keep the files locally on your cluster nodes. If you already have a load balancer then this is the simplest solution and performs best. The disadvantage is that if a node fails then all users connected to this node will lose their session and need to relogin.
- shared file system: This should only be used if your load balancer does not support session stickiness or you use a different system to distribute request across the cluster. A shared file system will decrease performance for all page loads.

Session data and temporary files are located in "tmp" + "sess" or "/var/lib/ldap-account-manager/tmp" + "/var/lib/ldap-account-manager/sess".

Appendix H. Troubleshooting

Reset configuration password

Server profiles

The password for the server profiles can be reset using the master configuration password. Open LAM configuration -> Edit server profiles -> Manage server profiles for this.

Main configuration

File system storage

In case you lost your master configuration password you need to manually edit the main configuration file (config.cfg) on the file system.

1. Locate config.cfg: On DEB/RPM installations it is in `/usr/share/ldap-account-manager/config` and for tar.bz2 in `config` folder.
2. Locate the "password" line in the file
3. Remove the password line in the configuration file

When you open LAM's start page you will now be asked to set a new password.

Database storage

Use a database admin tool (e.g. MySQL Workbench/phpMyAdmin) and connect to your database. Locate the table "main_configuration" and the row with value "config" in column "name". You will now need to edit this value which is in JSON format.

There is an entry "password" followed by a colon. Edit now the value in quotes that comes directly after. Enter your new password in clear text there. Do not remove the quotes.

```
{ "password": "{CRYPT:SHA512$6$wHnd1VwD0L4s.xsDz10tp1Q:nT8mFFxjhgA45R1rSEWbDVyJLcM4VY/e2VzhTkhkbf218G9M8WuaA--", "default": "rdetails": false, "logLevel": "7", "log": "/lam.log", "allowedHosts": "192.168.*.1
```

You can now login using your new password. Set the password once again via GUI in main configuration settings. This will then put again a hash value in the config.cfg file.

Reset IP restriction

If you entered a wrong value into the allowed IP list then LAM might lock you out of the system. You can reset the IP list like this.

File system storage

You need to manually edit the main configuration file (config.cfg) on the file system.

1. Locate config.cfg: On DEB/RPM installations it is in `/usr/share/ldap-account-manager/config` and for tar.bz2 in `config` folder.
2. Locate the "allowedHosts" entry in the file

3. Remove the line starting with "allowedHosts: "

Now you can edit the IP list again via LAM GUI.

Database storage

Use a database admin tool (e.g. MySQL Workbench/phpMyAdmin) and connect to your database. Locate the table "main_configuration" and the row with value "config" in column "name". You will now need to edit this value which is in JSON format.

There is an entry "allowedHosts" followed by a colon. Now, remove anything of the value in quotes that comes directly after. Do not remove the quotes.

Now you can edit the IP list again via LAM GUI.

Functional issues

Size limit

You will get a message like "LDAP sizelimit exceeded, not all entries are shown." when you hit the LDAP search limit.

- OpenLDAP: See the OpenLDAP settings to fix this.
- 389 server: set nsslapd-sizelimit in cn=config (may also be set per user)
- other LDAP servers: please see your server documentation

Invalid syntax errors:

If you get any strange errors like "Invalid syntax" or "Invalid DN syntax" please check if your LDAP schema matches LAM's requirements.

Schema test:

This can be done by running "Tools" -> "Tests" -> "Schema test" inside LAM.

If there are any object classes or attributes missing you will get a notice. See LDAP schema files for a list of used schemas. You may also want to deactivate unused modules in your LAM server profile (tab "Modules").

Schema test

| Users | | |
|-------------------|---|--------------------|
| Personal | ✓ | No problems found. |
| Unix | ✓ | No problems found. |
| Shadow | ✓ | No problems found. |
| Password policy | ✓ | No problems found. |
| Groups | | |
| Unix | ✓ | No problems found. |
| Password policies | | |
| Password policy | ✓ | No problems found. |

LDAP Logging:

If your schema is correct you can turn on LDAP logging to get more detailed error messages from your LDAP server.

OpenLDAP logging:

- slapd.conf: In /etc/ldap/slapd.conf turn logging on with the line "loglevel 256".
- slapd.d: In /etc/ldap/slapd.d/cn=config.ldif please change the attribute "olcLogLevel" to "Stats". Please add a line "olcLogLevel: Stats" if the attribute is missing.

After changing the configuration please restart OpenLDAP. It usually uses /var/log/syslog for log output.

PHP logging

Sometimes it can help to enable PHP logging inside LAM. You can do this in the logging area of LAM's main configuration. Set the logging option to "all" and check if there are any messages printed in your browser window. Please note that not every notice message is an error but it may help to find the problem.

Performance issues

LAM is tested to work with 10000 users with acceptable performance. If you have a larger directory or slow hardware then here are some points to increase performance.

The first step is to check if performance problems are caused by the LAM web server or the LDAP server. Please check which machine suffers from high system load (CPU/memory consumption).

High network latency may also be a problem. For large installations please make sure that LAM web server and LDAP server are located in the same building/server room.

If you run LAM on multiple nodes (DNS load balancing/hardware load balancer) then also check the clustering section.

LDAP server

Use indices

Depending on the queries it may help to add some more indices on the LDAP server. Depending on your LDAP software it may already suggest indices in its log files. See here for typical OpenLDAP indices.

Reduce query results by splitting LDAP management into multiple server profiles

If you manage a very large directory then it might already be separated into multiple subtrees (e.g. by country, subsidiary, ...). Do not use a single LAM server profile to manage your whole directory. Use different server profiles for each separated LDAP subtree where possible (e.g. one for German users and one for French ones).

Limit query results

LAM allows to set an LDAP search limit [general_settings] for each server profile. This will limit the number of entries returned by your LDAP server. Use with caution because it can cause problems (e.g. with automatic UID generation) when LAM is not able to read all entries.

The screenshot shows the 'Server settings' tab in the LAM web interface. The 'Server address' field is populated with 'ldap://ldap.example.com'. The 'Activate TLS' dropdown is set to 'no'. The 'LDAP search limit' dropdown is set to '-'. The 'DN part to hide' field is empty. The 'Access level' dropdown is set to 'Write access'. The 'Login method' dropdown is set to 'Fixed list'. The 'List of valid users' field is populated with 'uid=*,ou=users,dc=example,dc=com'. Below this, the 'Advanced options' section is expanded, showing 'Display name' as 'cn', 'Follow referrals' as 'no', 'Paged results' as 'yes', 'Show deleted entries' as 'yes', 'Referential integrity overlay' as 'no', and 'Hide password prompt for expired password' as 'no'.

LAM web server

Install a PHP accelerator

There are tools like OpCache [<http://php.net/manual/en/book.opcache.php>] (free) or Zend Server [<http://www.zend.com/en/products/server/>] (commercial) that provide caching of PHP pages to improve performance. They will reduce the time for parsing the PHP pages and IO load.

This is a simply way to enhance performance since OpCache is part of most Linux distributions.

OpCache statistics can be shown with opcache-status [<https://github.com/rlerdorf/opcache-status>].

PHP 5.6.27-0+deb8u1 with OpCache 7.0.6-dev

