

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 | 6 |
| System configuration | 7 |
| Upgrading LAM or migrate from LAM to LAM Pro | 8 |
| Upgrade LAM | 8 |
| Version specific upgrade instructions | 9 |
| Uninstallation of LAM (Pro) | 12 |
| Migration to a new server | 12 |
| 3. Configuration | 14 |
| General settings | 14 |
| License (LAM Pro only) | 14 |
| Security settings | 15 |
| Password policy | 15 |
| Logging | 16 |
| Additional options | 16 |
| Change master password | 16 |
| Server profiles | 16 |
| Manage server profiles | 16 |
| Editing a server profile | 17 |
| Cron jobs (LAM Pro) | 23 |
| Typical scenarios | 29 |
| 4. Managing entries in your LDAP directory | 31 |
| Typical usage scenarios | 32 |
| Users | 33 |
| Personal | 35 |
| Unix | 38 |
| Group of names and group of members (LAM Pro) | 41 |
| Organizational roles (LAM Pro) | 41 |
| Shadow | 42 |
| NIS net groups | 42 |
| Password self reset (LAM Pro) | 43 |
| Hosts | 44 |
| Samba 3 | 44 |
| Windows (Samba 4) | 46 |
| Filesystem quota (lamdaemon) | 48 |
| Filesystem quota (LDAP) | 49 |
| Kolab | 49 |
| Asterisk | 50 |
| EDU person | 50 |
| PyKota | 50 |
| Password policy (LAM Pro) | 51 |
| Account locking for 389ds (LAM Pro) | 52 |
| FreeRadius | 53 |
| Heimdal Kerberos (LAM Pro) | 54 |
| MIT Kerberos (LAM Pro) | 54 |
| NIS mail aliases | 55 |
| Courier mail | 56 |

| | |
|--|-----|
| Qmail (LAM Pro) | 57 |
| Mail routing | 57 |
| SSH keys | 58 |
| Authorized services | 58 |
| IMAP mailboxes | 59 |
| IP addresses (LAM Pro) | 60 |
| Account | 60 |
| Groups | 61 |
| Unix | 61 |
| Unix groups with rfc2307bis schema (LAM Pro) | 62 |
| Samba 3 | 63 |
| Windows (Samba 4) | 64 |
| Kolab | 65 |
| Mail routing | 65 |
| Quota | 66 |
| PyKota | 66 |
| Hosts | 67 |
| Account | 67 |
| Device (LAM Pro) | 67 |
| Samba 3 | 67 |
| Windows (Samba 4) | 67 |
| IP addresses (LAM Pro) | 68 |
| MAC addresses | 68 |
| Puppet | 68 |
| NIS net groups | 69 |
| Samba 3 domains | 70 |
| Group of (unique) names and group of members (LAM Pro) | 71 |
| Organizational roles (LAM Pro) | 72 |
| Asterisk | 73 |
| Kopano (LAM Pro) | 74 |
| Users | 74 |
| Contacts | 76 |
| Groups | 77 |
| Address lists | 78 |
| Dynamic groups | 78 |
| Servers | 79 |
| Zarafa (LAM Pro) | 80 |
| Configuration | 80 |
| Kolab shared folders | 84 |
| DHCP | 85 |
| Bind DLZ (LAM Pro) | 88 |
| Aliases (LAM Pro) | 92 |
| Mail aliases | 92 |
| NIS mail aliases | 92 |
| Courier mail aliases | 93 |
| NIS net groups | 93 |
| NIS objects (LAM Pro) | 93 |
| Automount objects (LAM Pro) | 94 |
| Oracle databases (LAM Pro) | 94 |
| Password policies (LAM Pro) | 96 |
| PyKota printers | 96 |
| PyKota billing codes | 97 |
| Custom fields (LAM Pro) | 97 |
| Custom scripts (LAM Pro) | 104 |
| Sudo roles (LAM Pro) | 106 |
| LDAP views based on nsvie (LAM Pro) | 107 |
| General information | 107 |
| Tree view (LDAP browser) | 108 |

| | |
|---|-----|
| 5. Tools | 109 |
| Profile editor | 109 |
| File upload | 110 |
| Multi edit | 111 |
| OU editor | 112 |
| PDF editor | 112 |
| Schema browser | 114 |
| Server information | 114 |
| Tests | 115 |
| Lamdaemon test | 115 |
| Schema test | 115 |
| 6. Access levels and password reset page (LAM Pro) | 117 |
| Access levels | 117 |
| Password reset page | 117 |
| 7. Self service (LAM Pro) | 120 |
| Preparations | 120 |
| OpenLDAP ACLs | 120 |
| Other LDAP servers | 120 |
| Creating a self service profile | 120 |
| Edit your new profile | 121 |
| General settings | 121 |
| Page layout | 124 |
| Module settings | 126 |
| Samba 3 | 126 |
| Password self reset | 127 |
| User self registration | 129 |
| Custom fields | 131 |
| Adapt the self service to your corporate design | 136 |
| Custom header | 136 |
| CSS files | 136 |
| A. LDAP schema files | 137 |
| B. Security | 140 |
| LAM configuration passwords | 140 |
| Use of SSL | 140 |
| LDAP with SSL and TLS | 140 |
| Setup SSL certificates in LAM general settings | 140 |
| Setup SSL certificates on system level | 140 |
| Selinux | 141 |
| Chrooted servers | 142 |
| Protection of your LDAP password and directory contents | 142 |
| Apache configuration | 142 |
| Sensitive directories | 142 |
| Use LDAP HTTP authentication for LAM | 143 |
| Self Service behind proxy in DMZ (LAM Pro) | 143 |
| Nginx configuration | 145 |
| RPM based installations | 145 |
| DEB based installations | 145 |
| tar.bz2 based installations | 145 |
| C. Typical OpenLDAP settings | 147 |
| D. Setup of email (SMTP) server | 148 |
| E. Setup for home directory and quota management | 149 |
| Installation | 149 |
| LDAP Account Manager configuration | 149 |
| Setup sudo | 150 |
| Setup Perl | 150 |
| Set up SSH | 150 |
| Troubleshooting | 150 |
| F. Setup password self reset schema (LAM Pro) | 152 |

| | |
|---|-----|
| New installation | 152 |
| Schema update | 153 |
| G. Adapt LAM to your corporate design | 155 |
| H. Clustering LAM | 157 |
| I. Troubleshooting | 158 |
| Reset configuration password | 158 |
| Functional issues | 158 |
| Performance issues | 159 |
| LDAP server | 159 |
| LAM web server | 160 |

List of Tables

| | |
|------------------------------------|-----|
| 1.1. Glossary | 3 |
| 2.1. Locales | 8 |
| 3.1. Options | 25 |
| 3.2. Options | 26 |
| 3.3. Options | 27 |
| 3.4. Options | 27 |
| 3.5. Options | 28 |
| 3.6. Options | 28 |
| 3.7. Options | 29 |
| 3.8. Options | 29 |
| 4.1. LDAP attribute mappings | 37 |
| 4.2. Zone file | 91 |
| 4.3. | 103 |
| 4.4. Action types | 104 |
| 7.1. General options | 122 |
| 7.2. Self service fields | 124 |
| 7.3. | 130 |
| 7.4. | 135 |
| A.1. LDAP schema files | 137 |

Overview

LDAP Account Manager (LAM) manages user, group and host accounts in an LDAP directory. LAM runs on any webserver with PHP5 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 - 2017 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 (>= 5.6.0)
- 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)
 - Internet Explorer 11 (**compatibility mode turned off**)
 - Opera (max. 2 years old)

The default password to edit the configuration options is "lam".

License:

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

Default password:

The default password for the LAM configuration is "lam".

Have fun!

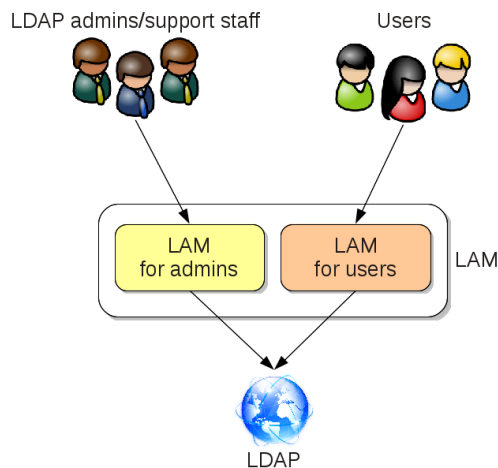
The LAM development team

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 - 5.0 (Logged in as: admin > test > de)

Tree view Tools Help Logout

Users Groups

New user Delete selected users File upload

User count: 12

| Select all | User name | First name | Last name | UID number | GID number | Account status |
|--------------------------|-----------|------------|-----------|------------|------------|----------------|
| <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 | 16109 | |
| <input type="checkbox"/> | mfischer | Monika | Fischer | 15425 | 11259 | |
| <input type="checkbox"/> | rmontag | Ramona | Montag | 26140 | 16109 | |
| <input type="checkbox"/> | shuber | Sepp | Huber | 15419 | 10815 | |
| <input type="checkbox"/> | smiller | Steve | Miller | 26142 | 11820 | |
| <input type="checkbox"/> | thausner | Thomas | Hauser | 15423 | 10815 | |
| <input type="checkbox"/> | xmontag | Xaver | Montag | 26136 | 16109 | |

Functional areas:

1. Account tabs: These tabs allow to switch between different account types
2. Tree view: Provides an LDAP browser to edit LDAP entries on attribute level
3. Tools menu: Contains useful tools such as profile and PDF editor
4. Help: Link to manual

5. Logout: Logout of the application
6. List view: Lists all entries of the selected account type (e.g. users)
7. List configuration: Configuration settings for list view (e.g. number of entries per page)
8. 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 | Some |
| Last name | User |
| Email address | <input type="text" value="lampro@rg-se.de"/> |
| Telephone number | <input type="text" value="123456789"/> |
| Mobile telephone number | <input type="text" value="123456789"/> |
| Fax number | <input type="text"/> |
| Street | <input type="text" value="Some Street 123"/> |
| Postal address | <input type="text" value="12345 Some City"/> |
| Business unit | <input type="text" value="Finance"/> |

Password

New password

Reenter password

Password reset

Question

Answer

Backup email

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

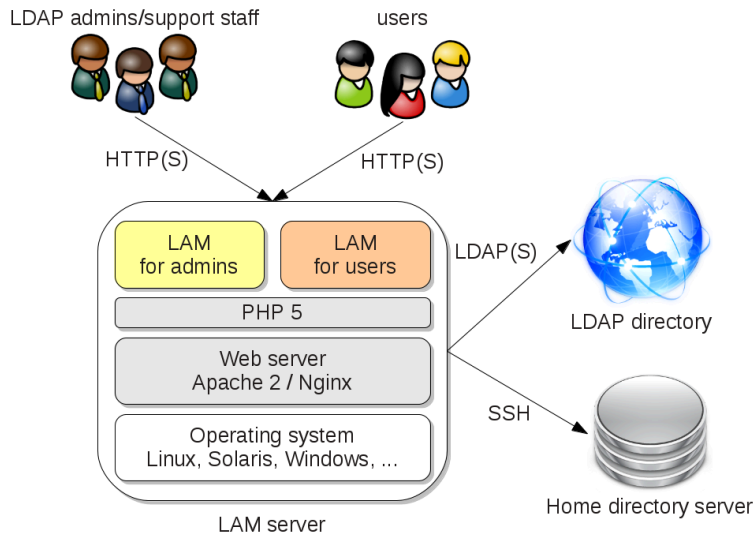
There are basically two groups of users for LAM:

- **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 independant 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 5.6.0) 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)
 - Internet Explorer 11 (**compatibility mode turned off**)
 - 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



LAM is part of the official Debian 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 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

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 homepage [<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 for Fedora/CentOS 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.

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.

System configuration

PHP

LAM runs with PHP5 ($\geq 5.2.4$). Needed changes in your php.ini:

```
memory_limit = 64M
```

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 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 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.

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 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

To 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.

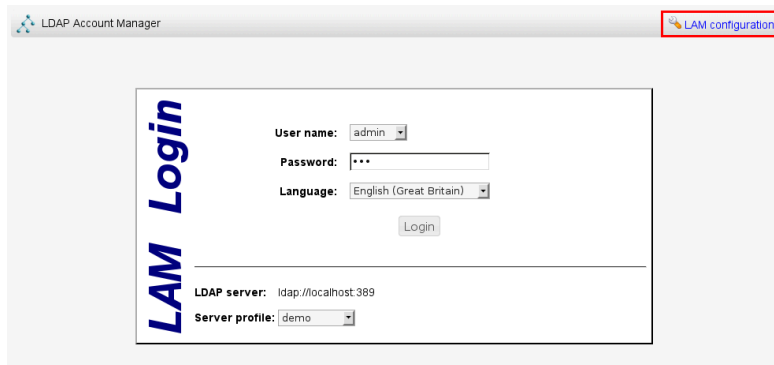
3. Open LAM (Pro) login page on new server and verify installation.

4. Uninstall LAM (Pro) on old server.

Chapter 3. Configuration

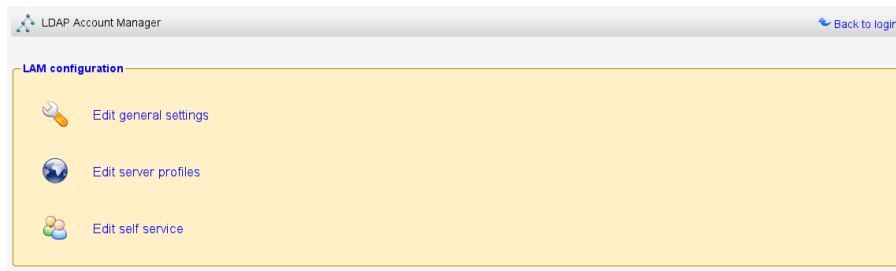
After you installed LAM you can configure it to fit your needs. The complete configuration can be done inside the application. There is no need to edit configuration files.

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



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.



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.

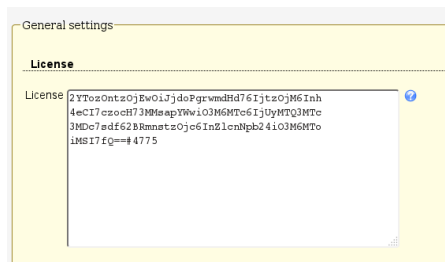
General settings

After selecting "Edit general settings" you will need to enter the master configuration password. The default password for new installations is "lam". Now you can edit the general settings.

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.



Security settings

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

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.

Session encryption will encrypt sensitive data like passwords in your session files. This is only available when PHP OpenSSL [<http://php.net/manual/en/book.openssl.php>] is active. This adds extra security but also costs performance. If you manage a large directory you might want to disable this and take other actions to secure your LAM server.

Security settings

Session timeout: 120

Allowed hosts: [Empty text area]

Allowed hosts (self service): [Empty text area]

Encrypt session SSL certificates: ☒ use system certificates

Idaps:// [Text field]

[Browse...] [Upload] [Import from server]

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 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 (Idaps://). 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.

SSL certificates use custom CA certificates

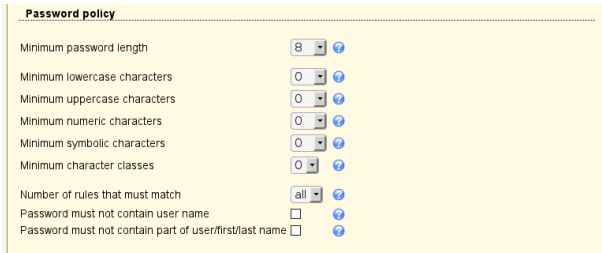
Idaps:// [Text field]

[Browse...] [Upload] [Import from server]

| Serial number | Valid to | Common name |
|----------------------|------------|-----------------|
| 10818998085225869735 | 06.04.2039 | RG SE CA |
| 666586449 | 21.02.2015 | PDC.samba4.test |

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.



Password policy

Minimum password length: 8

Minimum lowercase characters: 0

Minimum uppercase characters: 0

Minimum numeric characters: 0

Minimum symbolic characters: 0

Minimum character classes: 0

Number of rules that must match: all

Password must not contain user name: ☐

Password must not contain part of user/first/last name: ☐

You can set the minimum password length and also the complexity of the passwords.

Logging

LAM can log events (e.g. user logins). You can use system logging (syslog for Unix, event viewer for Windows) or log to a separate file. Please note that LAM may log sensitive data (e.g. passwords) at log level "Debug". Production systems should be set to "Warning" or "Error".

The PHP error reporting is only for developers. By default LAM does not show PHP notice messages in the web pages. You can select to use the php.ini setting here or printing all errors and notices.



Logging

Log level: Debug

Log destination: ☐ No logging, ☐ System logging, ☒ File

File: /tmp/lam.log

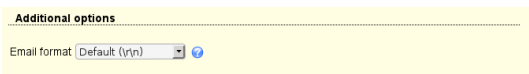
PHP error reporting: default

Additional options

Email format

Some email servers are not standards compatible. If you receive mails that look broken you can change the line endings for sent mails here. Default is to use "\r\n".

At the moment, this option is only available in LAM Pro as there is no mail sending in the free version. See here for setting up your SMTP server.

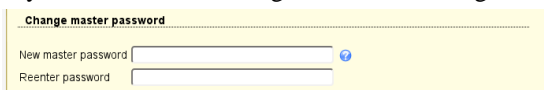


Additional options

Email format: Default (\r\n)

Change master password

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



Change master password

New master password:

Reenter password:

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.

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.

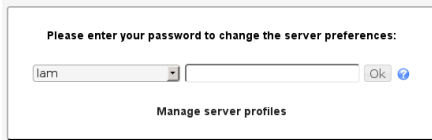
Built-in templates:

- 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

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.

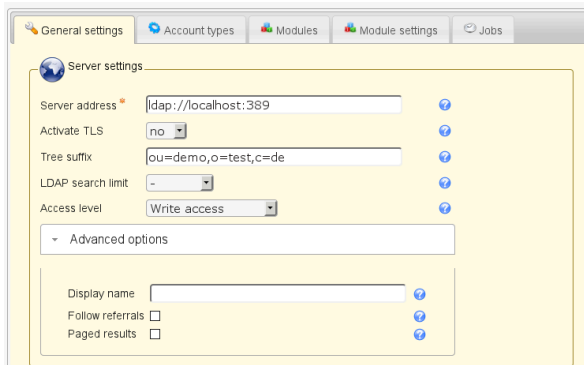


Each server profile contains the following information:

- **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

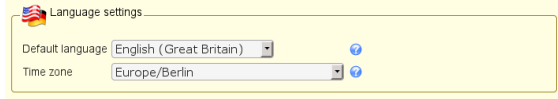
Sometimes, you may not want to display the server address on the login page. In this case you can setup a display name here (e.g. "Production").

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 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.

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.

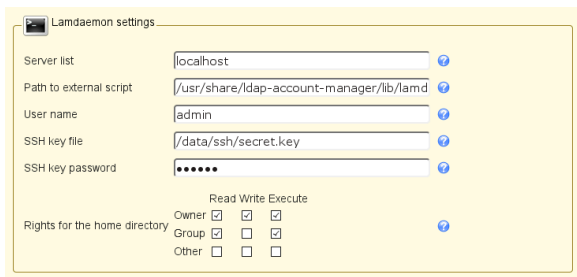
A screenshot of the 'Language settings' form. It has a title bar with a flag icon and the text 'Language settings'. Below the title bar, there are two dropdown menus. The first is labeled 'Default language' and has 'English (Great Britain)' selected. The second is labeled 'Time zone' and has 'Europe/Berlin' selected. There are small blue question mark icons to the right of each dropdown.

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.

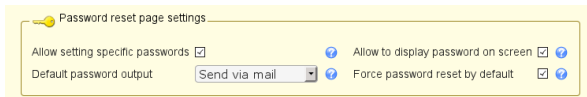
You can provide a fixed user name. If you leave the field empty then LAM will use your current account (the account you used to login to LAM).

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).

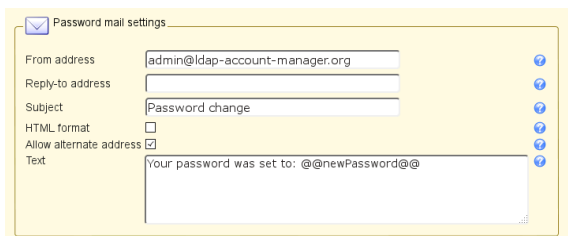
A screenshot of the 'Lamdaemon settings' form. It has a title bar with a folder icon and the text 'Lamdaemon settings'. Below the title bar, there are several input fields: 'Server list' with 'localhost', 'Path to external script' with '/usr/share/ldap-account-manager/lib/lamd', 'User name' with 'admin', 'SSH key file' with '/data/ssh/secret.key', and 'SSH key password' with a masked password '*****'. There are small blue question mark icons to the right of each field. Below these fields, there is a section for 'Rights for the home directory' with a table of permissions. The table has columns for 'Owner', 'Group', and 'Other', and rows for 'Read', 'Write', and 'Execute'. The 'Owner' row has all three permissions checked. The 'Group' row has 'Read' and 'Execute' checked. The 'Other' row has all three permissions unchecked. There is a small blue question mark icon to the right of the table.

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.

A screenshot of the 'Password reset page settings' form. It has a title bar with a key icon and the text 'Password reset page settings'. Below the title bar, there are four checkboxes: 'Allow setting specific passwords' (checked), 'Allow to display password on screen' (checked), 'Default password output' (set to 'Send via mail'), and 'Force password reset by default' (checked). There are small blue question mark icons to the right of each checkbox.

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).

A screenshot of the 'Password mail settings' form. It has a title bar with an envelope icon and the text 'Password mail settings'. Below the title bar, there are several input fields: 'From address' with 'admin@ldap-account-manager.org', 'Reply-to address' (empty), 'Subject' with 'Password change', 'HTML format' (unchecked), 'Allow alternate address' (checked), and 'Text' with 'Your password was set to: @@newPassword@@'. There are small blue question mark icons to the right of each field.

LAM supports two methods for login:

- Fixed list
- LDAP search

The screenshot shows the 'Security settings' form. Under the 'Login method' dropdown, 'Fixed list' is selected. Below it, the 'List of valid users' text area contains three LDAP DN entries: 'cn=admin,o=test,c=de', 'uid=john,ou=people,o=test,c=de', and 'uid=sally,ou=people,o=test,c=de'. The '2-factor authentication' section shows 'Provider' set to 'None'. The 'Profile password' section has empty fields for 'New password' and 'Reenter password'.

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))").

The screenshot shows the 'Security settings' form with 'LDAP search' selected in the 'Login method' dropdown. The 'LDAP suffix' field contains 'ou=people,o=test,c=de'. The 'LDAP filter' field contains 'uid=%USER%'. There are empty fields for 'Bind user' and 'Bind password'. The 'HTTP authentication' checkbox is unchecked. The '2-factor authentication' section shows 'Provider' set to 'None'. The 'Profile password' section has empty fields for 'New password' and 'Reenter password'.

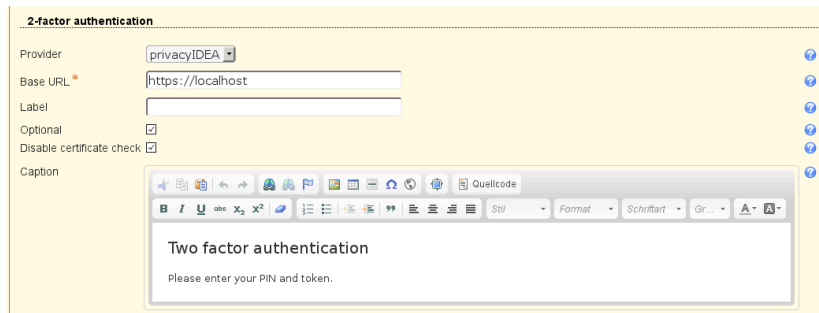
2-factor authentication

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).

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

- privacyIdea [<https://www.privacyidea.org/>]

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.



2-factor authentication

Provider:

Base URL:

Label:

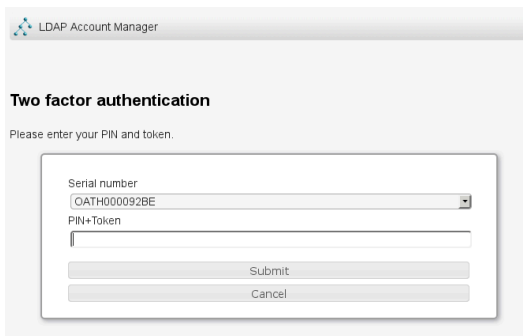
Optional: ☒

Disable certificate check: ☒

Caption:

Two factor authentication
Please enter your PIN and token.

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:

PIN+Token:

Password

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



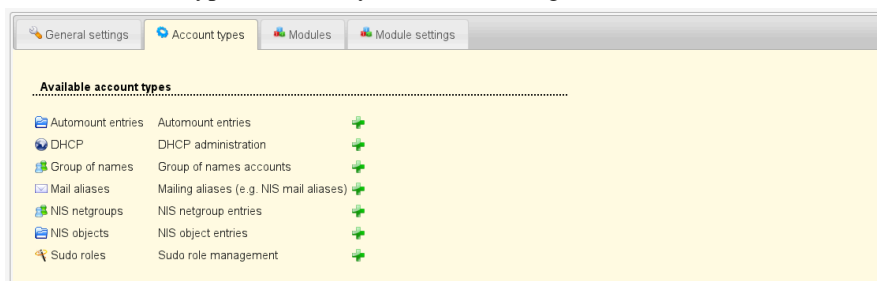
Profile password

New password:

Reenter 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.



Account types

Available account types:

| | | |
|-------------------|---|--------------------------|
| Automount entries | Automount entries | <input type="checkbox"/> |
| DHCP | DHCP administration | <input type="checkbox"/> |
| Group of names | Group of names accounts | <input type="checkbox"/> |
| Mail aliases | Mailing aliases (e.g. NIS mail aliases) | <input type="checkbox"/> |
| NIS netgroups | NIS netgroup entries | <input type="checkbox"/> |
| NIS objects | NIS object entries | <input type="checkbox"/> |
| Sudo roles | Sudo role management | <input type="checkbox"/> |

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.

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.

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.

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 this is located in package php5-sqlite.

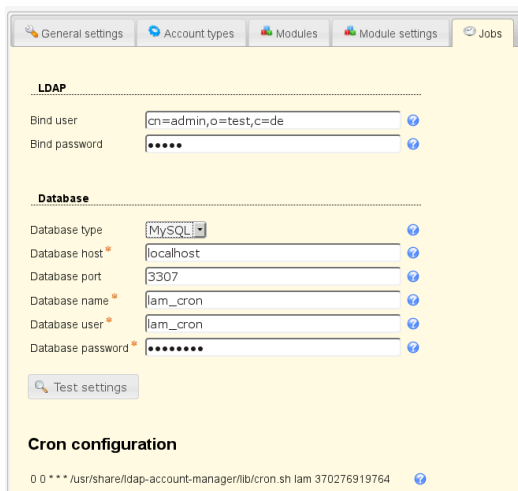
MySQL

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 this is located in package php5-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';
```

The screenshot shows a web-based configuration interface with tabs for 'General settings', 'Account types', 'Modules', 'Module settings', and 'Jobs'. The 'Module settings' tab is active, showing two sections: 'LDAP' and 'Database'. The 'LDAP' section has fields for 'Bind user' (cn=admin,o=test,c=de) and 'Bind password' (masked with dots). The 'Database' section has fields for 'Database type' (MySQL), 'Database host' (localhost), 'Database port' (3307), 'Database name' (lam_cron), 'Database user' (lam_cron), and 'Database password' (masked with dots). A 'Test settings' button is located below the database fields. At the bottom, there is a 'Cron configuration' section with a text field containing the command: '0 0 * * * /usr/share/ldap-account-manager/lib/cron.sh lam 370276919764'.

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 "--dryRun" at the end of the command. E.g.:

```
/usr/share/ldap-account-manager/lib/cron.sh lam 123456789 --dryRun
```

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.



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.

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

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.

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.

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

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).

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 |

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.

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 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: Delete or move expired accounts

You can automatically delete or move expired accounts.

Table 3.6. 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: Delete or move expired accounts

You can automatically delete or move expired accounts.

FreeRadius: Cleanup expired user accounts

Delay:

Action:

Target DN:

Table 3.7. 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: 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:

Target DN:

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 |

Job history

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

Job history

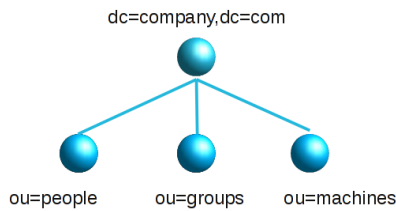
| Name | Time | Result | Messages |
|---|---------------------|--------|----------|
| Windows: Notify users about password expiration | 2016-01-16 18:35:44 | Ok | |
| Windows: Notify users about password expiration | 2015-11-27 20:58:55 | Ok | |
| Windows: Notify users about password expiration | 2015-11-27 20:58:23 | 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.

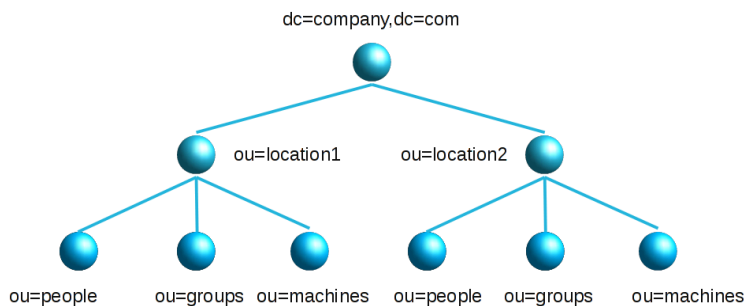
Simple: One LDAP directory managed by a small group of admins

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.

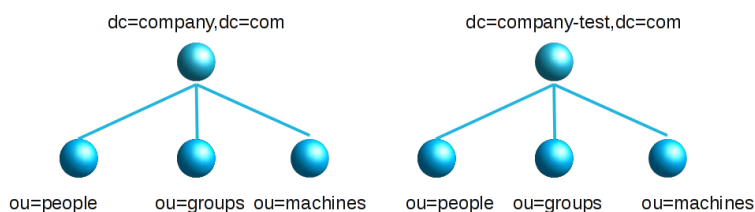


In this situation it is recommended to create one server profile for each admin group (e.g. department). Setup the LDAP suffixes in the server profiles to point to the needed organisational units. E.g. use `ou=people,ou=department1,dc=company,dc=com` or `ou=department1,ou=people,dc=company,dc=com` as 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.

Chapter 4. Managing entries in your LDAP directory

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

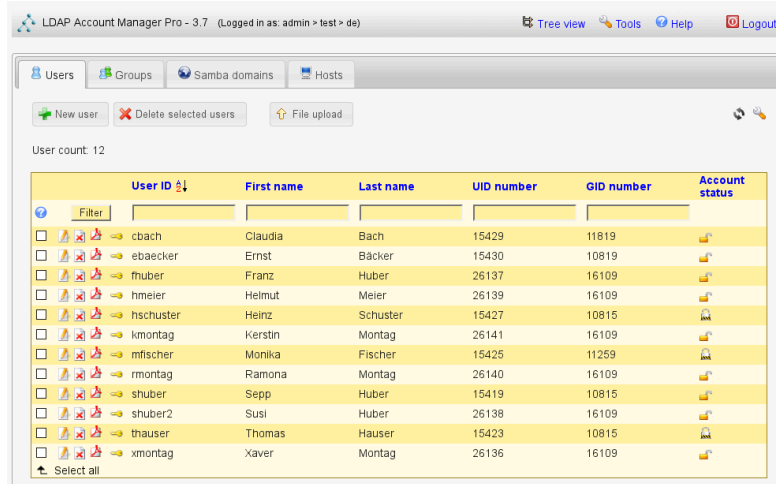
Please note that not all account types are manageable with the free LAM release. LAM Pro provides some more account types (e.g. group of names, aliases, ...) and modules (e.g. Kopano, custom scripts, ...) to support additional LDAP object classes. All LAM Pro features are marked in this manual.

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.

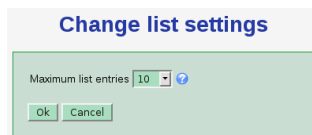
The header part includes the links to manage all account types (e.g. users and groups) and open the tree view (LDAP browser). There is also the logout link and a tools entry.

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



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.



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.

The screenshot shows a web interface for managing LDAP accounts. At the top, there are buttons for 'Save', 'Reset changes', and 'Set password', along with a dropdown menu set to 'aaa' and a 'Load profile' button. The main header displays the user's name 'Claudia Bach', email 'cbach@ldap-account-manager.org', and phone numbers. Below this, a sidebar on the left has tabs for 'Personal', 'Unix', and 'Custom scripts'. The 'Personal' tab is active, showing fields for 'First name' (Claudia), 'Last name' (Bach), 'Initials', and 'Description' (Claudia Bach). To the right of these fields is a 'Delete photo' button. Below the personal information, there are sections for 'Address' (Street, Post office box, Postal code, Location, State, Postal address, Office name, Room number) and 'Contact data' (Telephone number, Home telephone number, Mobile number, Fax number, Email address). The 'Work details' section at the bottom shows the 'Job title' as 'Manager'. The interface is light yellow with blue accents and includes help icons (question marks) next to many fields.

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:

- 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:

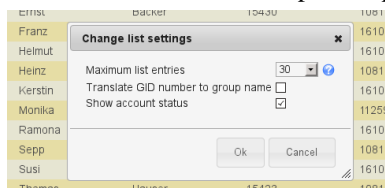
- Users (Personal + Unix + PyKota)
- Groups (Unix + PyKota)
- Printers (PyKota)
- Billing codes (PyKota)

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.

| Select all | User name | First name | Last name | UID number | GID number |
|--------------------------|-----------|------------|-----------|------------|------------|
| <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 |

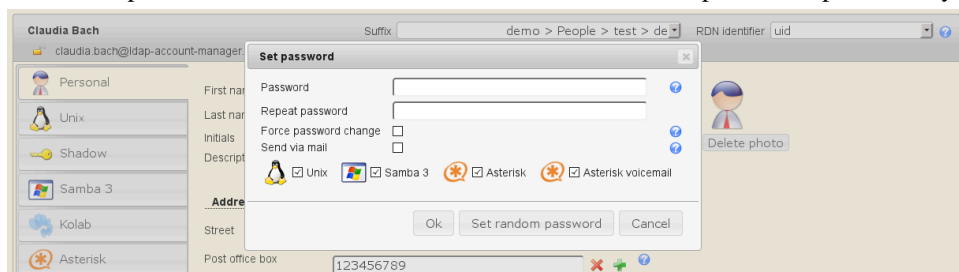
Show account status: If you activate this option then there will be an additional column displayed that shows if the account is locked or expired. You can see more details when moving the mouse cursor over the lock icon. This function supports Unix, Samba, PPolicy, Windows and 389ds locking+deactivation.

| Select all | User name | First name | Last name | UID number | GID number | Account status |
|--------------------------|-----------|------------|-----------|------------|------------|----------------|
| <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 | |

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.

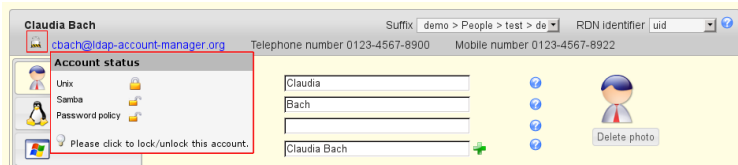
If a module supports to enforce a password change then you will see the appropriate checkbox. LAM Pro also offers to send the password via email after the account is saved. Email options are specified in your LAM server profile.



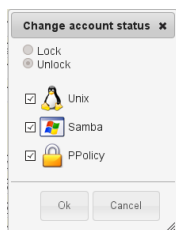
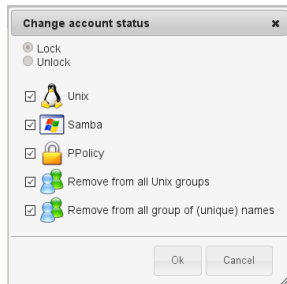
Quick account (un)locking:

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.



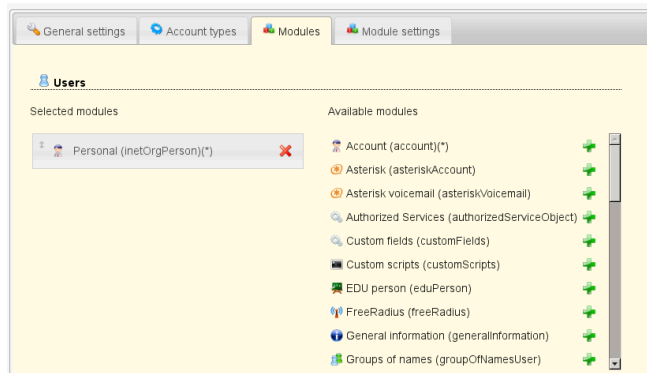
Personal

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 (please install PHP Imagick/ImageMagick [<http://www.php.net/manual/en/book.imagick.php>] for full file format support). 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.



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.

Managing entries in your LDAP directory

The screenshot shows the 'Module settings' tab in the LDAP account manager. The 'Personal' section is active, displaying a list of fields that can be managed. The fields are organized into three groups: 'Hidden options', 'Read-only fields', and 'Photo'.

Hidden options

| | | | | |
|---|--|--|--|--|
| <input type="checkbox"/> 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 checked="" type="checkbox"/> Pager |
| <input 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"/> User name |

Advanced options

Add addressbook (ou=addressbook) ☐

Read-only fields

| | | | | |
|--|---|--|--|--|
| <input type="checkbox"/> 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 | | |

Photo

Maximum width (px)

Maximum height (px)

Maximum file size (kB)

User management

The screenshot shows the 'User management' interface for a user named Claudia Bach. The interface is divided into several sections: 'Personal', 'Address', 'Contact data', and 'Work details'. The 'Personal' section is currently selected, showing fields for First name, Last name, Initials, and Description. The 'Address' section shows fields for Street, Post office box, Postal code, Location, State, Postal address, Office name, and Room number. The 'Contact data' section shows fields for Telephone number, Home telephone number, Mobile number, Fax number, and Email address. The 'Work details' section shows fields for Job title, Car license, Employee number, Employee type, Business category, Department(s), Organisation, and Manager.

Personal

First name: Claudia

Last name: Bach

Initials:

Description: Claudia Bach

Address

Street: MyStreet 123

Post office box: 4645656

Postal code: 12345

Location:

State:

Postal address:

Office name:

Room number: A 1.23

Contact data

Telephone number: 0123-4567-8900

Home telephone number: 0123-4567-8911

Mobile number: 0123-4567-8922

Fax number:

Email address: cbach@ldap-account-manager.org

Work details

Job title: Manager

Car license:

Employee number:

Employee type:

Business category:

Department(s):

Organisation:

Manager:

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

The screenshot shows the 'New user certificate' section in the 'User management' interface. It displays a list of existing certificates with their serial numbers and paths. Below the list, there is a 'New user certificate' section with a 'Browse...' button and an 'Upload' button.

Existing certificates:

| | |
|----------------------|---|
| 14476788081586606336 | /C=DE/ST=Bavaria/L=City/O=RGSE/CN=test |
| 17839378481148738733 | /C=DE/ST=Bavaria/L=City/O=RGSE/CN=test2 |
| 15038736106651474403 | /C=DE/ST=Bavaria/L=City/O=RGSE/CN=test3 |

New user certificate

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):

- \$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 screenshot shows a web interface for editing a user profile. The 'Personal' tab is selected. The 'Common name' field is populated with the wildcard '\$firstname \$lastname'. Other fields include 'User name', 'First name' (First), 'Last name' (Last), 'Initials', and 'Description'. A 'Suffix' field is also present at the top right.

This screenshot is identical to the one above, but the 'Common name' field now displays the result of the wildcard substitution: 'First Last'.

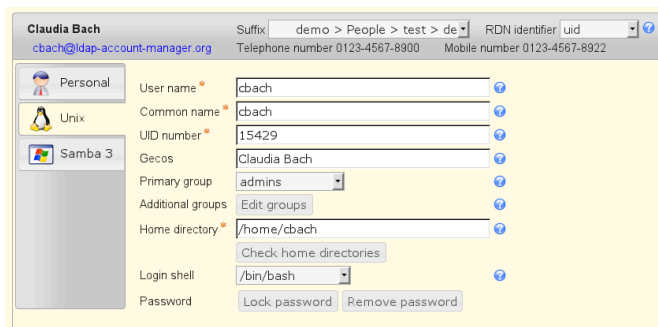
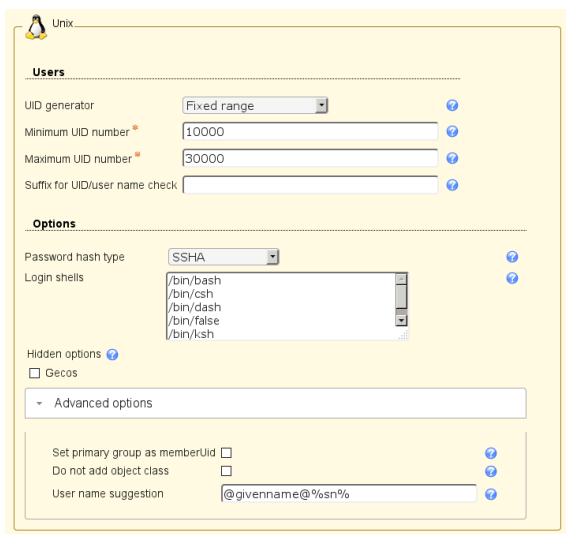
Unix

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.

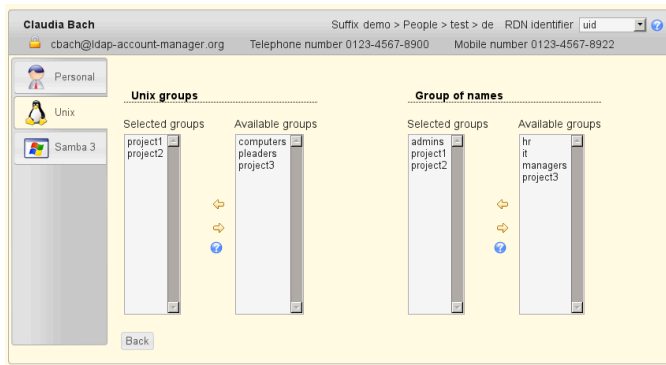
- Password hash type: If possible use CRYPT-SHA512 or SSHA to protect your user's passwords. The option SASL will set the password to "{SASL}<user name>".
- Login shells: List of valid login shells that can be selected when editing an account.
- Hidden options: Some input fields can be hidden to simplify 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.



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

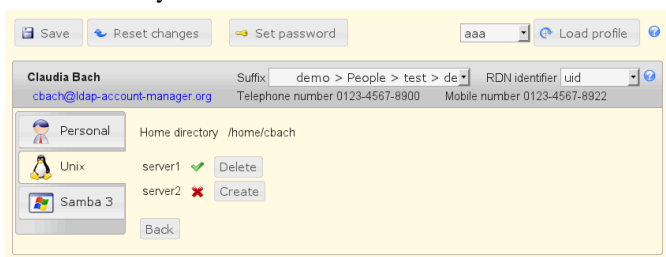
To enable "Group of names" please either add the groups module "groupOfNames"/"groupOfUniqueNames" or add the account type "Group of names".

Managing entries in your LDAP directory



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.



Wildcards

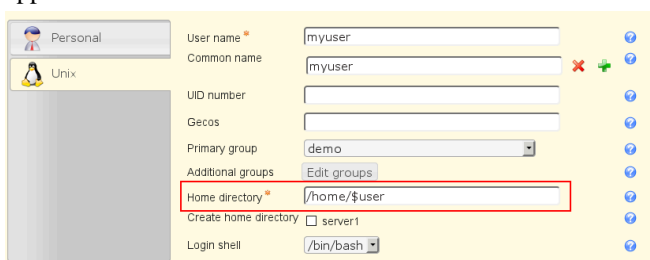
This module provides the following wildcards (others may be provided by other modules):

- \$user: User name
- \$group: Groupe 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.



The screenshot shows a user configuration form for 'myuser'. The 'Home directory' field is highlighted with a red rectangle and contains the value '/home/myuser'. Other fields include 'User name' (myuser), 'Common name' (myuser), 'UID number' (empty), 'Gecos' (empty), 'Primary group' (demo), 'Additional groups' (Edit groups), 'Create home directory' (checkbox, server1), and 'Login shell' (/bin/bash).

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.

The screenshot shows the 'Modules' configuration window. The 'Selected modules' list includes 'Personal (inetOrgPerson)(*)' and 'Groups of names (groupOfNamesUser)'. The 'Available modules' list includes various other modules like 'Account (account)(*)', 'Asterisk (asteriskAccount)', 'Asterisk voicemail (asteriskVoicemail)', 'Authorized Services (authorizedServiceObject)', 'Custom fields (customFields)', 'Custom scripts (customScripts)', 'EDU person (eduPerson)', 'FreeRadius (freeRadius)', 'General information (generalInformation)', and 'Hosts (hostObject)'.

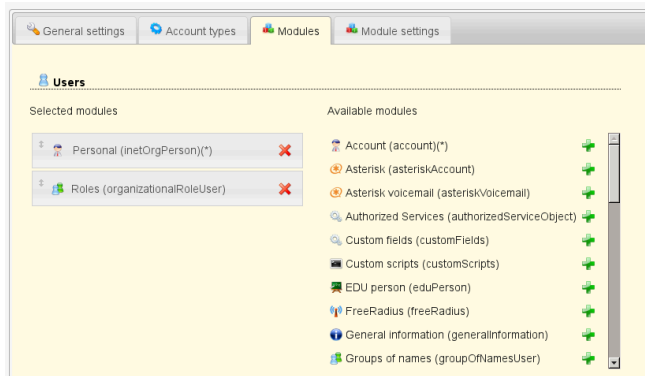
The module automatically detects if groups are based on "groupOfNames", "groupOfUniqueNames" or "groupOfMembers" and sets the correct attribute.

The screenshot shows the user profile for 'Claudia Bach'. The 'Selected groups' list includes 'admins' and 'project1'. The 'Available groups' list includes 'hr', 'it', 'managers', 'project2', and 'project3'. The 'Group of names' module is selected.

Organizational roles (LAM Pro)

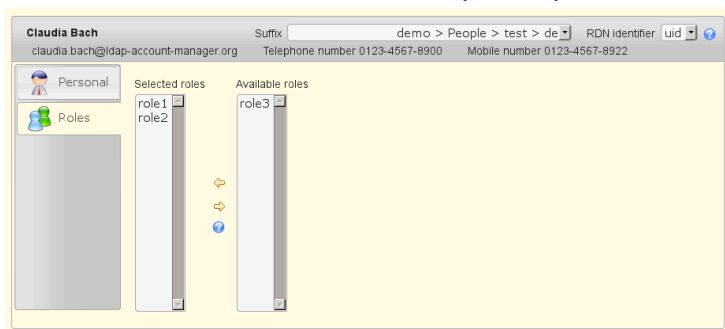
LAM can manage role memberships in organizationalRole objects. To activate this feature please add the user module "Roles (organizationalRoleUser)" to your LAM server profile.

Managing entries in your LDAP directory



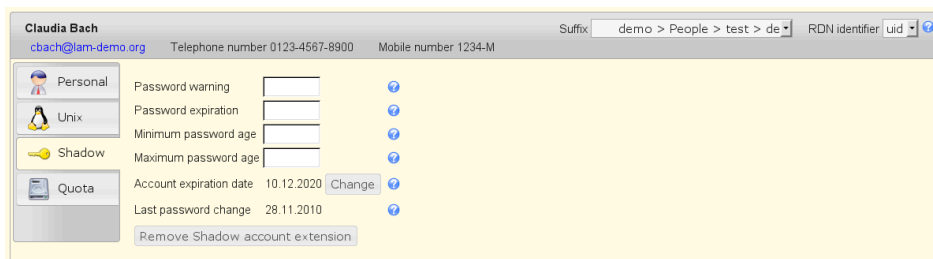
User editing

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



Shadow

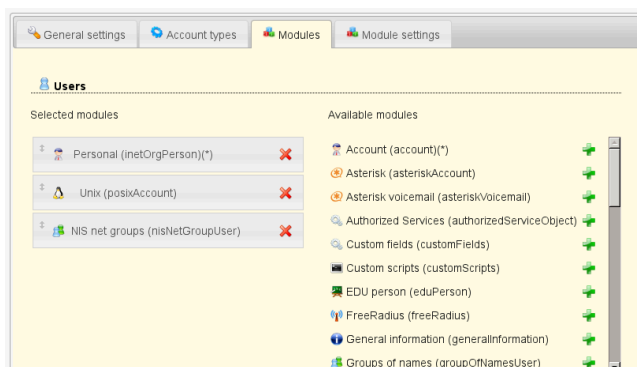
LAM supports the management of the LDAP substitution of /etc/shadow. Here you can setup password policies for your Unix accounts and also view the last password change of a user.



NIS net groups

Configuration

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



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.

The screenshot shows the 'Users' tab in the LAM Pro interface. At the top, there are tabs for 'Users', 'Groups', and 'NIS netgroups'. Below these are buttons for 'Save', 'Reset changes', and 'Set password', along with a 'default' dropdown and a 'Load profile' link. The user profile for 'Claudia Bach' is displayed, including her email 'claudia.bach@ldap-account-manager.org', telephone number '0123-4567-8900', and mobile number '0123-4567-8922'. The 'Personal' tab is selected, showing fields for 'Group' (administrators), 'Host name' (server1), and 'Domain name' (empty). Below these are fields for 'NIS net-groups' (group01, group02) and a dropdown for 'administrators'. Red 'X' icons indicate errors in the domain name and group02 fields, while a green plus icon is next to the administrators dropdown.

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.

The screenshot shows the 'Modules' tab in the LAM Pro interface. It displays a list of 'Available modules' on the right, including 'Account (account)(*)', 'Asterisk (asteriskAccount)', 'Asterisk voicemail (asteriskVoicemail)', 'Authorized Services (authorizedServiceObject)', 'Custom fields (customFields)', 'Custom scripts (customScripts)', 'EDU person (eduPerson)', 'FreeRadius (freeRadius)', 'General information (generalInformation)', and 'Groups of names (groupOfNamesUser)'. Each module has a green plus icon next to it, indicating it is available for selection. On the left, under 'Selected modules', there are three modules listed with red 'X' icons: 'Personal (inetOrgPerson)(*)', 'Unix (posixAccount)', and 'Password self reset (passwordSelfReset)'.

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.

The screenshot shows the 'Password self reset' module settings. It includes a 'Security questions' section with a text area containing three questions: 'What is the name of your favourite pet?', 'What is the name of your favourite TV show?', and 'What is the brand of your first car?'. Below this is a 'Number of questions' dropdown set to '3'. There is a checkbox for 'Allow custom security questions' which is currently unchecked. At the bottom, there is a checkbox for 'Hidden options' (checked) and a checkbox for 'Backup email' (unchecked).

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.

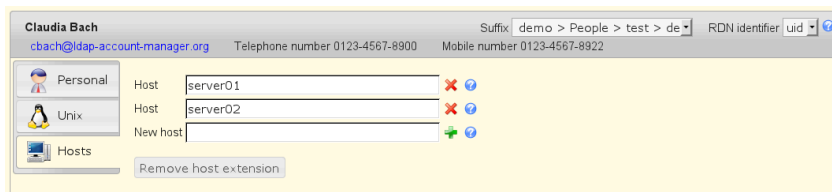
Samba 4 note: Due to a bug [https://bugzilla.samba.org/show_bug.cgi?id=10094] in Samba 4 you need to add the extension, save, and then select a question and set the answer. If you add the extension, set question/answer and then save all together this will cause an LDAP error and no changes will be saved.



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.

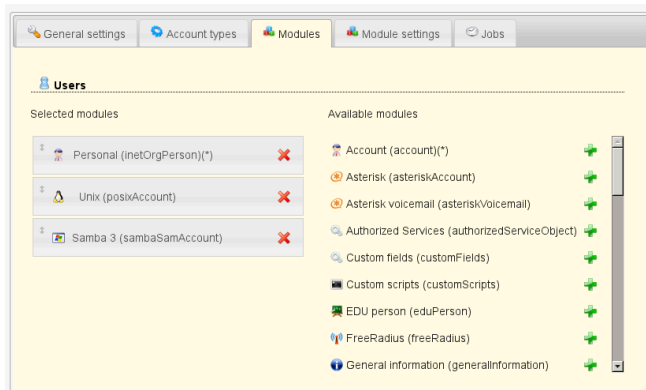


Samba 3

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.

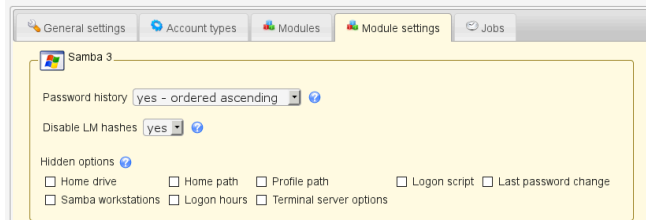
Managing entries in your LDAP directory



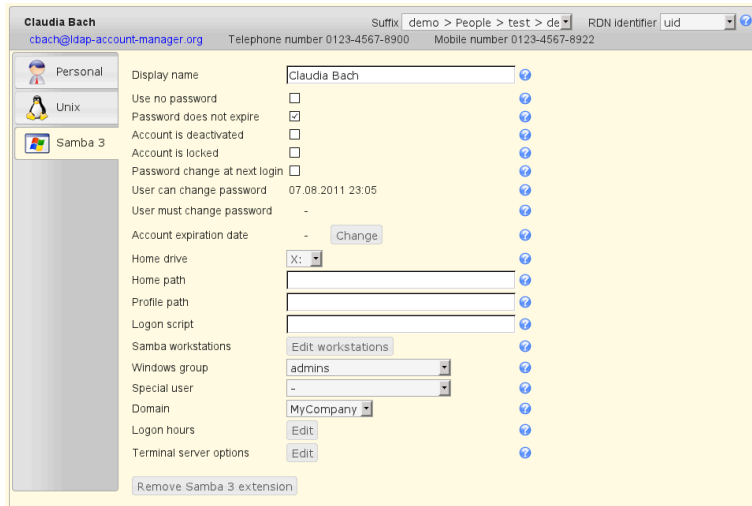
In the configuration options you can enable password history checking. Depending on your LDAP server you might need ascending or descending order. Just switch the setting if the password history is not correctly updated.

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.



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



Logon hours can be changed.

Managing entries in your LDAP directory

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

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

| 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.

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

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

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)

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

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

LDAP suffix: DC=samba4,DC=test

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

Advanced options

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.

General settings Account types Modules Module settings

Users

Selected modules

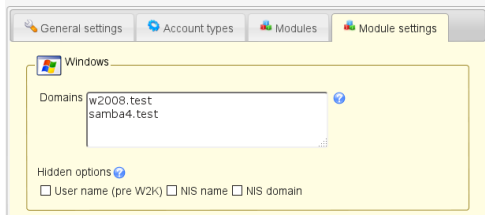
- Windows (windowsUser)(*)

Available modules

- Account (account)(*)
- Asterisk (asteriskAccount)
- Asterisk voicemail (asteriskVoicemail)
- Authorized Services (authorizedServiceObject)
- Custom fields (customFields)
- Custom scripts (customScripts)
- EDU person (eduPerson)
- FreeRadius (freeRadius)
- General information (generalInformation)
- Groups of names (groupOfNamesUser)

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.



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.

Wildcards

This module provides the following wildcards (others may be provided by other modules):

- \$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

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.

Windows

General

User name * myuser w2012

User name (pre W2K)

First name First

Last name Last

Common name * \$firstname \$lastname

Windows

General

User name * myuser w2012

User name (pre W2K)

First name First

Last name Last

Common name * First Last

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.

Claudia Bach
cbach@lam-demo.org Telephone number 0123-4567-8900 Mobile number 1234-M

Suffix demo > People > test > de RDN identifier uid

localhost

| Mountpoint | Used blocks | Soft block limit | Hard block limit | Grace block period | Used inodes | Soft inode limit | Hard inode limit | Grace inode period |
|---|-------------|------------------|------------------|--------------------|-------------|------------------|------------------|--------------------|
| /daten/projekte/lam/quotaTest/userOnlyMount | 0 | 1000 | 2000 | | 0 | 2000 | 3000 | |
| /daten/projekte/lam/quotaTest/userAndGroupMount | 0 | 500 | 1000 | | 0 | 500 | 750 | |
| / | 0 | 10000 | 15000 | | 0 | 2000 | 3000 | |

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)(*) Kolab (kolabUser) | Custom scripts (customScripts) EDU person (eduPerson) FreeRadius (freeRadius) General information (generalInformation) Groups of names (groupOfNamesUser) |

Attention: LAM will add the object class "mailrecipient" by default. This object class is available on 389 directory server but may not be present on e.g. OpenLDAP. Please deactivate the following setting (LAM server profile, module settings) if you do not use this object class.

Kolab

Manage object class "mailrecipient" ☒

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.

Attention: The mailbox server cannot be changed after the account has been saved. Please make sure that the value is correct.

Kolab users should not be directly deleted with LAM. You can mark an account for deletion which then is done by the Kolab server itself. This makes sure that the mailbox etc. is also deleted.

Managing entries in your LDAP directory

The screenshot shows the 'Claudia Bach' account page in the LDAP account manager. The left sidebar has icons for Personal, Unix, Samba 3, and Kolab. The main content area is divided into sections: 'Personal' (Mailbox home server: qmail.ldap-account-manager.org), 'Invitation policy' (Anyone, Manual, Always accept, Always reject, Always accept), 'Email aliases' (cbach@ldap-account-manager.org), 'Delegates' (hscluster@localhost, claudia.bach@ldap-account-manager.org), and 'Options' (Allowed recipients: ~evil.com, Allowed senders: ~evil.com). There is a 'Mark account for deletion' button at the bottom.

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

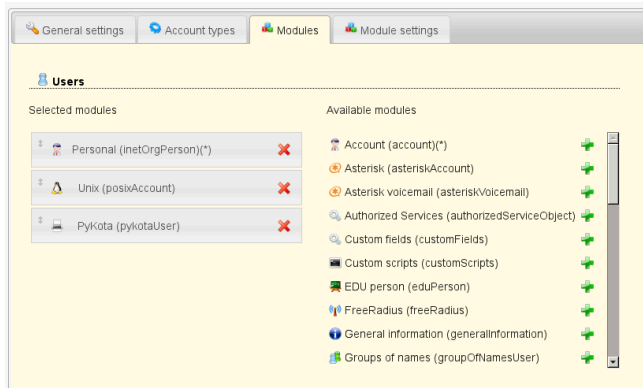
EDU person accounts are mainly used in university networks. You can specify the principal name, nick names and much more.

The screenshot shows the 'EDU person' section of the 'Claudia Bach' account page. The left sidebar has icons for Personal, Unix, Samba 3, and EDU person. The main content area shows fields for: Principal name (cbach), Primary affiliation (employee), Scoped affiliations (@cs.berkeley.edu), Affiliations (library-walk-in, affiliate, employee, affiliate), Nick names (claudia), Entitlements (urn:mace:washington.edu:confocalMicroscope), Organisation (o=Hogwarts,dc=hswm,dc=wiz), Primary organisational unit (ou=Potions,o=Hogwarts,dc=hswm,dc=wiz), Organisational units (ou=Potions,o=Hogwarts,dc=hswm,dc=wiz), Assurance profiles (urn:mace:incommon:IAQ:sample, http://idm.example.org/LOA#sample), and a 'Remove EDU person extension' button.

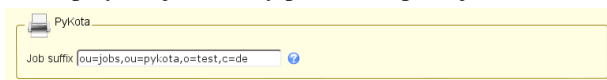
PyKota

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.

Managing entries in your LDAP directory

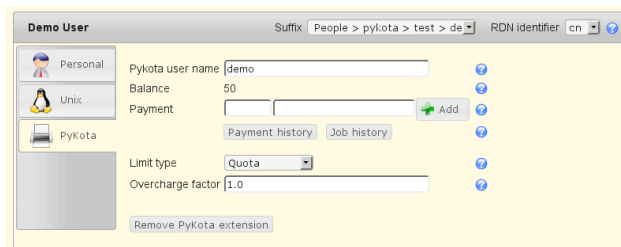


To display the job history please setup the job DN on tab "Module settings":

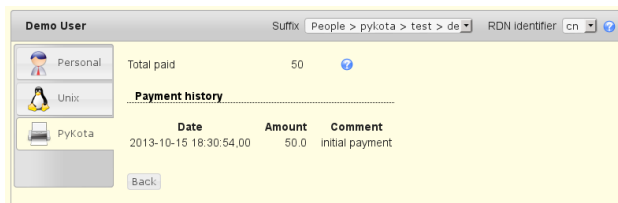


Now you can add the PyKota extension to your user accounts. Here you can setup the printing options and add payments for this user.

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



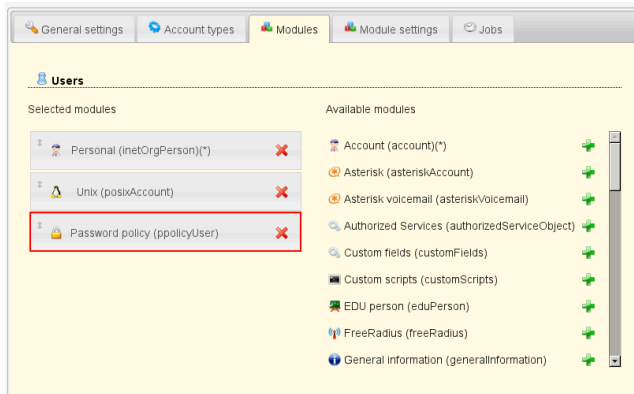
You may also view the payment and job history.



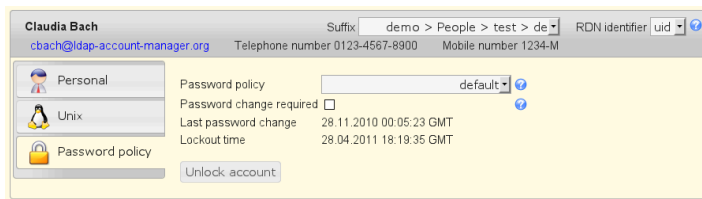
Password policy (LAM Pro)

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 type.



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



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.

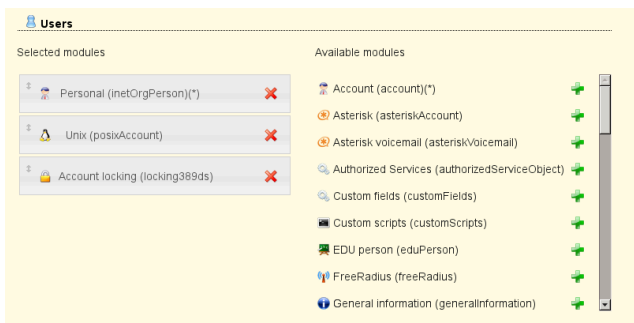
Account locking for 389ds (LAM Pro)

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

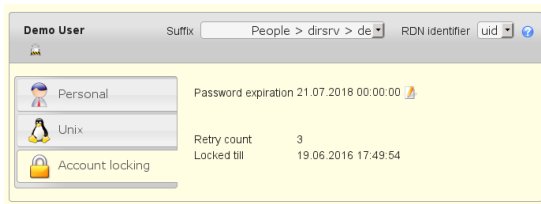
Please add the user module "Account locking (locking389ds)".



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.

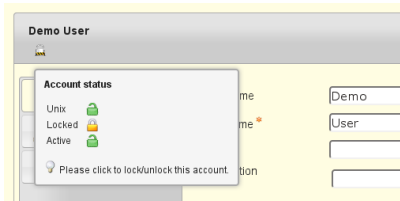
The limit of failed login attempts and lockout duration is configured on your LDAP server and not within LAM.



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

Here you can also (de)activate the account.

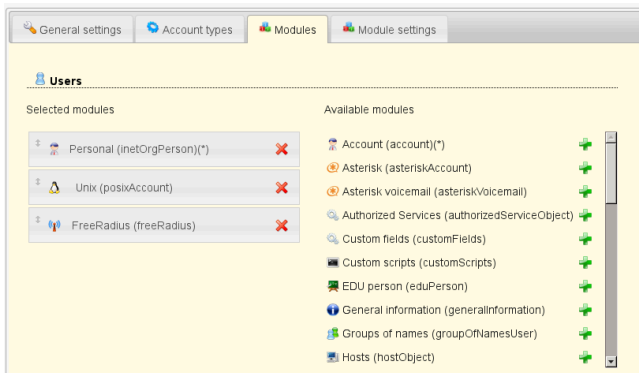
Note: Accounts are only locked by the LDAP server due to failed password attempts. You cannot manually lock an account. Deactivate it in case you want to disable login for a user.



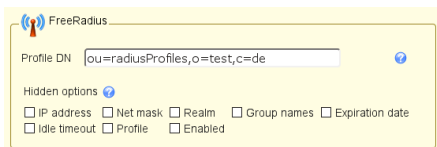
FreeRadius

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

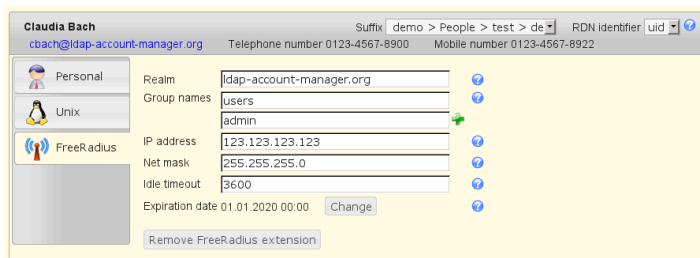
To activate the FreeRadius plugin please activate the FreeRadius user module in your server profile:



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".



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.



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.

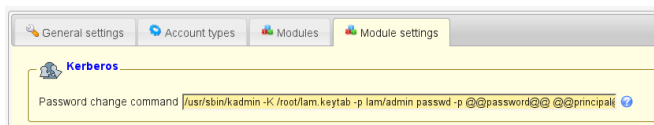
Setup password changing

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.

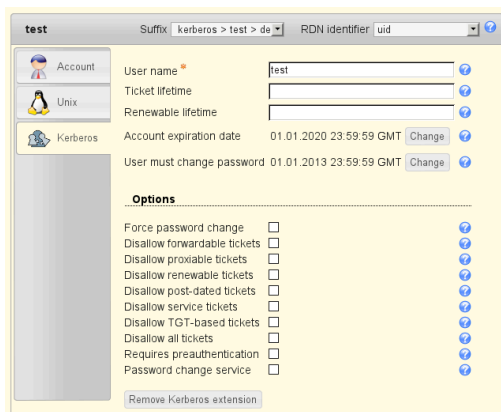
Example to create a keytab: `ktutil -k /root/lam.keytab add -p lam@LAM.LOCAL -e aes256-cts-hmac-sha1-96 -V 1`

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.



User management

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



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.

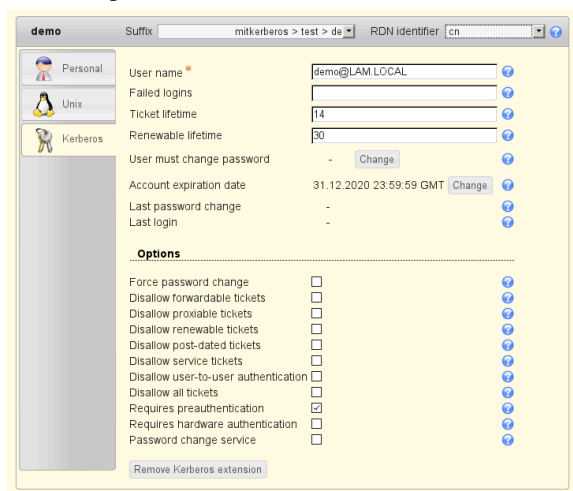
Example commands:

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



User management

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

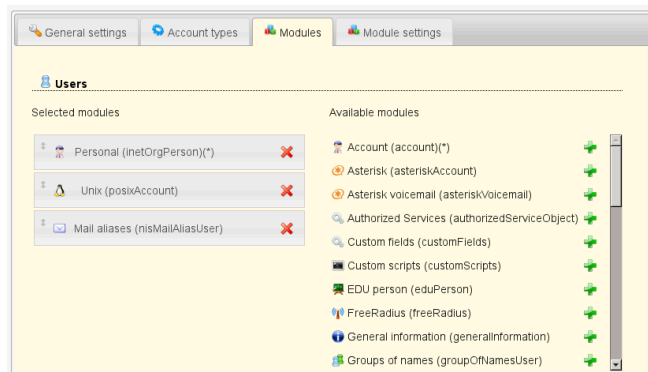


NIS mail aliases

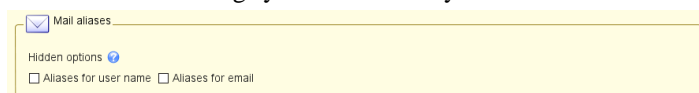
This module allows to add/remove the user in mail alias entries.

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)":

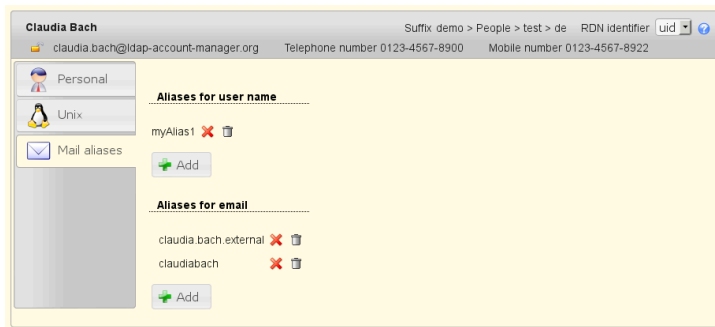


On tab Module settings you can select if you want to set the user name or email as recipient in alias entries.

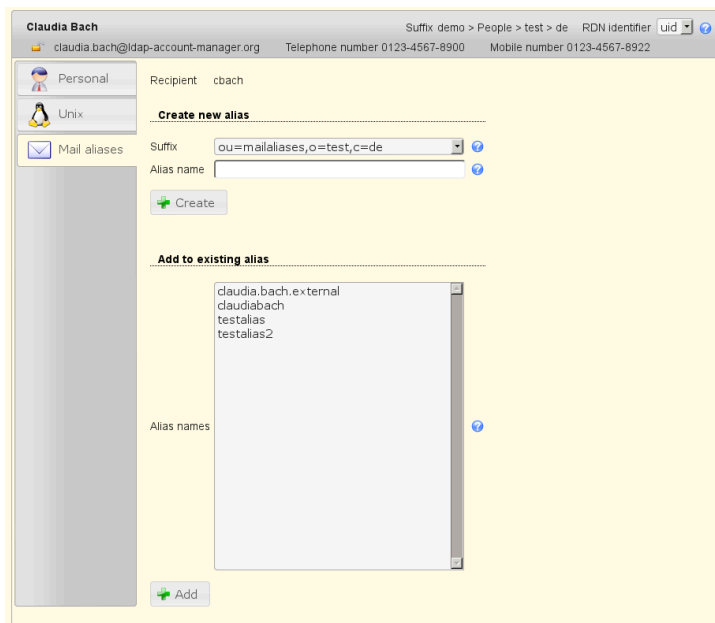


Now you will see the mail aliases tab when editing an user.

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.



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

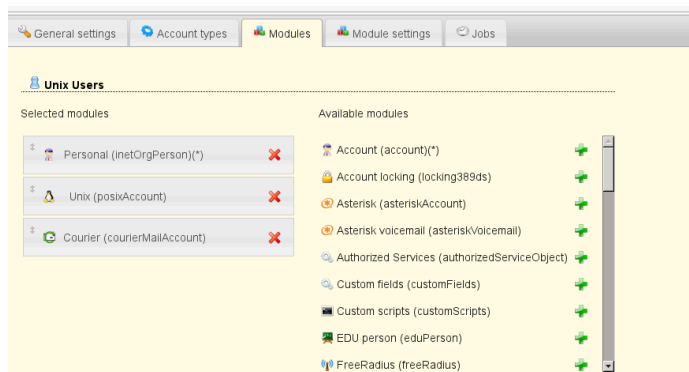


Courier mail

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.



Usage:

Managing entries in your LDAP directory

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: courier2 > test > de RDN identifier: cn

Personal
Home directory: /home/demo
Mailbox folder: /mnt/mail/demo/
Mailbox host: mailserver
Mail quota: 500 MB
Disable IMAP use: ☐
Disable POP3 use: ☐
Disable Webmail use: ☒
Disable Shared Folder use: ☒
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.

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
Alternate address: cbach@ldap-account-manager.org
Forwarding address: cbach-backup@ldap-account-manager.org
UID number: 1234
GID number: 1111
Server address: qmail.ldap-account-manager.org
Message store: /mails/cbach
Account status: Active
Configuration type: LDAP + qmail
Delivery mode: Default
Autoreply text: I am out of office. Your mails will be answered soon.
Delivery program:
Deletion date: 1.1.2020
Change

Quota
Quota size: 1000000000
Message count limit: 10000
Message size limit: 100000000
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.

Gmail

Hidden options

☐ Quota size ☐ Message count limit ☐ Message size limit ☐ UID number ☐ GID number
☐ Autoreply text ☐ Server address ☐ Message store ☐ Delivery program ☐ Deletion date
☐ Configuration type

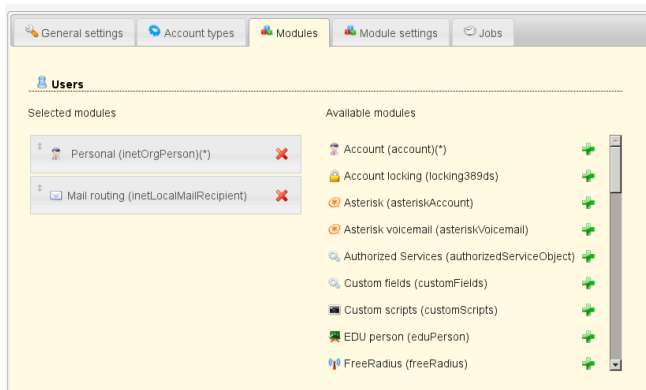
Mail routing

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.

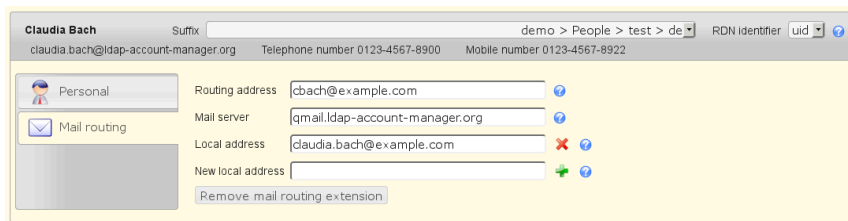
Managing entries in your LDAP directory



Usage:

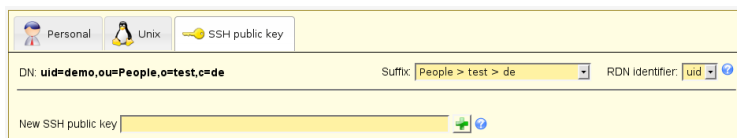
You can specify a routing address, the mail server and a number of local addresses to route.

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



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

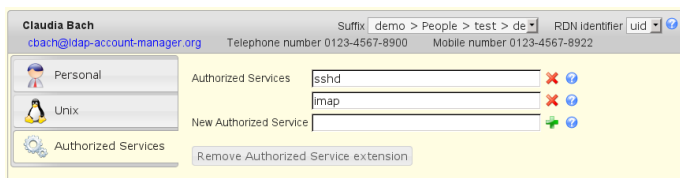


Authorized services

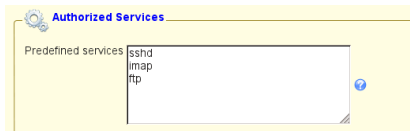
You can setup PAM to check if a user is allowed to run a specific service (e.g. sshd) by reading the LDAP attribute "authorizedService". This way you can manage all allowed services via LAM.

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

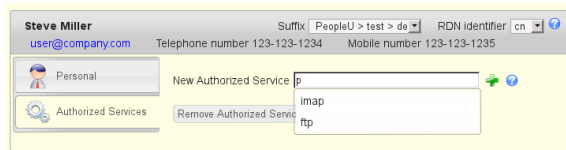
Inside LAM you can now set the allowed services. You may also setup default services in your account profiles.



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



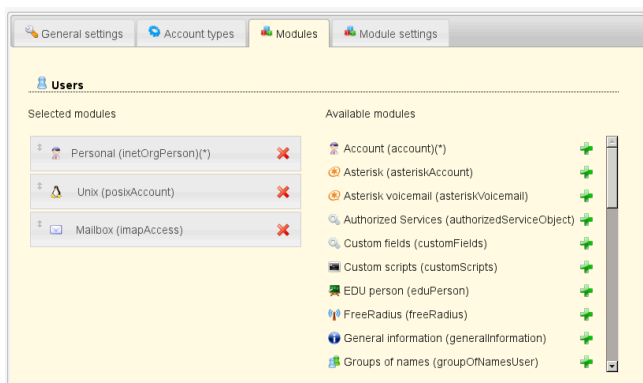
The autocompletion will show all values that contains the entered text. To display the whole list you can press backspace in the empty input field. Of course, you can also insert a service name that is not in the list.



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:



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.

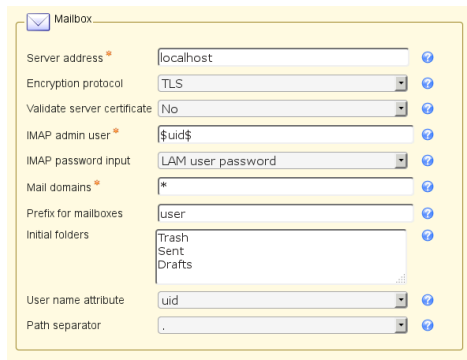
You need to install the SSL certificate of the CA that signed your server certificate. This is usually done by installing the certificate in /etc/ssl/certs. Different Linux distributions may offer different ways to do this. For Debian please copy the certificate in "/usr/local/share/ca-certificates"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

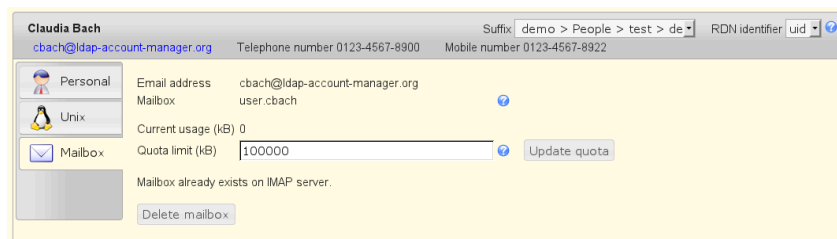
Managing entries in your LDAP directory



Mailbox configuration form with the following fields:

- Server address: localhost
- Encryption protocol: TLS
- Validate server certificate: No
- 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.



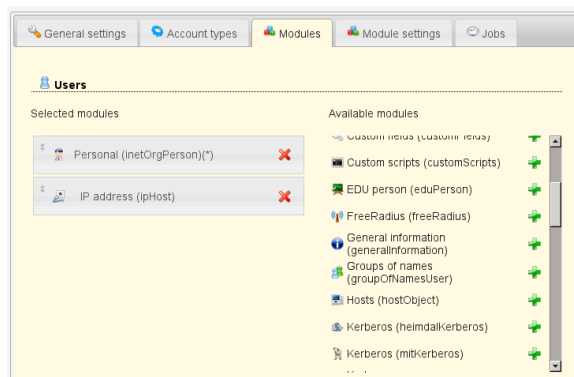
User account edit form for Claudia Bach (cbach@ldap-account-manager.org). The "Mailbox" tab is active, showing:

- Email address: cbach@ldap-account-manager.org
- Mailbox: user.cbach
- Current usage (kB): 0
- Quota limit (kB): 100000
- Buttons: Update quota, Delete mailbox
- Status: Mailbox already exists on IMAP server.

IP addresses (LAM Pro)

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

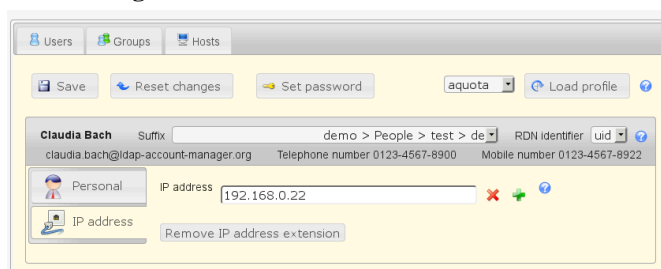
Configuration



Module configuration window showing "Users" selected. The "Available modules" list includes:

- Custom scripts (customScripts)
- EDU person (eduPerson)
- FreeRadius (freeRadius)
- General information (generalInformation)
- Groups of names (groupOfNamesUser)
- Hosts (hostObject)
- Kerberos (heimdalkerberos)
- Kerberos (mitk(erberos))

User editing



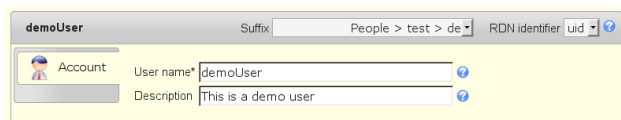
User editing form for Claudia Bach. The "IP address" tab is active, showing:

- IP address: 192.168.0.22
- Buttons: 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".

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



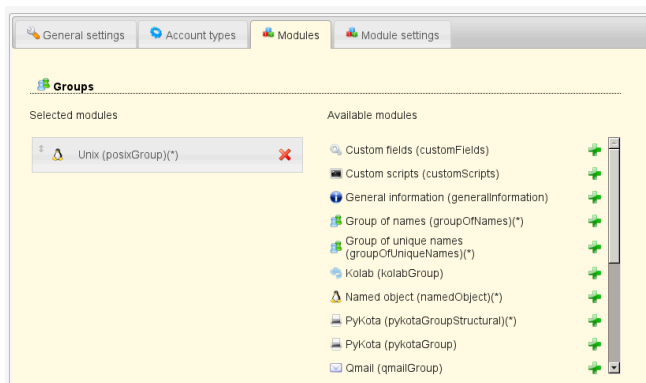
Groups

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

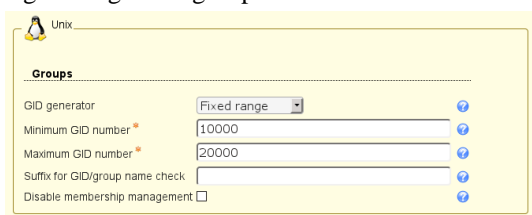
Please add the account type "Groups" and then select account module "Unix (posixGroup)".



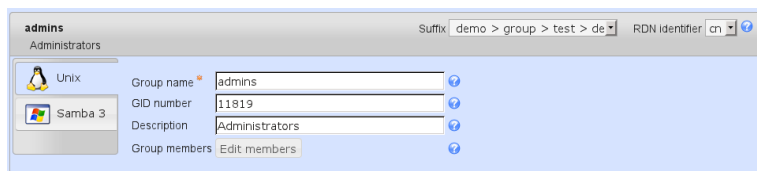
GID generator: LAM will suggest GID numbers for your accounts. Please note that it may happen that there are duplicate IDs assigned if users create groups at the same time. Use an overlay [<http://www.openldap.org/doc/admin24/overlays.html>] like "Attribute Uniqueness" (example) if you have lots of LAM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

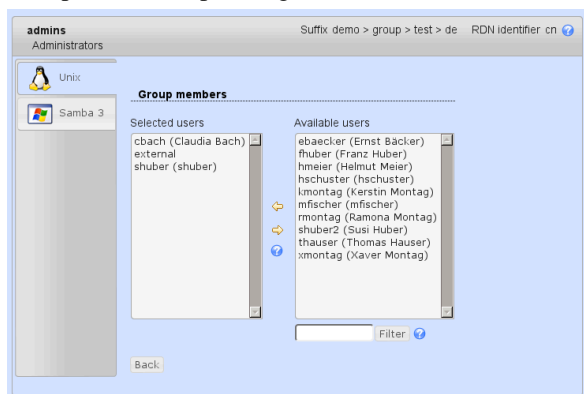
Disable membership management: Disables group membership management. This is useful if memberships are e.g. managed via group of names.



Group management:



Group membership management:



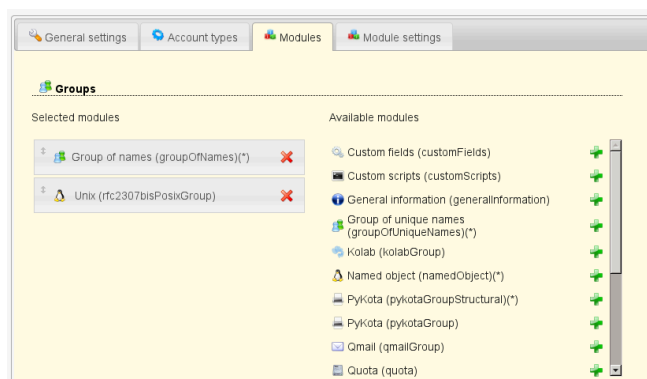
Unix groups with rfc2307bis schema (LAM Pro)

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:



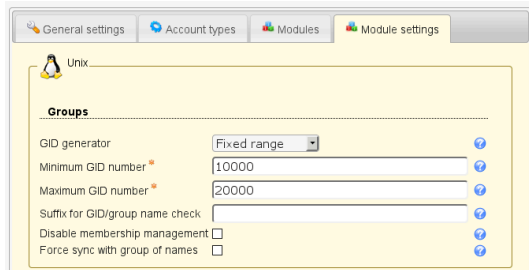
GID generator: LAM will suggest GID numbers for your accounts. Please note that it may happen that there are duplicate IDs assigned if users create groups at the same time. Use an overlay [<http://www.openldap.org/doc/admin24/overlays.html>] like "Attribute Uniqueness" (example) if you have lots of LAM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

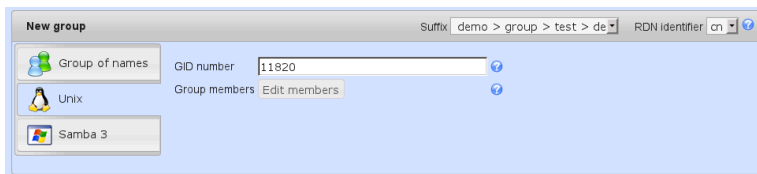
- **Magic number:** Use this if your LDAP server assigns the GID numbers automatically (e.g. DNA by 389 server). Enter the server's magic number setting.

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

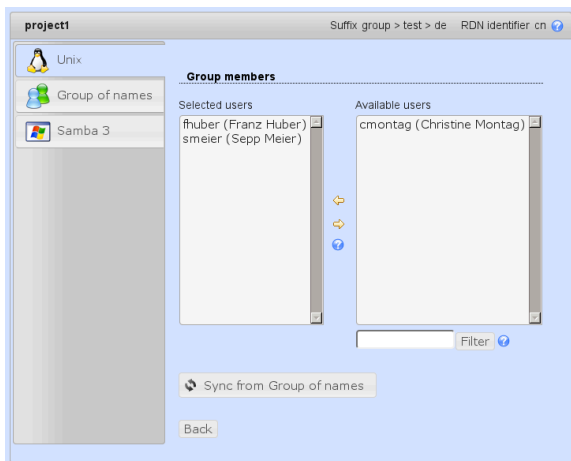
Force sync with group of names: This will automatically set the group memberships of the Unix part to the same members as set on group of names tab.



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



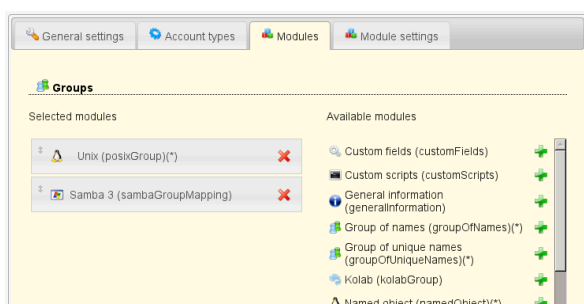
Group members can be edited and also synced with Group of (unique) names.



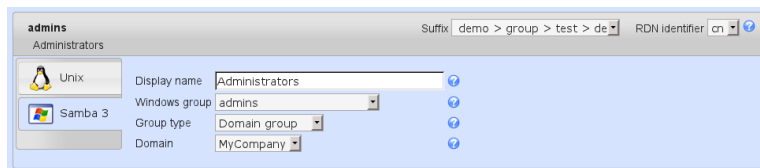
Samba 3

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

Module activation:

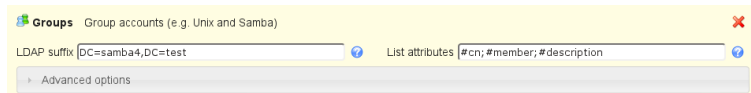


Group editing:

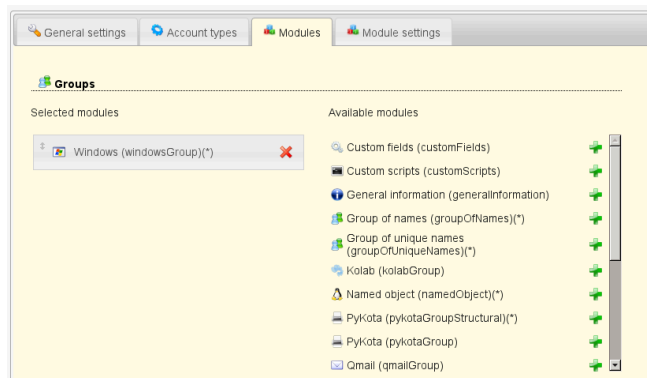


Windows (Samba 4)

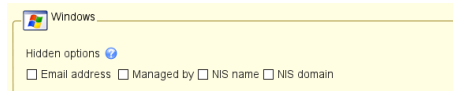
LAM can manage your Windows groups. Please enable the account type "Groups" in your LAM server profile and then add the group module "Windows (windowsGroup)(*)".



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.



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



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:

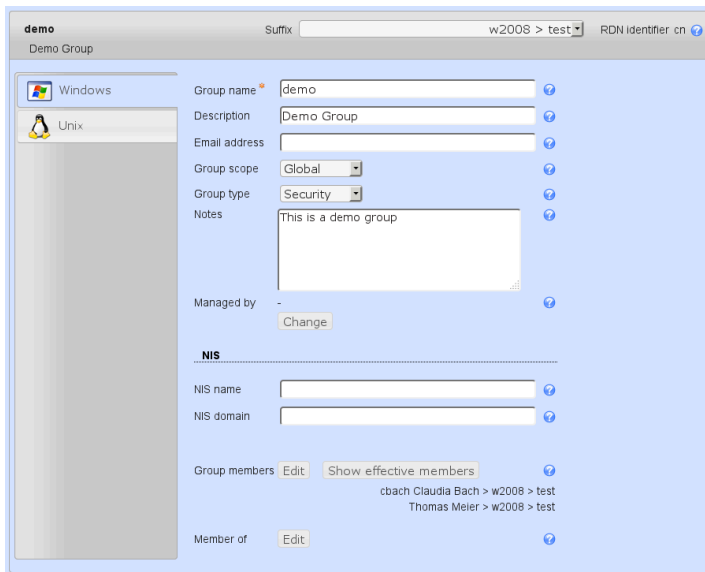
- Global: Use this for groups with frequent changes. Global groups are not replicated to other domains.
- Universal: Groups with universal scope are used to consolidate groups that span domains. They are globally replicated.
- Domain local: Groups with domain local scope can be used to set permissions 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.

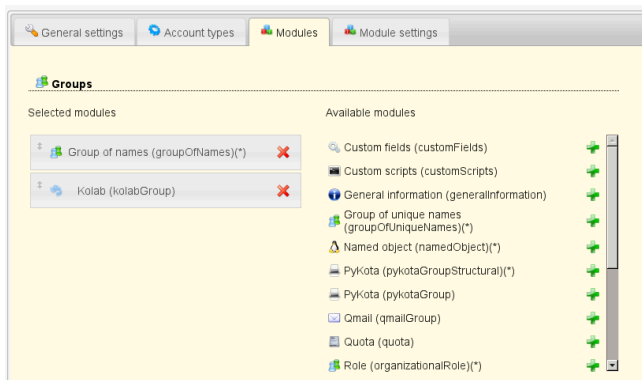
With "Show effective members" you can show a list of all members of this group including members of subgroups and their subgroups.

Managing entries in your LDAP directory

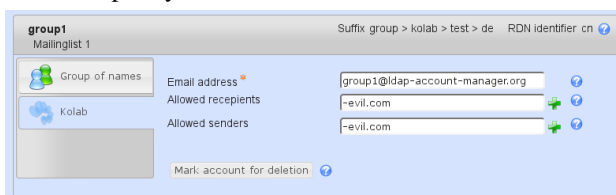


Kolab

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



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



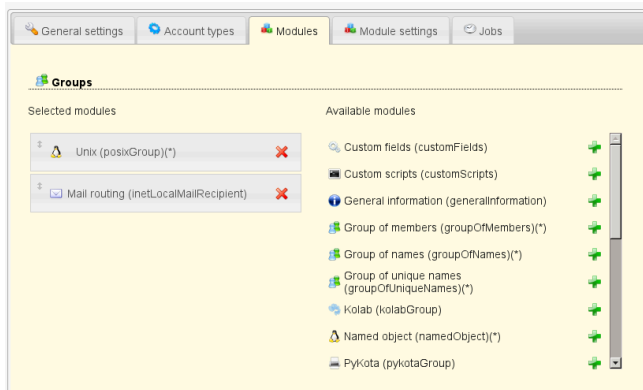
Mail routing

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.

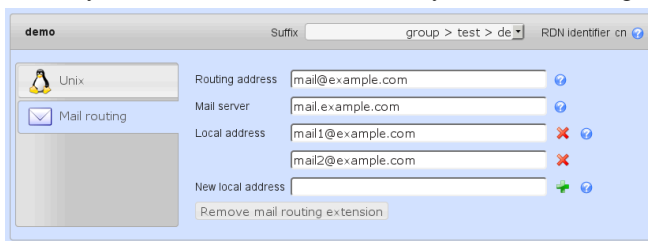
Managing entries in your LDAP directory



Usage:

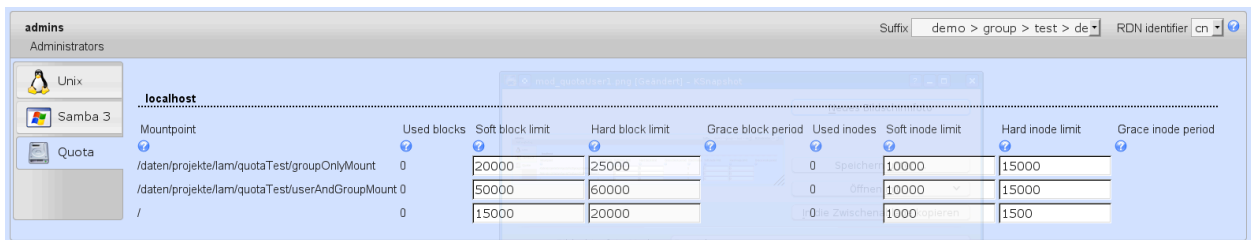
You can specify a routing address, the mail server and a number of local addresses to route.

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



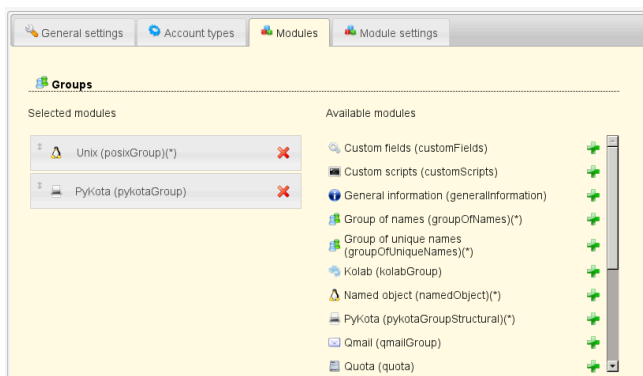
Quota

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.



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 (pykotaGroupStructural(*))" and "PyKota (pykotaGroup)" in all other cases.



Now you can add the PyKota extension to your groups.

The screenshot shows a web interface for configuring the PyKota extension. At the top, there's a breadcrumb trail: "demo > Suffix groups > pykota > test > de". Below this, there are two tabs: "Unix" and "PyKota". The "PyKota" tab is active, showing a form with "Pykota group name" set to "demo" and "Limit type" set to "Quota". There is a "Remove PyKota extension" button at the bottom.

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 "Device" configuration page for an entry named "demoserver". The breadcrumb trail is "cn=demoserver,ou=demo,ou=machines,o=test,c=de". The "Suffix" is "demo > machines > test > de" and the "RDN identifier" is "cn". The form includes fields for "Name" (demoserver), "Description", "Serial number", "Location", and "Owner" (kmontag > demo > People > test > de). There are "Change" and "Remove" buttons.

Samba 3

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

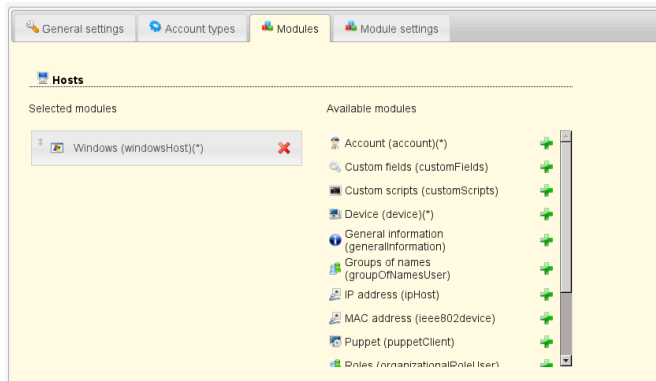
The first screenshot shows the "Account" configuration for "pc01\$". The breadcrumb trail is "pc01\$ > pc01". The "Suffix" is "demo > machines > test > de" and the "RDN identifier" is "uid". The form includes fields for "User name" (pc01\$), "Common name" (pc01), "UID number" (25000), "Gecos", "Primary group" (admins), and "Password" (with "Lock password" and "Remove password" buttons). The second screenshot shows the "Samba 3" configuration for the same entry. It includes fields for "Display name" (PC 01), "Domain" (MyCompany), and "Reset password" (with a "Reset" button). There is a "Remove Samba 3 extension" button at the bottom.

Windows (Samba 4)

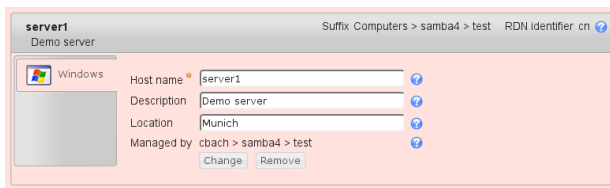
LAM can manage your Windows servers and workstations. Please enable the account type "Hosts" in your LAM server profile and then add the host module "Windows (windowsHost)(*)".

The screenshot shows the "Hosts" configuration page. The breadcrumb trail is "Hosts > Host accounts (e.g. Samba)". The "LDAP suffix" is "CN=Computers,DC=samba4,DC=test" and the "List attributes" is "#cn;#description;#location". There is an "Advanced options" link at the bottom.

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.



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

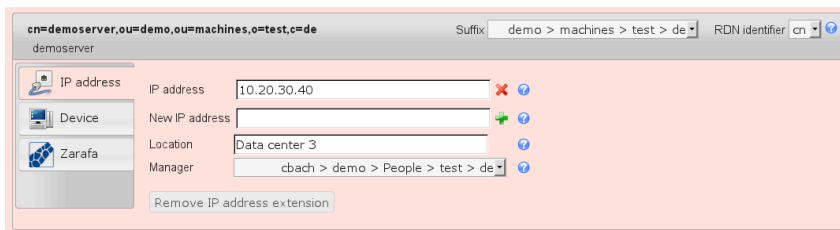


IP addresses (LAM Pro)

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

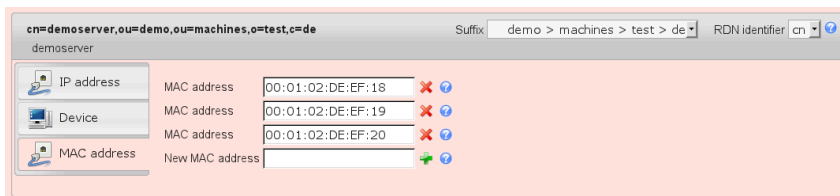
- IP addresses (IPv4/IPv6)
- location of the host
- manager: the person who is responsible for the host

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



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.

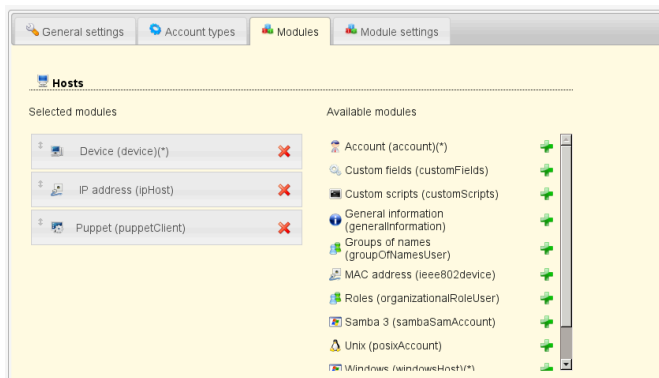


Puppet

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

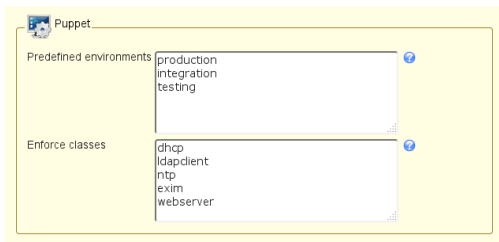
Configuration

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.



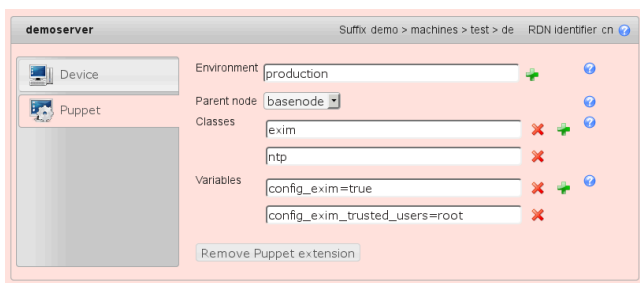
On tab "Module settings" in your LAM server profile you may also setup some common environment names. LAM will use them to provide autocompletion hints when editing the environment for a node.

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



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.

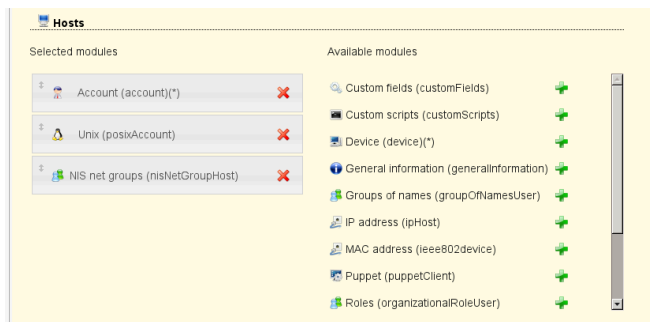


NIS net groups

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.



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.

| Group | User name | Domain name |
|---------|-----------|-------------|
| group01 | user1 | |
| group02 | user2 | |

Filter: demo

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).

| Available account types | | |
|-------------------------|-------------------------------|----------|
| Aliases | Alias entries | + |
| Asterisk extensions | Asterisk extensions entries | + |
| DHCP | DHCP administration | + |
| NIS netgroups | NIS netgroup entries | + |
| NIS objects | NIS object entries | + |
| Password policies | Password policies (ppolicy) | + |
| 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.

Domain name: MyCompany
Domain SID: S-1-2-33-1234-1234-1234

Password policy

| | |
|--|---------|
| Minimal password length | 0 |
| Password history length | 0 |
| Logon for password change | Off |
| Disconnect users outside logon hours | On |
| Allow machine password changes | - |
| Lockout users after bad logon attempts | |
| Minimum password age | 36400 |
| Maximum password age | 1209600 |
| Lockout duration | |
| Reset time after lockout | |

RID settings

| | |
|----------------|------|
| Next RID | |
| Next user RID | |
| Next group RID | |
| RID base | 1000 |

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

Active account types

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

LDAP suffix: ou=People,o=test,c=de List attributes: #uid;#givenName;#sn;#uidNumber;#gidNumber

Advanced options

Groups of names Group of names accounts

LDAP suffix: ou=gon,o=test,c=de List attributes: #cn;#owner;#member

Advanced options

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

General settings Account types Modules Module settings

Groups of names

Selected modules: Group of names (groupOfNames)(*)

Available modules:

- Custom fields (customFields)
- Custom scripts (customScripts)
- General information (generalInformation)
- Group of unique names (groupOfUniqueNames)(*)
- Role (organizationalRole)(*)
- Zarafa (zarafaGroup)

General settings Account types Modules Module settings Jobs

Groups of names

Selected modules: Group of members (groupOfMembers)(*)

Available modules:

- Custom fields (customFields)
- Custom scripts (customScripts)
- General information (generalInformation)
- Group of names (groupOfNames)(*)
- Group of unique names (groupOfUniqueNames)(*)
- Role (organizationalRole)(*)
- Zarafa (zarafaGroup)

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.

General settings Account types Modules Module settings

Group of names

Members are optional ☐

Display format: uid

Hidden options

☐ Owners ☐ Description

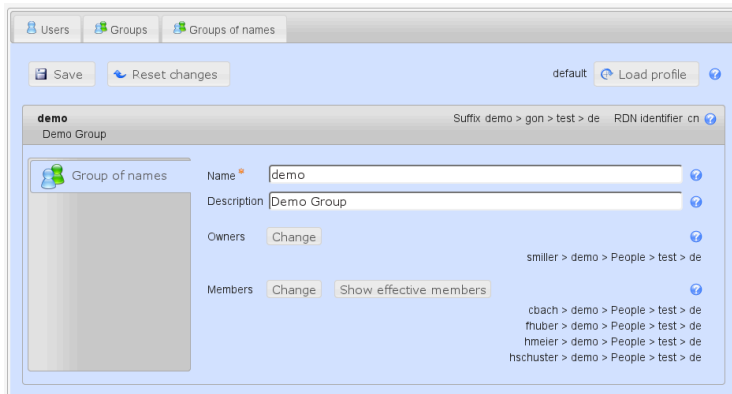
Group management:

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.

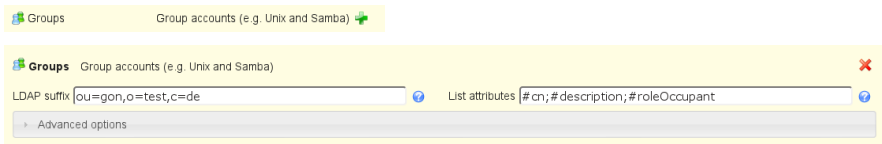


Organizational roles (LAM Pro)

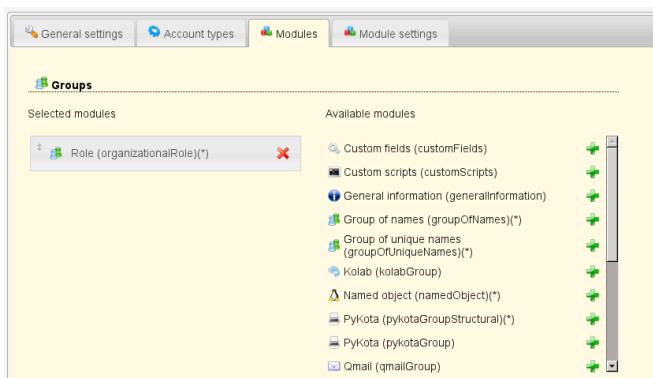
This module manages roles via the organizationalRole object class. There is also a user module to manage memberships on the user edit page.

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".

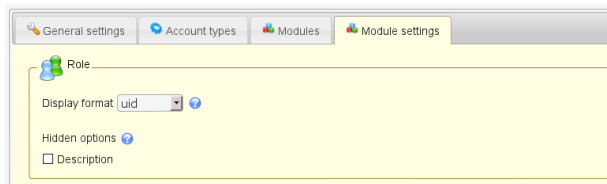


Then add the module "Role (organizationalRole)".



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

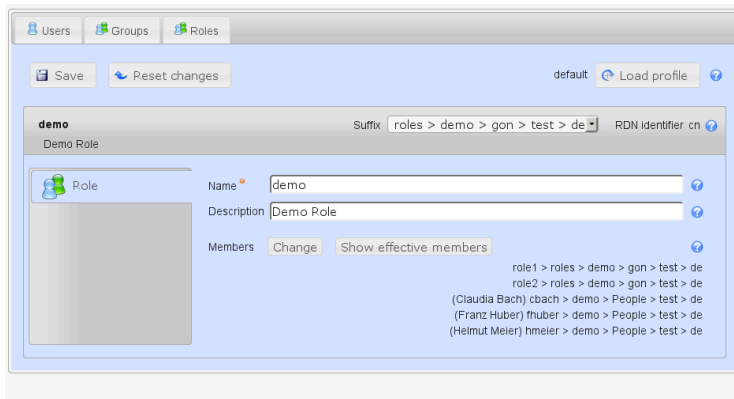
Managing entries in your LDAP directory



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).

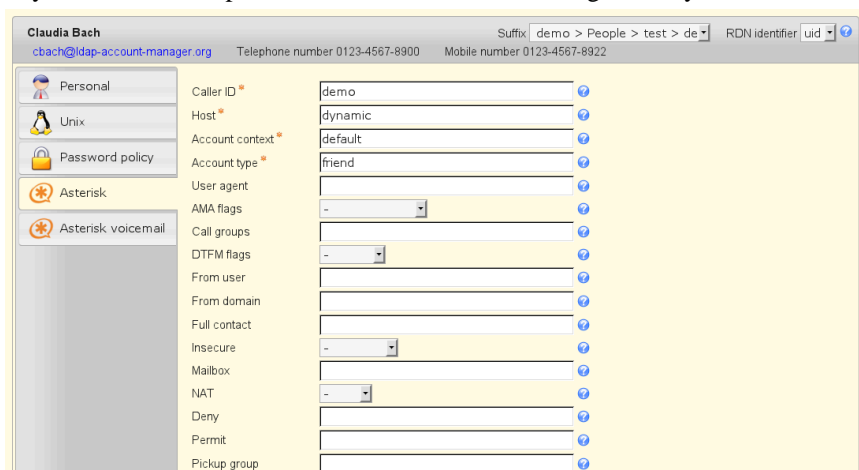
To show members of nested roles click on "Show effective members". Please note that for large roles this will run lots of queries against your LDAP server.



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.



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: myrealm

Hidden options

| | | | |
|--|---|---|---|
| <input type="checkbox"/> 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 | | | |

Of course, the voicemail part of Asterisk is also supported.

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

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

Personal: Mailbox: demo, Account context: context

Unix: Full name, Email address, Pager, Options, Voicemail context

Asterisk: Asterisk voicemail

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.

demo Suffix: asteriskExt > test > de RDN identifier: cn

Asterisk extension: Extension name: demo, Account context: demoContext

Rules:

Application: app1, Application data: data1

Application: app2, Application data: data2

Extension owners: Change admin > test > de

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:

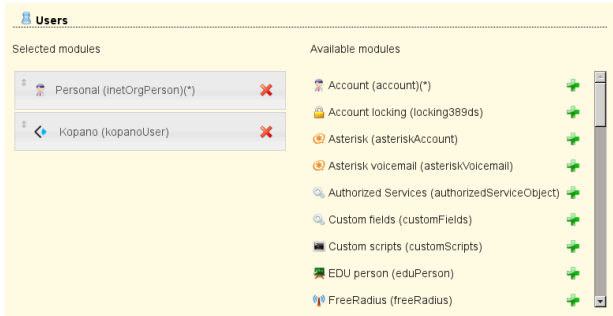
Users User accounts (e.g. Unix, Samba and Kolab)

Adjust the suffix and list attributes to your needs.

Managing entries in your LDAP directory



Then select the Kopano user module (tab Modules). You can combine it with Personal module, Unix or Windows.



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 Zarafa ldap.cfg:

"Send as" attribute: dn

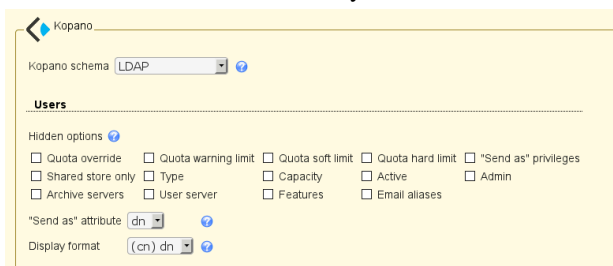
```
ldap_user_sendas_attribute_type = dn
```

"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.



Usage

Managing entries in your LDAP directory

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.

The screenshot shows the user configuration page for 'Claudia Bach' (cbach@ldap-account-manager.org). The 'Kopano' tab is active. The interface includes sections for 'Email aliases', '*Send as*' privileges, 'Quota' settings (override, warning limit, soft limit, hard limit), 'Resource settings' (Type, Capacity), 'Archiving' (Archive servers), and 'Options' (Hidden, Shared store only, Active, Admin, User server, Features). A 'Remove Kopano extension' button is at the bottom.

Contacts

Configuration

The configuration is similar to users. Instead of the Kopano user module please select the contact module.

The screenshot shows the 'Contacts' configuration page. It includes fields for 'LDAP suffix' (ou=kopano2,o=test,c=de), 'List attributes' (#uid;#givenName;#sn;#mail), 'Custom label' (Contacts), and 'Additional LDAP filter'. Below these are checkboxes for 'Read-only', 'Hidden', 'No new entries', and 'Disallow delete'. The bottom section shows 'Selected modules' (Personal, Kopano contact) and a list of 'Available modules' (Account, Account locking, Asterisk, Asterisk voicemail, Authorized Services, Custom fields, Custom scripts, EDU person, FreeRadius).

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 ☐

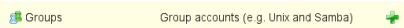
Active ☒

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:



Adjust the suffix and list attributes to your needs.

Groups Group accounts (e.g. Unix and Samba)

LDAP suffix ou=kopano,o=test,c=de

List attributes #cn;#description;#member

Custom label

Additional LDAP filter

Read-only ☐ Hidden ☐ No new entries ☐ Disallow delete ☐

Then select the Kopano group module (tab Modules). You can combine it with groups of names module, Unix or Windows.

Groups

Selected modules

Available modules

Group of names (groupOfNames(*)

Kopano (kopanoGroup)

Custom fields (customFields)

Custom scripts (customScripts)

General information (generalInformation)

Group of members (groupOfMembers(*)

Group of unique names (groupOfUniqueNames(*)

Kolab (kolabGroup)

Mail routing (inetLocalMailRecipient)

Named object (namedObject(*)

Pykota (pykotaGroup)

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.

Managing entries in your LDAP directory

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):

Adjust the suffix and list attributes to your needs.

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

Kopano address list (kopanoAddressList(*)

Available modules

Custom fields (customFields)

Custom scripts (customScripts)

General information (generalInformation)

Usage

LAM Pro will now display the Kopano address list tab.

Users Groups Kopano address lists Kopano dynamic groups Contacts Hosts

New address list Delete selected address lists File upload

Address list count: 1

| Select all | List name | Base | Filter |
|--------------------------|-----------|-------------|---------------------------|
| <input type="checkbox"/> | all | o=test,c=de | (objectclass=kopano-user) |

Kopano address list

List name all

Base o=test,c=de

Filter (objectclass=kopano-user)

Hidden ☐



Active ☒

Dynamic groups

Configuration

Managing entries in your LDAP directory

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.

Kopano dynamic groups Kopano dynamic groups 

LDAP suffix  List attributes 



Custom label  Additional LDAP filter 

Read-only ☐  Hidden ☐  No new entries ☐  Disallow delete ☐ 







Then select the Kopano dynamic group module (tab Modules).

Kopano dynamic groups

Selected modules

-  Kopano dynamic group (kopanoDynamicGroup)(*) 




Available modules

-  Custom fields (customFields) 
-  Custom scripts (customScripts) 
-  General information (generalInformation) 




Usage

LAM Pro will now display the Kopano address list tab.



Users Groups **Kopano address lists** Kopano dynamic groups Contacts Hosts

 New group  Delete selected groups  File upload


Group count: 1


| Select all | Group name | Email | Email aliases | Base | Filter |
|--------------------------|--|---|---------------|-----------------------|----------|
| <input type="checkbox"/> |   munich |  munich@ldap-account-manager.org | | ou=kopano,o=test,c=de | l=Munich |


Select all

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

To enable Kopano support for servers please activate the Kopano server module for the hosts account type in your server profile (tab account types):



 Hosts Host accounts (e.g. Samba) 

Adjust the suffix and list attributes to your needs.

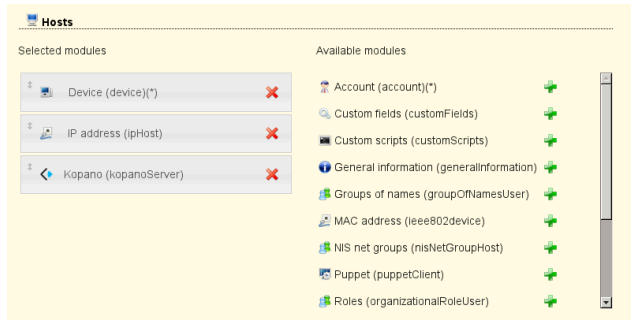
Hosts Host accounts (e.g. Samba) 

LDAP suffix  List attributes 

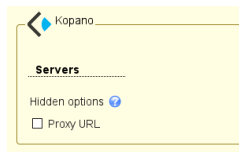
Custom label  Additional LDAP filter 

Read-only ☐  Hidden ☐  No new entries ☐  Disallow delete ☐ 

Then select the Kopano server module (tab Modules).

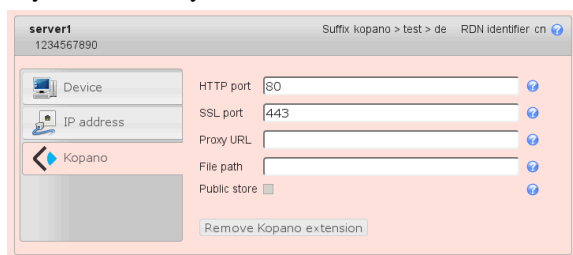


Next configure the module to your needs (tab Module settings).



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.



Zarafa (LAM Pro)

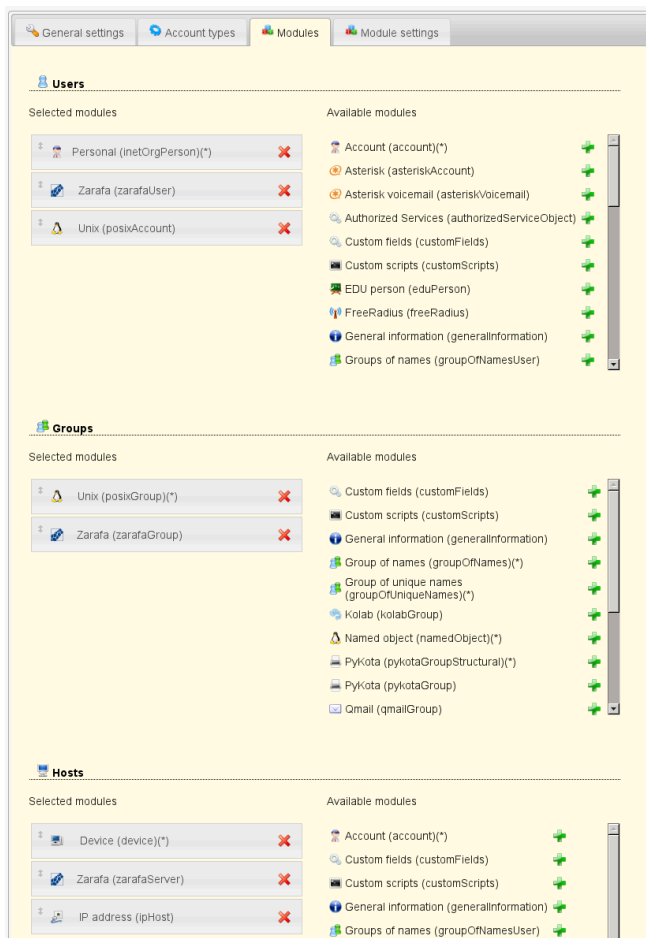
Zarafa is an OpenSource collaboration software. LAM Pro provides support to manage Zarafa server entries, users and groups. It covers all settings for these types including resource and quota settings.

LAM Pro is an official Zarafa Certified Integration.

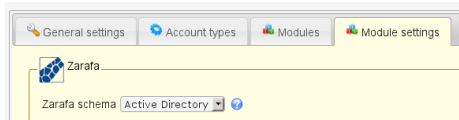


Configuration

To enable Zarafa support in LAM Pro please activate the Zarafa modules for the Users, Groups and Hosts account types in your server profile:



Attention: LAM Pro uses the Zarafa OpenLDAP schema as 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 configure which parts of the Zarafa user options should be enabled. E.g. if you do not want to manage quotas per user then you can hide these options on the tab "Module settings".

"Send as" attribute: Here you can specify how "Send as" privileges should be managed. LAM supports "uid" and "dn".

If you select "uid" the LAM will store user names in the `zarafaSendAsPrivilege` attribute. This way you are restricted to specify user accounts as "Send as" allowed.

You can also set this option to "dn" and LAM will store DN's in the `zarafaSendAsPrivilege` attribute. In this case you may specify users and groups as "Send as" allowed.

Examples for your Zarafa `ldap.cfg`:

"Send as" attribute: **dn**

```
ldap_user_sendas_attribute_type = dn
```

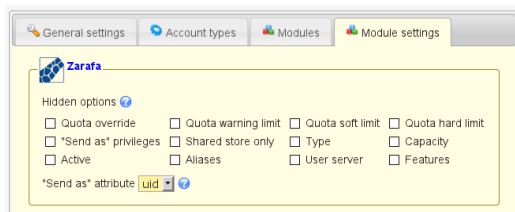
"Send as" attribute: **uid**

`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.

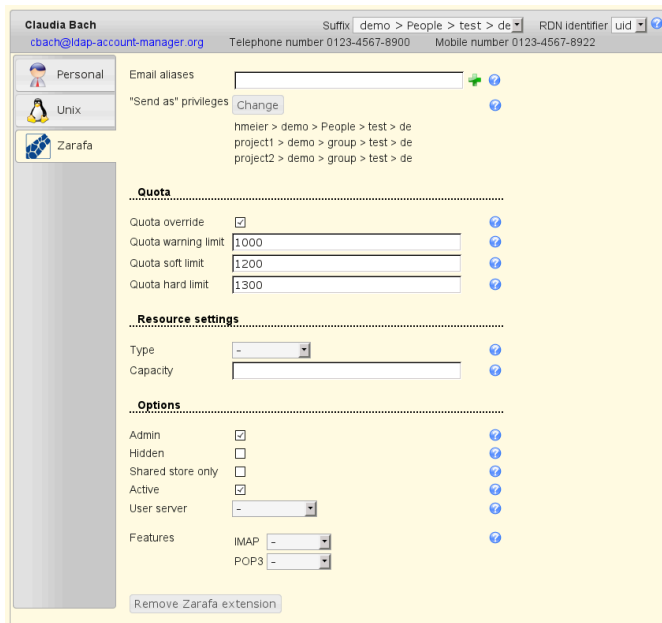
Features: Zarafa 7 allows to enable IMAP/POP3 for each user. Please hide the option "Features" if you use Zarafa 6.x.



Users

This is an example of the user edit page with all possible settings. 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 Zarafa extension can be added and removed at any time for every user.

Please note that the option "Features" requires Zarafa 7. Please hide this option in the LAM server profile if you run Zarafa 6.x.



Contacts

LAM Pro can manage your Zarafa contact entries. You can set the email aliases and "send as" privileges. Additionally, accounts may be hidden in the address book or disabled.

Please note that you can either use the Zarafa user module or Zarafa contact. LAM Pro will disable the other tab when enabling one of them.

Claudia Bach
cbach@company.com

Suffix: People > Idap-account-manager > org RDN identifier: uid

Personal
Email aliases: cbach@ldap-account-manager.org

Unix
"Send as" privileges: Change

Zarafa contact
efischer > People > Idap-account-manager > org
emontag > People > Idap-account-manager > org
fmaier > People > Idap-account-manager > org
project1 > group > Idap-account-manager > org

Options
Hidden: ☐
Active: ☒

Remove Zarafa extension

Groups

This is the edit page for groups. You can enter an email address and additional aliases for your groups. It is also possible to specify options (e.g. hide from address book). The extension can be added/removed dynamically.

Please note that the option "Send-as privileges" requires the Zarafa 7.0.3 schema. Please hide this option in the LAM server profile if you run Zarafa < 7.0.3.

zgroup1
Suffix: zarafa > test > de RDN identifier: cn

Unix
Zarafa

Email
Email: zgroup1@ldap-account-manager.org
Email aliases: zgt1@ldap-account-manager.org

"Send as" privileges: Change
cbach > zarafa > test > de
smeier > zarafa > test > de
zgroup2 > zarafa > test > de

Options
Security group: ☒
Hidden: ☐
Active: ☒

Remove Zarafa extension

Servers

The Zarafa extension for host accounts allows to set the connection ports and file path. You can add/remove the extension at any time.

Setting the public store option is only possible for new host entries.

Please note that the proxy URL option requires the Zarafa 7.1 schema. Please hide this option in your LAM server profile if you use an older version.

server1
Zarafa server 1
Suffix: zarafa > test > de RDN identifier: cn

Device
HTTP port: 80
SSL port: 443
Proxy URL: https://zproxy.example.com:237/server1
File path:
Public store: ☒

Remove Zarafa extension

Address lists

Zarafa allows to store address lists in LDAP. You need to define a search base and LDAP filter for each address list. E.g. entering "ou=people,dc=company,dc=com" as base and "uid=*" will select all users that are stored in "ou=people,dc=company,dc=com".

You can also hide your lists from the address book or temporarily disable them.

The screenshot shows the 'allUsers' address list configuration. At the top, there are buttons for 'Save', 'Reset changes', a dropdown menu set to 'aaa', and a 'Load profile' button. Below this, the 'Suffix' is 'zarafa-lists > ldap-account-manager > org' and the 'RDN identifier' is 'cn'. The main configuration area includes: 'List name' (allUsers), 'Base' (ou=people,dc=ldap-account-manager,c), 'Filter' (uid=*), 'Hidden' (unchecked), and 'Active' (checked).

Dynamic groups

Zarafa allows to define dynamic groups in LDAP. You need to define a search base and LDAP filter for each group. E.g. entering "ou=people,dc=company,dc=com" as base and "uid=*" will select all users that are stored in "ou=people,dc=company,dc=com".

Dynamic groups may have an email address and multiple email alias addresses.

You can also hide your dynamic groups from the address book or temporarily disable them.

The screenshot shows the 'allUsers' dynamic group configuration. The 'Suffix' is 'zarafa-groups > ldap-account-manager > org' and the 'RDN identifier' is 'cn'. The main configuration area includes: 'Group name' (allUsers), 'Base' (ou=people,dc=ldap-account-manager,c), 'Filter' (uid=*), 'Email' (allUsers@ldap-account-manager.org), 'Email aliases' (all@ldap-account-manager.org), and 'Options' (Hidden unchecked, Active checked).

Kolab shared folders

Please add the account type "Kolab shared folders" in your LAM server profile and set the correct LDAP suffix.

The screenshot shows the 'Available account types' section. It lists 'Kolab shared folders' and 'Kolab shared folders (e.g. mail folders)' with a green plus icon next to the latter.

The screenshot shows the 'Kolab shared folders' configuration section. It includes fields for 'LDAP suffix' (ou=shared_folders,dc=localdomain) and 'List attributes' (#cn; #kolabDelegate; #alias). There is an 'Advanced options' link below.

Then add the "Kolab shared folder" module on tab "Modules".

The screenshot shows the 'Modules' section. It lists 'Selected modules' (Kolab shared folder (kolabSharedFolder)*) and 'Available modules' (Custom fields (customFields), Custom scripts (customScripts), General Information (generalInformation)).

Now you can start to add shared folders inside LAM.

The screenshot shows the 'webtest' configuration window for a 'Kolab shared folder'. The interface includes fields for Name, Email address, Mailbox home server, Target IMAP folder, Type, Allowed recipients, and Allowed senders. Below these are sections for 'Email aliases' and 'Delegates'. The 'Allowed recipients' and 'Allowed senders' fields contain 'admin.admin@localdomain'. The 'Email aliases' section has 'webt@localdomain'. The 'Delegates' section has 'admin.admin@localdomain'. There are also buttons for adding and removing entries, and a 'Mark account for deletion' button.

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:

The screenshot shows the 'Available account types' section. It lists 'DHCP' with a sub-entry 'DHCP administration'. There is a green plus button next to 'DHCP administration'.

Set suffix:

The screenshot shows the 'Active account types' section for 'DHCP'. It displays the 'LDAP suffix' as 'cn=dhcp,o=test,c=de' and the 'List attributes' as '#cn;#dhcpRange;#fixed_ips'. There is an 'Advanced options' link below.

Add modules:

The screenshot shows the 'DHCP' module configuration section. It lists 'Selected modules' and 'Available modules'. The 'Selected modules' list includes 'DHCP settings (dhcp_settings)(*)', 'Ranges (range)', 'DDNS (ddns)', and 'Hosts (fixed_ip)'. The 'Available modules' list includes 'Custom fields (customFields)', 'Custom scripts (customScripts)', and 'General information (generalInformation)'. There are red minus buttons next to the selected modules and green plus buttons next to the available modules.

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}XXXXXXXXXXXX";
ldap-base-dn "ou=dhcp,dc=ldap-account-manager,dc=org";
ldap-method dynamic;
ldap-debug-file "/var/log/dhcp-ldap-startup.log";
```

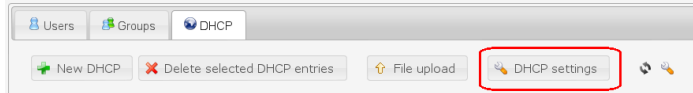
slapd.conf changes:

```
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:



You can easily create new subnet entries.

A screenshot of the 'DHCP settings' form for a subnet. The form is titled '192.168.1.0 Demo subnet' and has a breadcrumb trail 'Suffix server > test > de' and 'RDN identifier cn'. On the left, there is a sidebar with icons for 'DHCP settings', 'Hosts', 'Ranges', and 'DDNS'. The main area contains the following fields: 'Subnet' (192.168.1.0), 'Domain name' (demo), 'Lease time' (empty), 'Maximum lease time' (empty), 'DNS' (192.168.1.1), 'Default gateway' (192.168.1.1), 'Netbios name servers' (192.168.1.1), 'Netbios node type' (H-Node (0x08)), 'Subnet mask' (255.255.255.0), 'Net mask' (24), and 'Description' (Demo subnet). Each field has a help icon (blue question mark) to its right.

It is also possible to specify a list of fixed IPs.

A screenshot of the 'DHCP settings' form for a subnet, showing the 'Hosts' tab. The form is titled '192.168.1.0 Demo subnet' and has a breadcrumb trail 'Suffix server > test > de' and 'RDN identifier cn'. On the left, there is a sidebar with icons for 'DHCP settings', 'Hosts', 'Ranges', and 'DDNS'. The main area contains a table with three columns: 'PC name', 'MAC address', and 'IP address'. The table has three rows of data: 'pc02' with MAC '11:22:33:44:55:ab' and IP '192.168.1.11', 'pc03' with MAC '11:22:33:44:55:a2' and IP '192.168.1.12', and 'pc04' with MAC '11:22:33:44:55:a1' and IP '192.168.1.13'. Each row has a red X icon to its right. At the bottom, there is an empty row with a green plus icon to its right.

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.

A screenshot of the 'DHCP settings' form for a subnet, showing the 'Ranges' and 'Pools' tabs. The form is titled '192.168.1.0 Demo subnet' and has a breadcrumb trail 'Suffix server > test > de' and 'RDN identifier cn'. On the left, there is a sidebar with icons for 'DHCP settings', 'Hosts', 'Ranges', and 'DDNS'. The main area contains the following fields: 'Range from' (192.168.1.1), 'Range to' (192.168.1.10), 'Delete range' (red X icon), 'Range from' (192.168.1.20), 'Range to' (192.168.1.30), 'Delete range' (red X icon), 'Range from' (192.168.1.40), 'Range to' (192.168.1.50), 'Delete range' (red X icon), 'New range' (green plus icon), 'Pools' section, 'Name' (pool1), 'Failover peer' (peer2), 'Delete pool' (trash icon), 'Range from' (192.168.1.80), 'Range to' (192.168.1.90), 'Delete range' (red X icon), 'New range' (green plus icon), and 'New pool' (green plus icon). Each field has a help icon (blue question mark) to its right.

If you activated DDNS in the server entry then you may also specify the DDNS settings for this subnet.

The screenshot shows the '192.168.1.0 Demo subnet' configuration window. On the left, there is a sidebar with icons for 'DHCP settings', 'Hosts', 'Ranges', and 'DDNS'. The 'DDNS' tab is selected. The main area contains three input fields: 'IP address of the DNS server' with the value '192.168.1.1', 'Zone names' with the value 'zone', and 'Reverse zone names' with the value '1.168.192.in-addr.arpa'. Each field has a help icon to its right. At the top right of the window, there is a status bar showing 'Suffix server > test > de' and 'RDN identifier cn'.

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 DLZ patch.

Configuration

First, you need to add the Bind DNS account type and the Bind DLZ module:

This screenshot shows the 'Account types' tab in the configuration interface. Under the heading 'Available account types', there is a single entry: 'Bind DNS' with the description 'Bind DNS entries'. To the right of this entry is a green plus icon, indicating it can be added.

Please set the LDAP suffix either to an existing DNS zone (dlzZone) or an organizational unit that should include your DNS zones.

This screenshot shows the 'Active account types' section. The 'Bind DNS' entry is now active. Below it, the 'LDAP suffix' is configured as 'ou=bind,o=test,c=de'. To the right, the 'List attributes' field contains '#dlzHostName;#zoneName'. There is a red 'X' icon to the right of the entry, and an 'Advanced options' link at the bottom.

This screenshot shows the 'Module settings' tab for the 'Bind DNS' module. On the left, under 'Selected modules', there is a button for 'DNS entry (bindDLZ)(*)' with a red 'X' icon. On the right, under 'Available modules', there are three entries: 'Custom fields (customFields)', 'Custom scripts (customScripts)', and 'General information (generalInformation)', each with a green plus icon.

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.

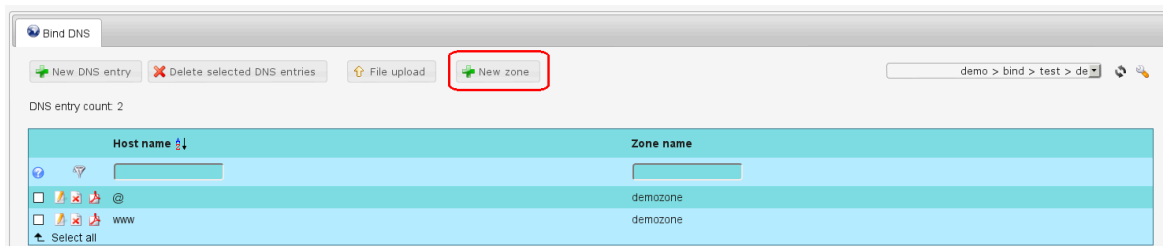
This screenshot shows the 'DNS entry' settings. There is a checkbox labeled 'Automatic PTR changes' which is currently checked.

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".

Managing entries in your LDAP directory

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.



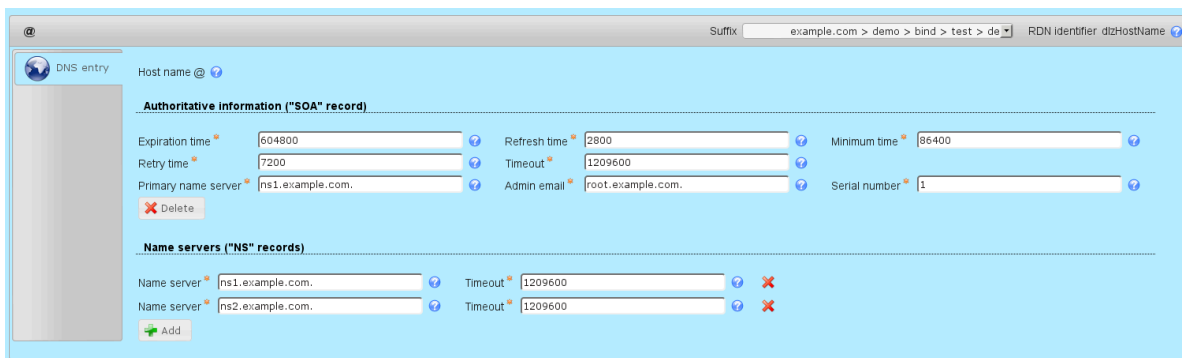
DNS entries

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

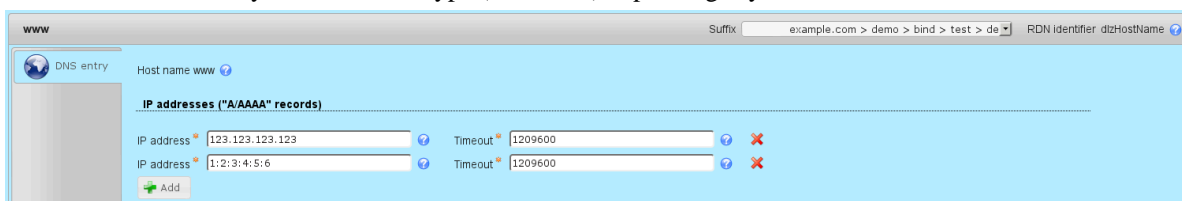
Authoritative (SOA) and name server (NS) records

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).



IP addresses (A/AAAA)

LAM will automatically set the correct type (A/AAAA) depending if you enter an IPv4 or IPv6 address.



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.

The screenshot shows a web interface for managing a DNS entry named '123.123'. The 'Reverse DNS entries ("PTR" records)' section is active, displaying a table with columns for 'Host name' and 'Timeout'. A single record is shown with 'Host name' as 'www.demozone.' and 'Timeout' as '1209600'. There are 'Add' and 'Remove' buttons for each record.

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 a web interface for managing a DNS entry named 'www2'. The 'Alias name ("CNAME" record)' section is active, displaying a table with columns for 'Alias name' and 'Timeout'. A single record is shown with 'Alias name' as 'www' and 'Timeout' as '1209600'. There are 'Add' and 'Remove' buttons for each record.

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 a web interface for managing a DNS entry named 'www'. The 'Mail servers ("MX" records)' section is active, displaying a table with columns for 'Mail server', 'Preference', and 'Timeout'. Two records are shown: one with 'Mail server' as '123.123.123.123', 'Preference' as '50', and 'Timeout' as '1209600'; the other with 'Mail server' as '123.123.123.124', 'Preference' as '60', and 'Timeout' as '1209600'. There are 'Add' and 'Remove' buttons for each record.

Text records (TXT)

Text records can be added to store a description or other data (e.g. SPF information).

The screenshot shows a web interface for managing a DNS entry named 'server1'. The 'Text ("TXT" records)' section is active, displaying a table with columns for 'Text' and 'Timeout'. Two records are shown: one with 'Text' as 'This is a test server' and 'Timeout' as '1209600'; the other with 'Text' as 'Managed by LAM Pro' and 'Timeout' as '1209600'. There are 'Add' and 'Remove' buttons for each record.

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).

The screenshot shows the LAM web interface for managing DNS entries. The top bar indicates the current entry is '_ldap._tcp' with a suffix of 'lam.de > bind > test > de' and an RDN identifier of 'dn:HostName'. The left sidebar shows a tree view with 'DNS entry' selected. The main content area is titled 'Services ("SRV" records)' and displays two existing records. Each record has fields for Priority (10), Weight (80 and 20), Port (389), Server (ldap.example.com. and ldap2.example.com.), and Timeout (1209600). There are 'Delete' buttons for each record and an 'Add' button at the bottom. Below the SRV records, there is a section for 'Text ("TXT" records)' with an 'Add' button.

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:

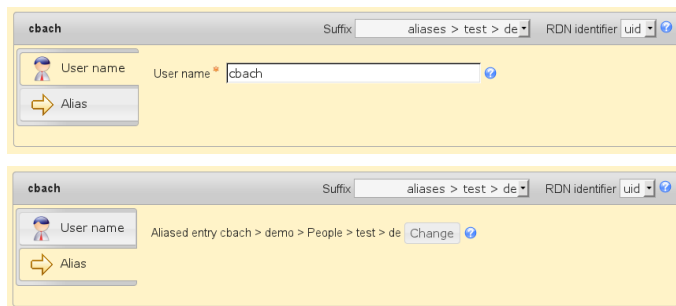
```
dn: dlzZoneName=example.com,ou=bind,dc=example,dc=com
dlzzoneName: example.com
objectclass: dlzZone
objectclass: top
```

Here is the corresponding CSV file: bindUpload.csv [resources/bindUpload.csv]

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.

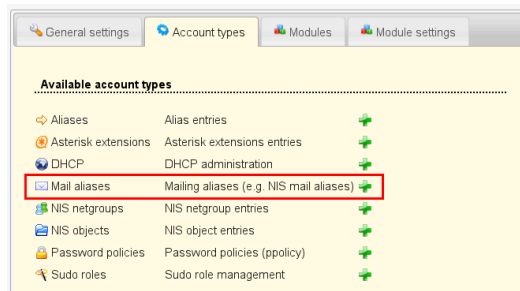
Currently, only user accounts can be aliased with the "uidObject" object class.



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:

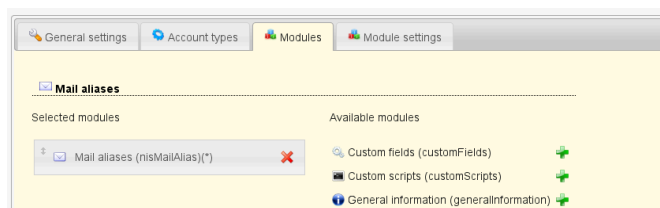


NIS mail aliases

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.



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 'demo' window with the 'Suffix mailaliases > test > de' path. The 'Mail aliases' tab is active. It contains a list of aliases with columns for 'Alias name', 'Recipient', and 'New recipient'. The first alias is 'demo' with recipient 'demo@example.com'. The second is 'some_user' with recipient 'some_user@example.com'. There are icons for adding, deleting, and editing entries.

Courier mail aliases

Mail aliases for Courier SMTP can be used when activating NIS mail aliases and Courier modules:

The screenshot shows the 'demo' window with the 'Suffix mailaliases > test > de' path. The 'Mail aliases' tab is active. It shows a list of 'Selected modules' and 'Available modules'. The 'Selected modules' list includes 'Mail aliases (nisMailAlias(*)' and 'Courier (courierMailAlias)'. The 'Available modules' list includes 'Custom fields (customFields)', 'Custom scripts (customScripts)', and 'General information (generalInformation)'.

You will then get the Courier tab for your mail aliases.

The screenshot shows the 'demo' window with the 'Suffix courier > test > de' path. The 'Courier' tab is active. It contains a list of aliases with columns for 'Email address', 'Recipient address', 'Mail source', and 'Description'. The first alias is 'demo@ldap-account-manager.org' with recipient 'project1@ldap-account-manager.org'. There are icons for adding, deleting, and editing 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 'demo' window with the 'Suffix netgroups > test > de' path. The 'NIS net group' tab is active. It contains a list of net groups with columns for 'Group name', 'Description', 'Subgroups', and 'Members'. The first net group is 'demo' with description 'Demo group' and subgroups 'administrators, group01, group02'. There are icons for adding, deleting, and editing entries.

NIS objects (LAM Pro)

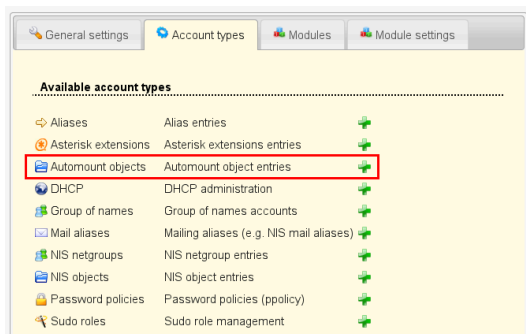
You can manage NIS objects with LAM Pro. This allows you define network mount points in LDAP.

Add the NIS objects type to your LAM configuration and then the NIS objects module. This will add the NIS objects tab to LAM.

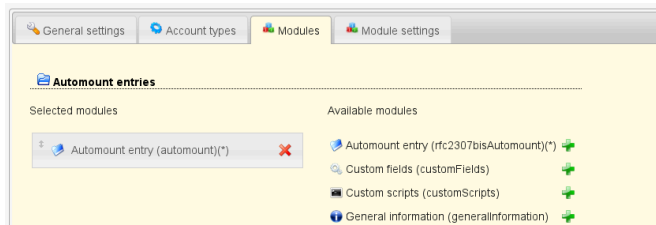
The screenshot shows the 'demo' window with the 'Suffix nisObjects > test > de' path. The 'NIS object' tab is active. It contains a list of NIS objects with columns for 'Name', 'Mapping name', 'Mapping entry', and 'Description'. The first NIS object is '/home' with mapping name 'auto.home' and mapping entry '-fstype=nfs,rw homserver:/home'. There are icons for adding, deleting, and editing entries.

Automount objects (LAM Pro)

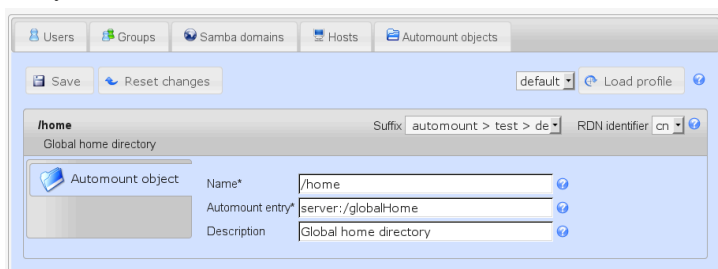
LAM Pro allows you to manage automount entries. Please activate the account type "Automount objects" in your LAM Pro server profile.



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:

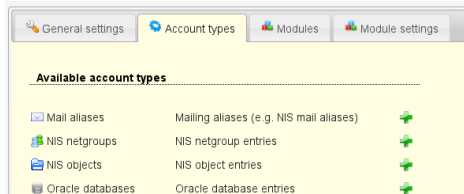
```
dn: cn=OracleContext,dc=example,dc=com
```

```
objectclass: orclContext
cn: OracleContext
```

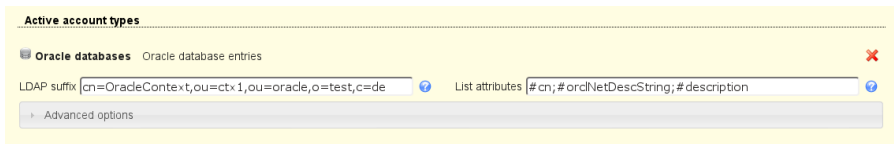
You can create it with LAM's tree view. Please note that "cn" must be set to "OracleContext".

LAM setup:

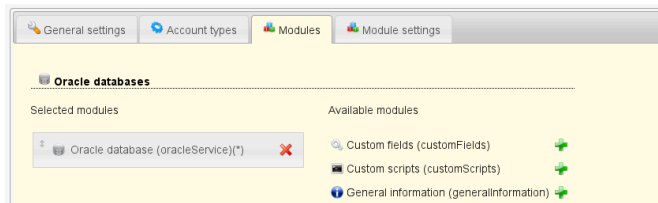
Edit your LAM server profile and add the Oracle account type:



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.



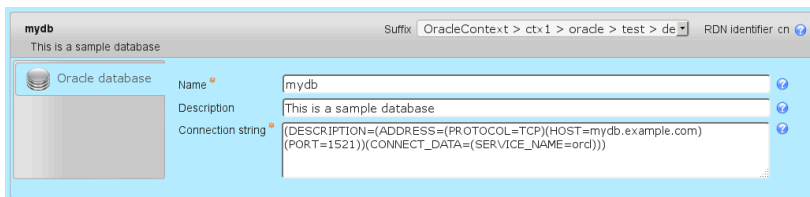
Next, add the Oracle module:



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.



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=OracleContext 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=1521)))
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 'Password policy' configuration window in LAM Pro. The window has a sidebar with a lock icon and the text 'Password policy'. The main area contains a list of settings for a policy named 'default'. The settings include: Name (default), Minimum password age (60), Maximum password age (31536000), Expire warning, Grace authentication limit, Password history length (10), Password quality check (no), Minimum password length, Lockout users (checkbox), Lockout duration, Maximum failure count, Failure count interval, Require password change on first login (checkbox), Allow password change (checkbox), and Password change requires old password (checkbox). Each setting has a help icon to its right.

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.

PyKota printers

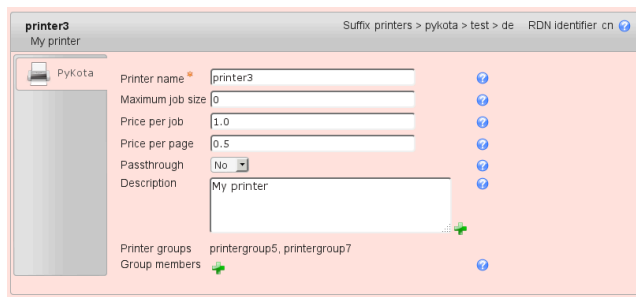
Please add the account type "Printers (PyKota printers)" on tab "Account types" in your server profile and setup the LDAP suffix where printers are stored.

The screenshot shows the 'Printers' configuration window in LAM Pro. The window has a sidebar with a printer icon and the text 'Printers'. The main area contains the configuration for 'Pykota printers'. The 'LDAP suffix' is set to 'ou=printers,ou=pykota,o=test,c=de'. The 'List attributes' field contains '#cn;#description;#pykotaPricePerPage;#pykotaPr'. There is an 'Advanced options' link at the bottom.

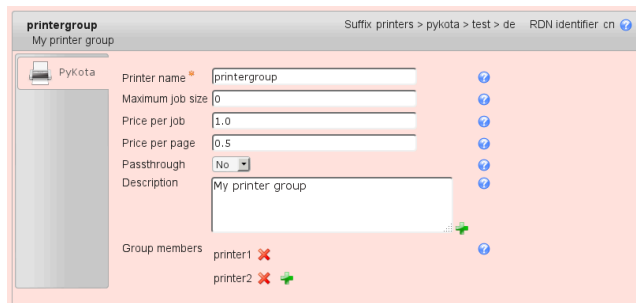
Then add the PyKota printer module on tab "Account modules".

The screenshot shows the 'Account modules' configuration window in LAM Pro. The window has a sidebar with a printer icon and the text 'Printers'. The main area contains the configuration for 'Pykota printers'. The 'Selected modules' list shows 'PyKota (pykotaPrinter)(*)' with a red 'X' icon. The 'Available modules' list shows 'Custom fields (customFields)', 'Custom scripts (customScripts)', and 'General information (generalInformation)' with green plus icons.

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.



You can also setup printer groups. Just add some members to your new group.

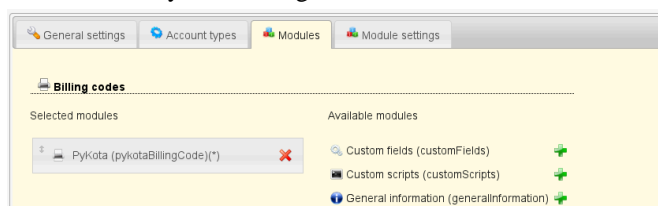


PyKota billing codes

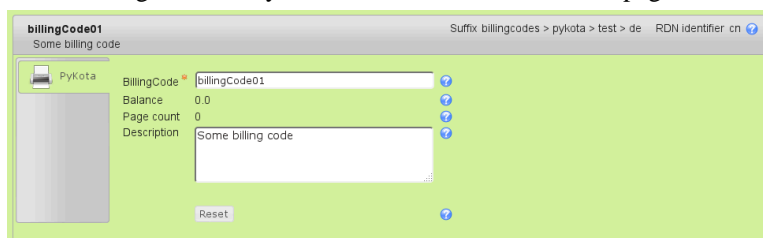
Please add the account type "Billing codes" on tab "Account types" in your server profile and setup the LDAP suffix where billing codes are stored.



Then add the PyKota billing code module on tab "Account modules".



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.



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 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
- Validation via regular expression
- Error message if validation fails

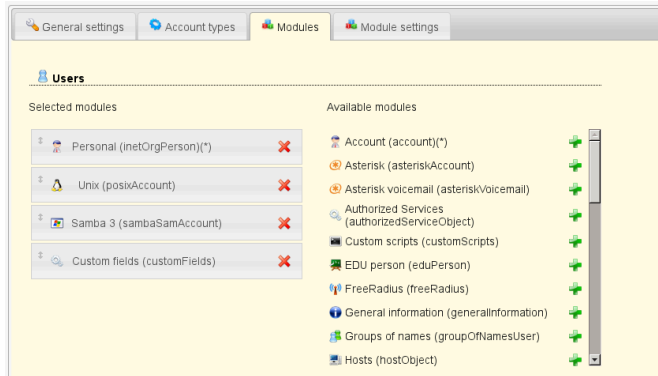
Limitations:

Custom fields cannot manage

- structural object classes
- 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.

Custom fields

Appearance

☐ Display multiple groups as accordion

Users

Label: User label

Icon: http://localhost/lam2/graphics/uid.png

Groups

Label: Group label

Icon: /lam/graphics/tux.png

Hosts

Label:

Icon:

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.

Custom fields

Create new group

Account type: Users

Alias: My application A

Create new group

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.

Custom fields

Create new group

Account type: Groups

Alias:

Create new group

My application A

Account type: Users

Alias: My application A

Object classes: application1

The group may look like when you edit a user.

Claudia Bach

Suffix demo > People > test > de RDN identifier uid

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

Personal

Unix

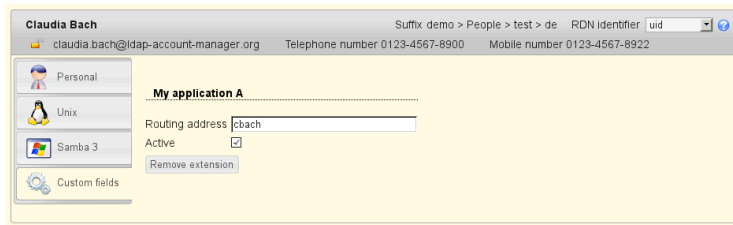
Samba 3

Custom fields

My application A

Add extension

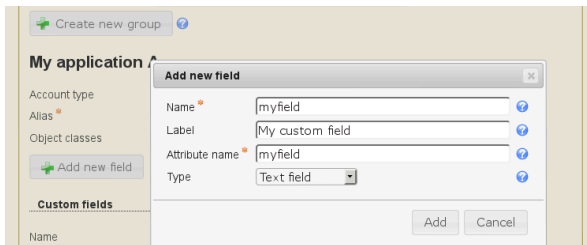
Managing entries in your LDAP directory



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:

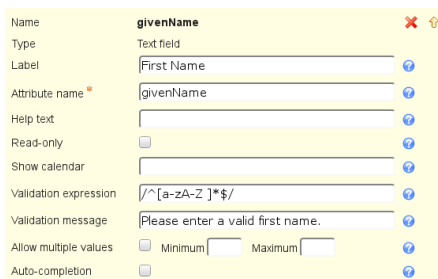
Text fields allow to specify a validation expression and error message.

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:

- dd.mm.yy: 31.12.2016
- yy-mm-dd: 2016-12-31
- d M, y: 31 Dec, 16
- d MM, y: 31 December, 2016



Presentation:



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.

Managing entries in your LDAP directory

| | | |
|-----------------------|--|---|
| Name | customPassword | ✖ |
| Type | Password | |
| Label | Custom Password | ? |
| Attribute name | customPassword | ? |
| Validation expression | /[a-zA-Z0-9]+\$/ | ? |
| Validation message | Password allows only letters and digits. | ? |
| Password hash type | SSHA | ? |

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.

| | | |
|-----------------------|-------------------------------|---|
| Name | postalAddress | ✖ |
| Type | Text area | |
| Label | Postal address | ? |
| Attribute name * | postalAddress | ? |
| Validation expression | /[0-9a-zA-Z]*\$m | ? |
| Validation message | Please enter a valid address. | ? |
| Columns | 40 | ? |
| Rows | 3 | ? |

Presentation:

| | |
|----------------|--|
| Postal address | Steve Miller My Street 123 12345 My 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.

| | | |
|-------------------------|--------------------------|---|
| Name | carLicense | ✖ |
| Type | Checkbox | |
| Label | Car license | ? |
| Attribute name * | carLicense | ? |
| Value for "checked" * | yes | ? |
| Value for "unchecked" * | no | ? |
| Default value | <input type="checkbox"/> | ? |

Presentation:

| | |
|-------------|-------------------------------------|
| 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".

| Name | businessCategory | ✖ | | | | | | | | | | | | |
|------------------|--|-------|-------|---|---|----|-----------------|----|----|-----|------------|-----|--------------|---|
| Type | Radio buttons | | | | | | | | | | | | | |
| Label | Business category | ? | | | | | | | | | | | | |
| Attribute name * | businessCategory | ? | | | | | | | | | | | | |
| Value mapping | <table><thead><tr><th>Value</th><th>Label</th></tr></thead><tbody><tr><td>-</td><td>-</td></tr><tr><td>hr</td><td>Human Resources</td></tr><tr><td>it</td><td>IT</td></tr><tr><td>man</td><td>Management</td></tr><tr><td>org</td><td>Organisation</td></tr></tbody></table> | Value | Label | - | - | hr | Human Resources | it | IT | man | Management | org | Organisation | ? |
| Value | Label | | | | | | | | | | | | | |
| - | - | | | | | | | | | | | | | |
| hr | Human Resources | | | | | | | | | | | | | |
| it | IT | | | | | | | | | | | | | |
| man | Management | | | | | | | | | | | | | |
| org | Organisation | | | | | | | | | | | | | |
| | Add more mapping fields | | | | | | | | | | | | | |

Presentation:

| | |
|-------------------|---|
| Business category | <input type="radio"/> - <input type="radio"/> Human Resources <input checked="" type="radio"/> IT <input type="radio"/> Management <input type="radio"/> 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.

| | | | | |
|-----------------------|---|-----------------|---|---|
| Name | departmentNumber | | ✖ | 🔗 |
| Type | Select list | | | |
| Label | Department | | ? | |
| Attribute name * | departmentNumber | | ? | |
| Help text | | | ? | |
| Read-only | <input type="checkbox"/> | | ? | |
| Allow multiple values | <input checked="" type="checkbox"/> Minimum <input type="text"/> Maximum <input type="text"/> | | ? | |
| Value mapping | Value | Label | ? | |
| | car | Automotive | | |
| | it | IT Consulting | | |
| | hr | Human Resources | | |
| | Add more mapping fields | | | |

Presentation:

| | |
|-----------------|--------------------|
| Department | Financial Services |
| Custom Password | |
| | Automotive |
| | Financial Services |
| | Insurance |
| | IT Consulting |

| | |
|------------|--------------------|
| Department | Automotive |
| | Financial Services |
| | Insurance |
| | IT Consulting |

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.

| | | | | |
|-----------------------|--|--|---|---|
| Name | manager | | ✖ | 🔗 |
| Type | LDAP search select list | | | |
| Label | Manager | | ? | |
| Attribute name * | manager | | ? | |
| Help text | | | ? | |
| Read-only | <input type="checkbox"/> | | ? | |
| Allow multiple values | <input type="checkbox"/> Minimum <input type="text"/> Maximum <input type="text"/> | | ? | |
| LDAP suffix * | ou=people,o=test,c=de | | ? | |
| LDAP filter * | (objectclass=*) | | ? | |
| Attribute name * | 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.

Presentation:

| | | |
|---------|-----------------------------------|---|
| Manager | cbach > demo > People > test > de | ? |
|---------|-----------------------------------|---|

Constant value

This will set the attribute to a constant value. You can also specify wildcards to inject other attribute's values.

| | | | | |
|------------------|------------------------------|--|---|---|
| Name | description | | ✖ | 🔗 |
| Type | Constant | | | |
| Label | Description | | ? | |
| Attribute name * | description | | ? | |
| Help text | | | ? | |
| Value * | %givenname%((givenname))%sn% | | ? | |

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.

Description Ernst Backer

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.

| | |
|----|--|
| CV | <div>Download ✕ Delete</div> <div>Download ✕ Delete</div> <div>Download ✕ Delete</div> <div>Upload file <input type="text"/> Browse... ?</div> |
|----|--|

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 ("").

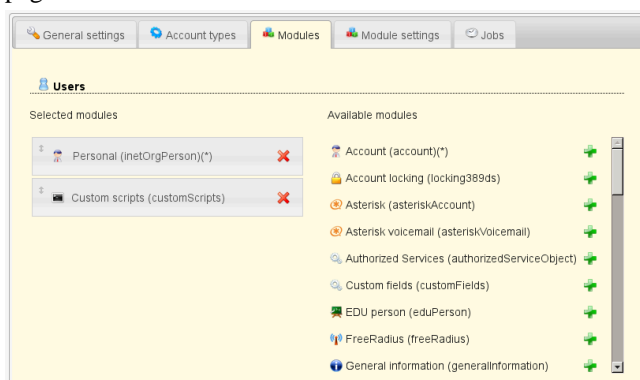
Special characters that must be escaped with "\": "\", ".", "(", ")",

E.g. /^[a-z0-9\\.]+\$ /i

Custom scripts (LAM Pro)

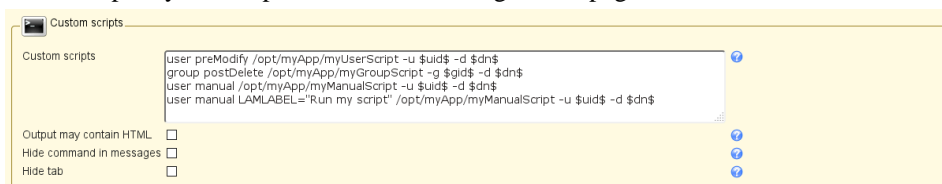
LAM Pro allows you to execute scripts whenever an account is created, modified or deleted. This can be useful to automate processes which needed manual work afterwards (e.g. sending your user a welcome mail or register a mailbox). Additionally, you can specify manual scripts that can be executed from 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.



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.

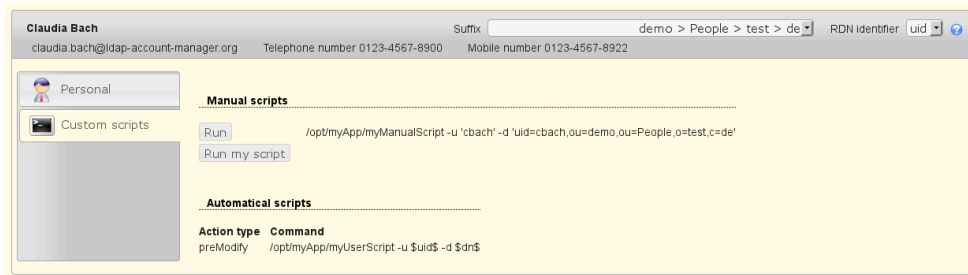
The following special wildcards are available for automatical scripts:

- **\$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
- **\$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

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.

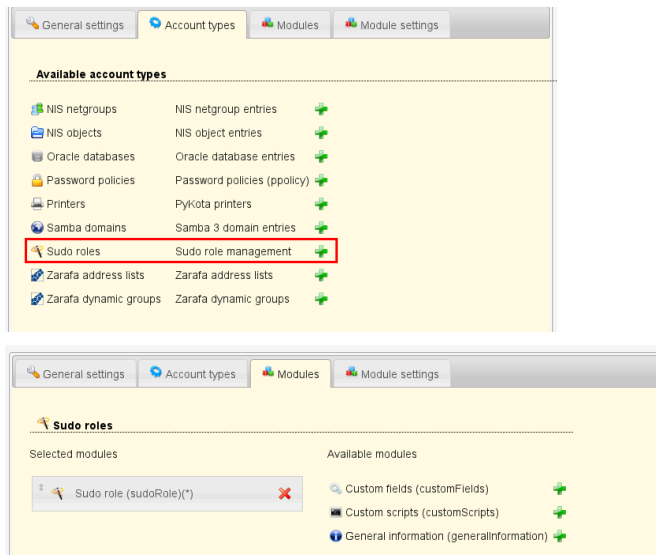
You can see a preview of the commands which will be automatically executed on the "Custom scripts" tab. Here you can also run the manual scripts.



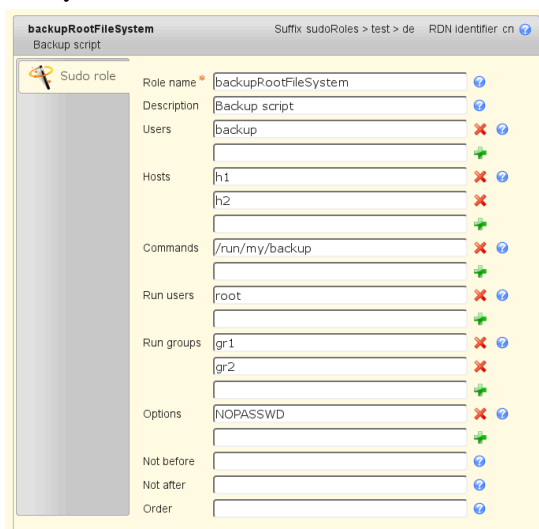
Sudo roles (LAM Pro)

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".



Now you can create sudo commands.



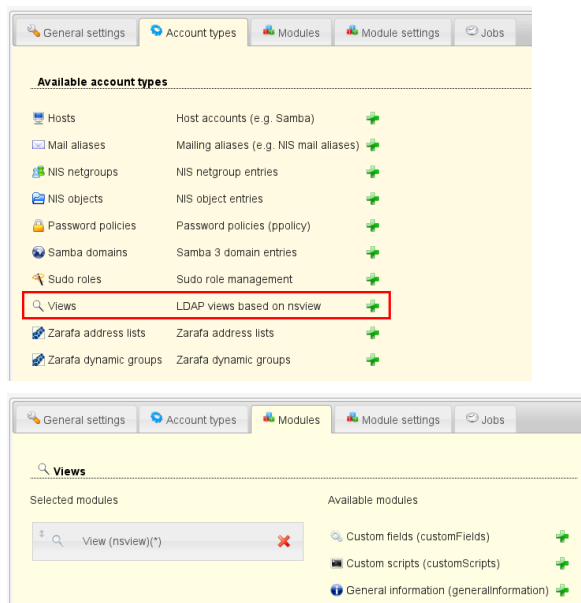
The sudo roles in LDAP work similar to those in /etc/sudoers. You can specify who may run which commands as which user. It is also possible to specify options like NOPASSWD.

LDAP views based on nsview (LAM Pro)

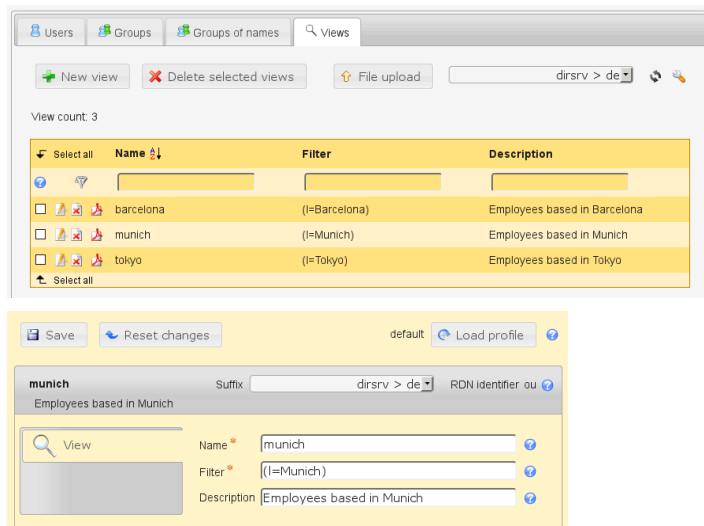
LAM Pro supports LDAP views based on the "nsview" object class. These views allow to create an organizational unit that shows a subset of your LDAP content. The subset is determined by an LDAP filter.

Configuration:

To activate view management in LAM Pro edit your server profile and add the type "LDAP views".



Now you are ready to create your views. Each view has a name, LDAP filter and an optional description.



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.

The screenshot shows the LDAP account manager interface for a user named Claudia Bach. The interface is divided into several sections: a header with the user's name and email (cbach@ldap-account-manager.org), a suffix field (demo > People > test > de), and an RDN identifier (uid). Below this, there are tabs for Personal, Unix, and General information. The General information tab is selected, showing details such as Created by (admin > test > de), Creation time (21.03.2007 17:03:30 GMT), Modified by (admin > test > de), Modification time (26.04.2011 17:33:18 GMT), Has subentries (no), and Groups (demo > gon > test > de).

Tree view (LDAP browser)

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.

The screenshot shows the LDAP browser interface. The left pane displays a tree view of the LDAP directory structure, including ou=demo, ou=test, c=de (5), ou=aliases, ou=domains, ou=groups, ou=machines, and ou=people. The right pane shows the details for the selected entry, ou=demo. The details include the DN (ou=demo,o=test,c=de) and a list of attributes: objectClass (required), organizationalUnit (structural), and ou (required, rdn). The ou attribute has a value of demo. There are buttons for Refresh, Export, Delete this entry, Compare with another entry, Add new attribute, View 5 children, Show internal attributes, Copy or move this entry, Rename, and Create a child entry. An 'Update object' button is at the bottom.

There are also some special functions available:

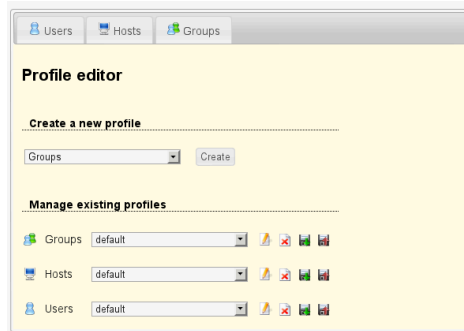
Export: This allows you to export entries to a file (e.g. LDIF or CSV format).

Show internal attributes: Shows internal attributes of the current entry. This includes information about the creator and creation time of the entry.

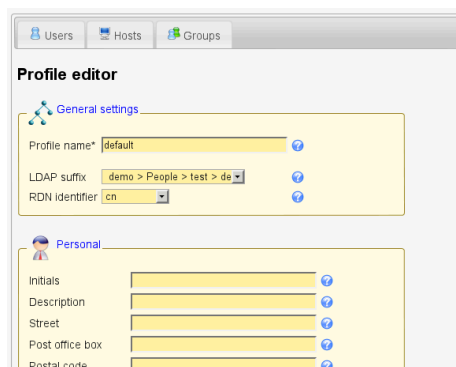
Chapter 5. Tools

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.

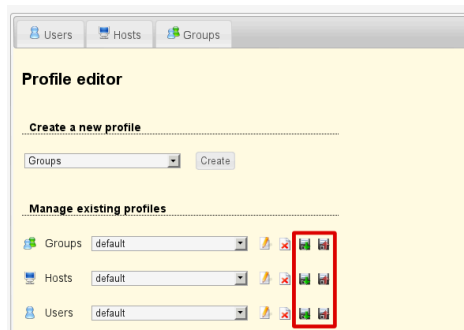


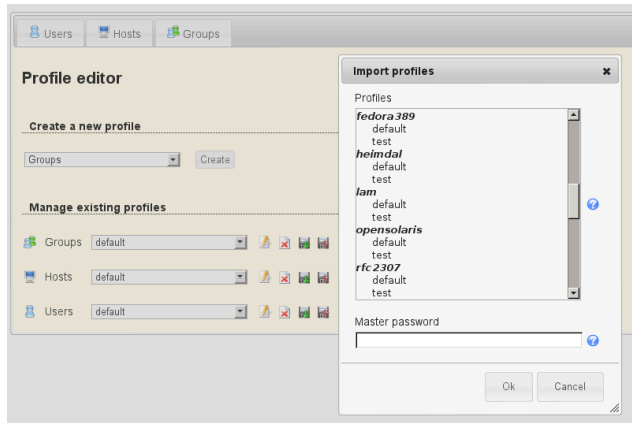
You can enter the LDAP suffix, RDN identifier and various other attributes depending on account type and activated modules.



Import/export:

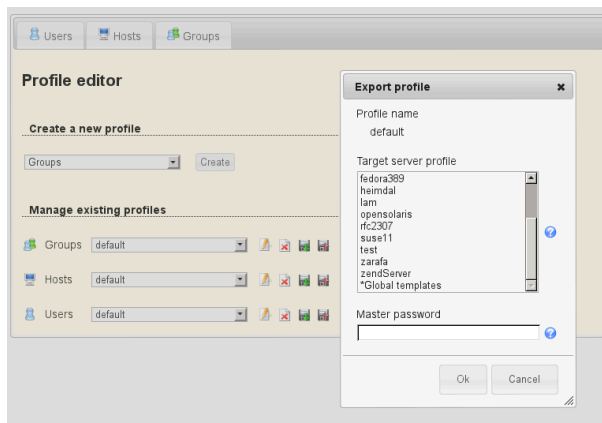
Profiles can be exported to and imported from other server profiles.





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.

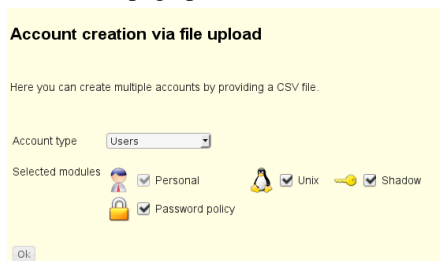
Use this if you would like to setup default profiles that are valid for all server profiles.



File upload

When you need to create lots of accounts then you can use LAM's file upload to create them. LAM will read a CSV formatted file and create the related LDAP entries. Please check the data in your 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.



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.

CSV file No file selected.

Create PDF files ☒

PDF structure

Font 

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 |

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 | | |
| Employee number | inetOrgPerson_employeeNumber | 123456 | | |
| Employee type | inetOrgPerson_type | Temp | | |

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.

Multi edit

LDAP suffix 

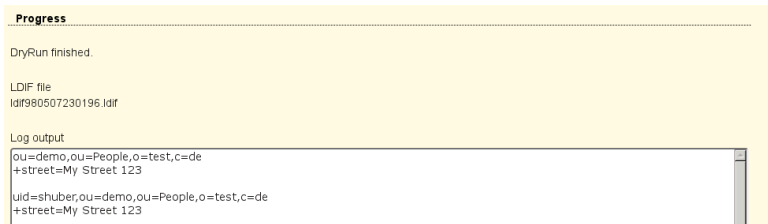
LDAP filter 

Operations

| Type | Attribute name | Value |
|------------------------------------|----------------|---------------|
| <input type="button" value="Add"/> | street | My Street 123 |
| <input type="button" value="Add"/> | | |
| <input type="button" value="Add"/> | | |

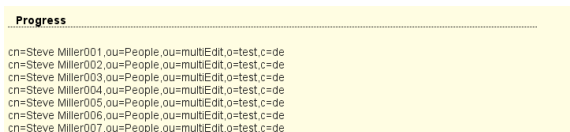
Dry run

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.



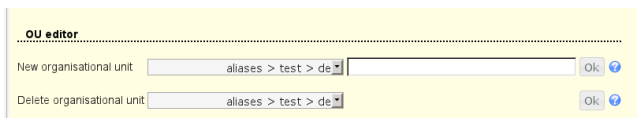
Apply changes

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.



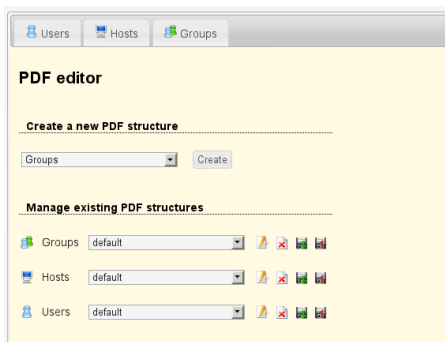
OU editor

This is a simple editor to add/delete organisational units in your LDAP tree. This way you can structure the accounts.



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.



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.

The screenshot shows a web interface for editing a 'default' profile. At the top, there's a 'Headline' field with 'User information' and a 'Logo' field with 'printLogo.jpg (140 x 60)'. Below this, there are two main sections: 'Personal user information' and 'Unix settings'. Each section has a 'Change' button and a list of LDAP attributes with their positions. For 'Personal user information', the attributes are: inetOrgPerson_title, inetOrgPerson_givenName, inetOrgPerson_sn, inetOrgPerson_street, inetOrgPerson_postalCode, inetOrgPerson_postalAddress, inetOrgPerson_mail, inetOrgPerson_telephoneNumber, inetOrgPerson_mobileTelephoneNumber, and inetOrgPerson_facsimileTelephoneNumber. For 'Unix settings', the attributes are: posixAccount_uid, posixAccount_userPassword, posixAccount_primaryGroup, posixAccount_additionalGroups, posixAccount_homeDirectory, posixAccount_loginShell, shadowAccount_shadowExpire, and inetOrgPerson_host. Each attribute has a 'Change' button and a set of arrows (up, down, left, right) to move it within the section.

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:

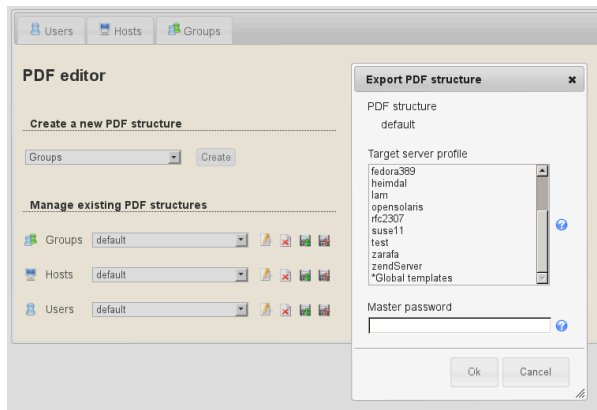
PDF structures can be exported to and imported from other server profiles.

The screenshot shows the 'PDF editor' interface. It has tabs for 'Users', 'Hosts', and 'Groups'. Under 'Create a new PDF structure', there's a dropdown menu for 'Groups' and a 'Create' button. Under 'Manage existing PDF structures', there are three rows for 'Groups', 'Hosts', and 'Users', each with a dropdown menu set to 'default' and a set of icons (add, delete, export, import) to the right. The 'export' icon is highlighted with a red box.

The screenshot shows the 'Import PDF structures' dialog box. It has a title bar with a close button. Inside, there's a section 'PDF structures' with a list of structures: 'iam', 'asterisk', 'default', 'freeRadius', 'heimdal', 'kolab', 'senjust', 'terminalServer', 'test', 'zarafa', 'opensolaris', 'asterisk', 'default', 'freeRadius', and 'heimdal'. Below the list is a 'Master password' field with a 'Show/Hide' icon. At the bottom are 'Ok' and 'Cancel' buttons.

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.



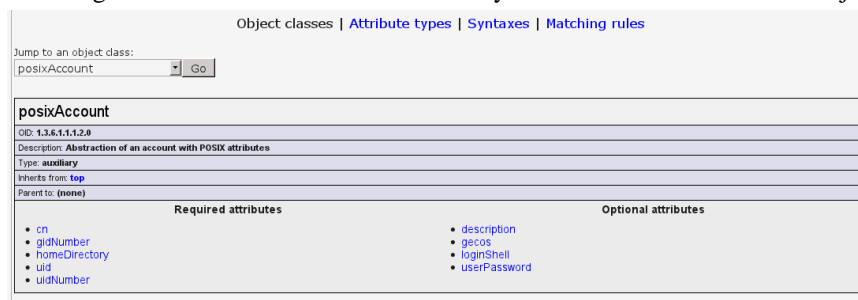
Logo management:

You can upload image files to put a custom logo on the PDF files. The image file name must end with .png or .jpg and the size must not exceed 2000x300px.



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.



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/monitoringldapd.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       CRAM-MD5, DIGEST-MD5, NTLM
Name                  OpenLDAP: slapd 2.4.25 (Apr 11 2011 20:13:50)
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              memberof, dds, ppolicy, glue
Max. file descriptors 1024

```

Server statistics

```

LDAP entries          26755
Referrals             0
Start time            20.05.2011 14:19:34 GMT
Server time           20.05.2011 17:37:15 GMT
Uptime                0:3:17

```

Connection statistics

```

Current connections   9
Total connections     1163
Bytes sent            3.51MB
PDUs sent             27473

```

Operation statistics

| | Initiated | Completed |
|--------------|------------|------------|
| Bind | 182 | 182 |
| Unbind | 142 | 142 |
| Search | 525 | 524 |
| Add | 0 | 0 |
| Modify | 10 | 10 |
| Delete | 0 | 0 |
| Modify RDN | 0 | 0 |
| Compare | 0 | 0 |
| Abandon | 0 | 0 |
| Extended | 3 | 3 |
| Total | 862 | 861 |

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.
Unix account                   ✓ Using roland2 to connect to remote server.
SSH connection                 ✓ SSH connection could be 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.

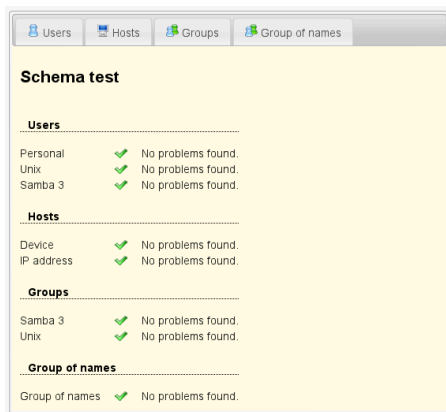
Lamdaemon test finished.

```

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.



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**

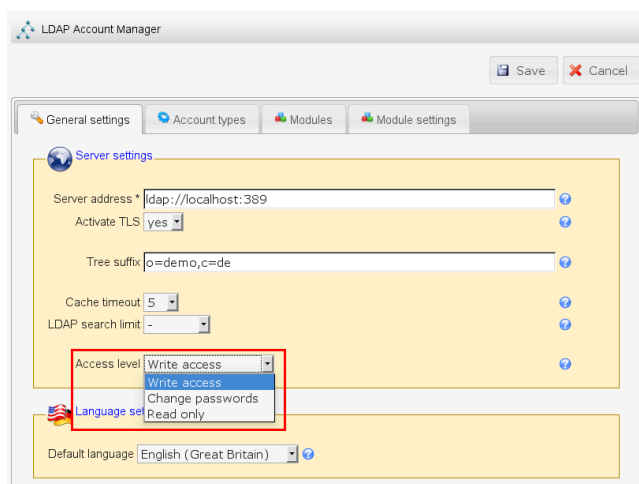
Similar to "Read only" except that the password reset page is available.

- **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.

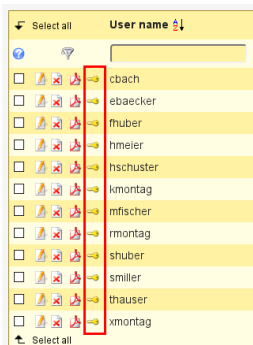
The access level can be set on the server configuration page:



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:



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. Please see email format option in case of broken mails. 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 | Password change options |
|--|---|
| User name: cbach | Change Unix password: <input checked="" type="checkbox"/> |
| Full name: Claudia Bach | Change Samba NT password: <input checked="" type="checkbox"/> |
| Email address: claudia.bach@ldap-account-manager.org | Update Samba password timestamp: <input checked="" type="checkbox"/> |
| Backup email: cbach@rg-se.de | Change Asterisk password: <input checked="" type="checkbox"/> |
| Telephone number: 0123-4567-8900 | Change Asterisk voicemail password: <input checked="" type="checkbox"/> |
| | Force 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:

Set specific password

Here you can specify the new password yourself.

Password:

Repeat password:

Send via mail: ☐

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.

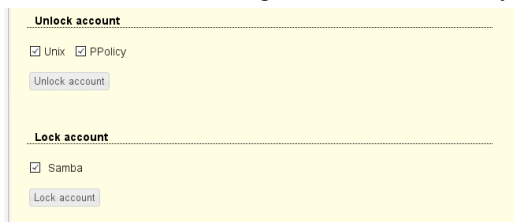
Options:

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.



The screenshot shows a web interface for account management. It is divided into two main sections: 'Unlock account' and 'Lock account'. The 'Unlock account' section is at the top and contains two checkboxes, 'Unix' and 'PPolicy', both of which are checked. Below these checkboxes is a button labeled 'Unlock account'. The 'Lock account' section is below the first one and contains a single checkbox labeled 'Samba', which is also checked. Below this checkbox is a button labeled 'Lock account'. The entire interface is set against a light yellow background.

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.

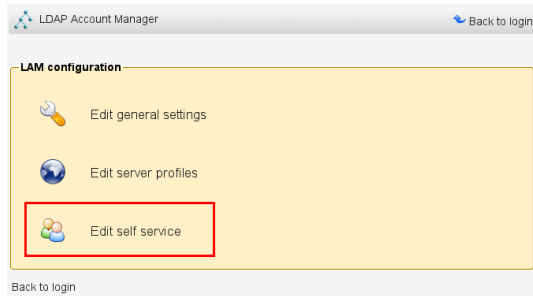
Other LDAP servers

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.

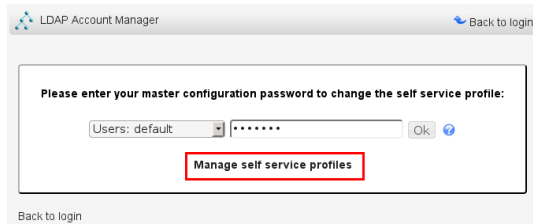
Creating a self service profile

A self service profile defines what input fields your users see and some other general settings like the login caption.

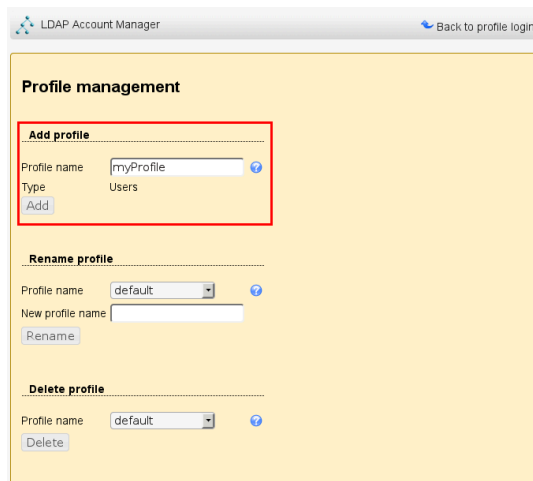
When you go to the LAM configuration page you will see the self service link at the bottom. This will lead you to the self service configuration pages



Now we need to create a new self service profile. Click on the link to manage the self service profiles.



Specify a name for the new profile and enter your master configuration password (default is "lam") to save the profile.



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.

LDAP Account Manager Self service profile: d_demo

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 [?](#) ☐ Activate TLS [?](#)

LDAP suffix [?](#) LDAP search attribute [?](#) ☐ Follow referrals [?](#)

LDAP user [?](#) LDAP password [?](#) ☒ Use for all operations [?](#)

Additional LDAP filter [?](#)

HTTP authentication ☐ [?](#) Enforce language ☐ [?](#)

Default language [?](#)

Time zone [?](#)

2-factor authentication

Provider [?](#)

Captions and labels

Login attribute label [?](#)

Password field label [?](#)

Login caption

Welcome to LAM self service. Please enter your user name and password.

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. |
| HTTP authentication | You can 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 authen- |

| | |
|-----------------------|--|
| | <p>entication in Apache please see this link [http://httpd.apache.org/docs/2.2/howto/auth.html].</p> |
| 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 at the login page. You can input HTML, too. |
| Main page caption | This text is displayed at self service main page where your users change their data. You can input HTML, too. |
| 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. |
| 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).

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

- privacyIdea [<https://www.privacyidea.org/>]

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.

2-factor authentication

Provider:

Base URL:

Label:

Optional: ☐

Disable certificate check: ☐

Caption:

Two factor authentication

Please provide your PIN and token.

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:

PIN+Token:

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).






Possible input fields

This is a list of input fields you may add to the self service page.

Table 7.2. Self service fields

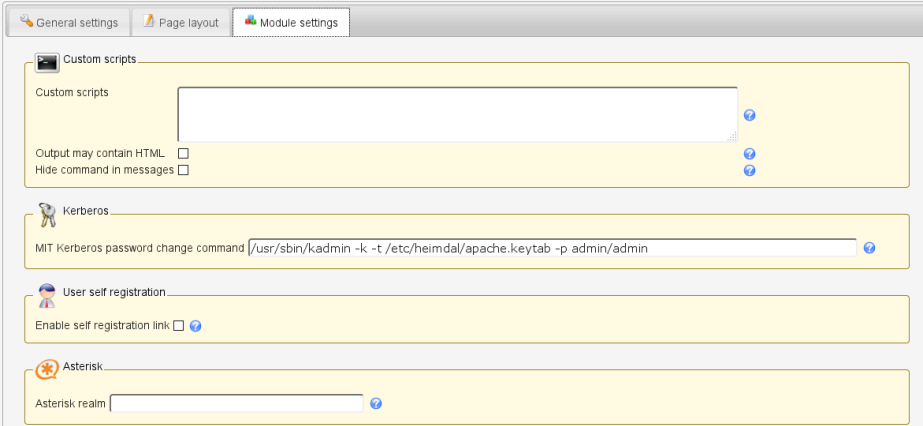
| Account type | Option | Description |
|--|---|--|
|  Asterisk (voicemail) | Sync Asterisk password with Unix password | This is a hidden field. It will update the Asterisk password each time the Unix password is changed. |
|  Kerberos | Sync Kerberos password with Unix password | This is a hidden field. 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 | |
|  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 | Last password change (read-only) | Displays the date and time of the user's last password change (Unix). |

| | | |
|--|--|---|
|  Windows | Password | Change the user's password |
| | Location | |
| | Office name | |
| | Postal code | |
| | Post office box | |
| | State | |
| | Street | |
| | Telephone number | |
| | Web site | |
|  Unix | Common name | |
| | 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. |
|  Kopano | "Send as" privileges | Define user who may send mails as this user |
| | Email aliases | Email aliases |
|  Zarafa | "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).



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 configuration window. The 'Domain suffix' is set to 'dc=ldap-account-manager,dc=org'. The 'Password history' dropdown is set to '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 self reset' configuration window. Key settings include:

- Enable password self reset link:** Checked.
- Identification method:** User name and email address.
- Minimum answer length:** 10.
- Link text:** Forgot password?
- Admin DN:** cn=admin,dc=ldap-account-manager,dc=o
- Admin password:** Masked with dots.
- Security questions:** Two questions are listed: 'What is the name of your favourite pet?' and 'What is the name of your favourite TV show?'.
- Allow custom security questions:** Unchecked.
- Sync Samba 3 password:** Checked.
- Send confirmation mail:** Checked.
- From address:** admin@ldap-account-manager.org
- Subject:** Password reset confirmation
- HTML format:** Unchecked.
- Text:** Dear Sir or Madam, please confirm your password reset request by clicking on the following link: @@resetLink@@.
- Do not ask security question:** Unchecked.
- Send notification mail:** Checked.
- From address:** admin@ldap-account-manager.org
- Subject:** Password reset notification
- HTML format:** Unchecked.
- Text:** Dear Sir or Madam, your password was reset to @@newPassword@@.

 A rich text editor is visible at the bottom for the header.

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. Please see email format option in case of broken mails. 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.

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

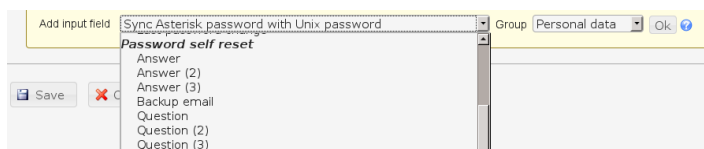
Turn on logging in LAM's main configuration settings. The exact reason is logged on notice level.

2. You do not see security question and answer fields when logged into self service.

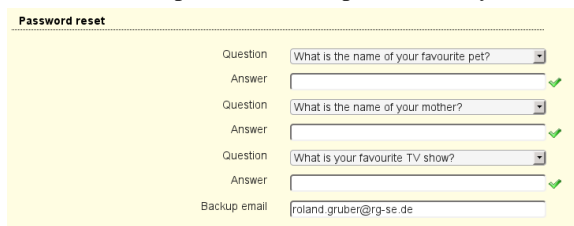
Probably, the user does not have the object class "passwordSelfReset" set. You can do this in admin interface. If you have multiple users to change then use the Multi Edit Tool to add the object class.

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.



This is an example how can be presented to your users on the self service page:



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?").

When a user clicks on the link then he will be asked for identification with his user name and email address.

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.

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".

Options:

Link text: This is the label for the link to the self registration. If empty "Register new account" will be used.

Admin DN and password: Please enter the LDAP DN and its password that should be used to create new users. This DN also needs to be able to do LDAP searches by uid in the self service part of your LDAP tree.

Object classes: This is a list of object classes that are used to build the new user accounts. Please enter one object class in each line. If you use LAM Pro password self reset feature then do not forget to add "passwordSelfReset" here.

Attributes: This is a list of additional attributes that the user can enter. Please note that user name, password and email address are mandatory anyway and need not be specified.

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. 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" | Label that is displayed on page | optional regular expression for validation (e.g. "/^[0-9a-zA-Z]+\$/") | 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" | Label that is displayed on page | optional regular expression for validation (e.g. "/^[0-9a-zA-Z]+\$/") | 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://perl.doc.perl.org/perlre.html>]. Validation is optional, you can leave these options blank.

Example:

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.

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.

Captcha support

LAM Pro can optionally display a captcha to verify that registrations are not from robots. The supported captcha provider is 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. Captchas will be displayed automatically when site+secret key are filled.

| Captcha | |
|----------------------|------------------------------------|
| reCAPTCHA site key | 6LcOYBwTAAAAAMpzVeD5wWE4jrFI0v0x |
| reCAPTCHA secret key | 6LcOYBwTAAAAAIIIDZnQ0DsORUdVhse1KO |

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>,...*

Please see email format option in case of broken mails.

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
- 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:

- dd.mm.yy: 31.12.2016
- yy-mm-dd: 2016-12-31
- d M, y: 31 Dec, 16
- d MM, y: 31 December, 2016

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.

| | | |
|-----------------------|--|---|
| Name | customPassword | ✖ |
| Type | Password | |
| Label | Custom Password | ? |
| Attribute name | customPassword | ? |
| Validation expression | /^[a-zA-Z0-9]*\$/ | ? |
| Validation message | Password allows only letters and digits. | ? |
| Password hash type | SSHA | ? |

Presentation in Self Service:

| | |
|-----------------|-------|
| 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.

| | | |
|-----------------------|-------------------------------|---|
| Name | postalAddress | ✖ |
| Type | Text area | |
| Label | Postal address | ? |
| Attribute name * | postalAddress | ? |
| Validation expression | /^([0-9a-zA-Z]*)\$/m | ? |
| Validation message | Please enter a valid address. | ? |
| Columns | 40 | ? |
| Rows | 3 | ? |

Presentation in Self Service:

| | |
|----------------|--|
| Postal address | Steve Miller My Street 123 12345 My 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.

| | | |
|-------------------------|--------------------------|---|
| Name | carLicense | ✖ |
| Type | Checkbox | |
| Label | Car license | ? |
| Attribute name * | carLicense | ? |
| 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".

| Name | businessCategory | ✖ | | | | | | | | | | | | | | |
|------------------|---|-------|-------|---|---|----|-----------------|----|----|-----|------------|-----|--------------|--|--|---|
| Type | Radio buttons | | | | | | | | | | | | | | | |
| Label | Business category | ? | | | | | | | | | | | | | | |
| Attribute name * | businessCategory | ? | | | | | | | | | | | | | | |
| Value mapping | <table border="1"> <thead> <tr> <th>Value</th> <th>Label</th> </tr> </thead> <tbody> <tr> <td>-</td> <td>-</td> </tr> <tr> <td>hr</td> <td>Human Resources</td> </tr> <tr> <td>it</td> <td>IT</td> </tr> <tr> <td>man</td> <td>Management</td> </tr> <tr> <td>org</td> <td>Organisation</td> </tr> <tr> <td></td> <td></td> </tr> </tbody> </table> | Value | Label | - | - | hr | Human Resources | it | IT | man | Management | org | Organisation | | | ? |
| Value | Label | | | | | | | | | | | | | | | |
| - | - | | | | | | | | | | | | | | | |
| hr | Human Resources | | | | | | | | | | | | | | | |
| it | IT | | | | | | | | | | | | | | | |
| man | Management | | | | | | | | | | | | | | | |
| org | Organisation | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | |
| | Add more mapping fields | | | | | | | | | | | | | | | |

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.

Name: **departmentNumber**

Type: Select list

Label: Department

Attribute name: departmentNumber

Help text:

Read-only: ☐

Allow multiple values: ☒ Minimum: Maximum:

Value mapping:

| Value | Label |
|-------|-----------------|
| car | Automotive |
| it | IT Consulting |
| hr | Human Resources |

Add more mapping fields

Presentation in Self Service:

Department: Financial Services

Custom Password: Automotive

Department: Automotive

Department: Financial Services

Department: Insurance

Department: IT Consulting

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.

Name: **manager**

Type: LDAP search select list

Label: Manager

Attribute name: manager

Help text:

Read-only: ☐

Allow multiple values: ☐ Minimum: Maximum:

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

LDAP filter: (objectclass=*)

Attribute name: 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.

Presentation:

Manager: cbach > demo > People > test > de

Constant value

This will set the attribute to a constant value. You can also specify wildcards to inject other attribute's values.

Name: **description**

Type: Constant

Label: Description

Attribute name: description

Help text:

Value: %givenname%((givenname))%sn%

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.

Description Ernst Bäcker

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 | userCertificate | ✖ |
| Type | File upload | |
| Label | userCertificate | 🔍 |
| Attribute name | userCertificate;binary | 🔍 |
| File extension | .crt | 🔍 |
| Maximum file size | 100000 | 🔍 |
| Multi value | <input checked="" type="checkbox"/> | 🔍 |

Presentation:

The uploaded data may also be downloaded via LAM.

Certificate

🔍 ✖

🔍 ✖

Upload a file

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`

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 | <input type="text" value="<h1>LAM self service</h1>"/> |
|-------------|--|

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.

| | |
|----------------------|--|
| Additional CSS links | <input type="text" value="http://www.ldap-account-manager.org/css/style.css"/> |
|----------------------|--|













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 | |
|  | 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://www.nrg4u.com/] | LAM Pro only |

| | Account type | Object class(es) | Schema name | Source | Notes |
|---|-------------------------|--|--------------------|--|---|
|  | 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/ | |
|  | 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 DLZ DNS | dlzZone, dlzHost, dlzSOARecord, dlzNSRecord, dlzARecord, dlzMXRecord, dlzCNameRecord, dlzPTRRecord | dlz.schema | part of Bind DLZ patch [http://bind-dlz.sourceforge.net/] | LAM Pro only |
|  | Aliases | alias, uidObject | core.schema | Part of OpenLDAP installation | LAM Pro only |
|  | NIS netgroups | nisNetgroup | nis.schema | Part of OpenLDAP installation | |

| | Account type | Object class(es) | Schema name | Source | Notes |
|---|-------------------|---|--|---|------------------------------|
|  | 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, oidrdbms.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 |
|  | 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 |
|  | 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 |
|  | Zarafa | zarafa-user, zarafa-group, zarafa-server | zarafa.schema | Part of Zarafa installation | LAM Pro only |
|  | IMAP mailboxes | - | - | - | Does not require any schema. |
|  | LDAP views | nsview, organizationalunit | built-in | Part of LDAP server installation (e.g. 389 server) | LAM Pro only |

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

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 accessibly 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 browseable

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>
```

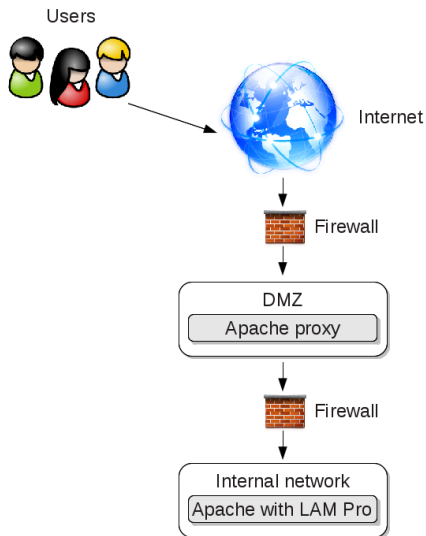
You can also require that your users belong to a certain Unix group in LDAP:

```
<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 *>
        Order deny,allow
        Allow from all
    </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 /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 /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.

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 PHP 5. In case you run with PHP 7 please update the parameter "fastcgi_pass" to "/var/run/php7-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 7.0. In case you run with PHP 7.1 or PHP 5 please update the parameter "fastcgi_pass" to "/var/run/php/php7.1-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/php5-fpm.sock" or "/var/run/php7-fpm.sock") to match your installation.

```
location /lam {  
    index index.html;  
    alias /usr/share/ldap-account-manager;  
    autoindex off;  
  
    location ~ /\.php$ {  
        fastcgi_split_path_info ^(.+\.(php))(/.+)$;  
        fastcgi_pass unix:/var/run/php5-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;  
}  
}
```

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:

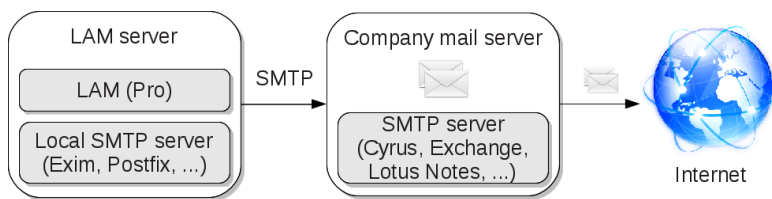
Indices will improve the performance when searching for entries in the LDAP directory. The following indices are recommended:

```
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 of email (SMTP) server

LAM always uses a local SMTP email server on the machine where LAM is installed. Therefore, there is no need to configure any SMTP settings inside LAM itself.

The local email server should be configured to forward all emails to your company mail server (so-called smarthost). You can use any SMTP software that ships with a Sendmail wrapper (e.g. Exim, Postfix, QMail or Sendmail itself).



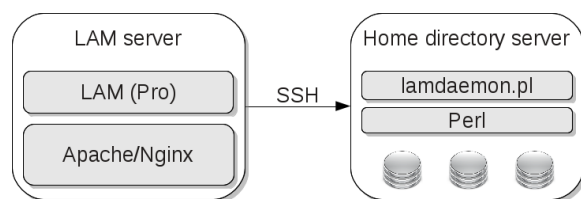
Appendix E. Setup for home directory and quota management

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

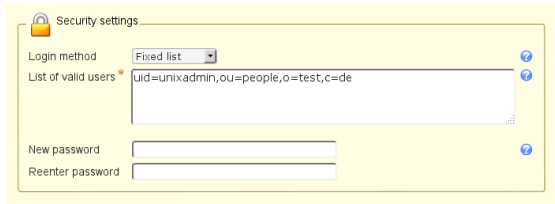
Please copy lib/lamdaemon.pl from the LAM tar.bz2 package to your quota/homedir server. The location may be anywhere (e.g. use /opt/lamdaemon). Please make the lamdaemon.pl script executable.

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 Debian 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 | | | | | |
| Path to external script | /usr/share/ldap-account-manager/lib/l | | | | | |
| Rights for the home directory | | | | | | |
| | Owner | Group | Other | Read | Write | Execute |
| | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |

Note that the builtin admin/manager entries do not work for lamdaemon. You need to login with a Unix account.



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_conf` 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 F. 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).

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 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 G. 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.

Example:

This will change the background color of all pages to turquoise. See 500_layout.css for LAM's default settings.

```
body {  
    background-color: #b6eeff;  
}
```

You can use the same way to change fonts, sizes and more.

E.g. this will reduce the default font size to 80%:

```
body {  
    font-size: 80%;  
}  
  
.ui-button-text-only {  
    font-size: 100%;  
}  
  
.ui-button-text-icon-primary {  
    font-size: 100%;  
}
```

Custom logo

```
/* image in login box */  
td.loginLogo {  
    background-image: url(/logos/mylogo.png);  
}  
  
/* image (24x24) in header line */  
a.lamLogo {  
    background-image: url(/logos/mylogo.png);  
}
```

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 H. 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 I. Troubleshooting

Reset configuration password

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.

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" entry in the file
3. Replace the password hash after "password: " with your new clear-text password (e.g. "secret")

After the change the line should look like this:

```
password: secret
```

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.

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

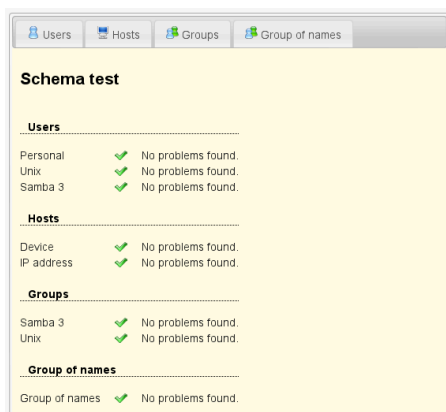
Invalid syntax errors:

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").



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

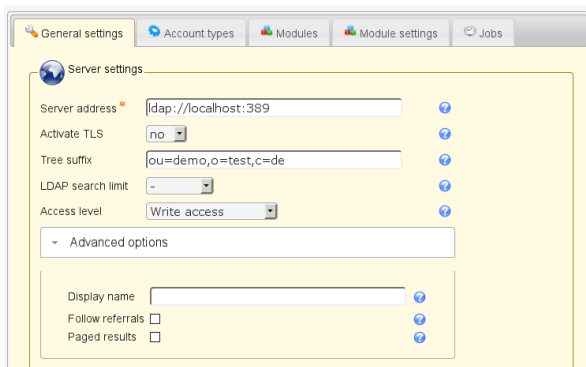
Depending on the queries it may help to add some more indices on the LDAP server. Depending on your LDAP software it may already suggest indices in its log files. See here for typical OpenLDAP indices.

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.



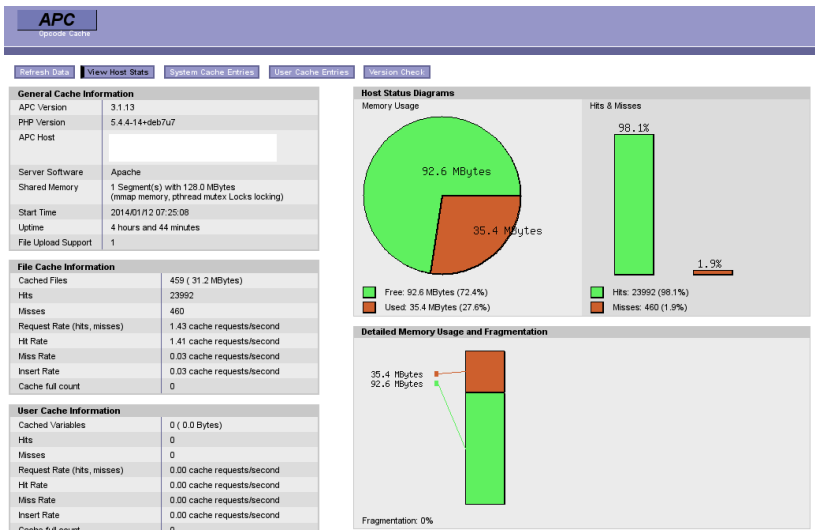
LAM web server

Install a PHP accelerator

There are tools like APC [<http://www.php.net/manual/en/book.apc.php>]/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.

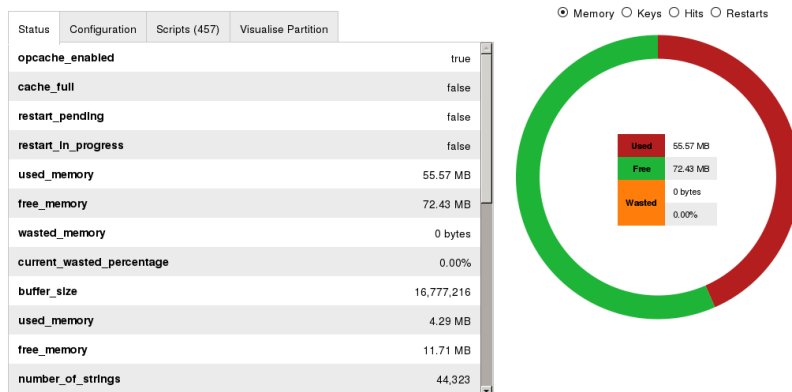
This is a simply way to enhance performance since APC/OpCache is part of most Linux distributions.

If you use APC then make sure that it uses enough memory (e.g. "apc.shm_size=128M"). You can check the memory usage with the file apc.php that is shipped with APC.



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



Disable session encryption

LAM encrypts sensitive data in your session files. You can disable it to reduce CPU load.

The 'Security settings' interface includes fields for session timeout, allowed hosts, and session encryption options. The 'Encrypt session' checkbox is checked, and the 'use system certificates' option is selected. There are buttons for 'Browse...', 'Upload', and 'Import from server'.

Session timeout: 120

Allowed hosts: [Empty text area]

Allowed hosts (self service): [Empty text area]

Encrypt session: ☒

SSL certificates: use system certificates

Buttons: Browse..., Upload, Import from server

Idaps:// [Empty text field]