LDAP Account Manager - Manual

LDAP Account Manager - Manual

Table of Contents

List of Tables

Overview

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

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

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

Key features:

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

Requirements:

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

License:

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

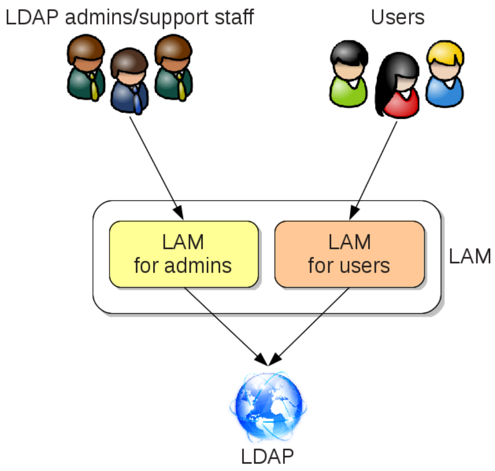
Have fun!
    The LAM development team

Chapter 1. Big picture

Overview

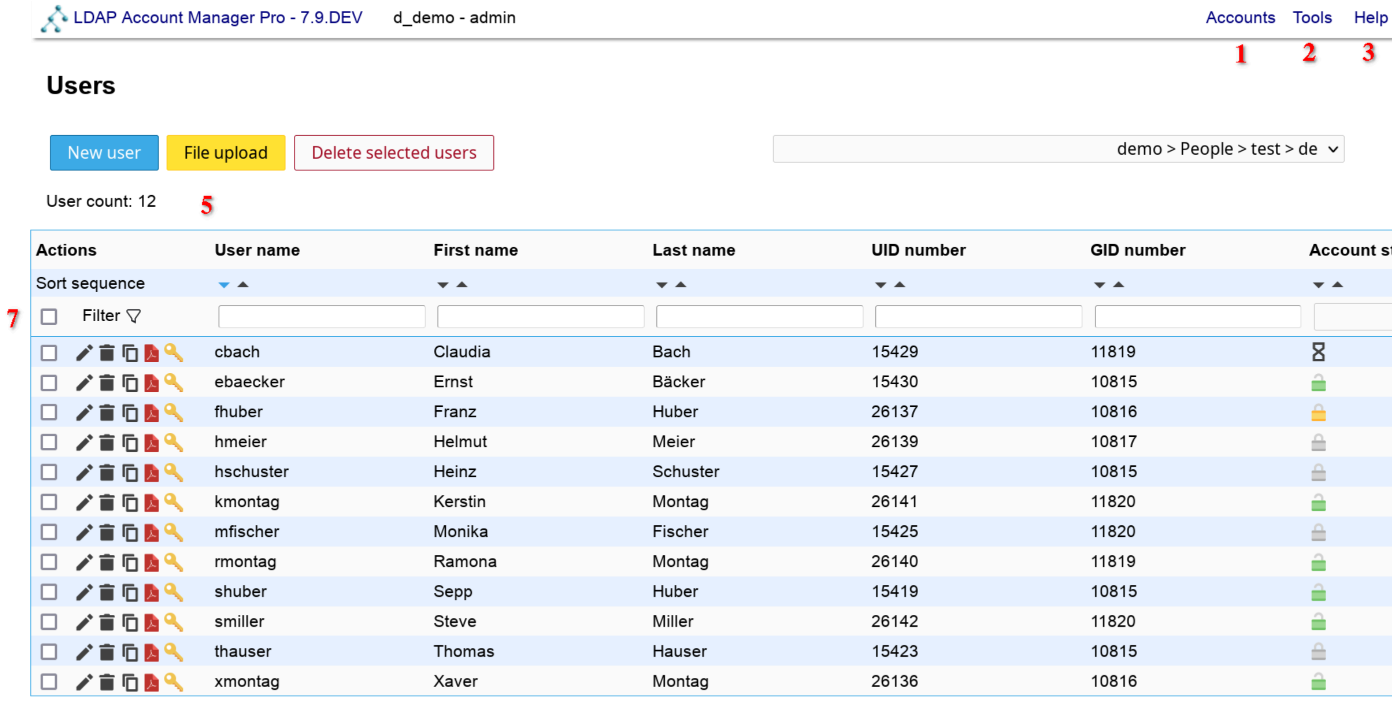
LAM has two major areas:

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



Admin interface

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



User count: 12

Actions	User name	First name	Last name	UID number	GID number	Account st
Sort sequence	▼▲	▼▲	▼▲	▼▲	▼▲	▼▲
☐ Filter ▽						
☐	cbach	Claudia	Bach	15429	11819	⌛
☐	ebaecker	Ernst	Bäcker	15430	10815	🔒
☐	fhuber	Franz	Huber	26137	10816	🔒
☐	hmeier	Helmut	Meier	26139	10817	🔒
☐	hschuster	Heinz	Schuster	15427	10815	🔒
☐	kmontag	Kerstin	Montag	26141	11820	🔒
☐	mfischer	Monika	Fischer	15425	11820	🔒
☐	rmontag	Ramona	Montag	26140	11819	🔒
☐	shuber	Sepp	Huber	15419	10815	🔒
☐	smiller	Steve	Miller	26142	11820	🔒
☐	thauser	Thomas	Hauser	15423	10815	🔒
☐	xmontag	Xaver	Montag	26136	10816	🔒

Functional areas:

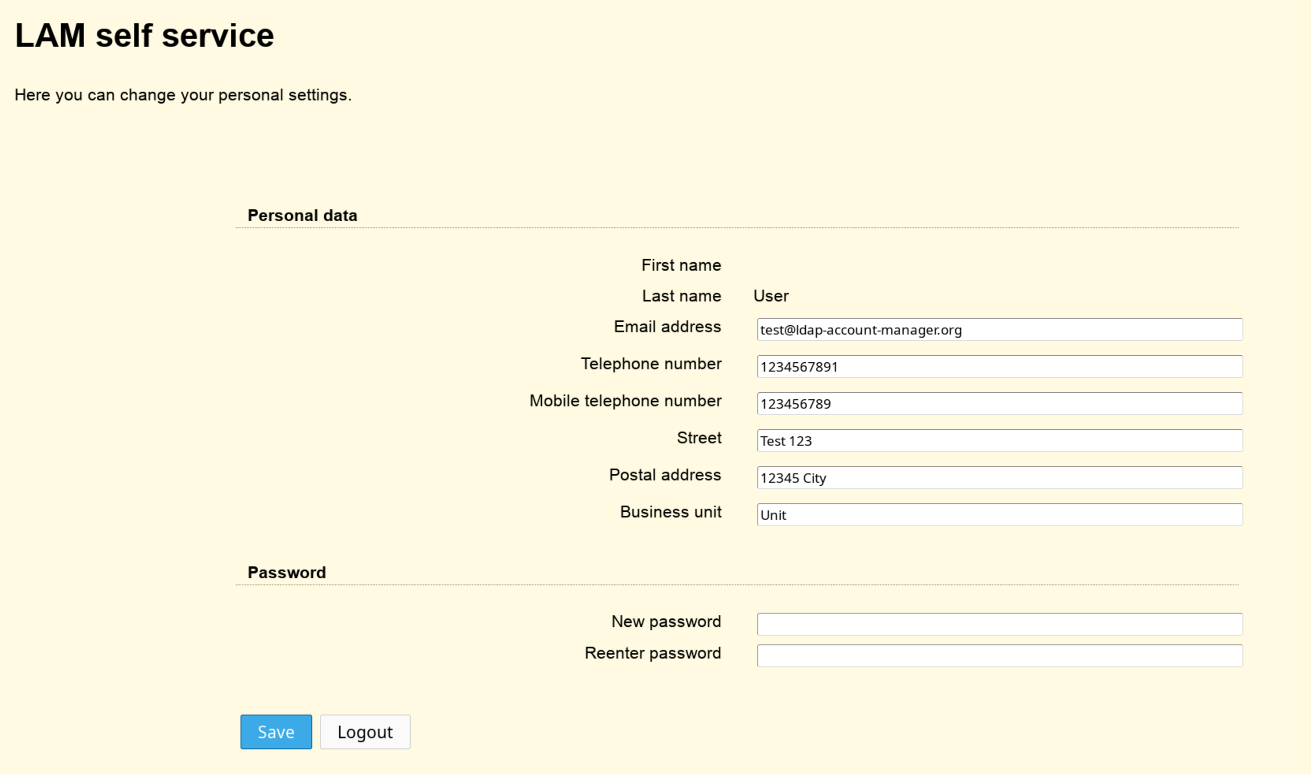
1. Account types: Here you can switsch between different account types (e.g. user/groups)

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

Self Service

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

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



LAM self service

Here you can change your personal settings.

Personal data

First name

Last name: User

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

Telephone number: 1234567891

Mobile telephone number: 123456789

Street: Test 123

Postal address: 12345 City

Business unit: Unit

Password

New password

Reenter password

Configuration

Configuration is done on multiple levels:

Global

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

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

Server profile

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

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

Self service

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

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

Profiles

Account profiles store default values for new LDAP entries.

PDF structures

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

Glossary

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

Table 1.1. Glossary

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

Architecture

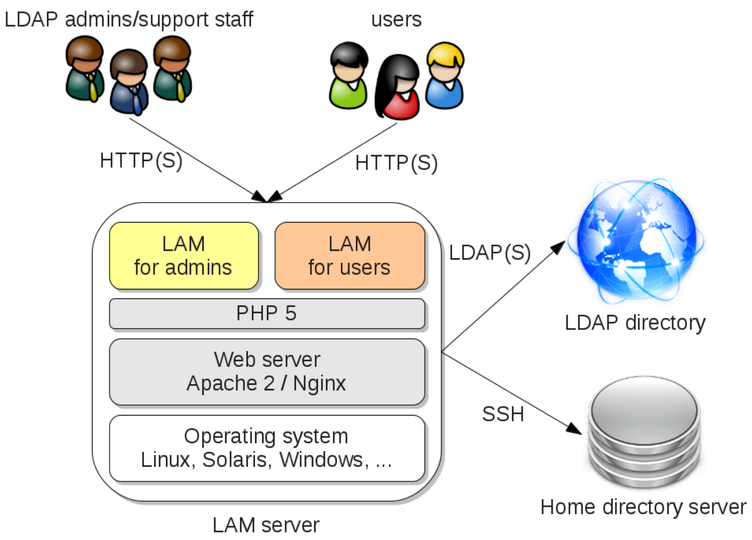
There are basically two groups of users for LAM:

- **LDAP administrators and support staff:**

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

- **Users:**

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



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

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

LAM runtime environment:

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

Home directory server:

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

LDAP directory:

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

Chapter 2. Installation

New installation

Requirements

LAM has the following requirements to run:

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

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

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

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

Prepackaged releases

LAM is available as prepackaged version for various platforms.

Debian/Ubuntu

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

apt-get install ldap-account-manager

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

Installation of the latest packages on Debian/Ubuntu

1. Install the LAM package

   dpkg -i ldap-account-manager_*.deb

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

2. Install the lamdaemon package (optional)

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

Suse/Fedora/CentOS

There are RPM packages available on the LAM 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 do not contain a dependency to PHP due to the various package names for it. Please make sure that you install Apache/Nginx with PHP.

Example installation for Apache + PHP 8 on OpenSuse 15:

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

Other RPM based distributions

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

FreeBSD

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

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

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

Installing the tar.bz2

Extract the archive

Please extract the archive with the following command:

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

Install the files

Manual copy

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

Then set the appropriate file permissions inside the LAM directory:

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

With configure script

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

- ./configure
- make install

Options for "./configure":

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

Configuration files

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

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

Webserver configuration

Please see the Apache or Nginx chapter.

Docker

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

System configuration

PHP

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

memory_limit = 128M

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

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

Locales for non-English translation

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

Table 2.1. Locales

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

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

```
locale -a
```

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

Upgrading LAM or migrate from LAM to LAM Pro

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

Upgrade LAM

Backup configuration files

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

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

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

LAM Pro only:

config/selfService/*.*

Uninstall current LAM (Pro) version

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

Debian/Ubuntu needs no removal of old packages.

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

Install new LAM (Pro) version

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

Restore configuration files

RPM:

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

DEB:

Nothing needs to be restored.

tar.bz2:

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

Final steps

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

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

Version specific upgrade instructions

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

9.1 -> 9.2

LAM Pro:

- Custom scripts: The settings in server profile were split by account type. If you use custom scripts then you need to perform these steps for each server profile that uses them (no scripts will be executed till migration was done):
  - Open server profile and switch to tab "Module settings"
  - Review the automated migration of the custom scripts settings (complex configurations will need manual adaptions)
  - Save the server profile

9.0 -> 9.1

No actions required.

8.9 -> 9.0

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

LAM Pro:

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

8.8 -> 8.9

No actions required.

8.7 -> 8.8

LAM Pro:

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

8.6 -> 8.7

LAM Pro:

- Self service profiles that were not saved with a LAM Pro version of the past 3 years must be saved with LAM Pro 8.6 before upgrading to LAM Pro 8.7.

- Self service profiles that have enabled "HTTP authentication" need to be reconfigured. Open the self service profile, select "HTTP authentication" as "Authentication method" (first tab, server settings) and save the self service profile.

8.1 -> 8.6

No actions required.

8.0 -> 8.1

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

7.6 -> 8.0

No actions required.

7.5 -> 7.6

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

7.2 -> 7.5

No actions required.

7.1 -> 7.2

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

6.7 -> 7.1

No actions required.

6.6 -> 6.7

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

6.5 -> 6.6

No actions required.

6.4 -> 6.5

No actions required.

6.3 -> 6.4

No actions needed.

6.2 -> 6.3

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

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

6.1 -> 6.2

No actions required.

6.0 -> 6.1

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

5.7 -> 6.0

No actions needed.

5.6 -> 5.7

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

5.5 -> 5.6

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

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

5.4 -> 5.5

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

5.1 -> 5.4

No special actions needed.

5.0 -> 5.1

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

4.9 -> 5.0

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

4.5 -> 4.9

No special actions needed.

4.4 -> 4.5

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

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

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

4.3 -> 4.4

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

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

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

4.2.1 -> 4.3

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

4.1 -> 4.2/4.2.1

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

4.0 -> 4.1

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

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

3.9 -> 4.0

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

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

Special install instructions:

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

3.7 -> 3.9

No changes.

3.6 -> 3.7

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

3.5.0 -> 3.6

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

3.4.0 -> 3.5.0

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

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

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

3.3.0 -> 3.4.0

No changes.

3.2.0 -> 3.3.0

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

3.1.0 -> 3.2.0

No changes.

3.0.0 -> 3.1.0

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

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

2.3.0 -> 3.0.0

No changes.

2.2.0 -> 2.3.0

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

1.1.0 -> 2.2.0

No changes.

Uninstallation of LAM (Pro)

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

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

Migration to a new server

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

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

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

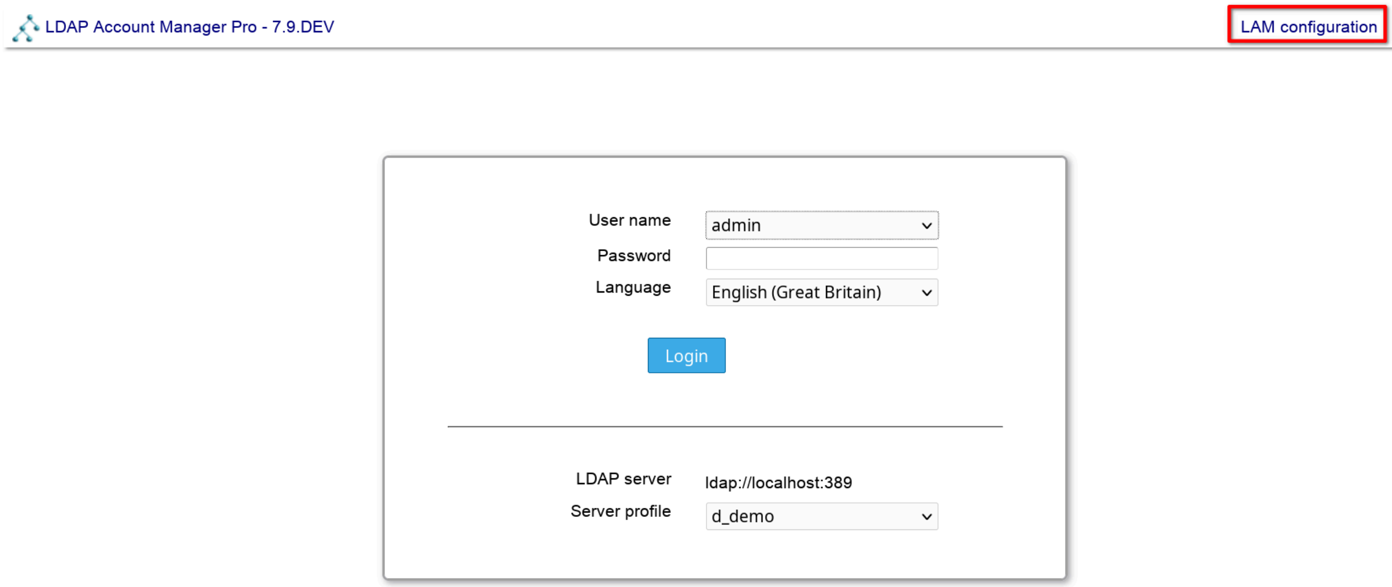
   - config/*.conf
   - config/config.cfg
   - config/pdf/*
   - config/profiles/*
   - config/selfService/*.* (needed for LAM Pro only)

   The files must be writable for the webserver user.
3. Open LAM (Pro) login page on new server and verify installation.
4. Uninstall LAM (Pro) on old server.

Chapter 3. Configuration

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

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

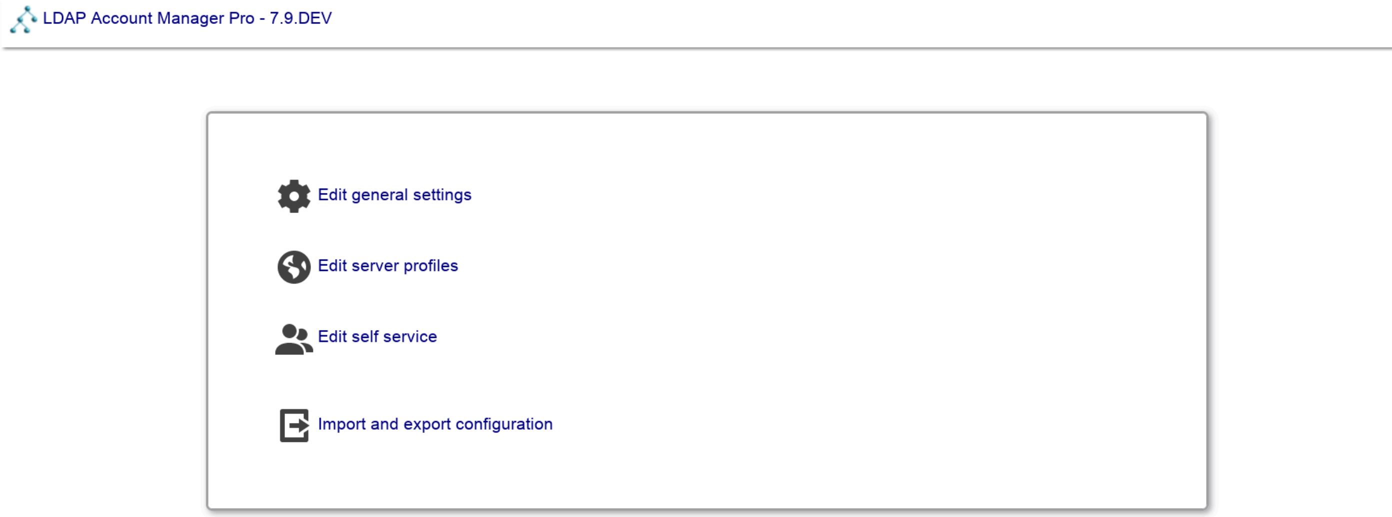


User name: admin
Password:
Language: English (Great Britain)

LDAP server: ldap://localhost:389
Server profile: d_demo

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

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


LDAP Account Manager Pro - 7.9.DEV
Edit general settings
Edit server profiles
Edit self service
Import and export configuration

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

General settings

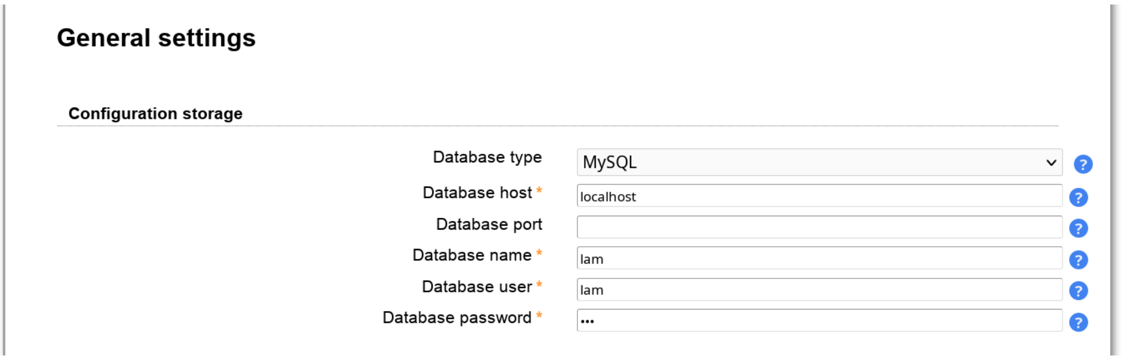
Configuration Database

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

Exceptions:

- Configuration storage options
- LAM Pro license
- CA certificates

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



General settings

Configuration storage

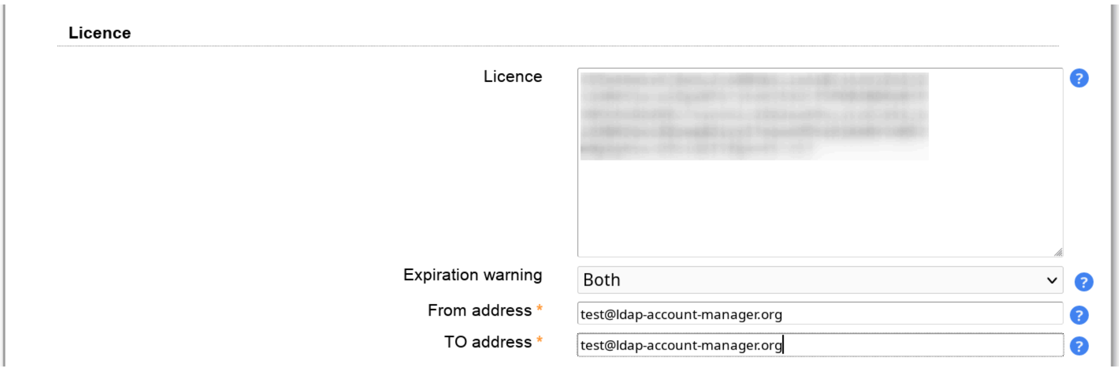
Database type	MySQL
Database host *	localhost
Database port	
Database name *	lam
Database user *	lam
Database password *	•••

License (LAM Pro only)

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

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

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



Licence

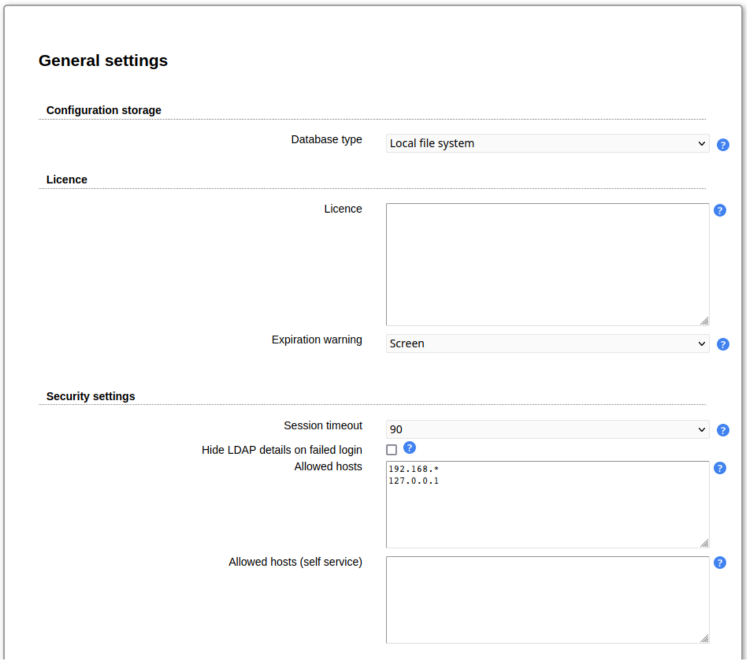
Licence	[redacted]
Expiration warning	Both
From address *	test@ldap-account-manager.org
TO address *	test@ldap-account-manager.org

Security settings

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

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

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



General settings

Configuration storage

Database type: Local file system

Licence

Licence:

Expiration warning: Screen

Security settings

Session timeout: 90

Hide LDAP details on failed login: □

Allowed hosts:

```
192.168.*
127.0.0.1
```

Allowed hosts (self service):

SSL certificate setup:

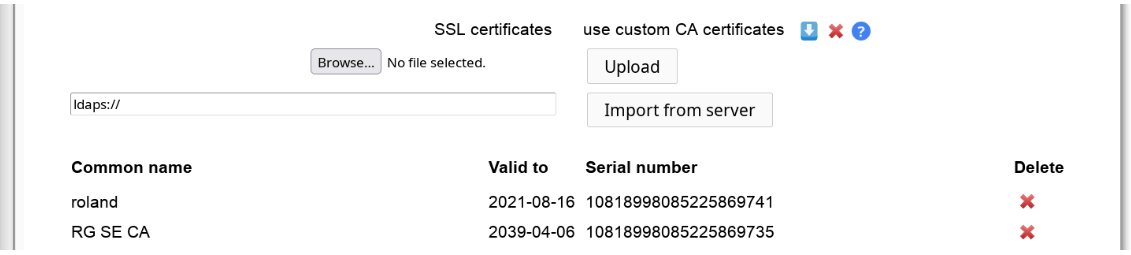
By default, LAM uses the CA certificates that are preinstalled on your system. This will work if you connect via SSL/TLS to an LDAP server that uses a certificate signed by a well-known CA. In case you use your own CA (e.g. company internal CA) you can import the CA certificates here.

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

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

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

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

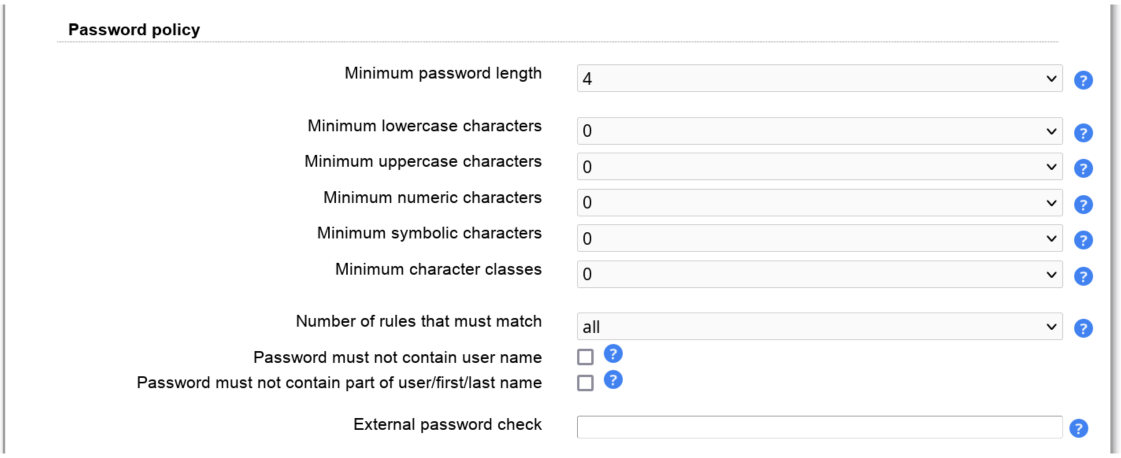


SSL certificates: use custom CA certificates

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

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	4
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	□
External password check	

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

External password check

Please note that this option is only displayed if you have installed the PHP Curl extension for your web server.

This will validate passwords using an external service. LAM supports the protocol used by Have I been Pwned [https://haveibeenpwned.com/API/v2#SearchingPwnedPasswordsByRange]. You can use the service directly or setup any custom service with the same API. If the service reports an error LAM will log an error message and the password will be accepted.

Example URL: https://api.pwnedpasswords.com/range/{SHA1PREFIX}

LAM will build a SHA1 hash of the password and send parts of it to the service.

The configured URL must contain the wildcard "{SHA1PREFIX}" which will be replaced with the 5 character hash prefix. The service must then return a list of text lines in the format "<hash suffix>:<number>".

"<hash suffix>" needs to be the suffix of a known insecure password. The "<number>" can be any numeric value and will be ignored by LAM.

Example:

Password hash: 21BD10018A45C4D1DEF81644B54AB7F969B88D65

Hash prefix sent to service: 21BD1

Returned line: 0018A45C4D1DEF81644B54AB7F969B88D65:1

This will reject the password.

Logging

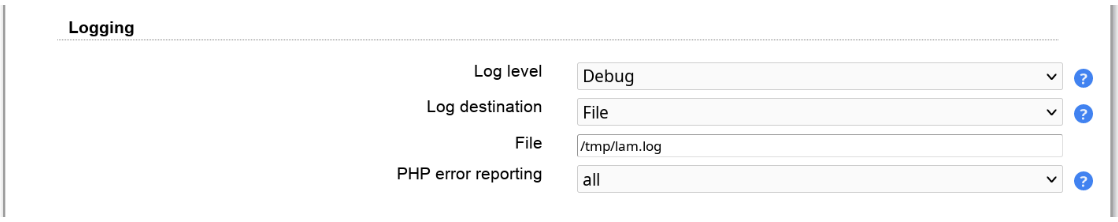
LAM can log events (e.g. user logins). You can use e.g. system logging (syslog for Unix, event viewer for Windows) or log to a separate file. Please note that LAM may log sensitive data (e.g. passwords) at log level "Debug". Production systems should be set to "Warning" or "Error".

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.

Log destinations:

- File: all messages will be written to the given file. LAM will create it if not yet existing.
- Syslog: uses local system logging (syslog for Unix, event viewer for Windows)
- Remote: sends log messages to a remote server that supports the Unix remote Syslogd [https://www.rsyslog.com/] protocol. Please enter destination as "server:port", e.g. "myserver:123".

- No logging: disabled logging



Logging

Log level	Debug
Log destination	File
File	/tmp/lam.log
PHP error reporting	all

Mail options (LAM Pro)

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

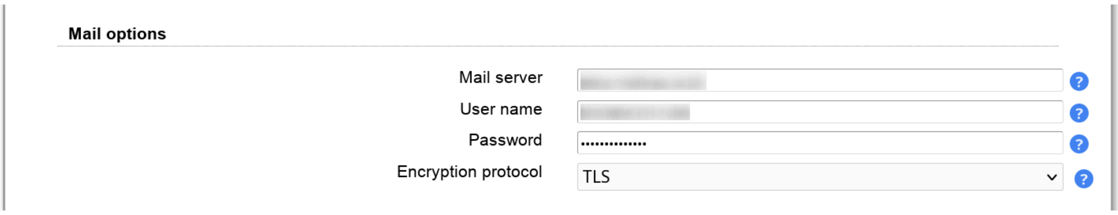
SMTP setup:

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

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

Password: enter the password for the user above

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



Mail options

Mail server	[redacted]
User name	[redacted]
Password	••••••••••••••
Encryption protocol	TLS

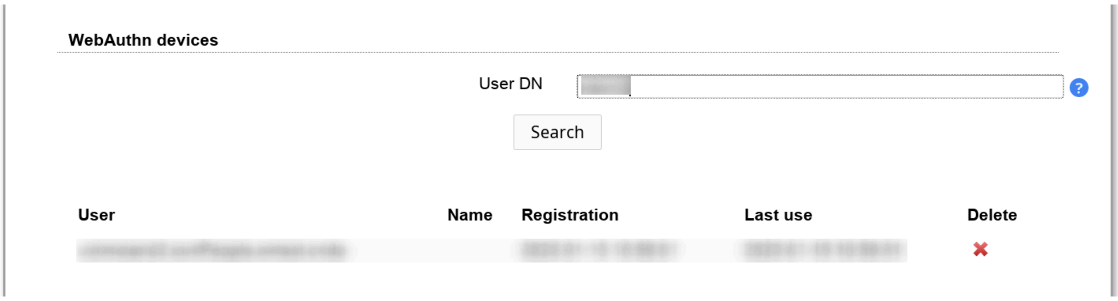
WebAuthn/FIDO2 devices

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

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

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

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



WebAuthn devices

User DN [redacted]

User	Name	Registration	Last use	Delete
[redacted]		[redacted]	[redacted]	✖

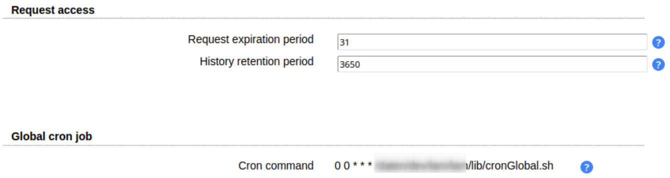
Module settings and global cron job (LAM Pro)

The global cron job is used to perform cleanup tasks.

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

Cleanup actions

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



Request access

Request expiration period: 31

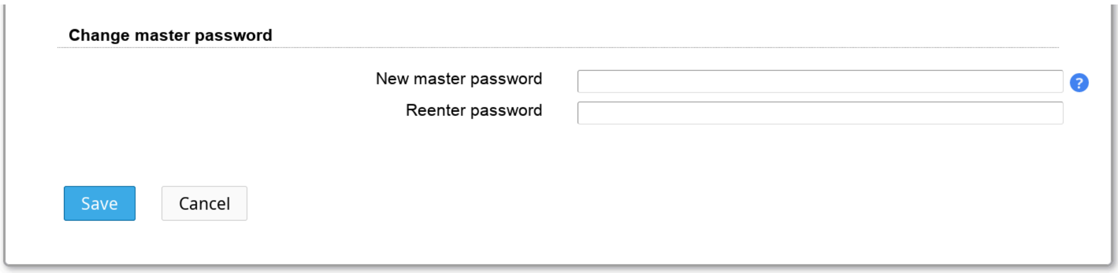
History retention period: 3650

Global cron job

Cron command: 0 0 * * * [redacted]/lib/cronGlobal.sh

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:

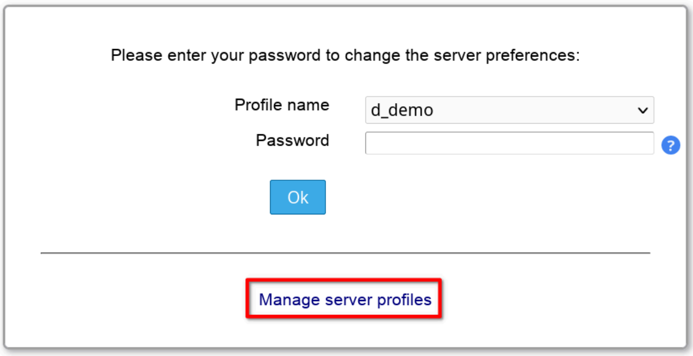
Reenter password:

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.



Please enter your password to change the server preferences:

Profile name: d_demo

Password:

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

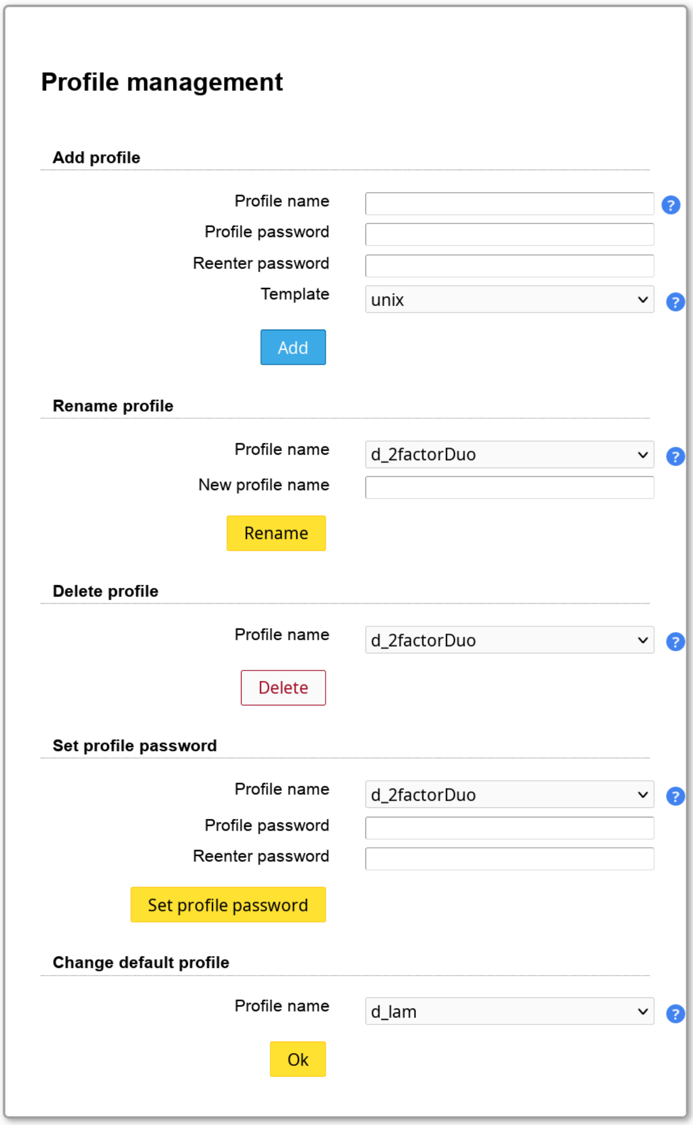
You may also specify the default server profile. This is the server profile which is preselected at the login page. It also specifies the language of the login and configuration pages.

Templates for new server profiles

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

Built-in templates:

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



Profile management

Add profile

Profile name

Profile password

Reenter password

Template: unix

Rename profile

Profile name: d_2factorDuo

New profile name

Delete profile

Profile name: d_2factorDuo

Set profile password

Profile name: d_2factorDuo

Profile password

Reenter password

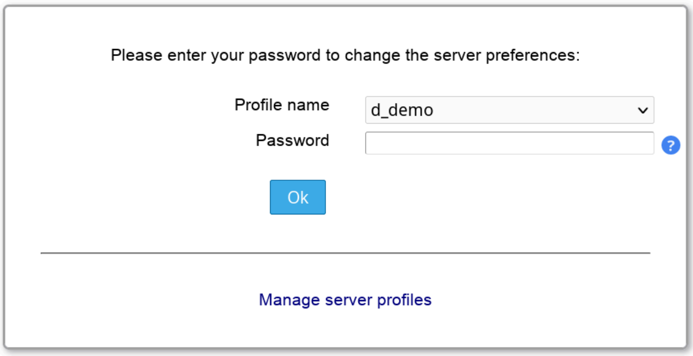
Change default profile

Profile name: d_lam

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

Editing a server profile

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



Please enter your password to change the server preferences:

Profile name: d_demo

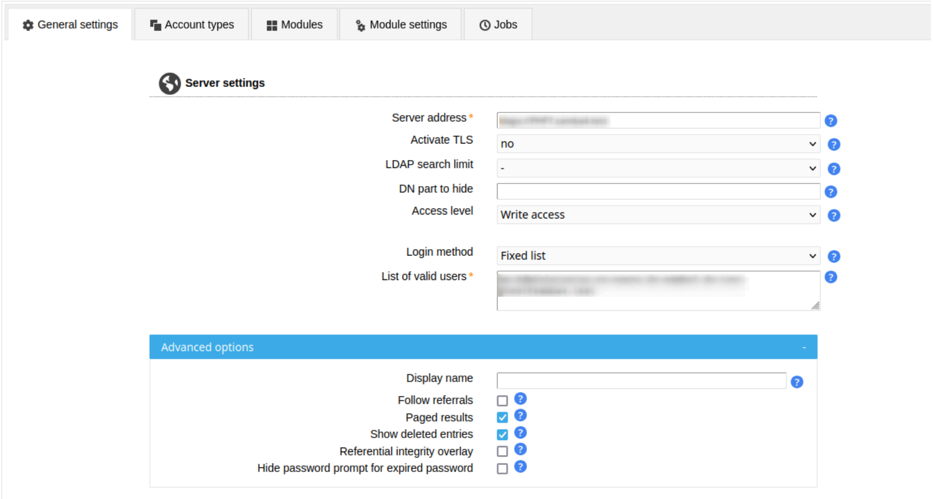
Password:

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.



Server settings

Server address *: [illegible]

Activate TLS: no

LDAP search limit: -

DN part to hide:

Access level: Write access

Login method: Fixed list

List of valid users *: [illegible]

Advanced options

Display name:

☐ Follow referrals

☑ Paged results

☑ Show deleted entries

☐ Referential integrity overlay

☐ Hide password prompt for expired password

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

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

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

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

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

Advanced options

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

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

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

Show deleted entries: This is for Active Directory and Samba 4 only. It will unhide LDAP entries in "CN=Deleted Objects,DC=...". You can use this to browse and restore these entries in tree view.

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

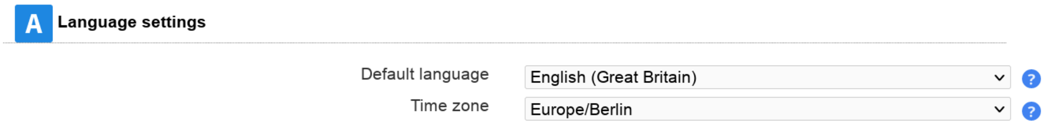
The following actions are skipped in this case:

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

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

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

Please also set your time zone here.



Language settings

Default language: English (Great Britain)

Time zone: Europe/Berlin

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

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

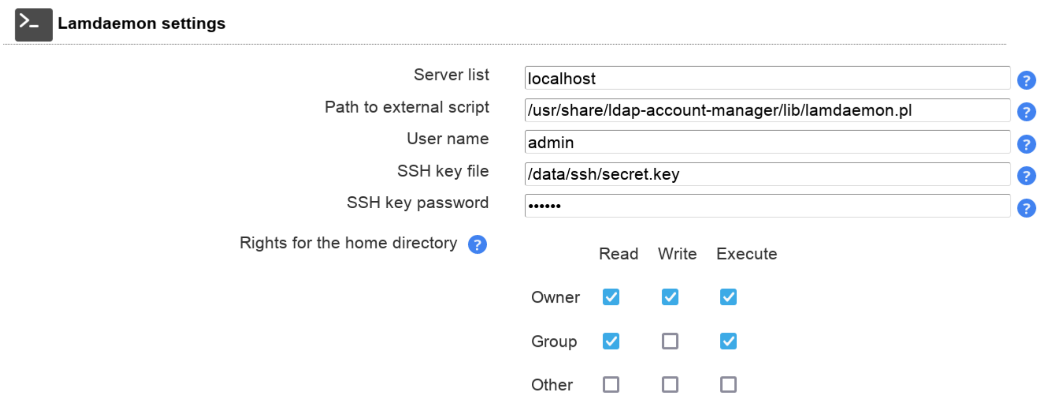
Script server format:

- "server": "server" is the DNS name of your script server
- "server:NAME": NAME is the display name of this server
- "server:NAME:/prefix": /prefix is the directory prefix for all operations. E.g. creating a home directory "/home/user" would create "/prefix/home/user" then.

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

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

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



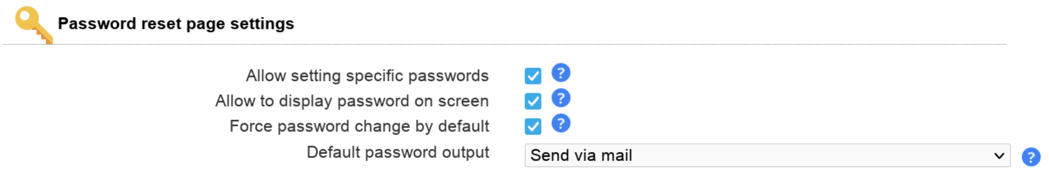
Lamdaemon settings

Server list	localhost
Path to external script	/usr/share/ldap-account-manager/lib/lamdaemon.pl
User name	admin
SSH key file	/data/ssh/secret.key
SSH key password	••••••

Rights for the home directory

	Read	Write	Execute
Owner	☑	☑	☑
Group	☑	□	☑
Other	□	□	□

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

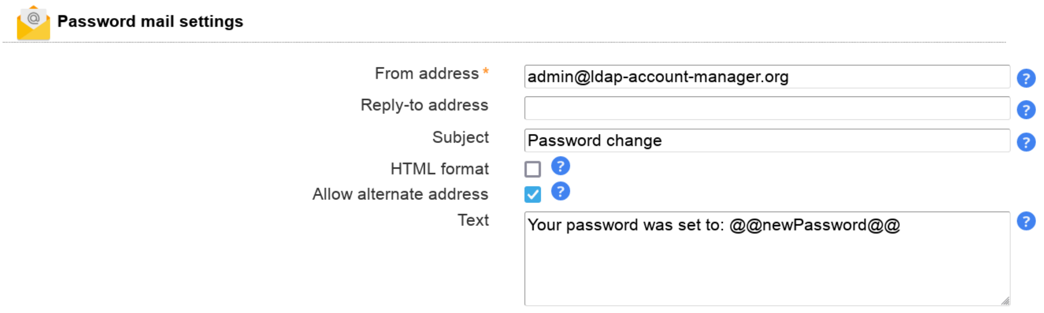


Password reset page settings

Allow setting specific passwords	☑
Allow to display password on screen	☑
Force password change by default	☑
Default password output	Send via mail

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

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

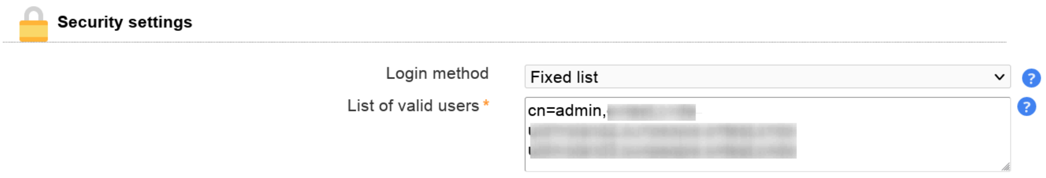


Password mail settings

From address *	admin@ldap-account-manager.org
Reply-to address	
Subject	Password change
HTML format	□
Allow alternate address	☑
Text	Your password was set to: @@newPassword@@

LAM supports two methods for login:

- Fixed list
- LDAP search



Security settings

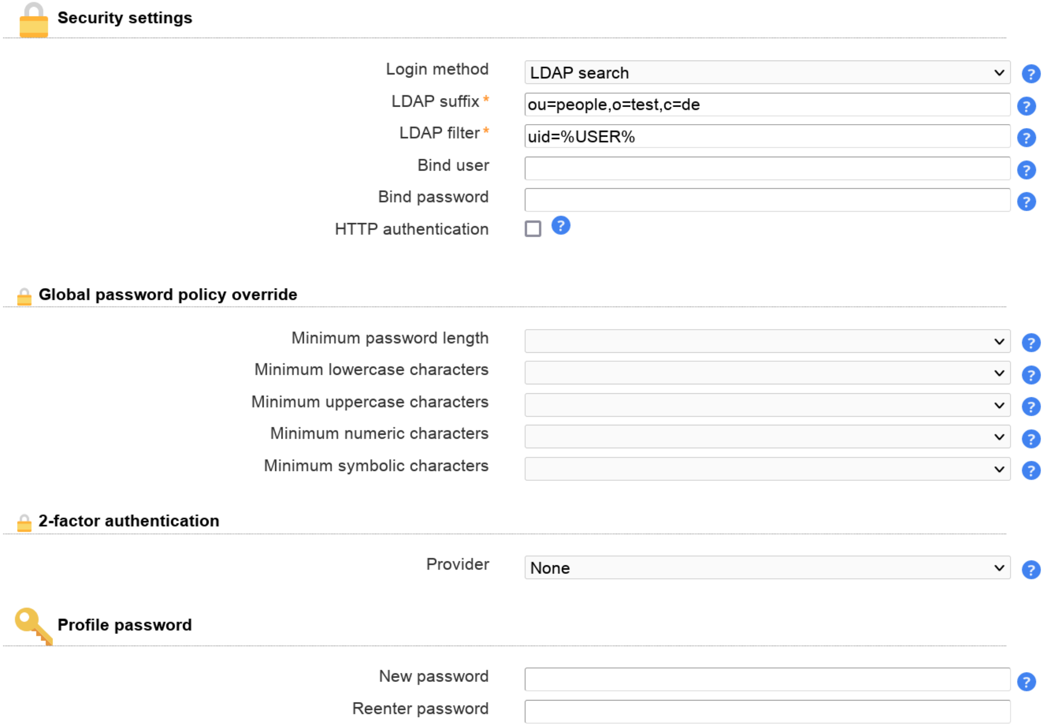
Login method	Fixed list
List of valid users *	cn=admin,[redacted]

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

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

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

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



Security settings

Login method: LDAP search

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

LDAP filter *: uid=%USER%

Bind user:

Bind password:

HTTP authentication: □

Global password policy override

Minimum password length:

Minimum lowercase characters:

Minimum uppercase characters:

Minimum numeric characters:

Minimum symbolic characters:

2-factor authentication

Provider: None

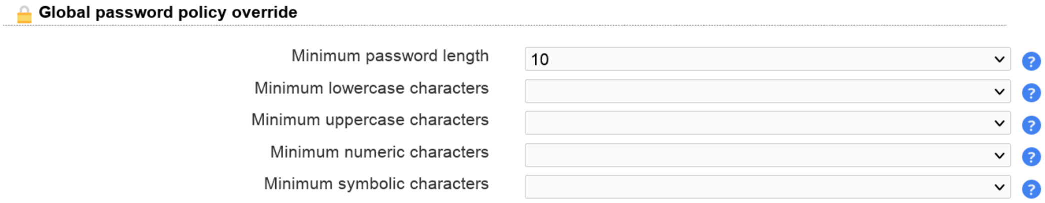
Profile password

New password:

Reenter password:

Global password policy override

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



Global password policy override

Minimum password length: 10

Minimum lowercase characters:

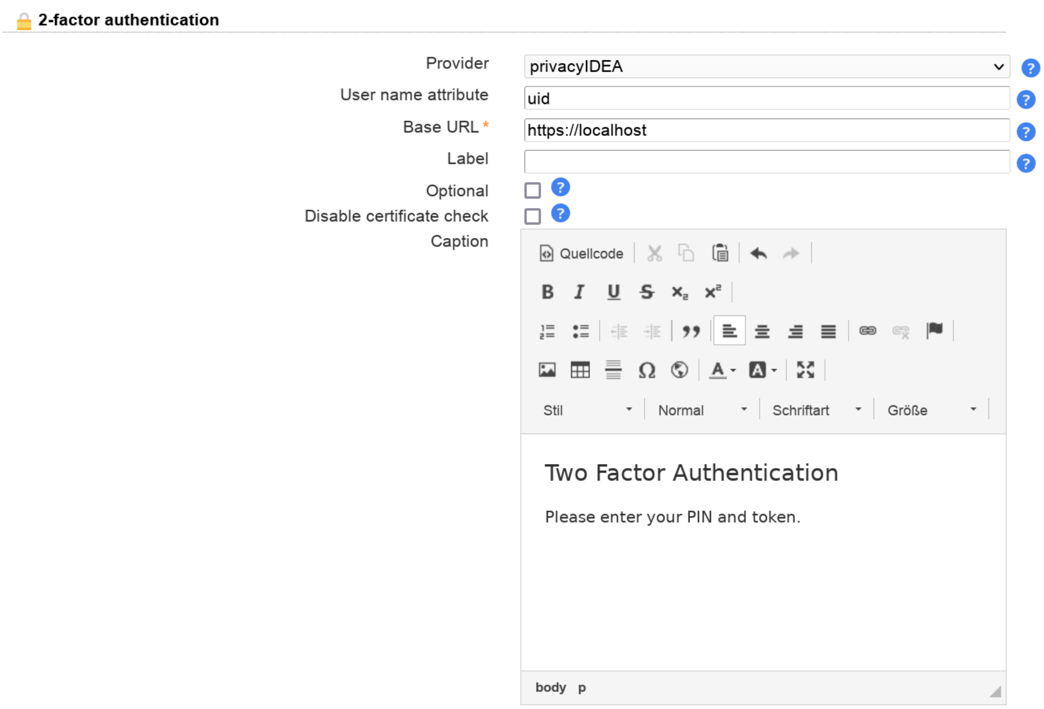
Minimum uppercase characters:

Minimum numeric characters:

Minimum symbolic characters:

2-factor authentication

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



2-factor authentication

Provider	privacyIDEA
User name attribute	uid
Base URL *	https://localhost
Label	
Optional	□
Disable certificate check	□
Caption	Two Factor Authentication Please enter your PIN and token.

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

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

Configuration options:

privacyIDEA

- Base URL: please enter the URL of your privacyIDEA instance
- User name attribute: please enter the LDAP attribute name that contains the user ID (e.g. "uid").
- Optional: By default LAM will enforce to use a token and reject users that did not setup one. You can set this check to optional. But if a user has setup a token then this will always be required.
- Disable certificate check: This should be used on development instances only. It skips the certificate check when connecting to verification server.

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

YubiKey

- Base URLs: please enter the URL(s) of your YubiKey verification server(s). If you run a custom verification API such as yubiserver then enter its URL (e.g. http://www.example.com:8000/wsapi/2.0/verify). The URL needs to end with "/wsapi/2.0/verify". For YubiKey cloud these are "https://api.yubico.com/wsapi/2.0/verify", "https://api2.yubico.com/wsapi/2.0/verify", "https://api3.yubico.com/wsapi/2.0/verify", "https://api4.yubico.com/wsapi/2.0/verify" and "https://api5.yubico.com/wsapi/2.0/verify". Enter one URL per line.

- Client id: this is only required for YubiKey cloud. You can register here: https://upgrade.yubico.com/getapikey/
- Secret key: this is only required for YubiKey cloud. You can register here: https://upgrade.yubico.com/getapikey/
- Optional: By default LAM will enforce to use a token and reject users that did not setup one. You can set this check to optional. But if a user has setup a token then this will always be required.
- Disable certificate check: This should be used on development instances only. It skips the certificate check when connecting to verification server.

Duo

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

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

WebAuthn/FIDO2

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

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

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

Okta

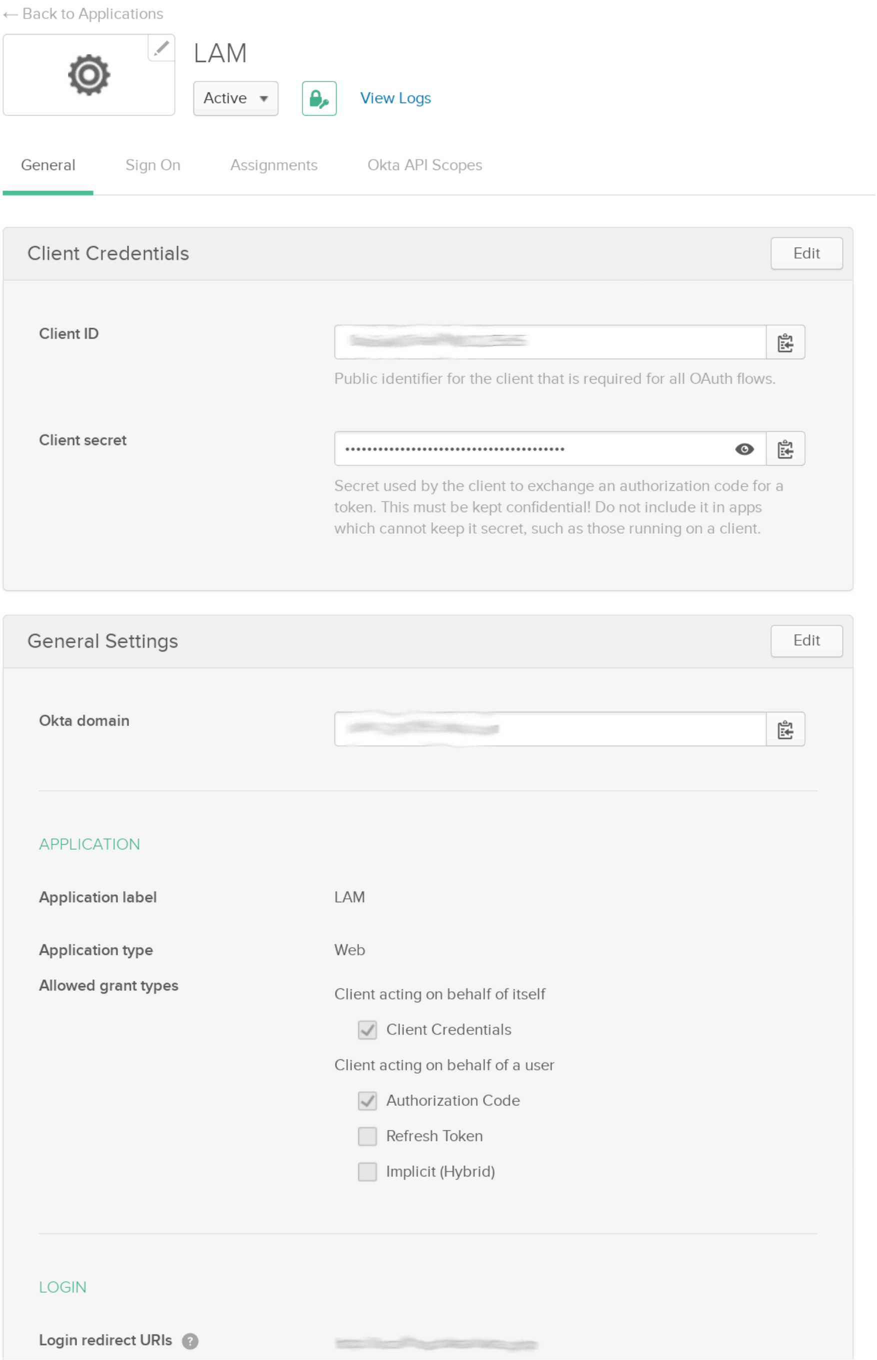
This requires to register a new application of type "Web".

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

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

LAM options:

- User name attribute: please enter the LDAP attribute name that contains the user ID (e.g. "mail").
- Base URL: please enter the URL of your Okta domain (e.g. https://mydomain.okta.com)
- Client id: please enter your application client id.
- Secret key: please enter your application secret key.



Client Credentials

Client ID: [redacted]

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

Client secret: ••

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

General Settings

Okta domain: [redacted]

APPLICATION

Application label: LAM

Application type: Web

Allowed grant types:

Client acting on behalf of itself

- ☑ Client Credentials

Client acting on behalf of a user

- ☑ Authorization Code
- ☐ Refresh Token
- ☐ Implicit (Hybrid)

LOGIN

Login redirect URIs: [redacted]

OpenID

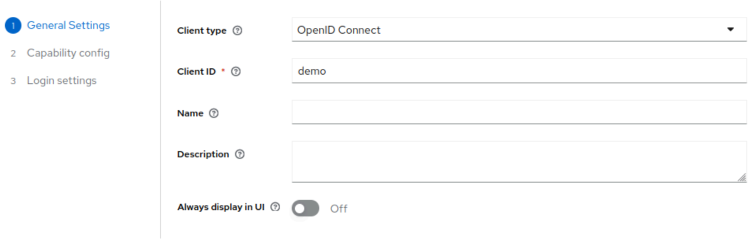
This will use an OpenID server as 2nd factor for authentication.

LAM options:

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

KeyCloack example configuration:

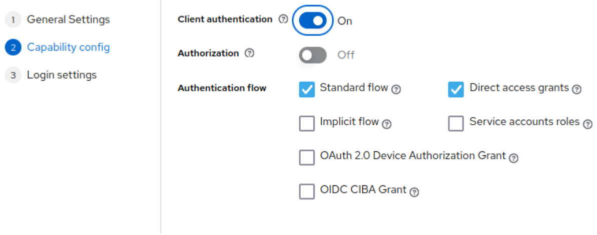
Create a new client, select "OpenID Connect" client type and enter a client ID.



1. General Settings
2. Capability config
3. Login settings

Client type	OpenID Connect
Client ID *	demo
Name	
Description	
Always display in UI	Off

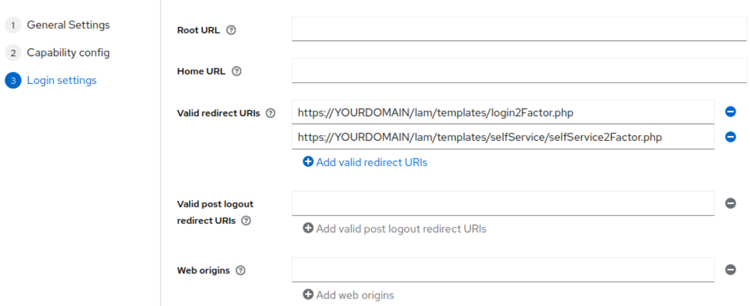
Now enable "Client authentication" and enter the valid redirect URLs in the last step.



1. General Settings
2. Capability config
3. Login settings

Client authentication	On	
Authorization	Off	
Authentication flow	☑ Standard flow	☑ Direct access grants
	□ Implicit flow	□ Service accounts roles
	□ OAuth 2.0 Device Authorization Grant	
	□ OIDC CIBA Grant	

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



1. General Settings
2. Capability config
3. Login settings

Root URL	
Home URL	
Valid redirect URIs	https://YOURDOMAIN/lam/templates/login2Factor.php https://YOURDOMAIN/lam/templates/selfService/selfService2Factor.php
Valid post logout redirect URIs	
Web origins	

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

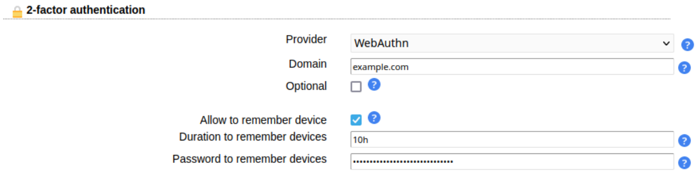
Example configuration values:

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

Remember device

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

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

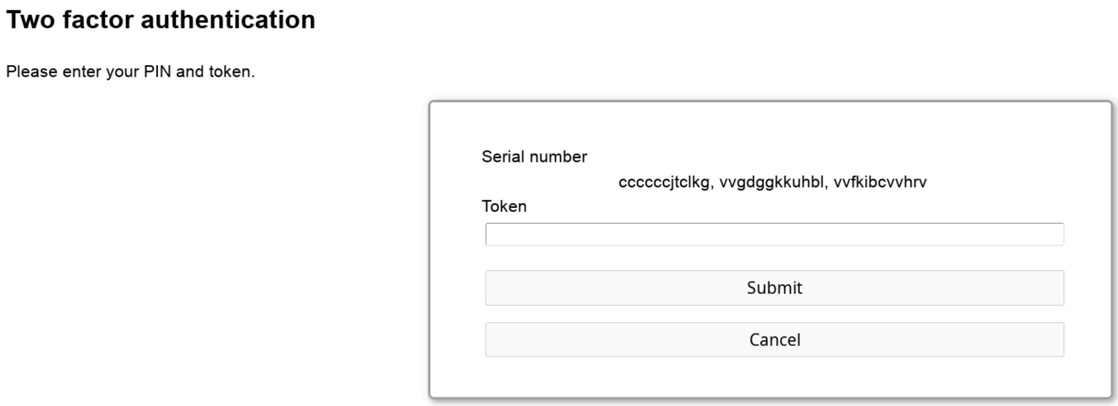


2-factor authentication

Provider	WebAuthn
Domain	example.com
Optional	□
Allow to remember device	☑
Duration to remember devices	10h
Password to remember devices	••••••••••••••••••••••••••••••

Login

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



Two factor authentication

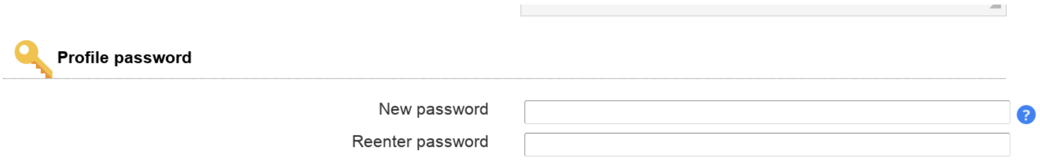
Please enter your PIN and token.

Serial number: cccccjtclkg, vvgdggkkuhbl, vvfkibcvvhrv

Token

Password

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



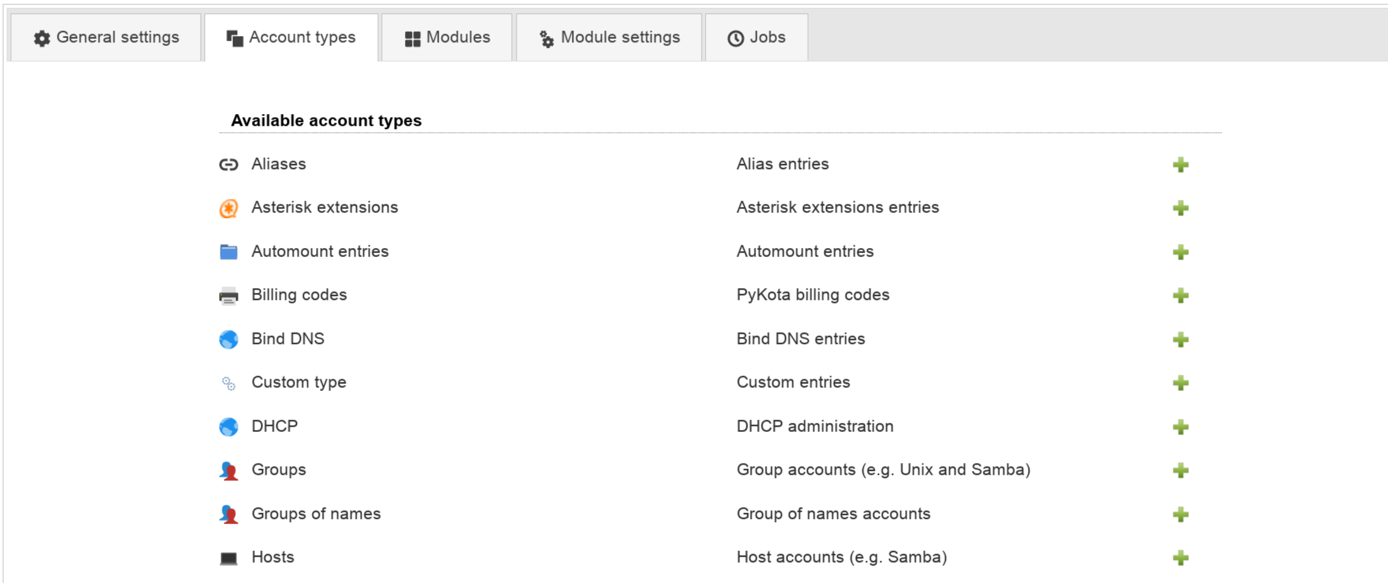
Profile password

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.



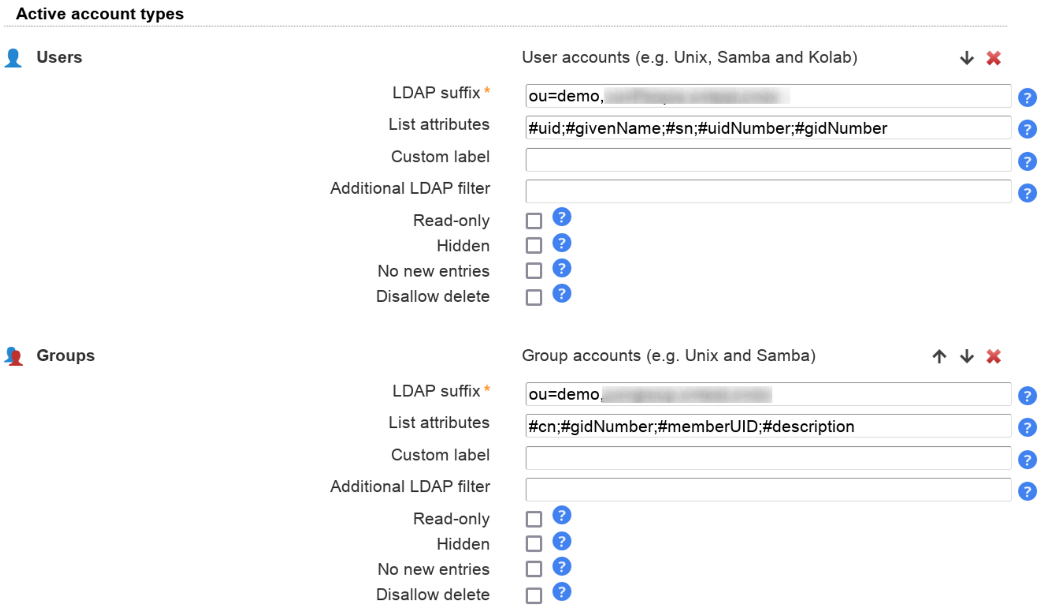
Available account types

Aliases	Alias entries	✚
Asterisk extensions	Asterisk extensions entries	✚
Automount entries	Automount entries	✚
Billing codes	PyKota billing codes	✚
Bind DNS	Bind DNS entries	✚
Custom type	Custom entries	✚
DHCP	DHCP administration	✚
Groups	Group accounts (e.g. Unix and Samba)	✚
Groups of names	Group of names accounts	✚
Hosts	Host accounts (e.g. Samba)	✚

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

Each account type has the following options:

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



Active account types

Users

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

LDAP suffix *: ou=demo,[redacted]
List attributes: #uid;#givenName;#sn;#uidNumber;#gidNumber
Custom label:
Additional LDAP filter:
Read-only ☐
Hidden ☐
No new entries ☐
Disallow delete ☐

Groups

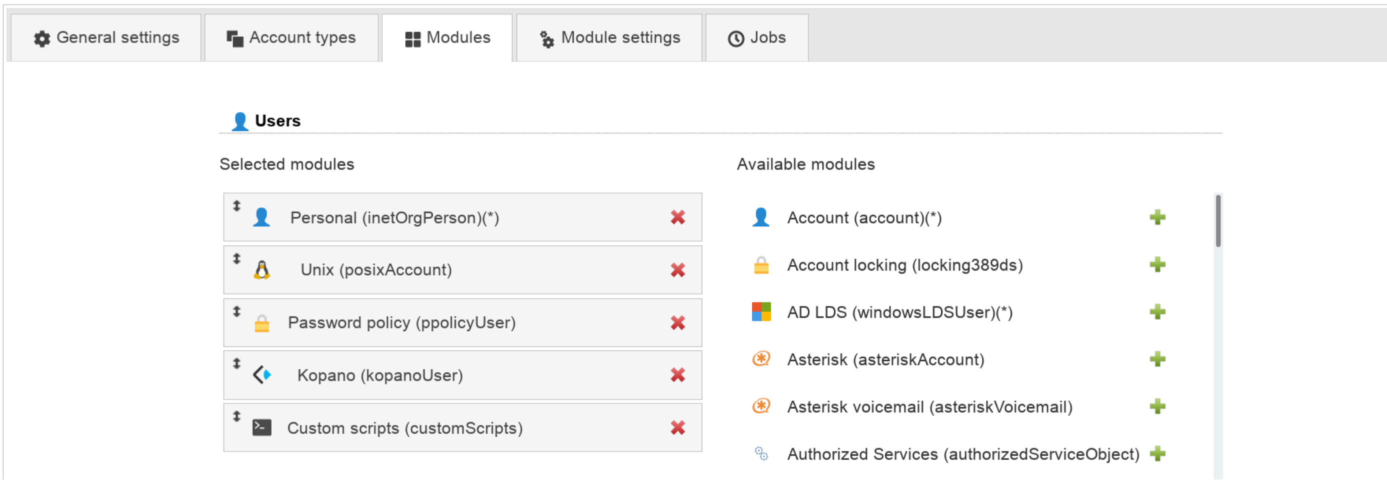
Group accounts (e.g. Unix and Samba)

LDAP suffix *: ou=demo,[redacted]
List attributes: #cn;#gidNumber;#memberUID;#description
Custom label:
Additional LDAP filter:
Read-only ☐
Hidden ☐
No new entries ☐
Disallow delete ☐

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

Modules

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



Users

Selected modules

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

Available modules

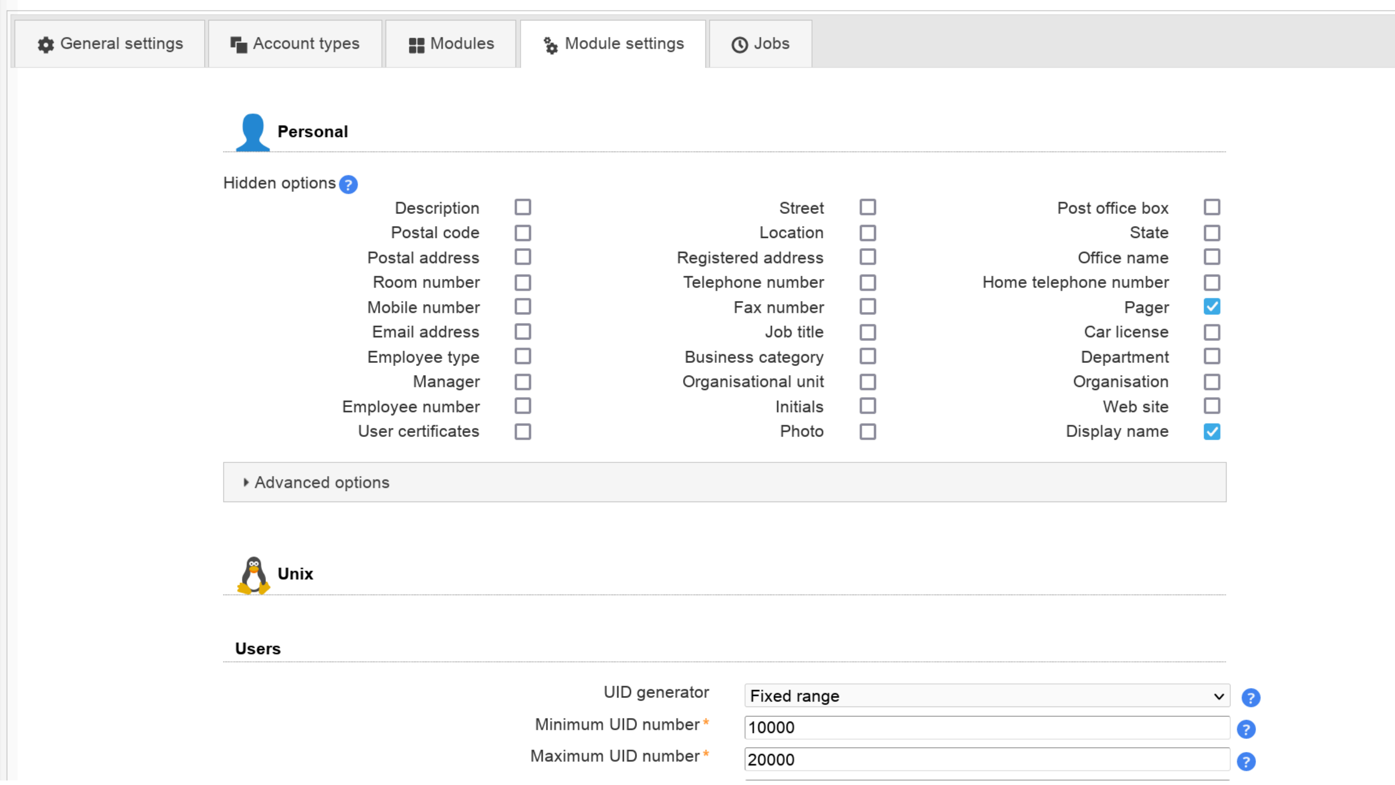
- Account (account)(*)
- Account locking (locking389ds)
- AD LDS (windowsLDSUser)(*)
- Asterisk (asteriskAccount)
- Asterisk voicemail (asteriskVoicemail)
- Authorized Services (authorizedServiceObject)

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

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

Module settings

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



Personal

Hidden options

Description	□	Street	□	Post office box	□
Postal code	□	Location	□	State	□
Postal address	□	Registered address	□	Office name	□
Room number	□	Telephone number	□	Home telephone number	□
Mobile number	□	Fax number	□	Pager	☑
Email address	□	Job title	□	Car license	□
Employee type	□	Business category	□	Department	□
Manager	□	Organisational unit	□	Organisation	□
Employee number	□	Initials	□	Web site	□
User certificates	□	Photo	□	Display name	☑

Unix

Users

UID generator	Fixed range
Minimum UID number*	10000
Maximum UID number*	20000

Cron jobs (LAM Pro)

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

LDAP and database configuration

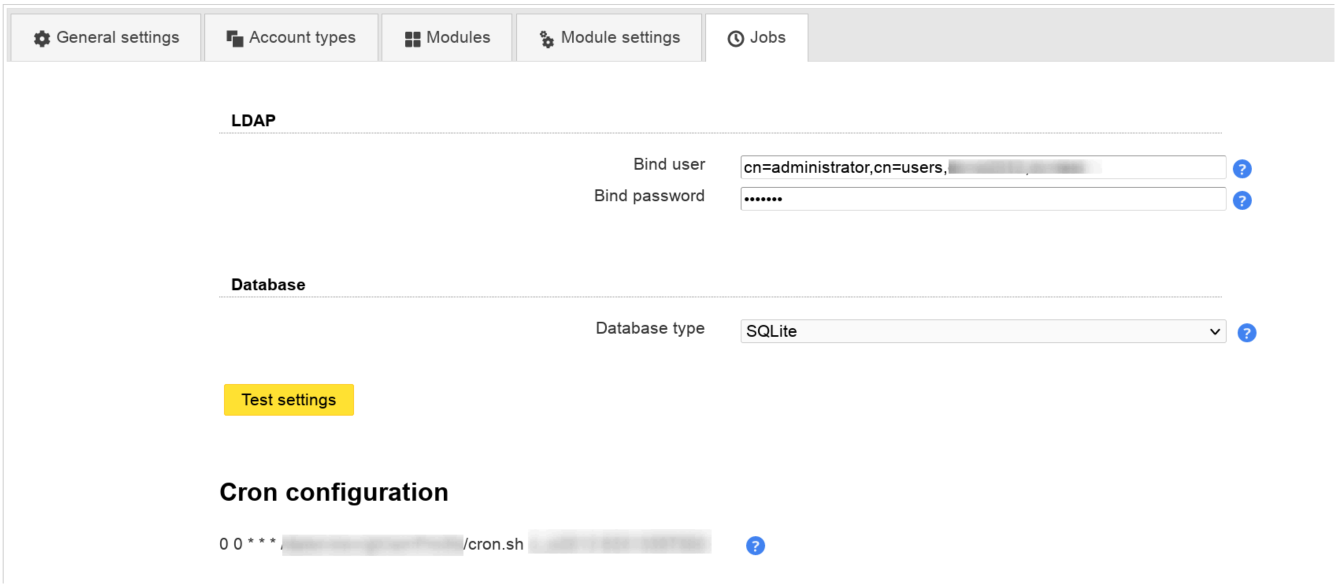
Please add the LDAP bind user and password for all jobs. This LDAP account will be used to perform all LDAP read and write operations.

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

SQLite

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

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



LDAP

Bind user: cn=administrator,cn=users,[redacted]

Bind password: •••••••

Database

Database type: SQLite

Cron configuration

0 0 * * * [redacted]/cron.sh [redacted]

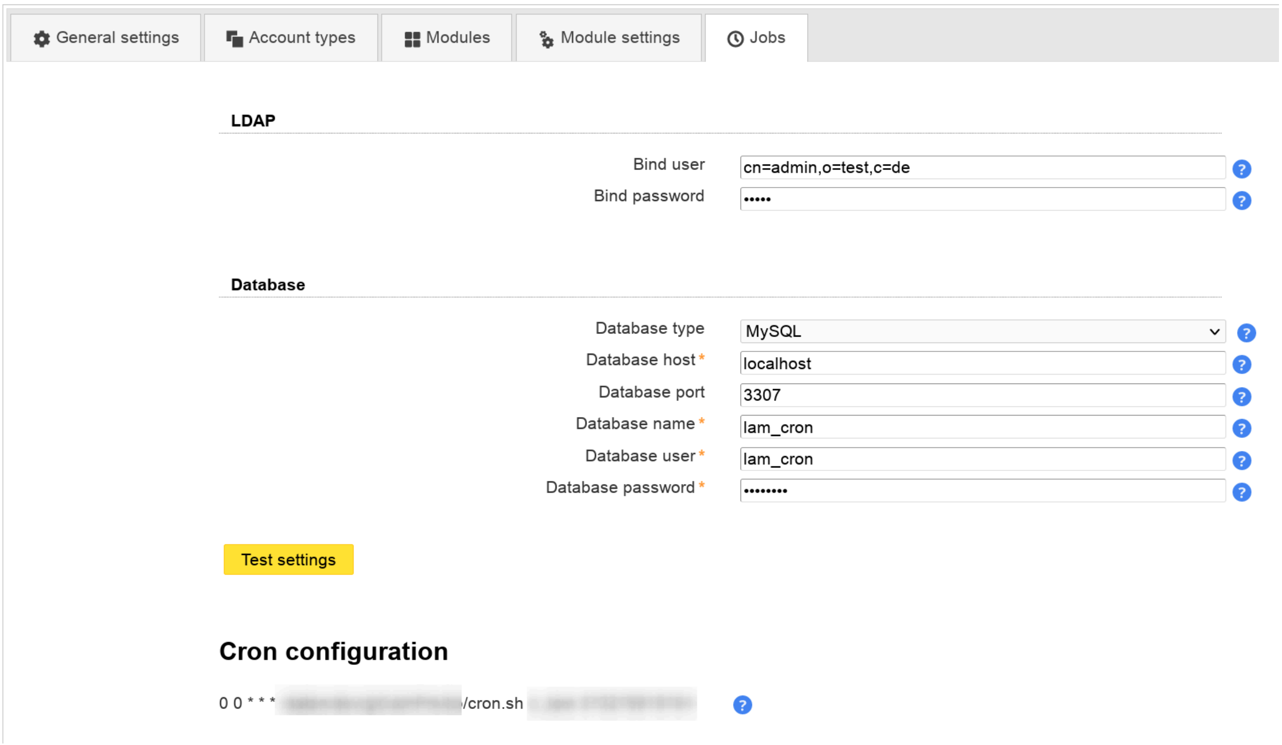
MySQL

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

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

Steps to create a MySQL database and user:

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



LDAP

Bind user: cn=admin,o=test,c=de
Bind password: •••••

Database

Database type: MySQL
Database host*: localhost
Database port: 3307
Database name*: lam_cron
Database user*: lam_cron
Database password*: ••••••••

Cron configuration

```
0 0 * * * [redacted]/cron.sh [redacted]
```

Test your settings

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

Cron entry

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

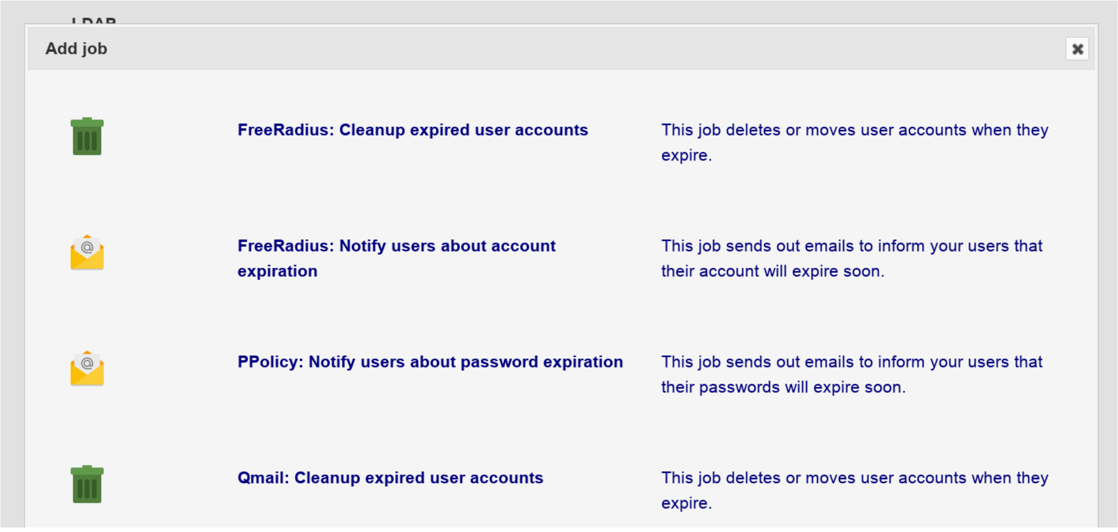
Dry-run: You can perform a dry-run of the job. This will not perform any actions but only print what would be done. For this please put "--dry-run" at the end of the command. E.g.:

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

Adding jobs

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

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



Add job

🗑	FreeRadius: Cleanup expired user accounts	This job deletes or moves user accounts when they expire.
✉	FreeRadius: Notify users about account expiration	This job sends out emails to inform your users that their account will expire soon.
✉	PPolicy: Notify users about password expiration	This job sends out emails to inform your users that their passwords will expire soon.
🗑	Qmail: Cleanup expired user accounts	This job deletes or moves user accounts when they expire.

Available jobs:

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

PPolicy: Notify users about password expiration

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

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

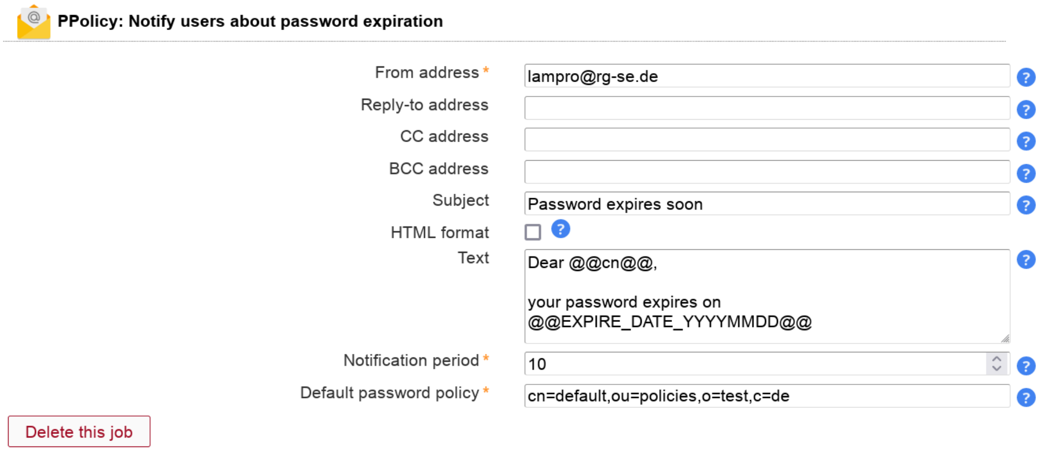
LAM calculates the expiration date based on the last password change and the assigned password policy (or the default policy) using attributes pwdMaxAge and pwdExpireWarning. Negative values are possible to send mails when LDAP's warning time already started.

Examples:

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

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

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



PPolicy: Notify users about password expiration

From address *	lampro@rg-se.de
Reply-to address	
CC address	
BCC address	
Subject	Password expires soon
HTML format	□
Text	Dear @@cn@@, your password expires on @@EXPIRE_DATE_YYYYMMDD@@
Notification period *	10
Default password policy *	cn=default,ou=policies,o=test,c=de

Table 3.1. Options

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

Wildcards:

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

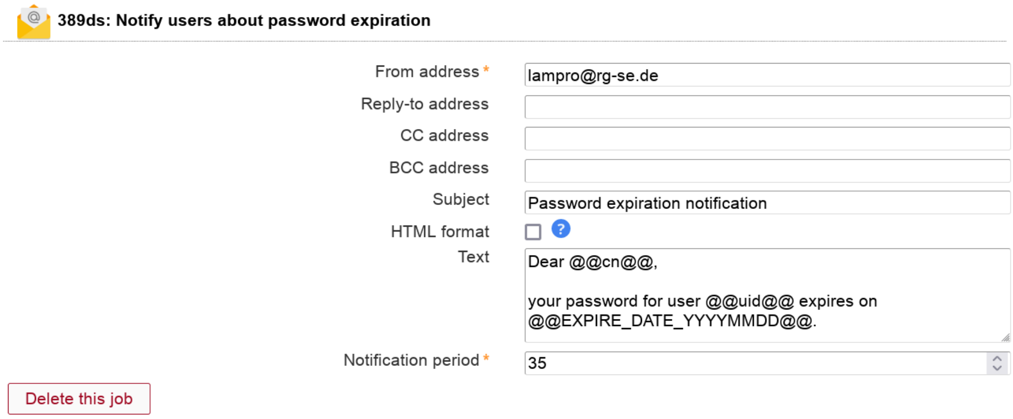
There are also two special wildcards for the expiration date. @@EXPIRE_DATE_DDMMYYYY@@ will print the date as e.g. "31.12.2016". @@EXPIRE_DATE_YYYYMMDD@@ will print the date as e.g. "2016-12-31".

389ds: Notify users about password expiration

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

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

LAM calculates the expiration date based on the attribute passwordExpirationTime.



389ds: Notify users about password expiration

From address * lampro@rg-se.de

Reply-to address

CC address

BCC address

Subject Password expiration notification

HTML format □

Text Dear @@cn@@,

your password for user @@uid@@ expires on @@EXPIRE_DATE_YYYYMMDD@@.

Notification period * 35

Delete this job

Table 3.2. Options

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

Wildcards:

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

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

Shadow: Notify users about password expiration

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

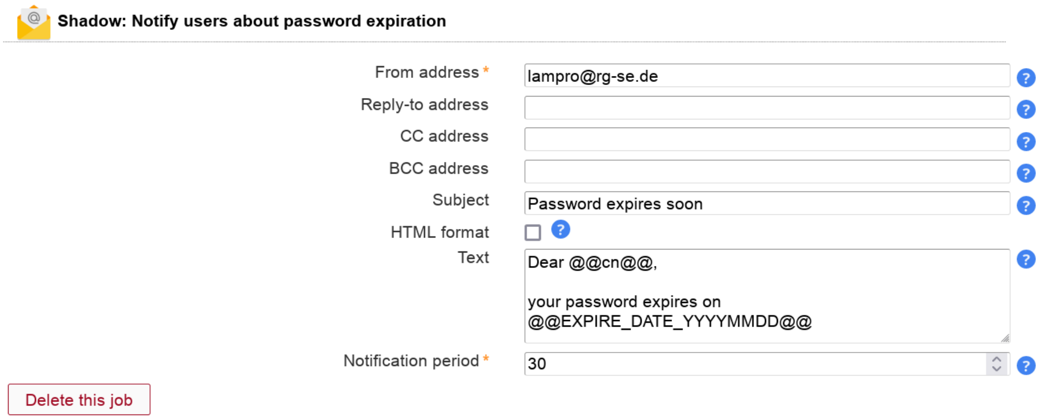
You need to activate the Shadow module for users to be able to add this job. The job can be added multiple times (e.g. to send a second warning at a later time).

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

Examples:

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

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



Shadow: Notify users about password expiration

From address * lampro@rg-se.de

Reply-to address

CC address

BCC address

Subject Password expires soon

HTML format □

Text Dear @@cn@@,

your password expires on
@@EXPIRE_DATE_YYYYMMDD@@

Notification period * 30

Table 3.3. Options

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

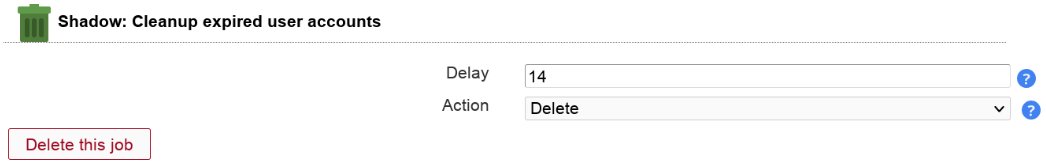
Wildcards:

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

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

Shadow: Delete or move expired accounts

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



Shadow: Cleanup expired user accounts

Delay 14

Action Delete

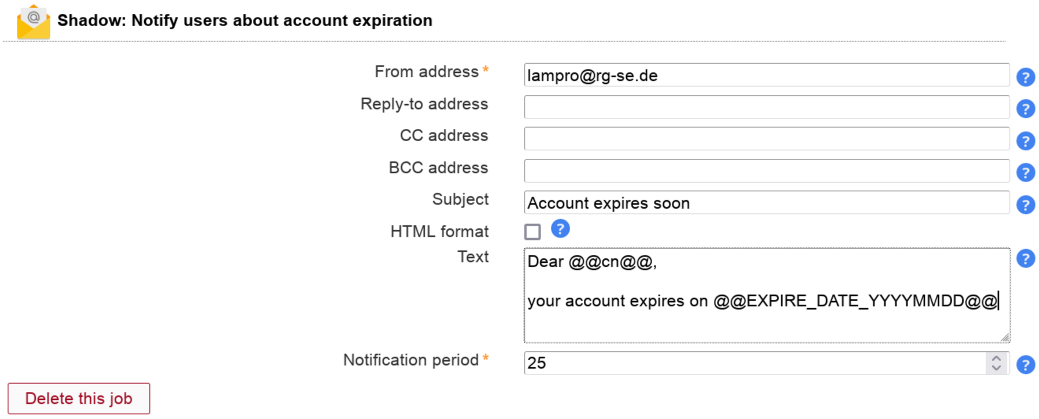
Table 3.4. Options

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

Shadow: Notify users about account expiration

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

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



Shadow: Notify users about account expiration

From address *	lampro@rg-se.de
Reply-to address	
CC address	
BCC address	
Subject	Account expires soon
HTML format	□
Text	Dear @@cn@@, your account expires on @@EXPIRE_DATE_YYYYMMDD@@
Notification period *	25

Table 3.5. Options

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

Wildcards:

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

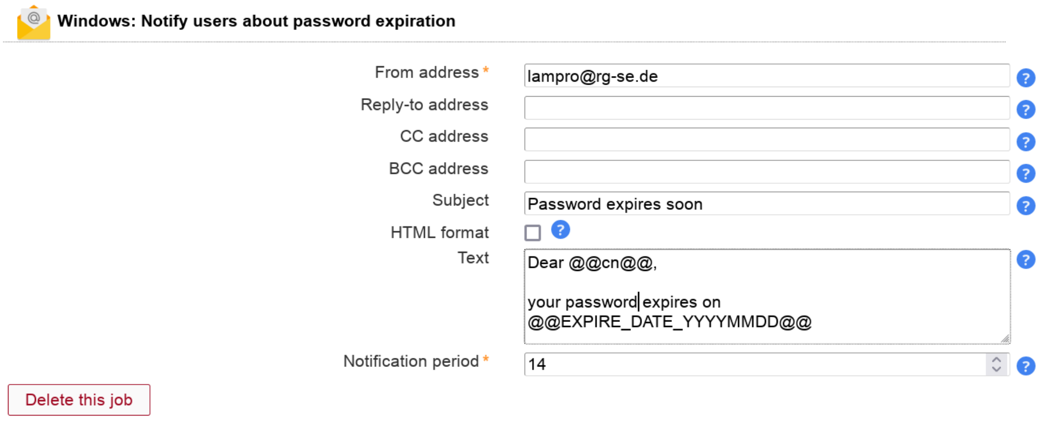
There are also two special wildcards for the expiration date. @@EXPIRE_DATE_DDMMYYYY@@ will print the date as e.g. "31.12.2016". @@EXPIRE_DATE_YYYYMMDD@@ will print the date as e.g. "2016-12-31".

Windows: Notify users about password expiration

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

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

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



Windows: Notify users about password expiration

From address *	lampro@rg-se.de
Reply-to address	
CC address	
BCC address	
Subject	Password expires soon
HTML format	□
Text	Dear @@cn@@, your password expires on @@EXPIRE_DATE_YYYYMMDD@@
Notification period *	14

Table 3.6. Options

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

Wildcards:

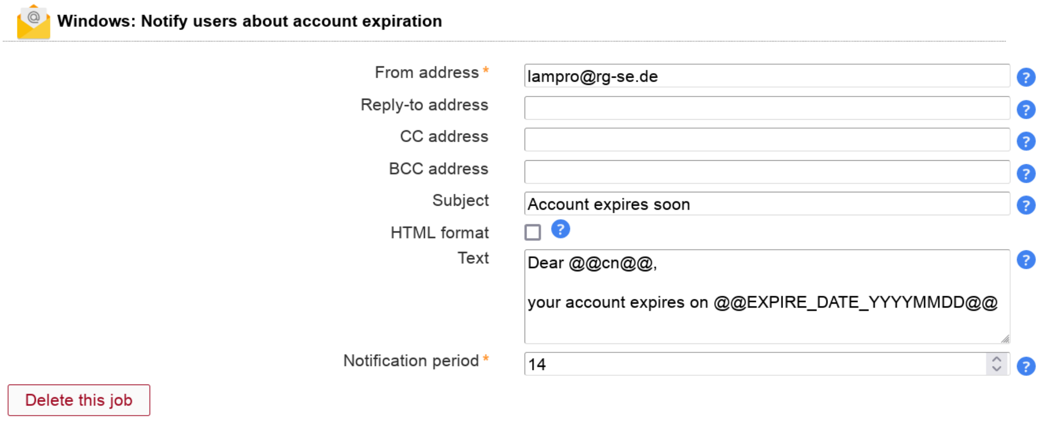
You can enter LDAP attributes as wildcards in the form @@ATTRIBUTE_NAME@@. E.g. to add the user's common name use "@@cn@@". For the common name it would be "@@cn@@".

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

Windows: Notify users about account expiration

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

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



Windows: Notify users about account expiration

From address *	lampro@rg-se.de
Reply-to address	
CC address	
BCC address	
Subject	Account expires soon
HTML format	□
Text	Dear @@cn@@, your account expires on @@EXPIRE_DATE_YYYYMMDD@@
Notification period *	14

Table 3.7. Options

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

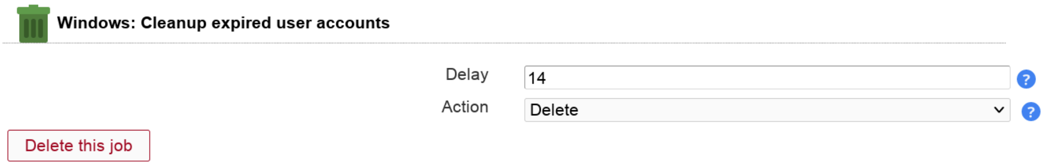
Wildcards:

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

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

Windows: Delete or move expired accounts

You can automatically delete or move expired accounts.



Windows: Cleanup expired user accounts

Delay: 14

Action: Delete

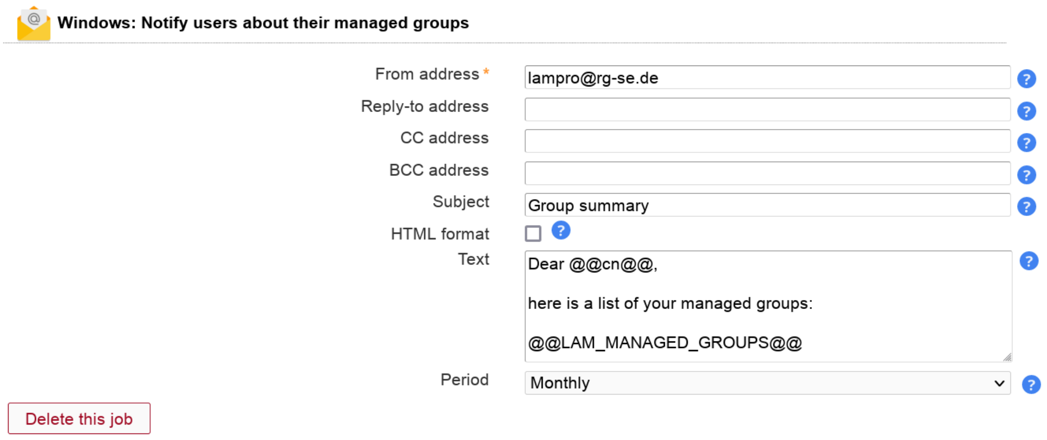
Table 3.8. Options

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

Windows: Notify users about their managed groups

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

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



Windows: Notify users about their managed groups

From address * lampro@rg-se.de

Reply-to address

CC address

BCC address

Subject Group summary

HTML format □

Text

Dear @@cn@@,

here is a list of your managed groups:

@@LAM_MANAGED_GROUPS@@

Period Monthly

Table 3.9. Options

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

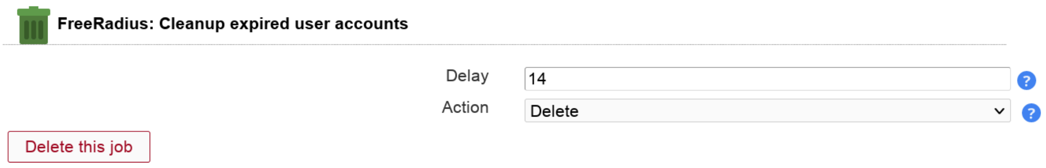
Wildcards:

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

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

FreeRadius: Delete or move expired accounts

You can automatically delete or move expired accounts.



FreeRadius: Cleanup expired user accounts

Delay 14

Action Delete

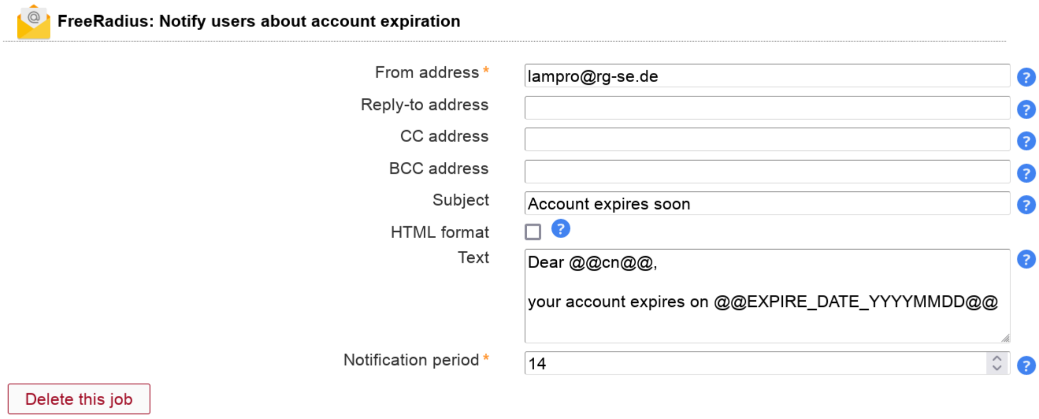
Table 3.10. Options

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

FreeRadius: Notify users about account expiration

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

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



FreeRadius: Notify users about account expiration

From address * lampro@rg-se.de

Reply-to address

CC address

BCC address

Subject Account expires soon

HTML format □

Text Dear @@cn@@,

your account expires on @@EXPIRE_DATE_YYYYMMDD@@

Notification period * 14

Table 3.11. Options

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

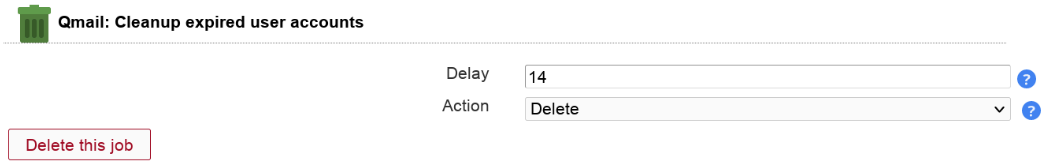
Wildcards:

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

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

Qmail: Delete or move expired accounts

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



Qmail: Cleanup expired user accounts

Delay 14

Action Delete

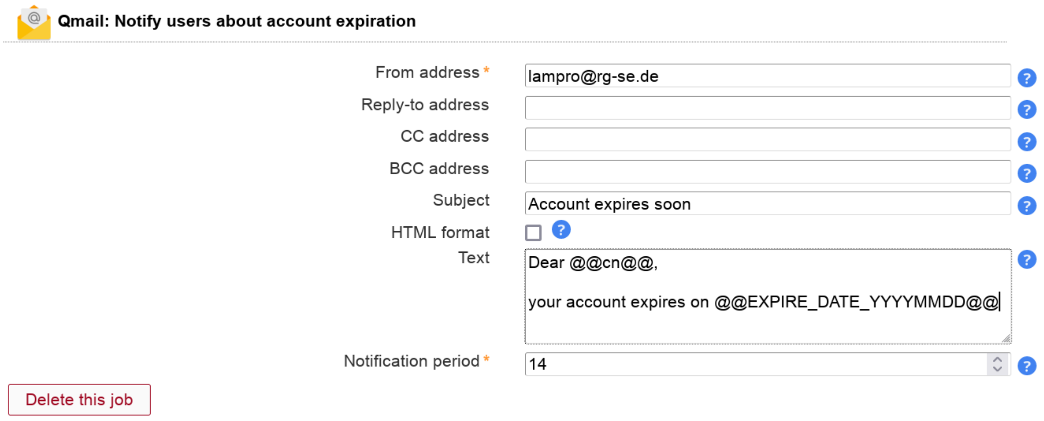
Table 3.12. Options

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

Qmail: Notify users about account expiration

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

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



Qmail: Notify users about account expiration

From address *	lampro@rg-se.de
Reply-to address	
CC address	
BCC address	
Subject	Account expires soon
HTML format	□
Text	Dear @@cn@@, your account expires on @@EXPIRE_DATE_YYYYMMDD@@
Notification period *	14

Delete this job

Table 3.13. Options

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

Wildcards:

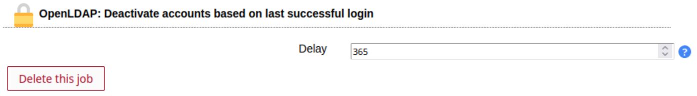
You can enter LDAP attributes as wildcards in the form @@ATTRIBUTE_NAME@@. E.g. to add the user's common name use "@@cn@@". For the common name it would be "@@cn@@".

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

OpenLDAP: Deactivate accounts based on last successful login

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

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



OpenLDAP: Deactivate accounts based on last successful login

Delay	365

Delete this job

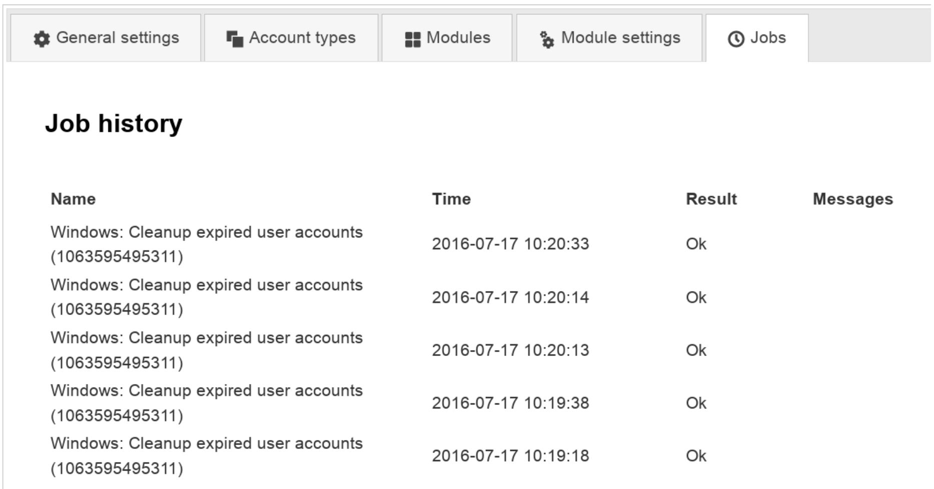
Table 3.14. Options

Option	Description

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

Job history

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



Job history

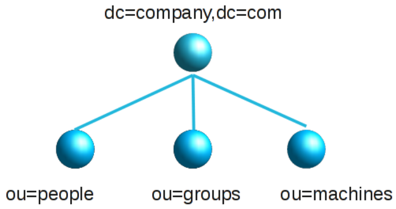
Name	Time	Result	Messages
Windows: Cleanup expired user accounts (1063595495311)	2016-07-17 10:20:33	Ok	
Windows: Cleanup expired user accounts (1063595495311)	2016-07-17 10:20:14	Ok	
Windows: Cleanup expired user accounts (1063595495311)	2016-07-17 10:20:13	Ok	
Windows: Cleanup expired user accounts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

Typical scenarios

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

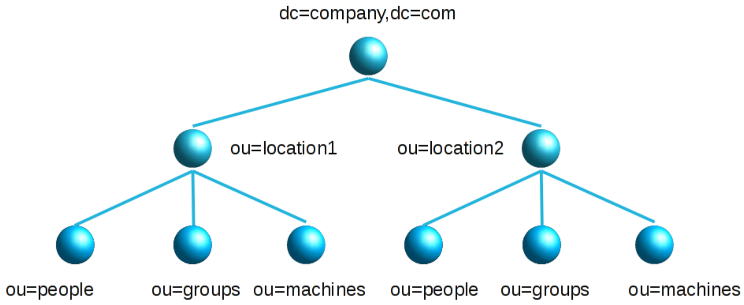
Simple: One LDAP directory managed by a small group of admins

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



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

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

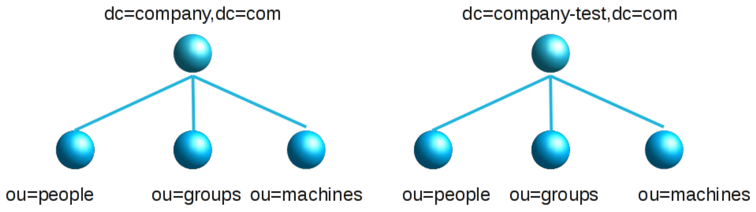


In this situation it is recommended to create one server profile for each admin group (e.g. department). Setup the LDAP suffixes in the server profiles to point to the needed organisational units. E.g. use ou=people,ou=department1,dc=company,dc=com or ou=department1,ou=people,dc=company,dc=com as LDAP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

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

Multiple LDAP servers

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



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

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

- Divide your LDAP tree in organisational units: This is usually the best performing option. Put your accounts in several organisational units and setup LAM as in the advanced scenario above.

- Increase memory limit: Increase the memory_limit parameter in your php.ini. This will allow LAM to read more entries. But this will slow down the response times of LAM.

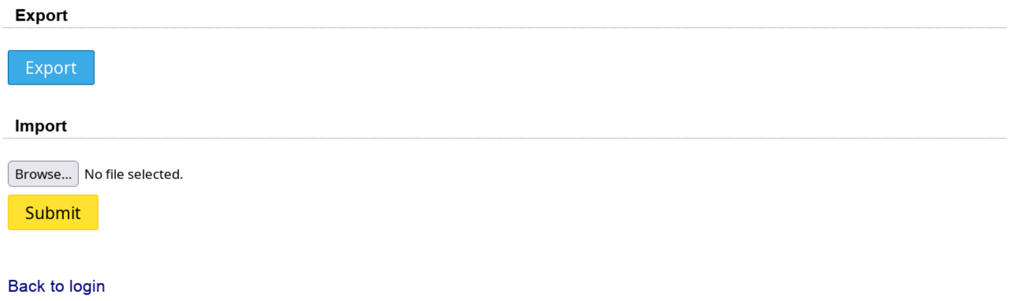
Self Service (LAM Pro)

See Self Service chapter.

Import and export configuration

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

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



Export

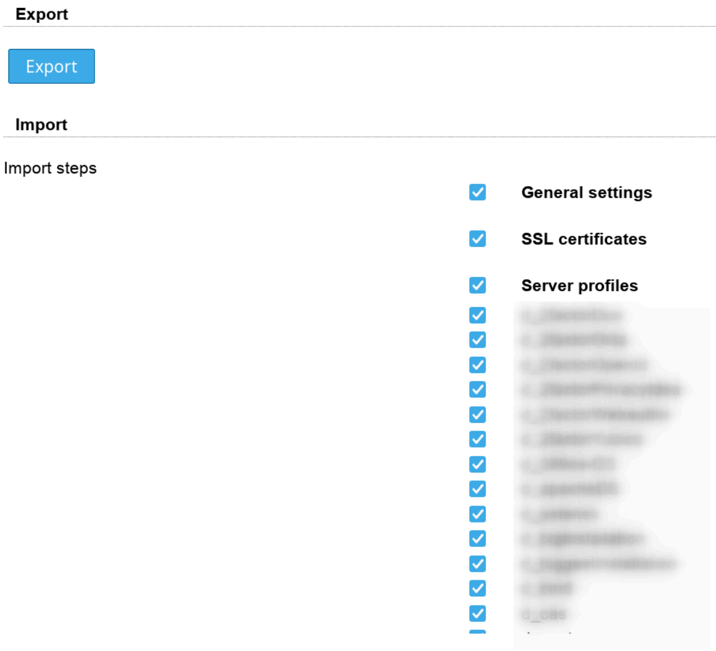
This will dump the whole configuration to one big single file. It is not possible to dump only parts of the configuration. During import you can select what exactly to import.

Import

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

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

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



Export

Import

Import steps

☑ General settings

☑ SSL certificates

☑ Server profiles

Chapter 4. Managing entries in your LDAP directory

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

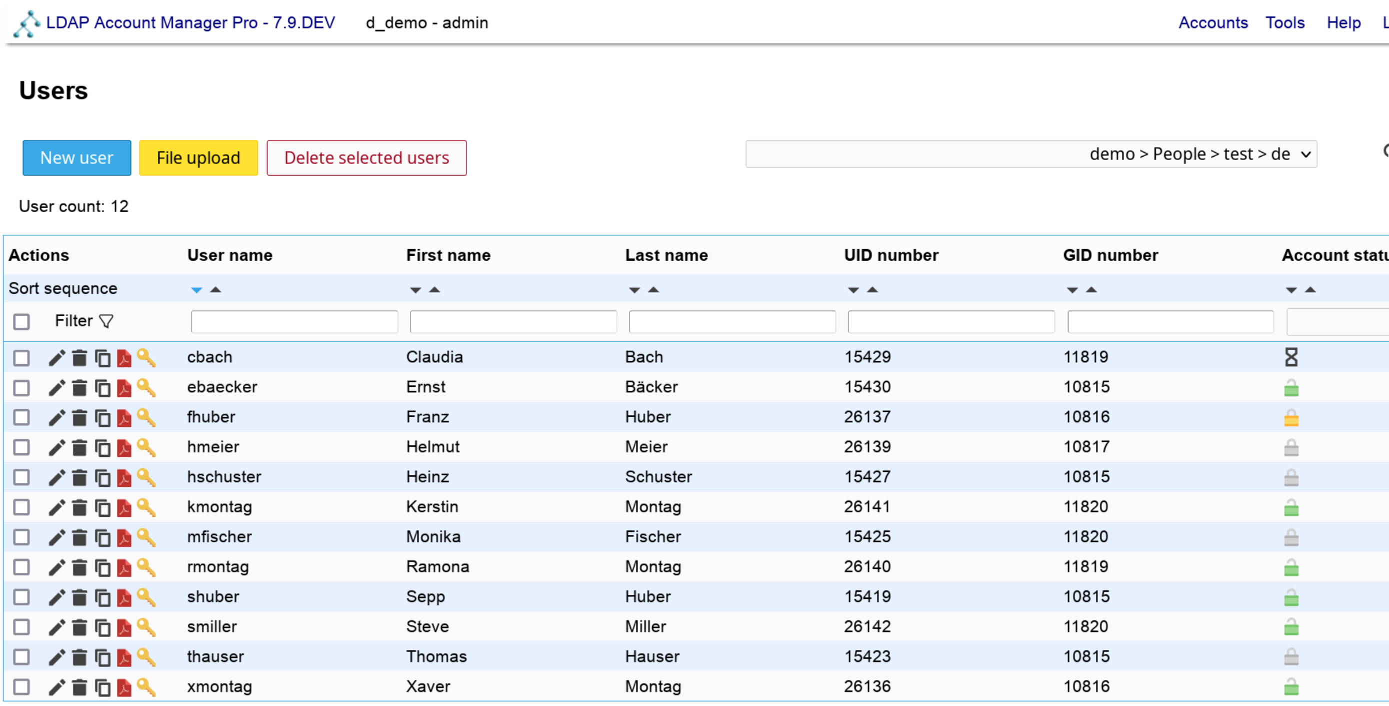
Please note that not all account types are manageable with the free LAM release. LAM Pro provides some more account types (e.g. group of names, aliases, ...) and modules (e.g. Kopano, custom scripts, ...) to support additional LDAP object classes. All LAM Pro features are marked in this manual.

Basic page layout:

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

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

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



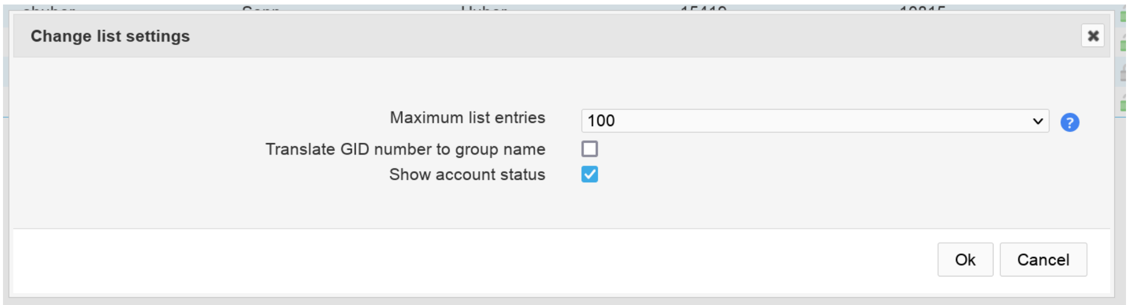
Users

User count: 12

Actions	User name	First name	Last name	UID number	GID number	Account statu
Sort sequence	▼▲	▼▲	▼▲	▼▲	▼▲	▼▲
☐ Filter ▽						
☐	cbach	Claudia	Bach	15429	11819	⌛
☐	ebaecker	Ernst	Bäcker	15430	10815	🟩
☐	fhuber	Franz	Huber	26137	10816	🟨
☐	hmeier	Helmut	Meier	26139	10817	⬜
☐	hschuster	Heinz	Schuster	15427	10815	⬜
☐	kmontag	Kerstin	Montag	26141	11820	🟩
☐	mfischer	Monika	Fischer	15425	11820	⬜
☐	rmontag	Ramona	Montag	26140	11819	🟩
☐	shuber	Sepp	Huber	15419	10815	🟩
☐	smiller	Steve	Miller	26142	11820	🟩
☐	thauser	Thomas	Hauser	15423	10815	⬜
☐	xmontag	Xaver	Montag	26136	10816	🟩

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

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



Change list settings

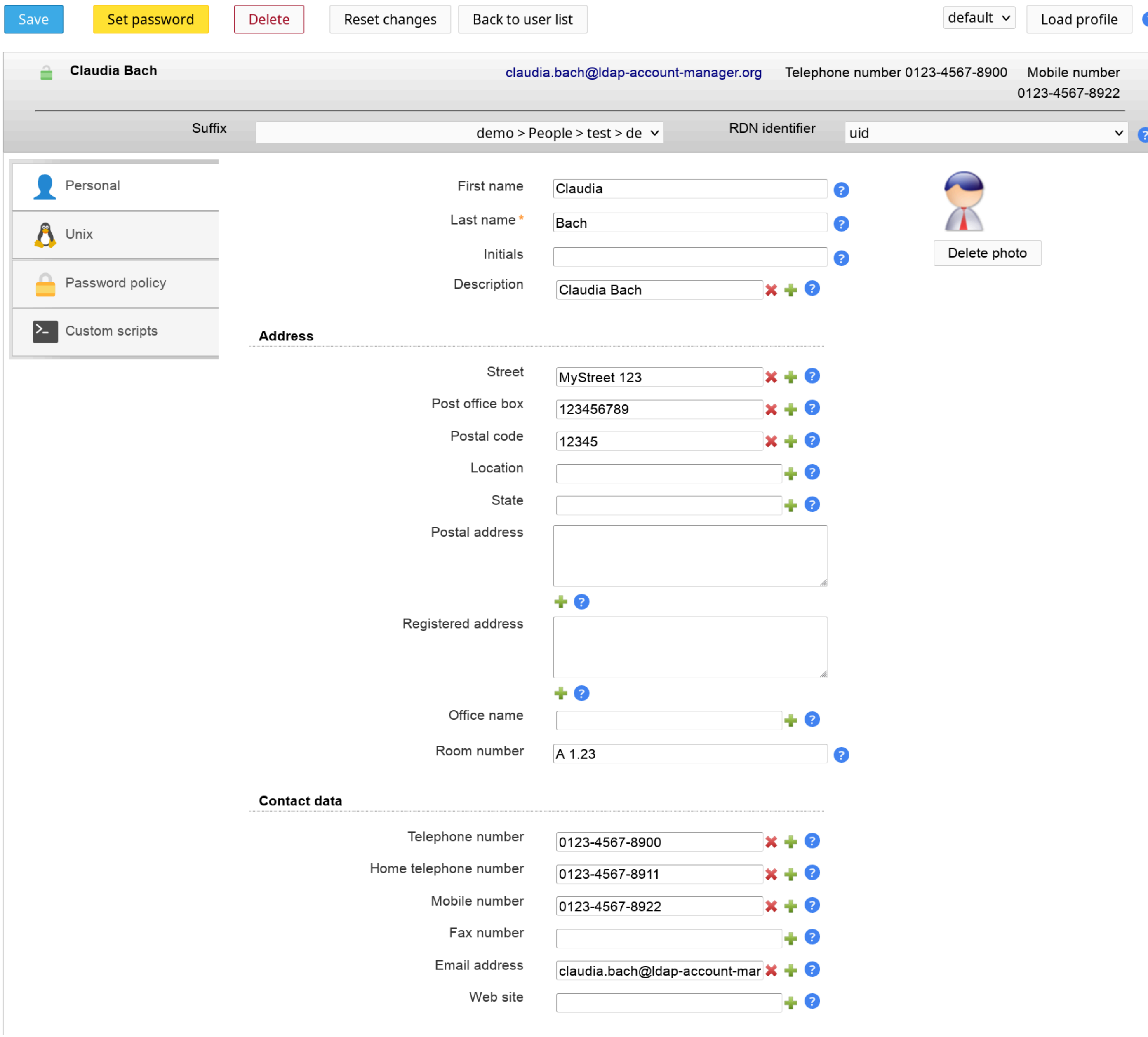
Maximum list entries: 100

Translate GID number to group name ☐

Show account status ☑

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.



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

First name: Claudia

Last name*: Bach

Initials:

Description: Claudia Bach

Address

Street: MyStreet 123

Post office box: 123456789

Postal code: 12345

Location:

State:

Postal address:

Registered 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: claudia.bach@ldap-account-mar

Web site:

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:

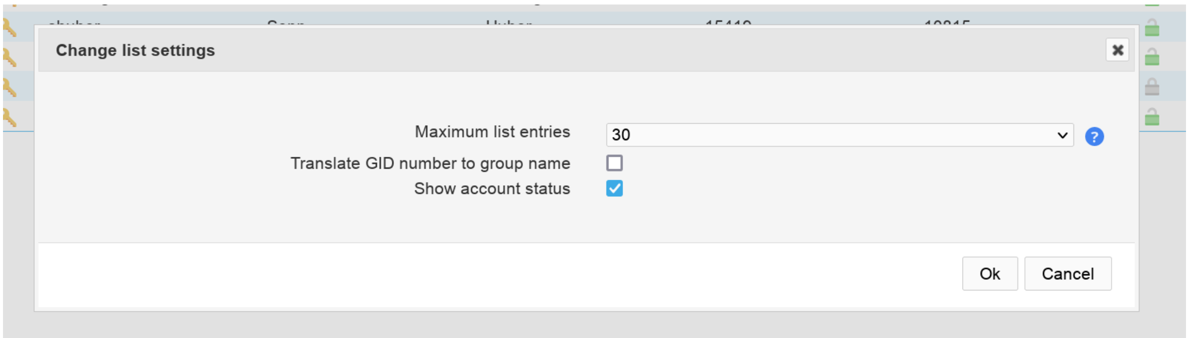
- Users (Personal + Unix + PyKota)
- Groups (Unix + PyKota)
- Printers (PyKota)
- Billing codes (PyKota)

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.



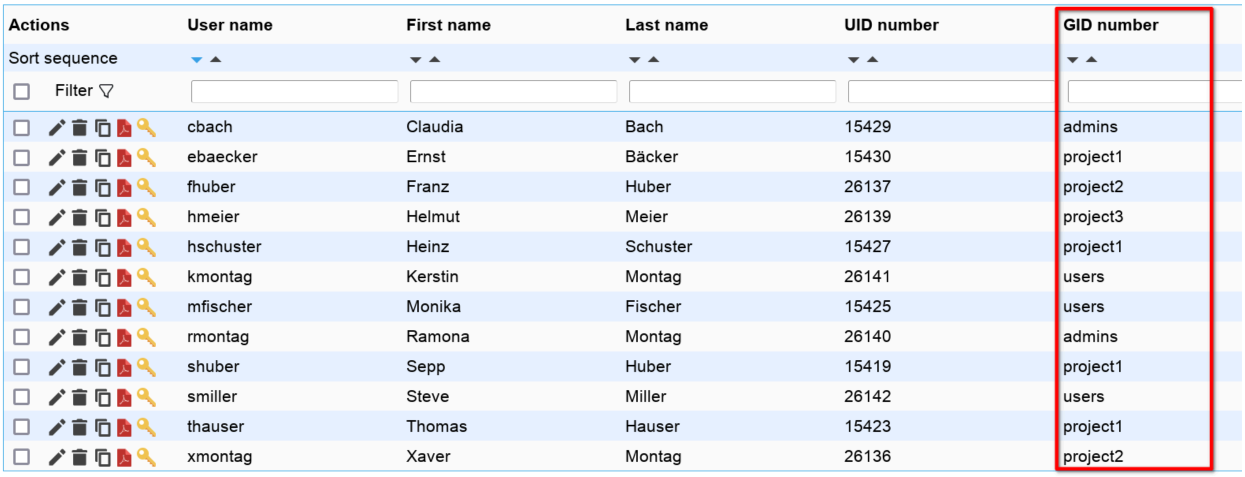
Change list settings

Maximum list entries: 30

Translate GID number to group name: ☐

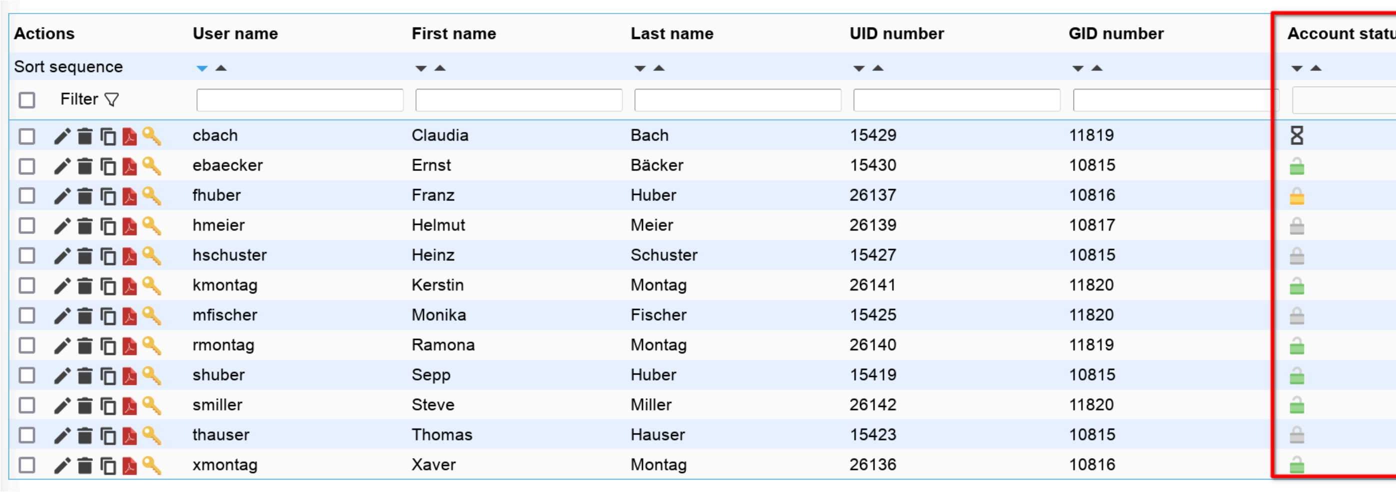
Show account status: ☑

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



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

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

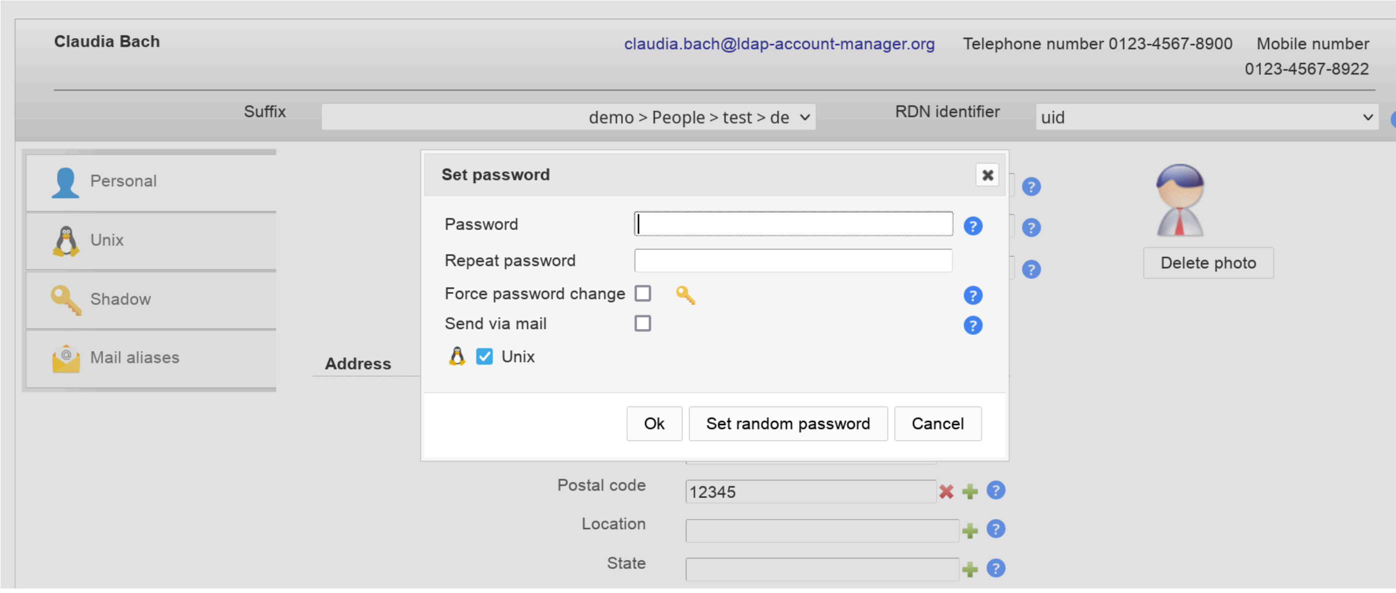


Actions	User name	First name	Last name	UID number	GID number	Account statu
Sort sequence	▼▲	▼▲	▼▲	▼▲	▼▲	▼▲
□ Filter ▽						
□	cbach	Claudia	Bach	15429	11819	⌛
□	ebaecker	Ernst	Bäcker	15430	10815	🔒
□	fhuber	Franz	Huber	26137	10816	🔒
□	hmeier	Helmut	Meier	26139	10817	🔒
□	hschuster	Heinz	Schuster	15427	10815	🔒
□	kmontag	Kerstin	Montag	26141	11820	🔒
□	mfischer	Monika	Fischer	15425	11820	🔒
□	rmontag	Ramona	Montag	26140	11819	🔒
□	shuber	Sepp	Huber	15419	10815	🔒
□	smiller	Steve	Miller	26142	11820	🔒
□	thauser	Thomas	Hauser	15423	10815	🔒
□	xmontag	Xaver	Montag	26136	10816	🔒

Password:

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

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



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

Set password

Password:

Repeat password:

Force password change ☐

Send via mail ☐

☑ Unix

Postal code: 12345

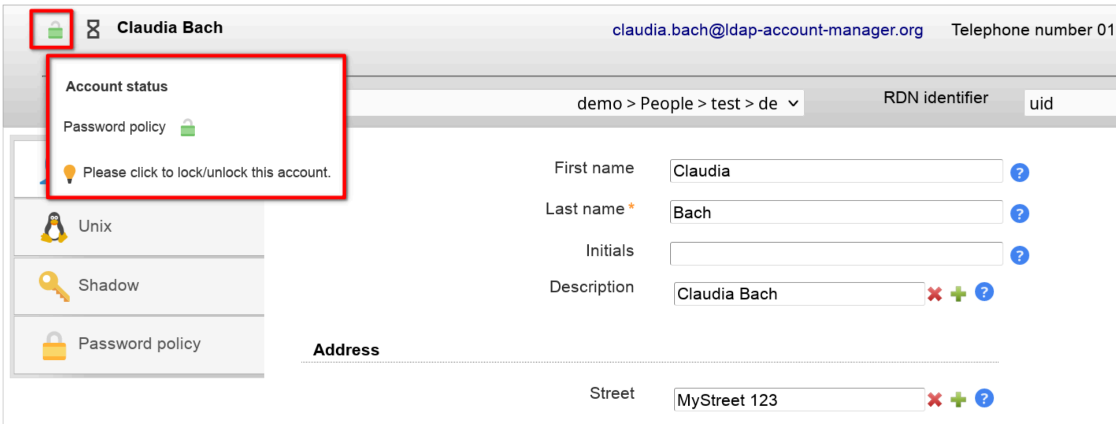
Location:

State:

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.



Claudia Bach

claudia.bach@ldap-account-manager.org

Telephone number 01

Account status

Password policy

Please click to lock/unlock this account.

demo > People > test > de

RDN identifier: uid

Unix

Shadow

Password policy

First name: Claudia

Last name*: Bach

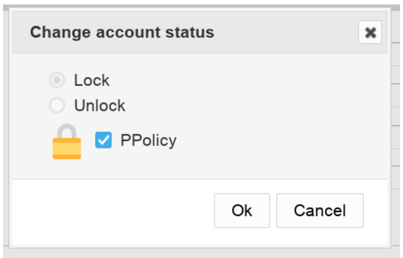
Initials:

Description: Claudia Bach

Address

Street: MyStreet 123

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.

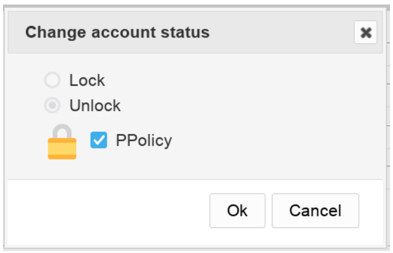


Change account status

● Lock

○ Unlock

☑ PPolicy



Change account status

○ Lock

● Unlock

☑ PPolicy

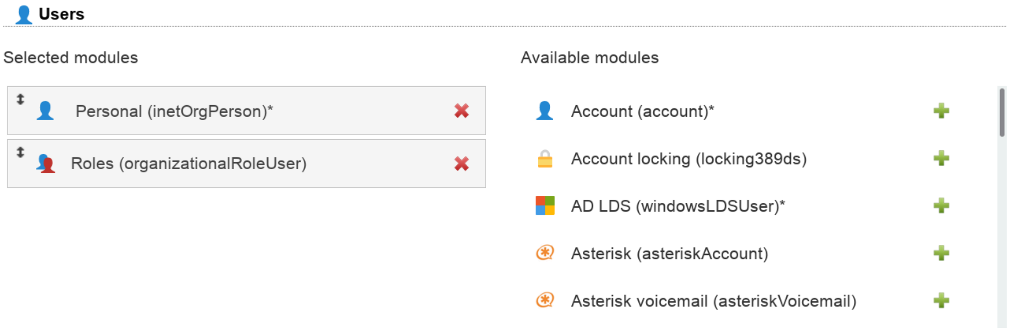
Personal

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

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

Configuration

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



Users

Selected modules

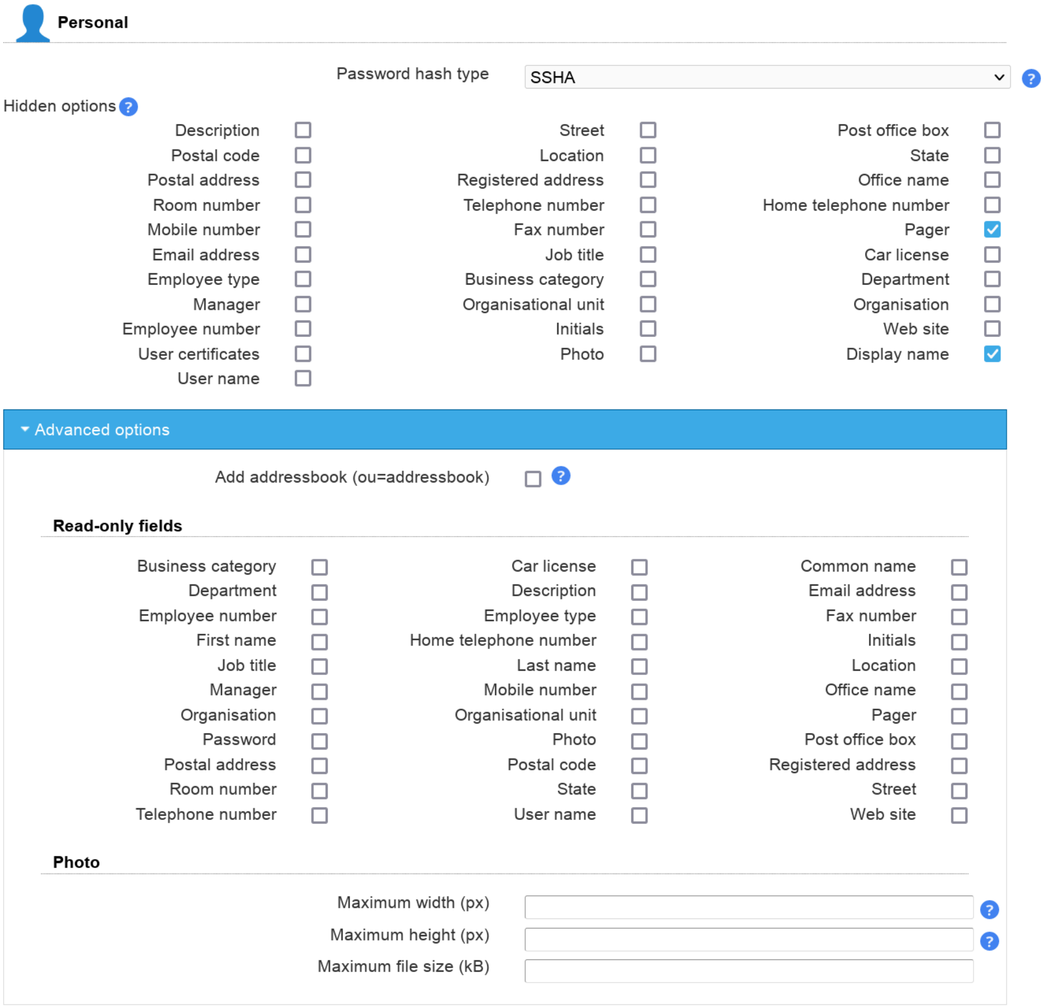
- Personal (inetOrgPerson)*
- Roles (organizationalRoleUser)

Available modules

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

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

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



Personal

Password hash type: SSHA

Hidden options

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

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

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

Advanced options

Add addressbook (ou=addressbook) ☐

Read-only fields

Business category ☐
Department ☐
Employee number ☐
First name ☐
Job title ☐
Manager ☐
Organisation ☐
Password ☐
Postal address ☐
Room number ☐
Telephone number ☐

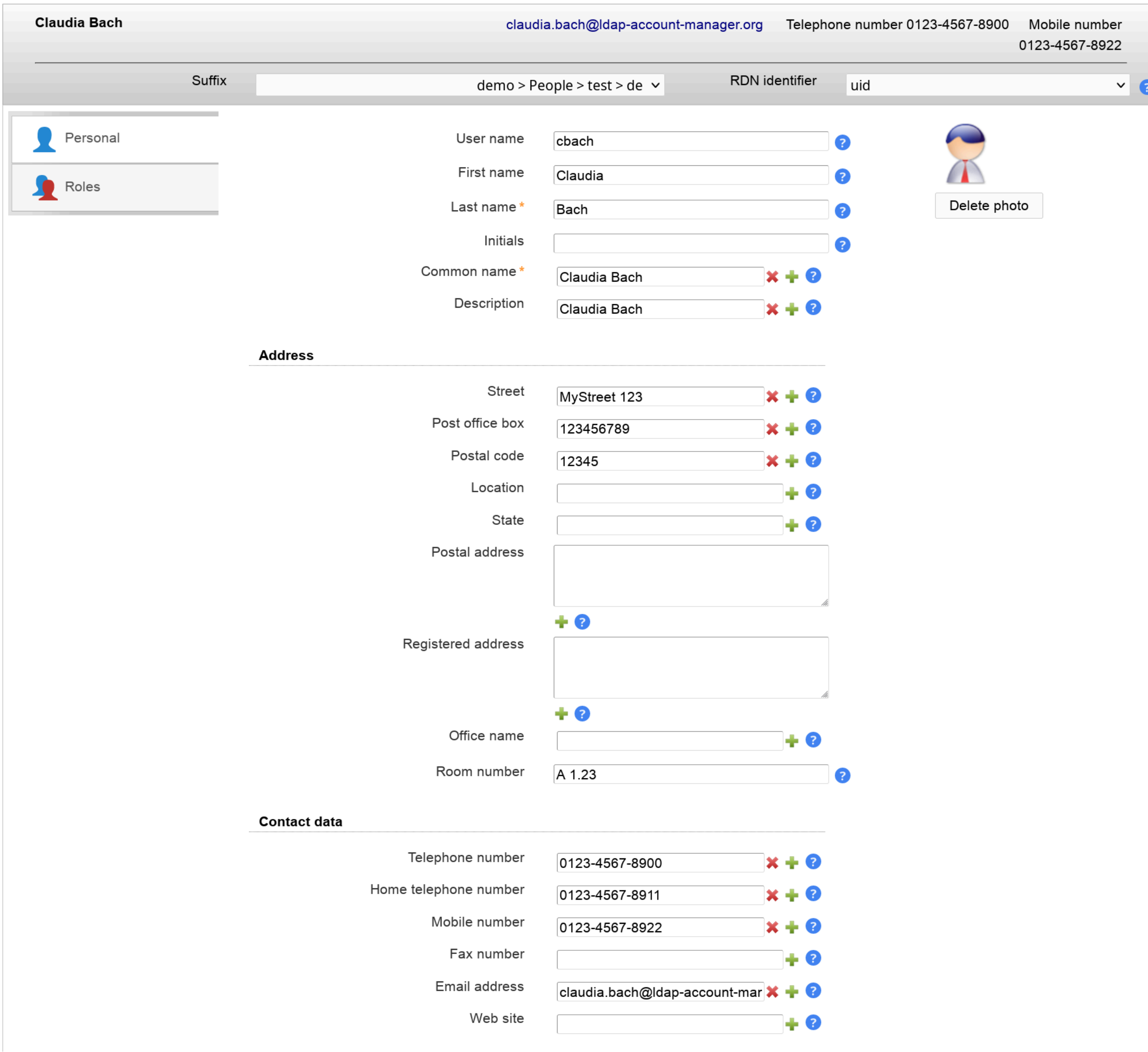
Car license ☐
Description ☐
Employee type ☐
Home telephone number ☐
Last name ☐
Mobile number ☐
Organisational unit ☐
Photo ☐
Postal code ☐
State ☐
User name ☐

Common name ☐
Email address ☐
Fax number ☐
Initials ☐
Location ☐
Office name ☐
Pager ☐
Post office box ☐
Registered address ☐
Street ☐
Web site ☐

Photo

Maximum width (px):
Maximum height (px):
Maximum file size (kB):

User management



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

User name: cbach
First name: Claudia
Last name*: Bach
Initials:
Common name*: Claudia Bach
Description: Claudia Bach

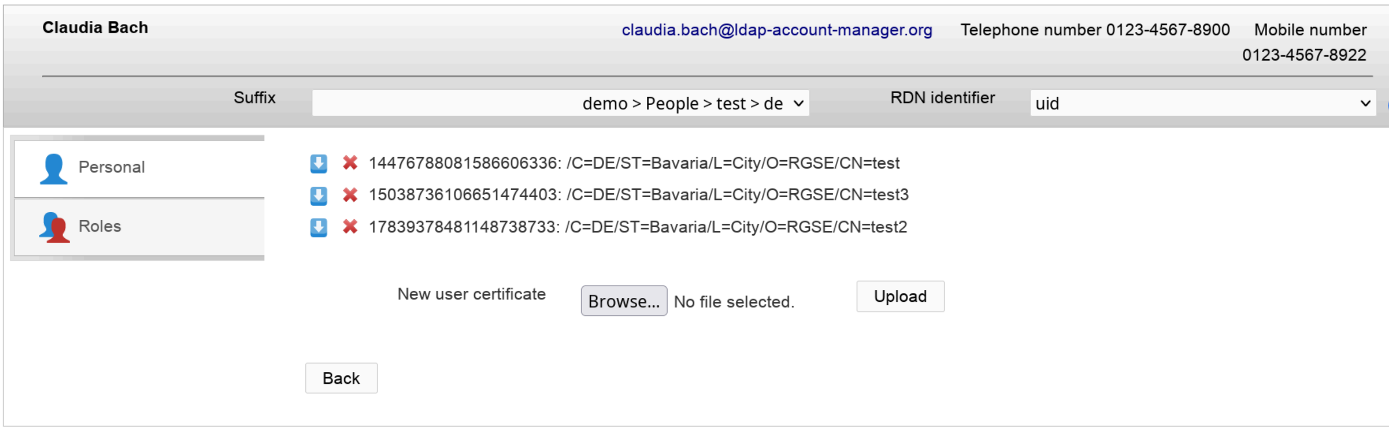
Address

Street: MyStreet 123
Post office box: 123456789
Postal code: 12345
Location:
State:
Postal address:
Registered 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: claudia.bach@ldap-account-mar
Web site:

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



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

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

New user certificate: Browse... No file selected.

Table 4.1. LDAP attribute mappings

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

Wildcards

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

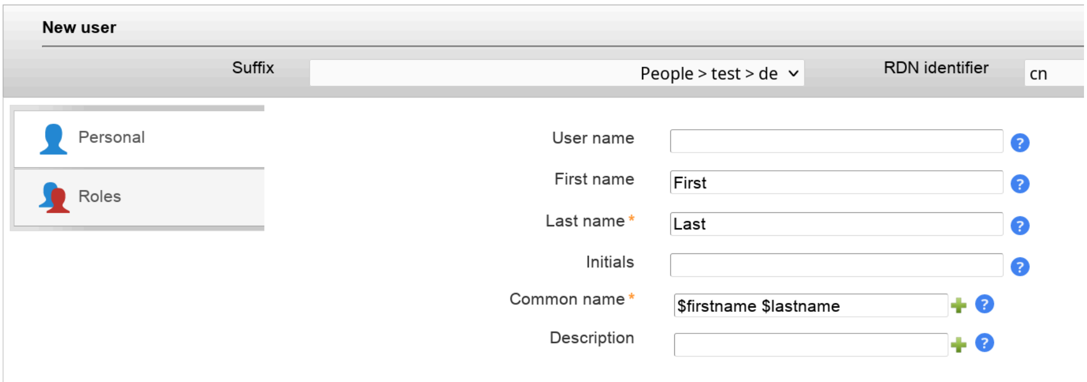
- $firstname: First name
- $lastname: Last name

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

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

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

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



New user

Suffix: People > test > de

RDN identifier: cn

User name:

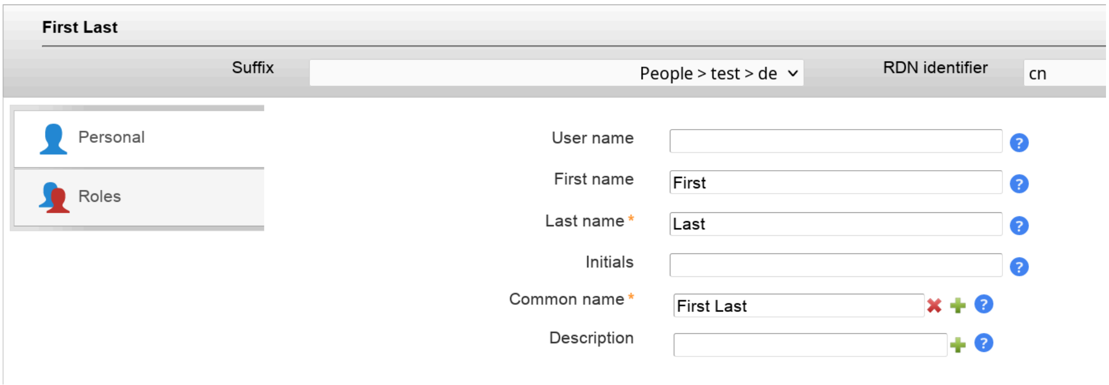
First name: First

Last name*: Last

Initials:

Common name*: $firstname $lastname

Description:



First Last

Suffix: People > test > de

RDN identifier: cn

User name:

First name: First

Last name*: Last

Initials:

Common name*: First Last

Description:

Unix

The Unix module manages Unix user accounts including group memberships.

There are several configuration options for this module:

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

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

  - Fixed range: LAM searches for free numbers within the given limits. LAM always tries to use a free UID that is greater than the existing UIDs to prevent collisions with deleted accounts.

  - Samba ID pool: This uses a special LDAP entry that includes attributes that store a counter for the last used UID/GID. Please note that this requires that you install the Samba schema and create an LDAP entry of object class "sambaUnixIdPool".

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

- Password hash type: If possible use CRYPT-SHA512 or SSHA to protect your user's passwords. The option SASL will set the password to "{SASL}<user name>". If you want to use an LDAP EXOP password operation to update the password then select LDAP_EXOP.

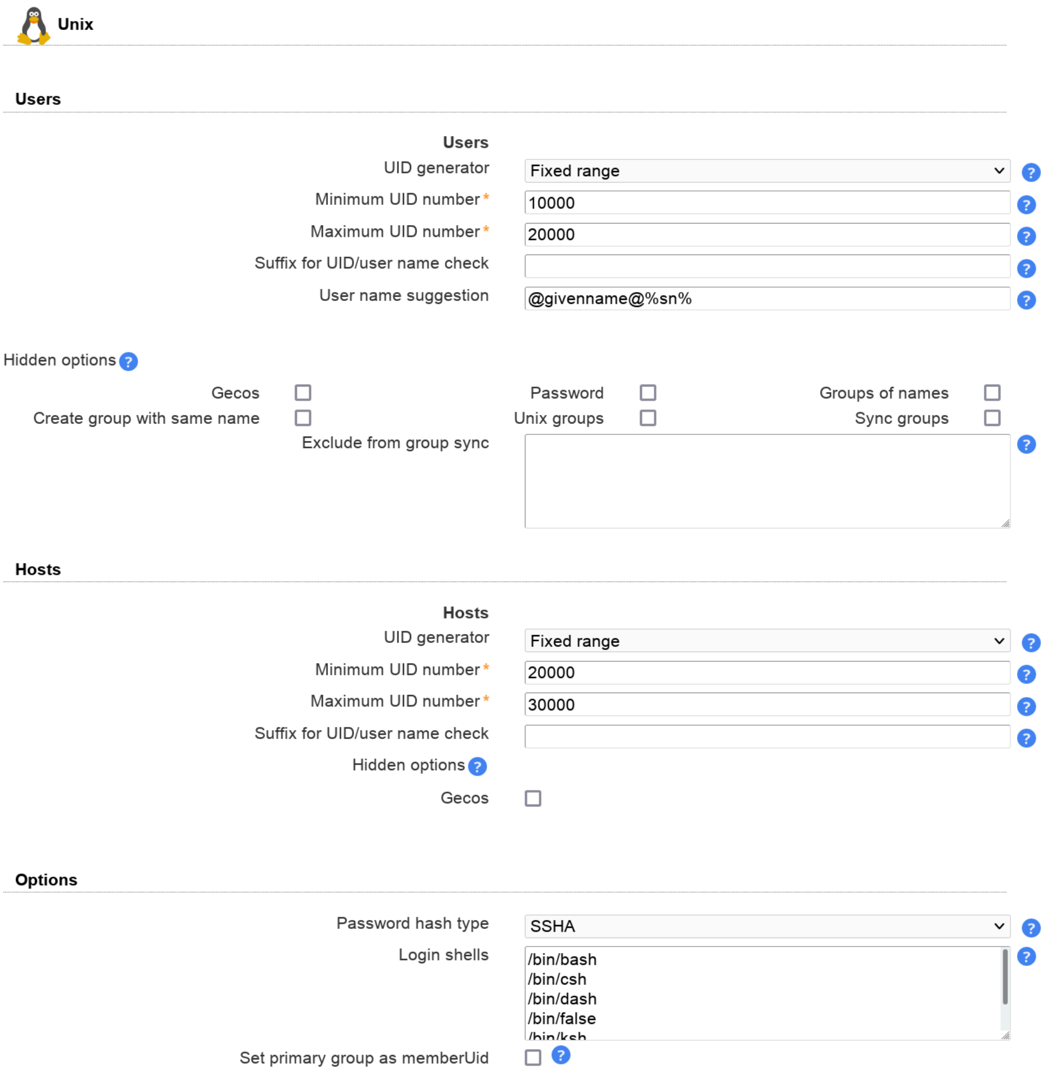
- Login shells: List of valid login shells that can be selected when editing an account.

- Hidden options: Some input fields can be hidden to simplify the GUI if you do not need them.

- Set primary group as memberUid: By default primary group membership is not set on group objects but only on user (gidNumber). Activate this if you need to have the primary group membership in group object, too.

- Do not add object class: This is for Windows only. When the checkbox is activated then the posixAccount object class will not be added to a user.

- User name suggestion: The user name is automatically filled as specified in the configuration (default smiller for Steve Miller). Of course, the suggested value can be changed any time. Common name is also filled with first/last name by default.



Unix

Users

Users

UID generator: Fixed range

Minimum UID number*: 10000

Maximum UID number*: 20000

Suffix for UID/user name check:

User name suggestion: @givenname@%sn%

Hidden options

Gecos	□	Password	□	Groups of names	□
Create group with same name	□	Unix groups	□	Sync groups	□

Exclude from group sync:

Hosts

Hosts

UID generator: Fixed range

Minimum UID number*: 20000

Maximum UID number*: 30000

Suffix for UID/user name check:

Hidden options

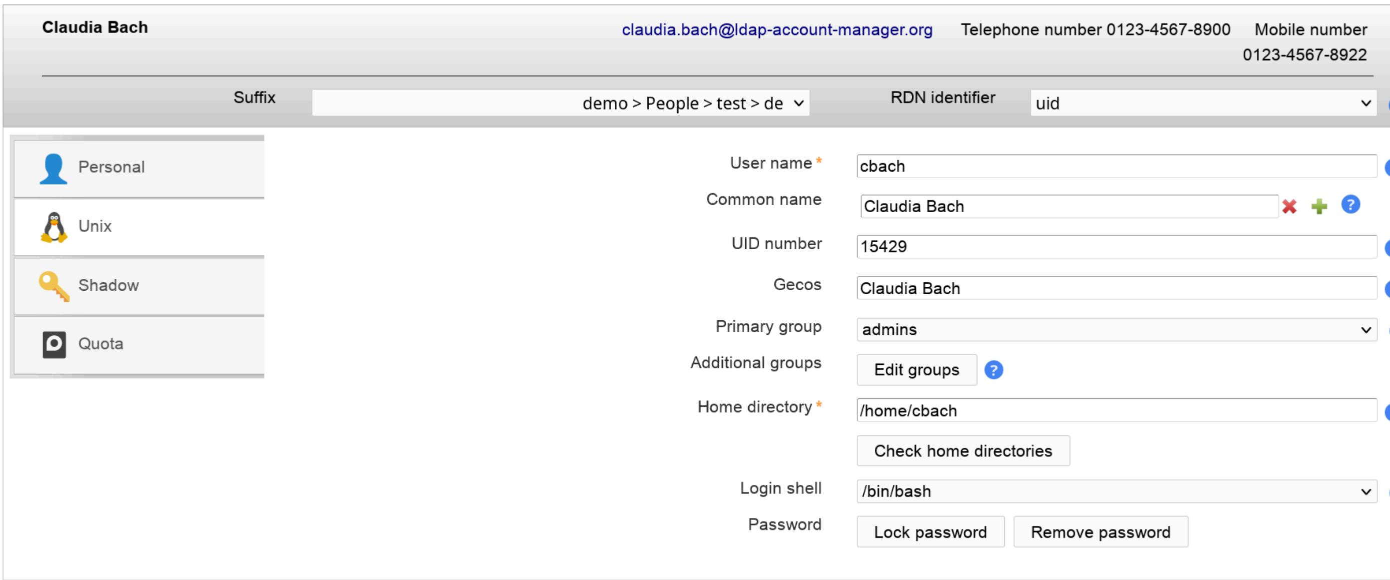
Gecos □

Options

Password hash type: SSHA

Login shells:
/bin/bash
/bin/csh
/bin/dash
/bin/false
/bin/ksh

Set primary group as memberUid □



Claudia Bach

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

Suffix: demo > People > test > de

RDN identifier: uid

User name*: cbach

Common name: Claudia Bach

UID number: 15429

Gecos: Claudia Bach

Primary group: admins

Additional groups: Edit groups

Home directory*: /home/cbach

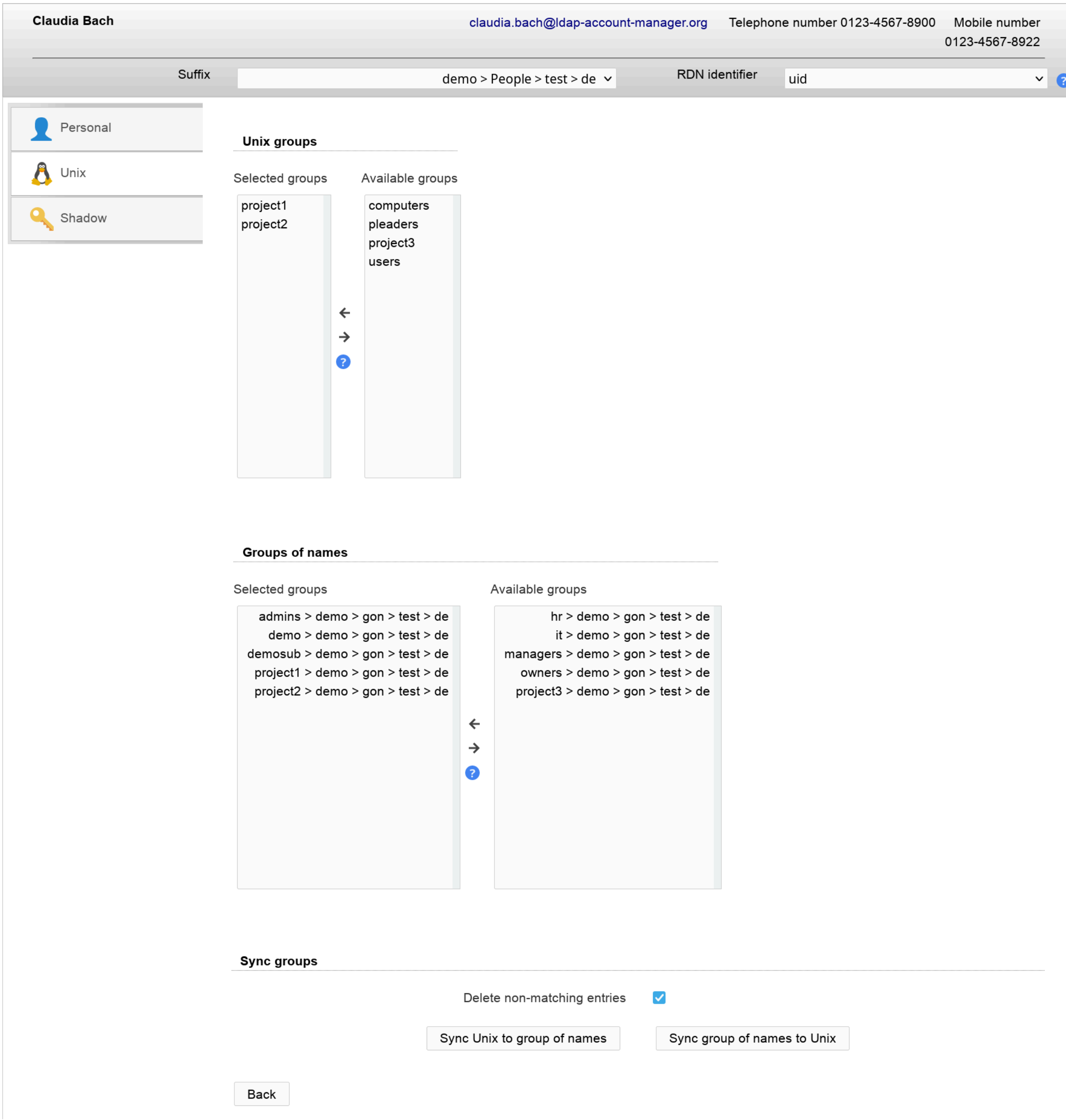
Check home directories

Login shell: /bin/bash

Password: Lock password Remove password

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

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



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

Suffix: demo > People > test > de

RDN identifier: uid

Unix groups

Selected groups:
project1
project2

Available groups:
computers
pleaders
project3
users

Groups of names

Selected groups:
admins > demo > gon > test > de
demo > demo > gon > test > de
demosub > demo > gon > test > de
project1 > demo > gon > test > de
project2 > demo > gon > test > de

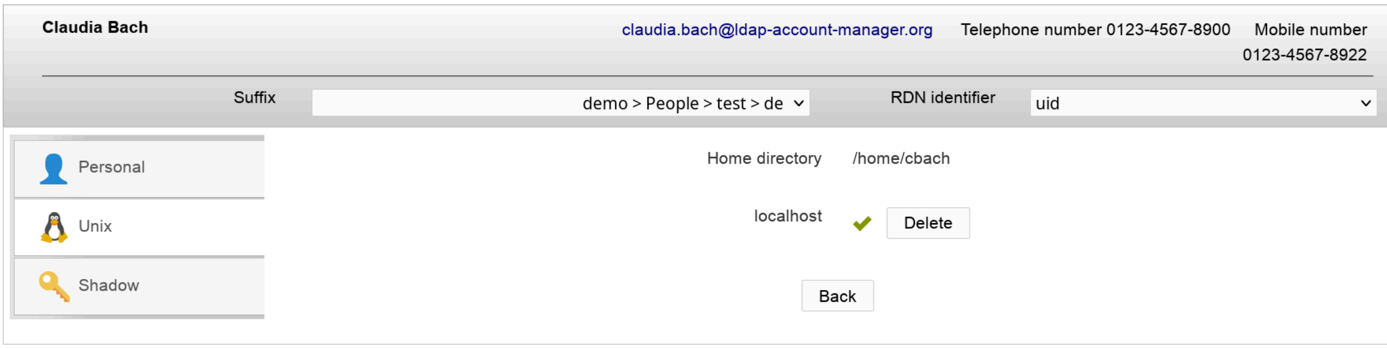
Available groups:
hr > demo > gon > test > de
it > demo > gon > test > de
managers > demo > gon > test > de
owners > demo > gon > test > de
project3 > demo > gon > test > de

Sync groups

Delete non-matching entries ☑

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.



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

Home directory: /home/cbach

localhost ✓

Wildcards

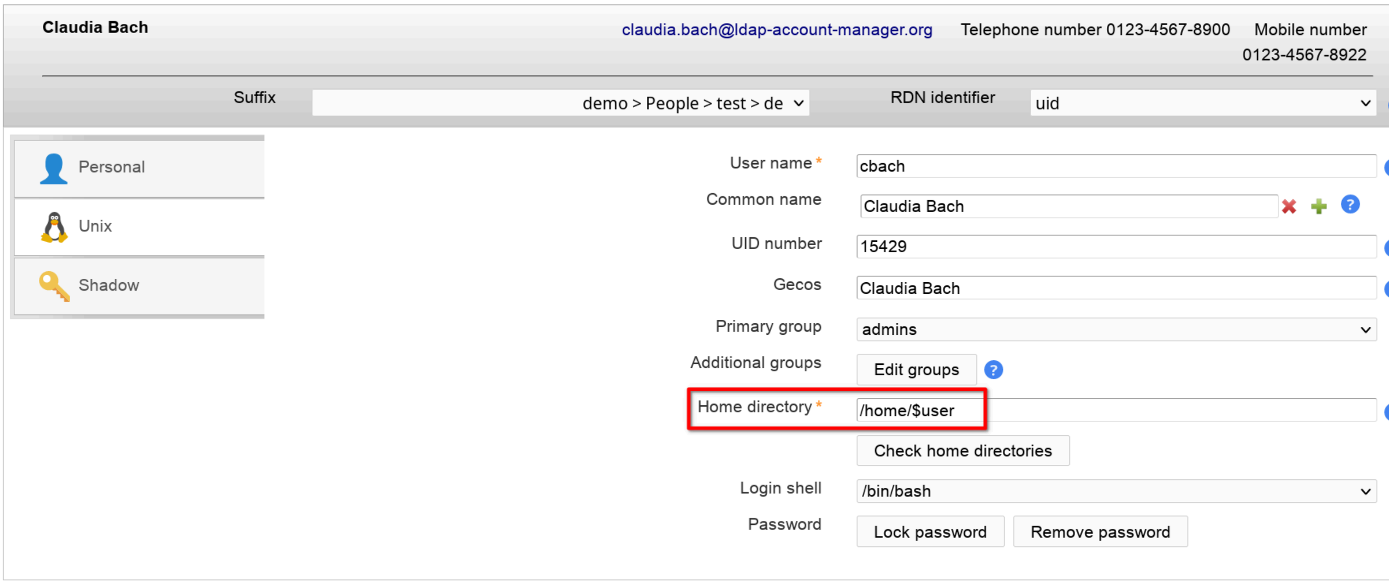
This module provides the following wildcards (others may be provided by other modules). Add a "_" after the "$" to get the value in lower-case (e.g. "$_user").

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

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

- Common name
- Gecos
- Home directory

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



Claudia 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

User name *: cbach

Common name: Claudia Bach

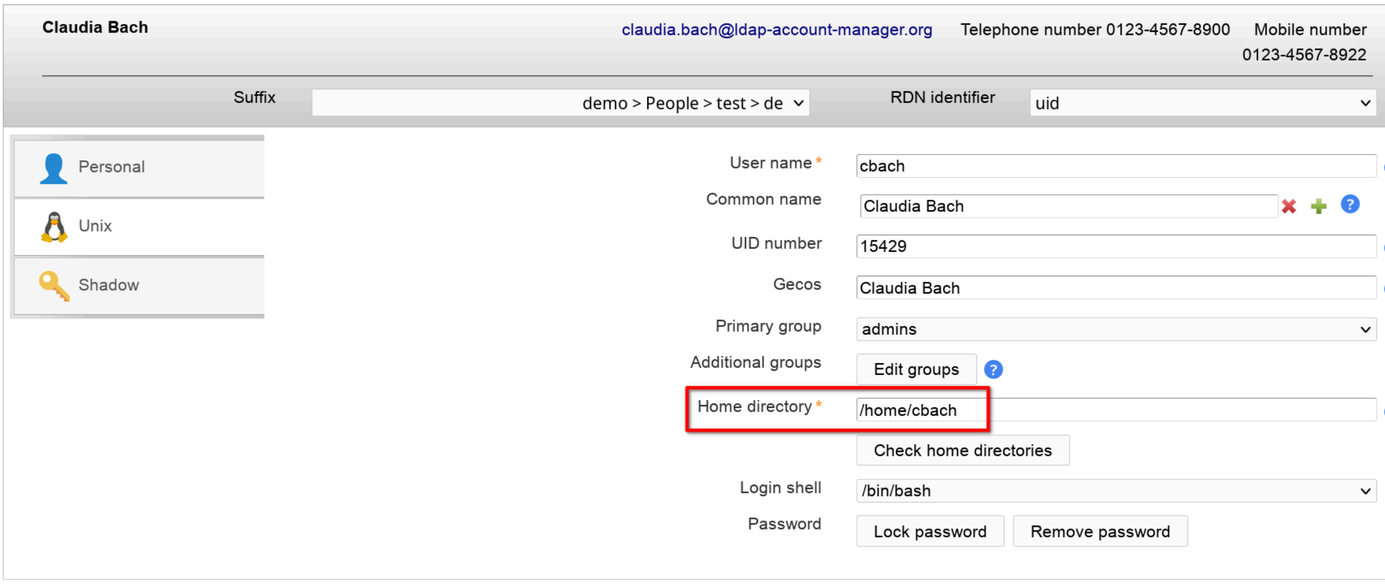
UID number: 15429

Gecos: Claudia Bach

Primary group: admins

Home directory *: /home/$user

Login shell: /bin/bash



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

User name *: cbach

Common name: Claudia Bach

UID number: 15429

Gecos: Claudia Bach

Primary group: admins

Additional groups: Edit groups

Home directory *: /home/cbach

Login shell: /bin/bash

Password: Lock password, Remove password

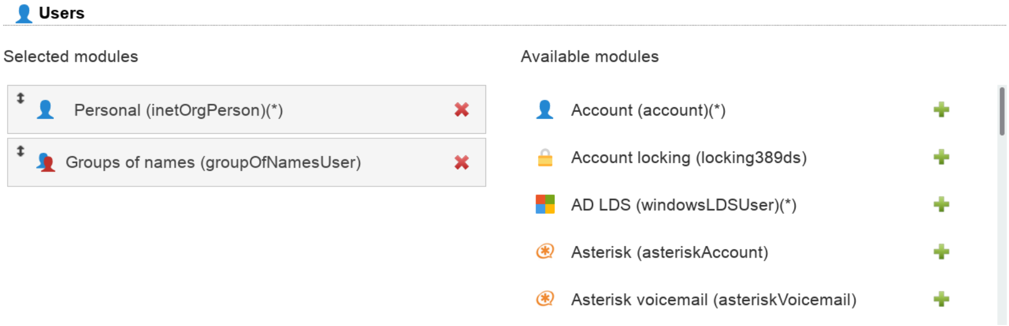
Group of names and group of members (LAM Pro)

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

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

Configuration

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

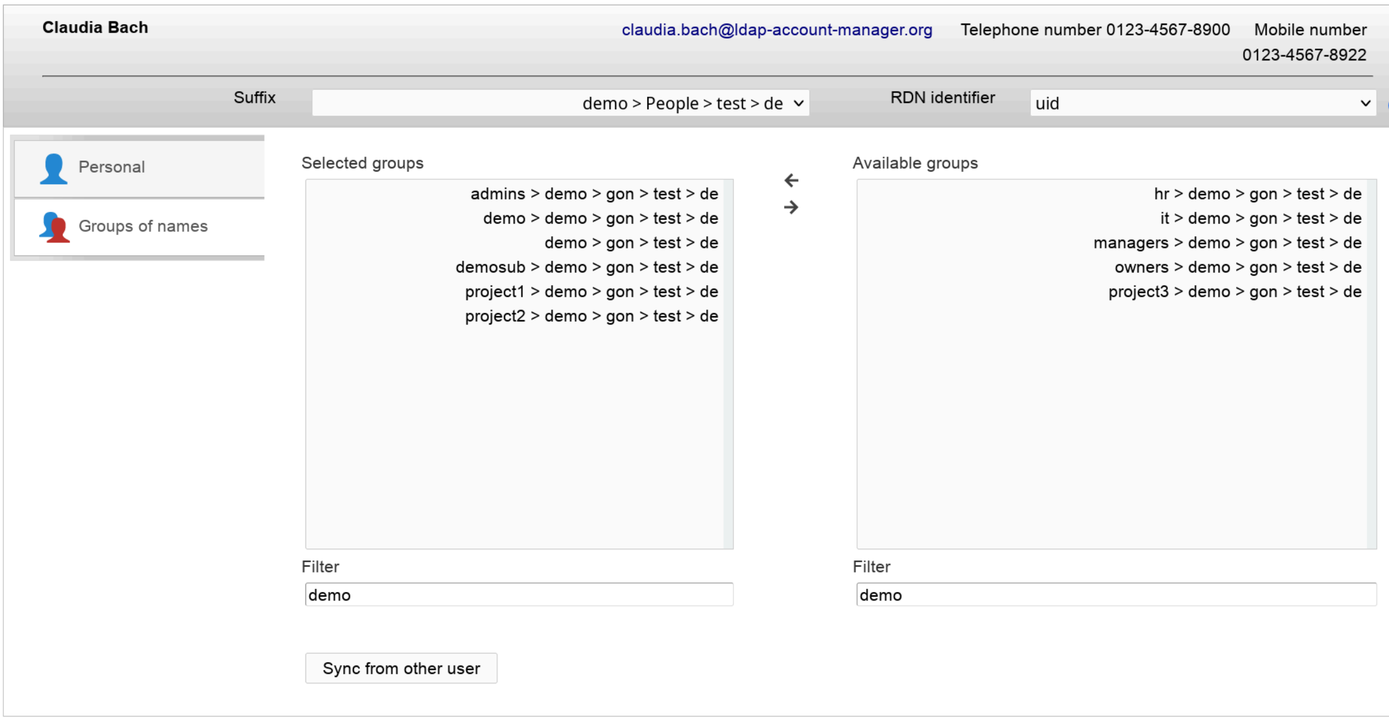


Users

Selected modules:
- Personal (inetOrgPerson)(*)
- Groups of names (groupOfNamesUser)

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

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



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

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

Selected groups:
admins > demo > gon > test > de
demo > demo > gon > test > de
demo > gon > test > de
demosub > demo > gon > test > de
project1 > demo > gon > test > de
project2 > demo > gon > test > de

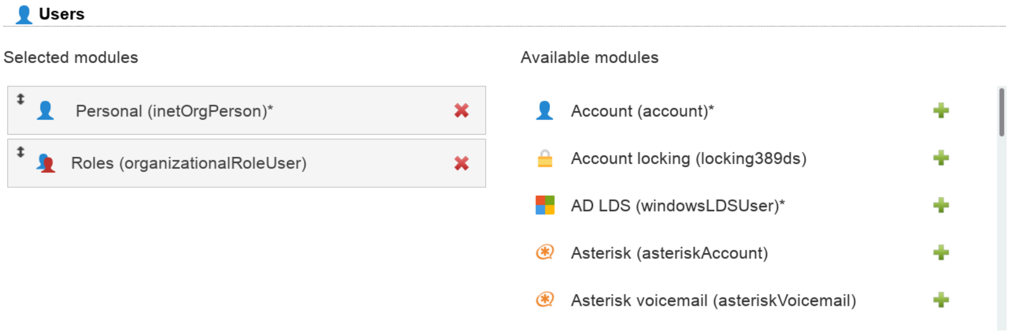
Available groups:
hr > demo > gon > test > de
it > demo > gon > test > de
managers > demo > gon > test > de
owners > demo > gon > test > de
project3 > demo > gon > test > de

Filter: demo

Filter: demo

Organizational roles (LAM Pro)

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

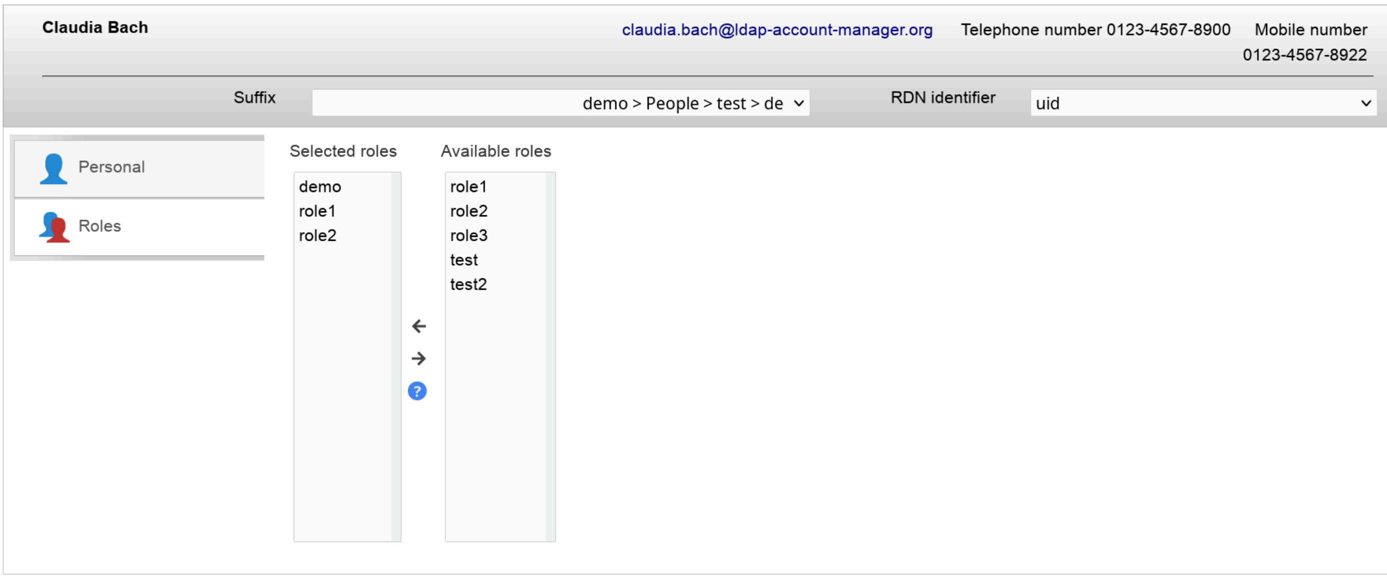


Selected modules:
Personal (inetOrgPerson)*
Roles (organizationalRoleUser)

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

User editing

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



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

Suffix: demo > People > test > de

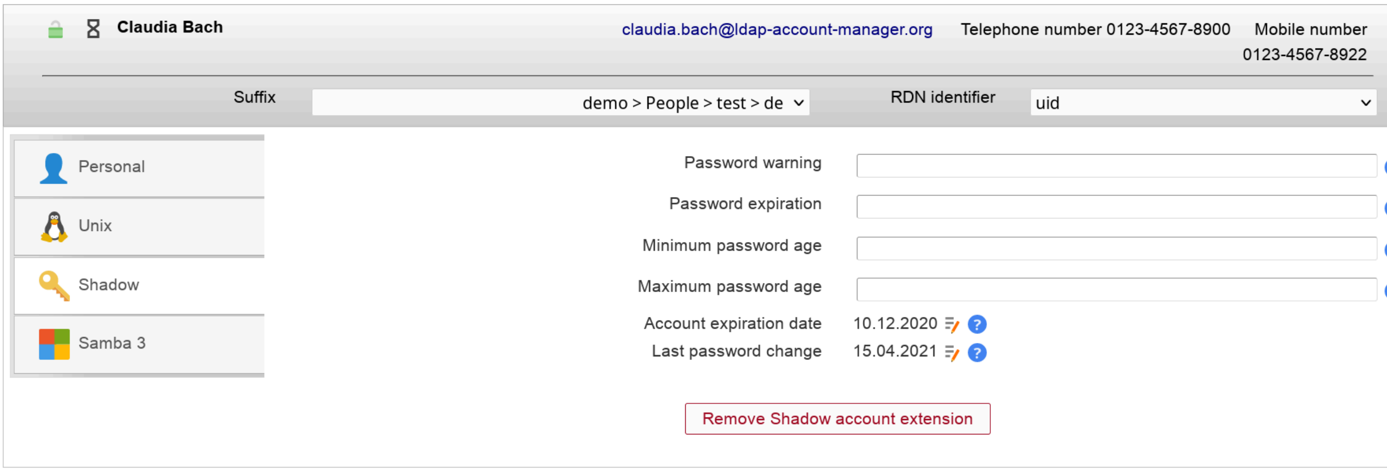
RDN identifier: uid

Selected roles: demo, role1, role2

Available roles: role1, role2, role3, test, test2

Shadow

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



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

Suffix: demo > People > test > de

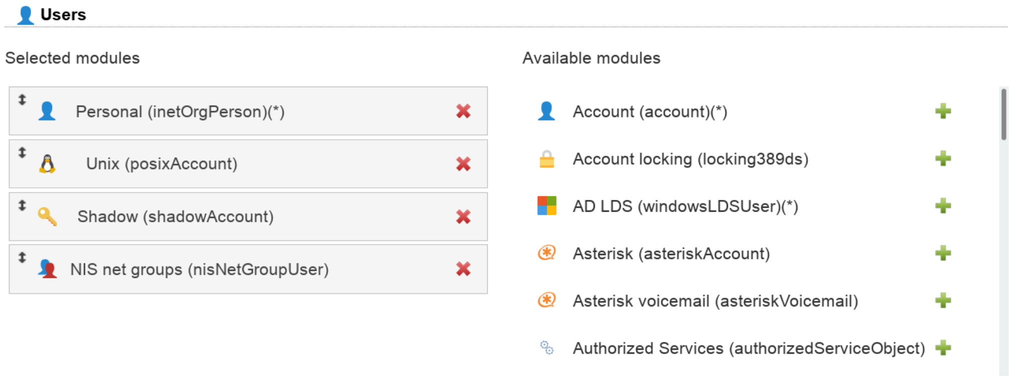
RDN identifier: uid

Password warning	
Password expiration	
Minimum password age	
Maximum password age	
Account expiration date	10.12.2020
Last password change	15.04.2021

NIS net groups

Configuration

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



Users

Selected modules

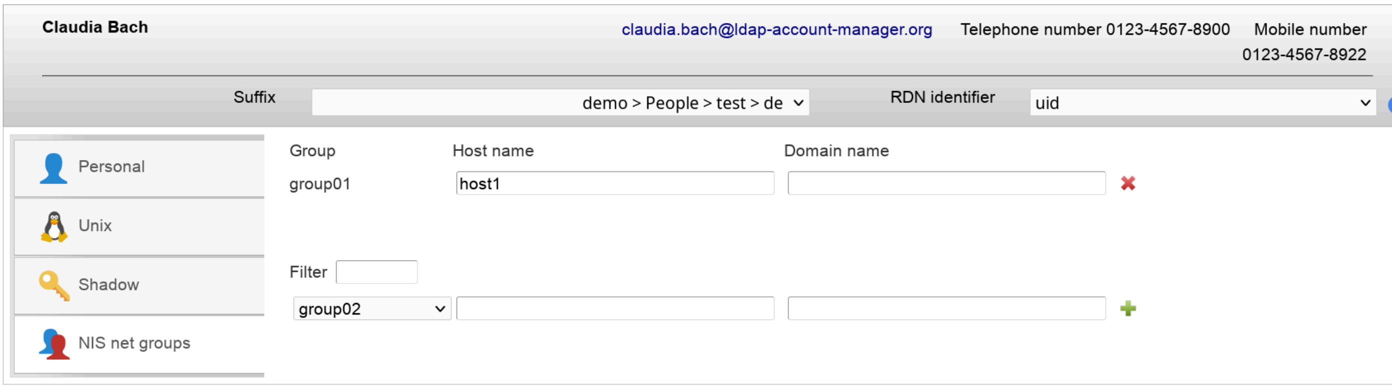
- Personal (inetOrgPerson)(*)
- Unix (posixAccount)
- Shadow (shadowAccount)
- NIS net groups (nisNetGroupUser)

Available modules

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

User editing

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



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

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

Group	Host name	Domain name
group01	host1	

Filter:
group02

Password self reset (LAM Pro)

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

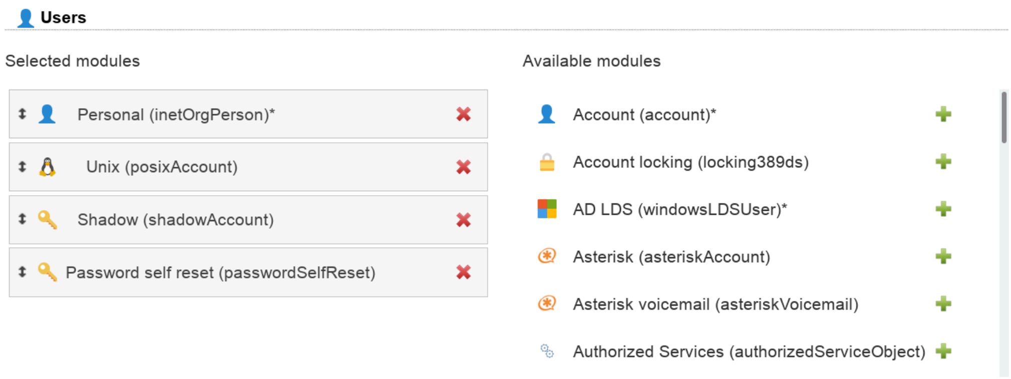
Please note that self service and LAM admin interface are separated functionalities. You need to specify the list of possible security questions in both self service profile(s) and server profile(s).

Schema installation

Please install the LDAP schema as described here.

Activate password self reset module

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



Users

Selected modules

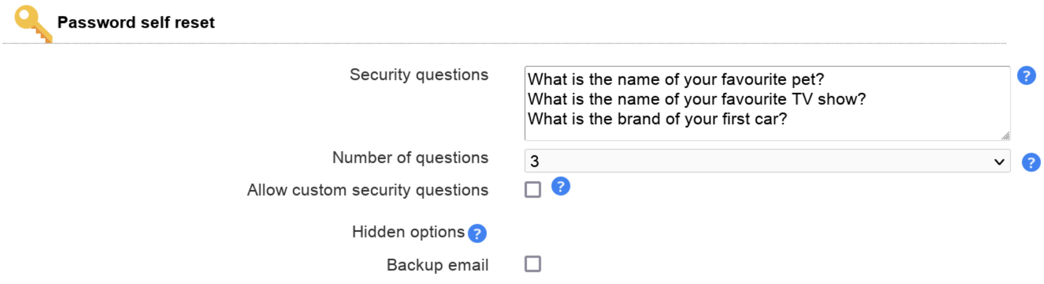
- Personal (inetOrgPerson)*
- Unix (posixAccount)
- Shadow (shadowAccount)
- Password self reset (passwordSelfReset)

Available modules

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

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

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



Password self reset

Security questions:
What is the name of your favourite pet?
What is the name of your favourite TV show?
What is the brand of your first car?

Number of questions: 3

Allow custom security questions: □

Hidden options

Backup email: □

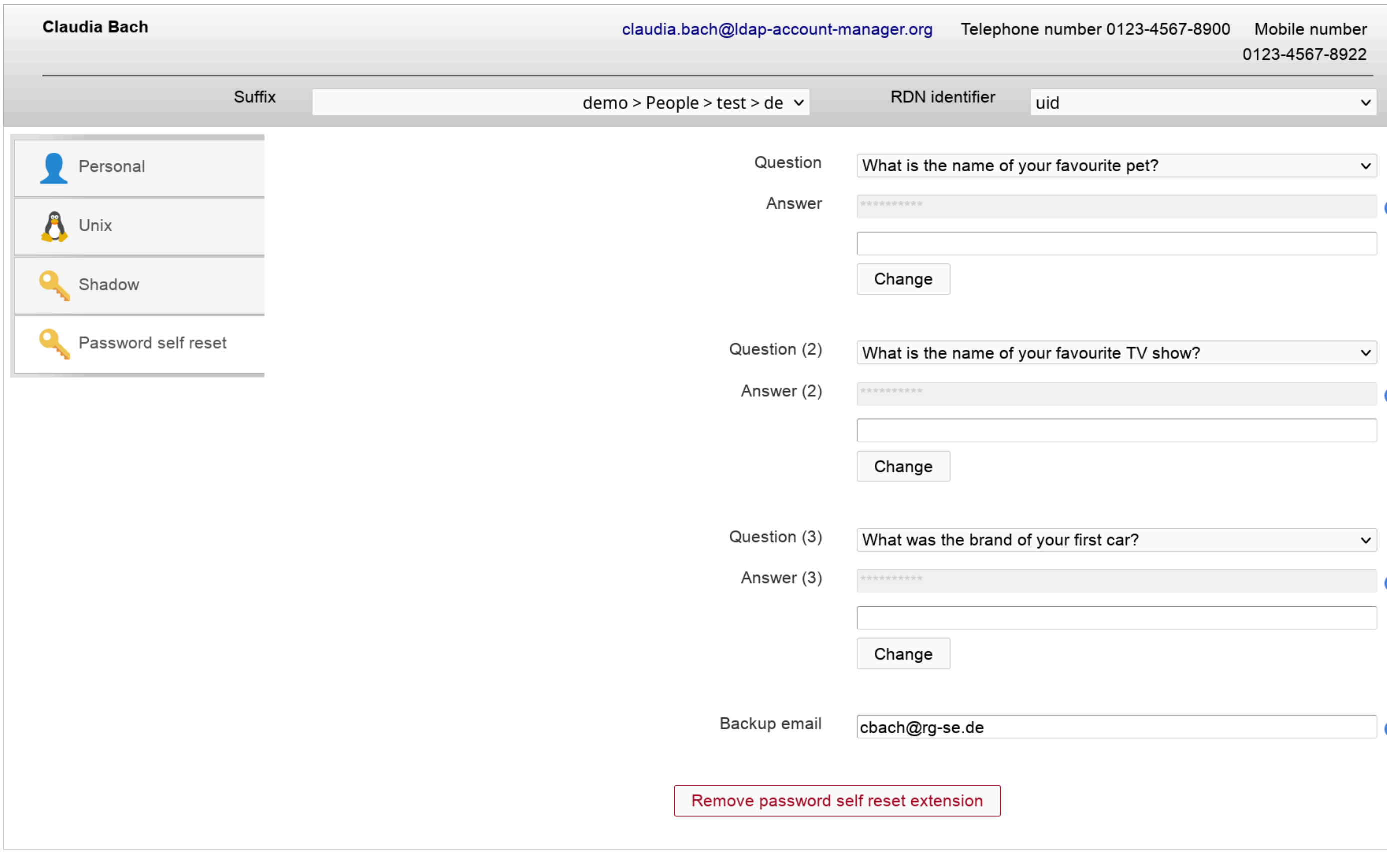
Edit users

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

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

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

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



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

Suffix: demo > People > test > de

RDN identifier: uid

Question: What is the name of your favourite pet?

Answer: ***********

Question (2): What is the name of your favourite TV show?

Answer (2): ***********

Question (3): What was the brand of your first car?

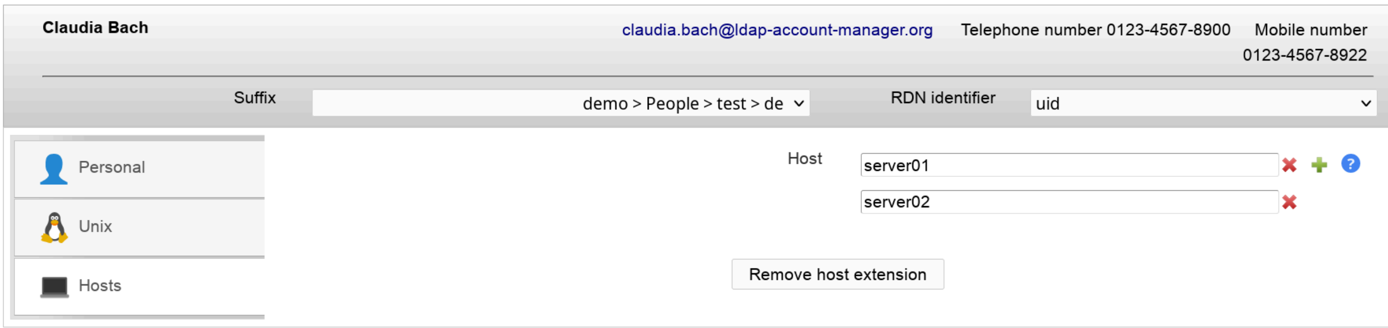
Answer (3): ***********

Backup email: cbach@rg-se.de

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.



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

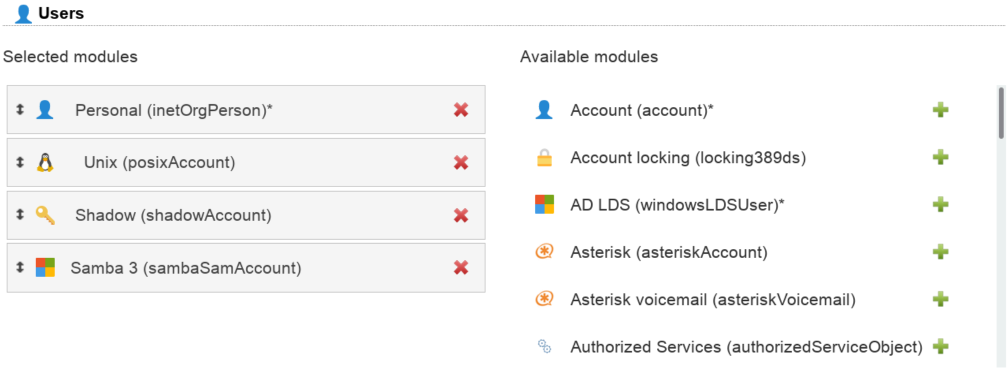
Host: server01

server02

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.



Users

Selected modules

- Personal (inetOrgPerson)*
- Unix (posixAccount)
- Shadow (shadowAccount)
- Samba 3 (sambaSamAccount)

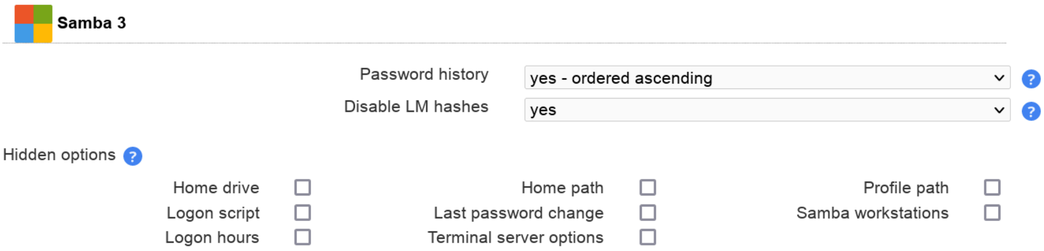
Available modules

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

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.



Samba 3

Password history: yes - ordered ascending

Disable LM hashes: yes

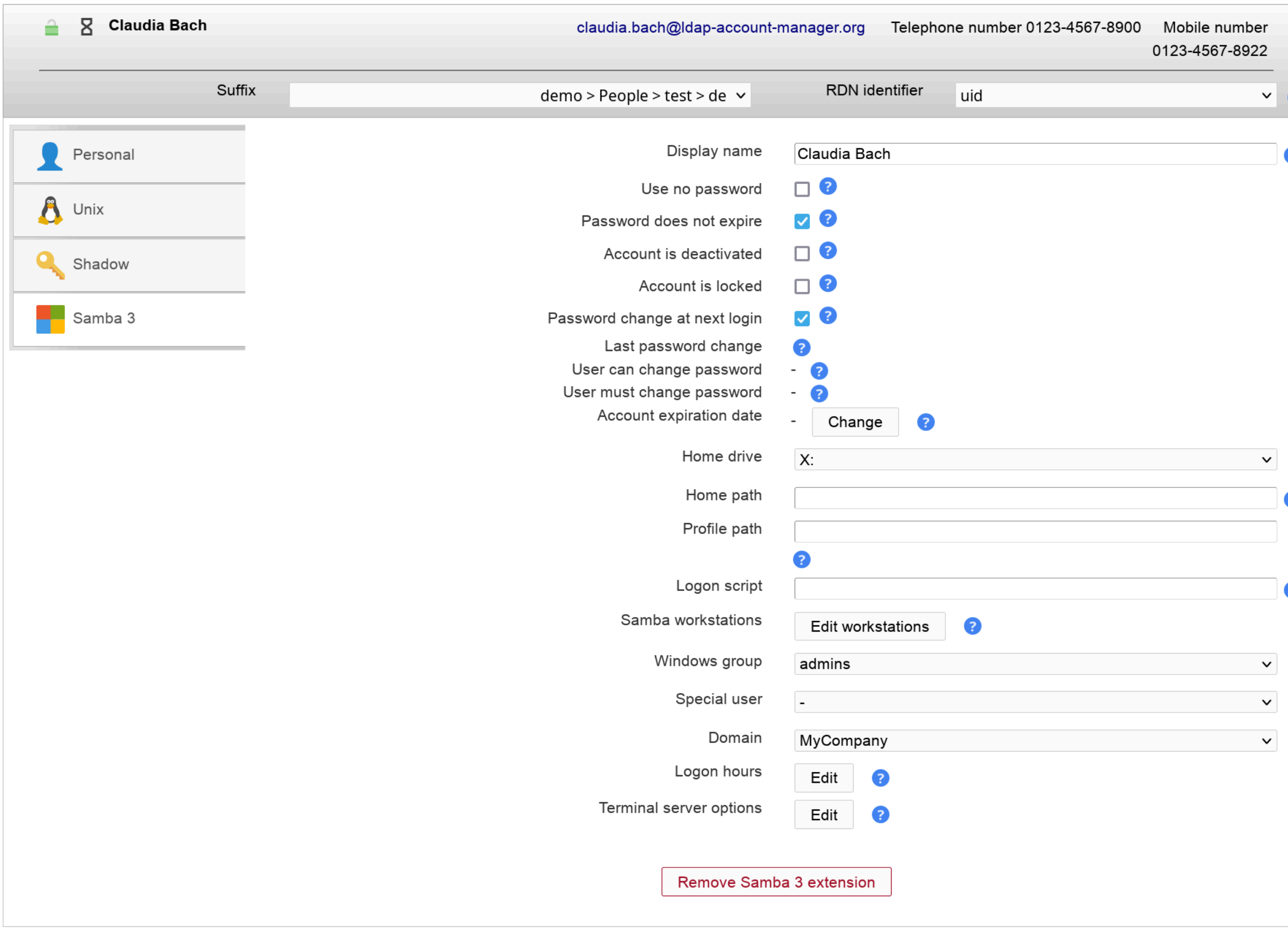
Hidden options

Home drive □ Home path □ Profile path □

Logon script □ Last password change □ Samba workstations □

Logon hours □ Terminal server options □

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



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

Display name	Claudia Bach
Use no password	□
Password does not expire	☑
Account is deactivated	□
Account is locked	□
Password change at next login	☑
Last password change	
User can change password	-
User must change password	-
Account expiration date	- Change
Home drive	X:
Home path	
Profile path	
Logon script	
Samba workstations	Edit workstations
Windows group	admins
Special user	-
Domain	MyCompany
Logon hours	Edit
Terminal server options	Edit

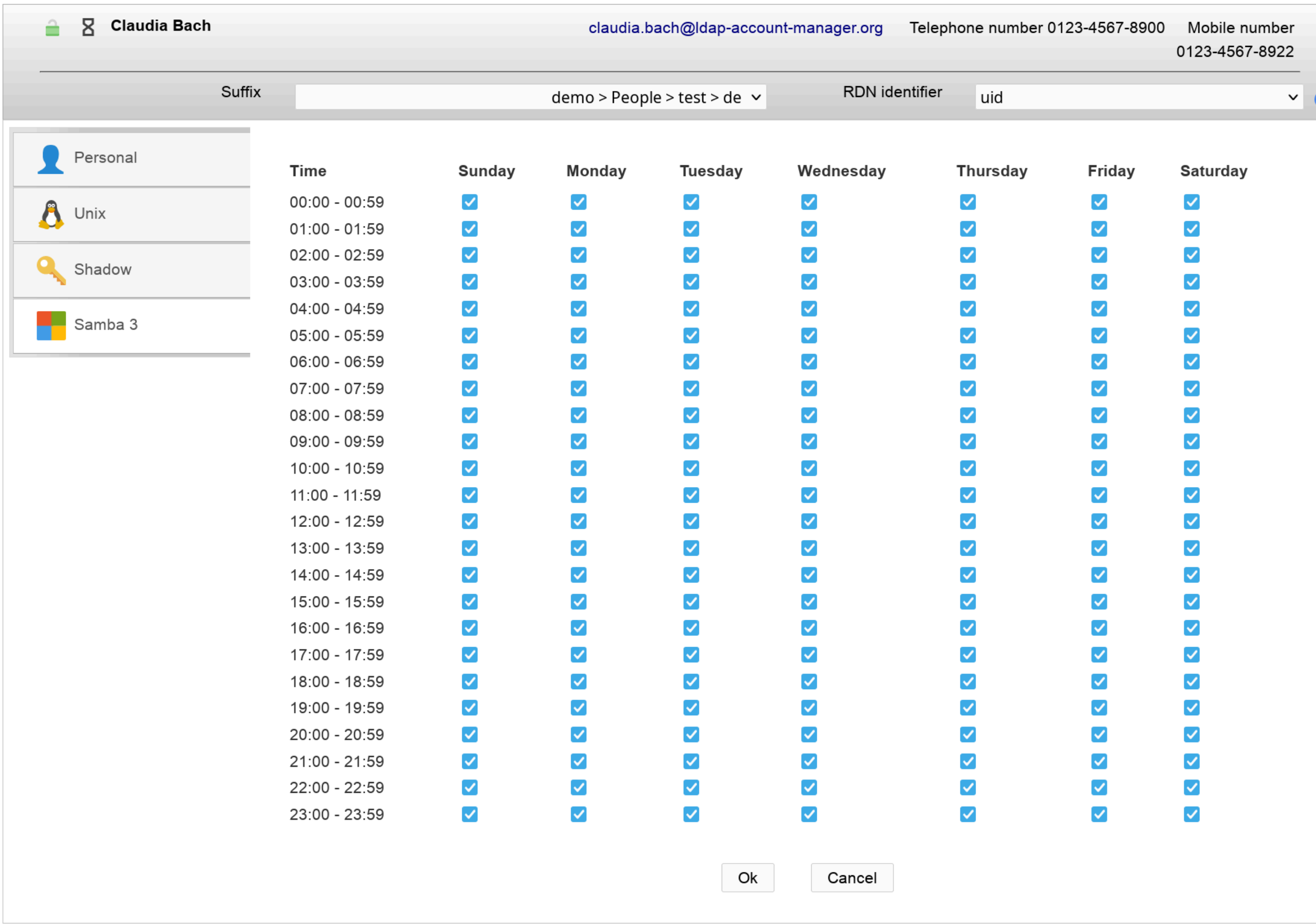
Wildcards

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

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

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

Logon hours



Claudia Bach

claudia.bach@ldap-account-manager.org

Telephone number 0123-4567-8900

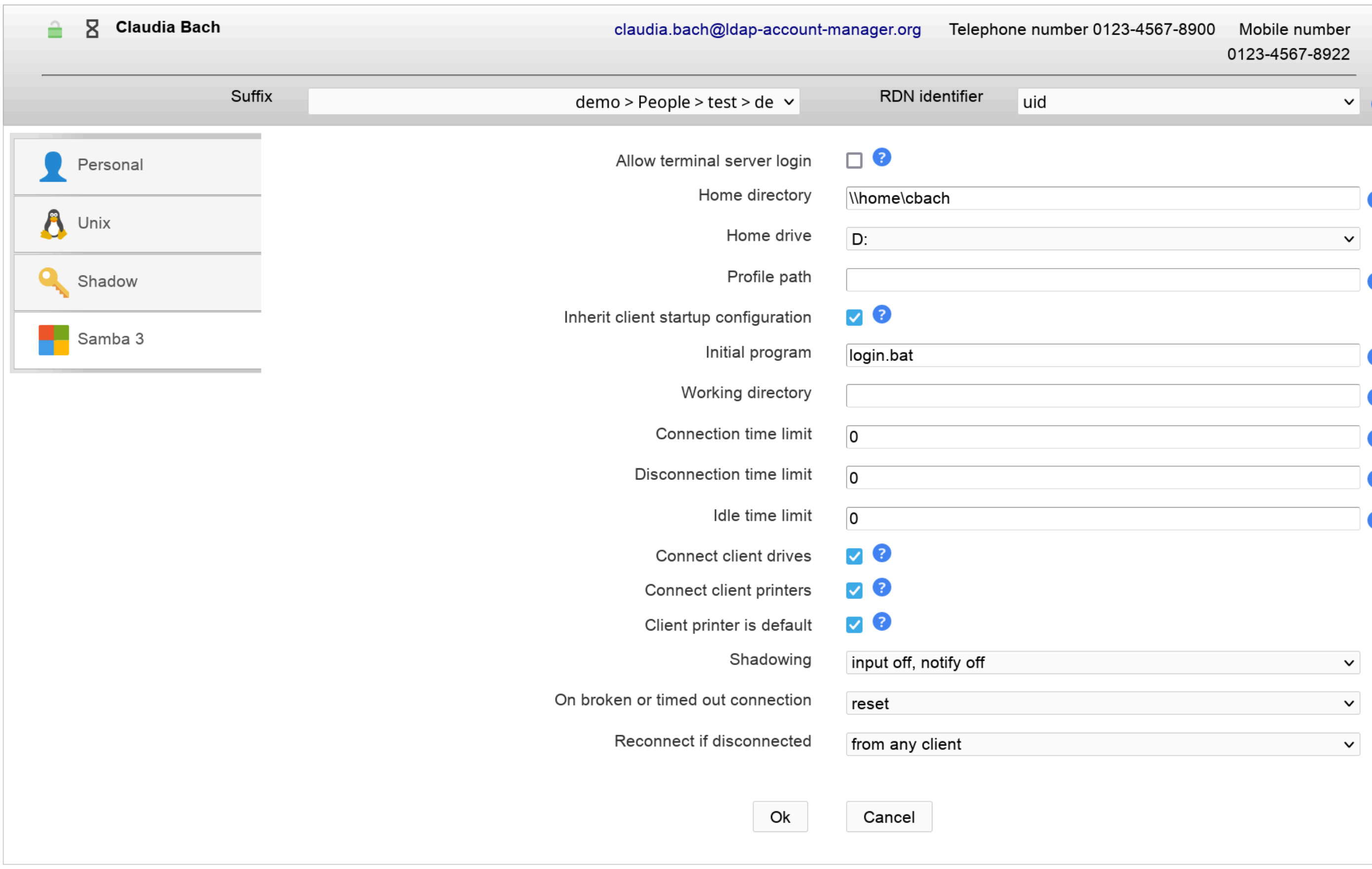
Mobile number 0123-4567-8922

Suffix: demo > People > test > de

RDN identifier: uid

Time	Sunday	Monday	Tuesday	Wednesday	Thursday	Friday	Saturday
00:00 - 00:59	☑	☑	☑	☑	☑	☑	☑
01:00 - 01:59	☑	☑	☑	☑	☑	☑	☑
02:00 - 02:59	☑	☑	☑	☑	☑	☑	☑
03:00 - 03:59	☑	☑	☑	☑	☑	☑	☑
04:00 - 04:59	☑	☑	☑	☑	☑	☑	☑
05:00 - 05:59	☑	☑	☑	☑	☑	☑	☑
06:00 - 06:59	☑	☑	☑	☑	☑	☑	☑
07:00 - 07:59	☑	☑	☑	☑	☑	☑	☑
08:00 - 08:59	☑	☑	☑	☑	☑	☑	☑
09:00 - 09:59	☑	☑	☑	☑	☑	☑	☑
10:00 - 10:59	☑	☑	☑	☑	☑	☑	☑
11:00 - 11:59	☑	☑	☑	☑	☑	☑	☑
12:00 - 12:59	☑	☑	☑	☑	☑	☑	☑
13:00 - 13:59	☑	☑	☑	☑	☑	☑	☑
14:00 - 14:59	☑	☑	☑	☑	☑	☑	☑
15:00 - 15:59	☑	☑	☑	☑	☑	☑	☑
16:00 - 16:59	☑	☑	☑	☑	☑	☑	☑
17:00 - 17:59	☑	☑	☑	☑	☑	☑	☑
18:00 - 18:59	☑	☑	☑	☑	☑	☑	☑
19:00 - 19:59	☑	☑	☑	☑	☑	☑	☑
20:00 - 20:59	☑	☑	☑	☑	☑	☑	☑
21:00 - 21:59	☑	☑	☑	☑	☑	☑	☑
22:00 - 22:59	☑	☑	☑	☑	☑	☑	☑
23:00 - 23:59	☑	☑	☑	☑	☑	☑	☑

You can also setup terminal server settings.



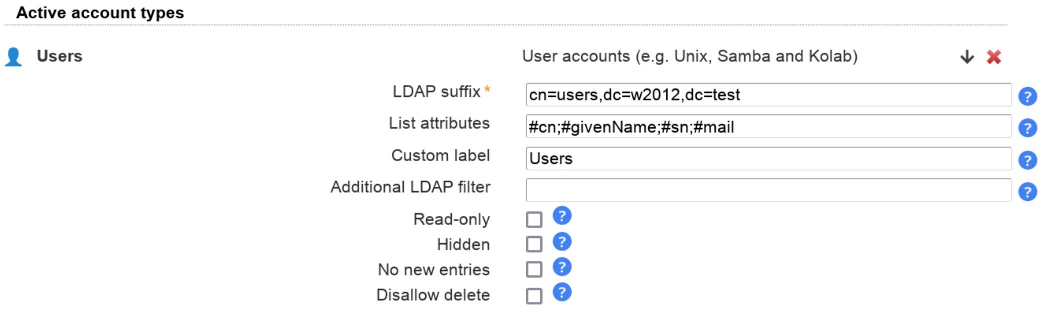
Claudia Bach claudia.bach@ldap-account-manager.org Telephone number 0123-4567-8900 Mobile number 0123-4567-8922

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

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

Windows (Samba 4/Active Directory)

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

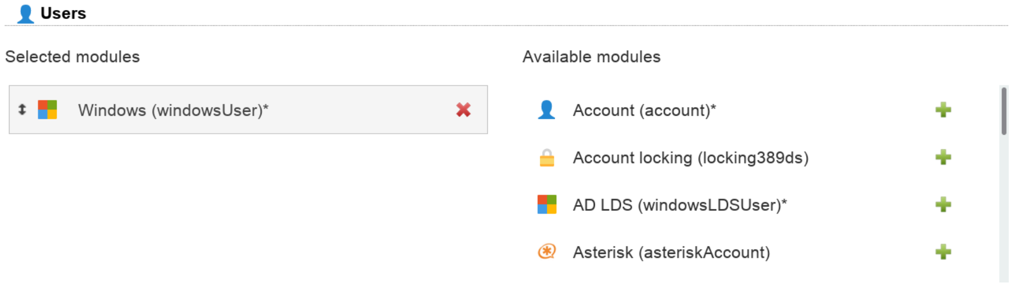


Active account types

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

LDAP suffix *	cn=users,dc=w2012,dc=test
List attributes	#cn;#givenName;#sn;#mail
Custom label	Users
Additional LDAP filter	
Read-only	□
Hidden	□
No new entries	□
Disallow delete	□

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



Users

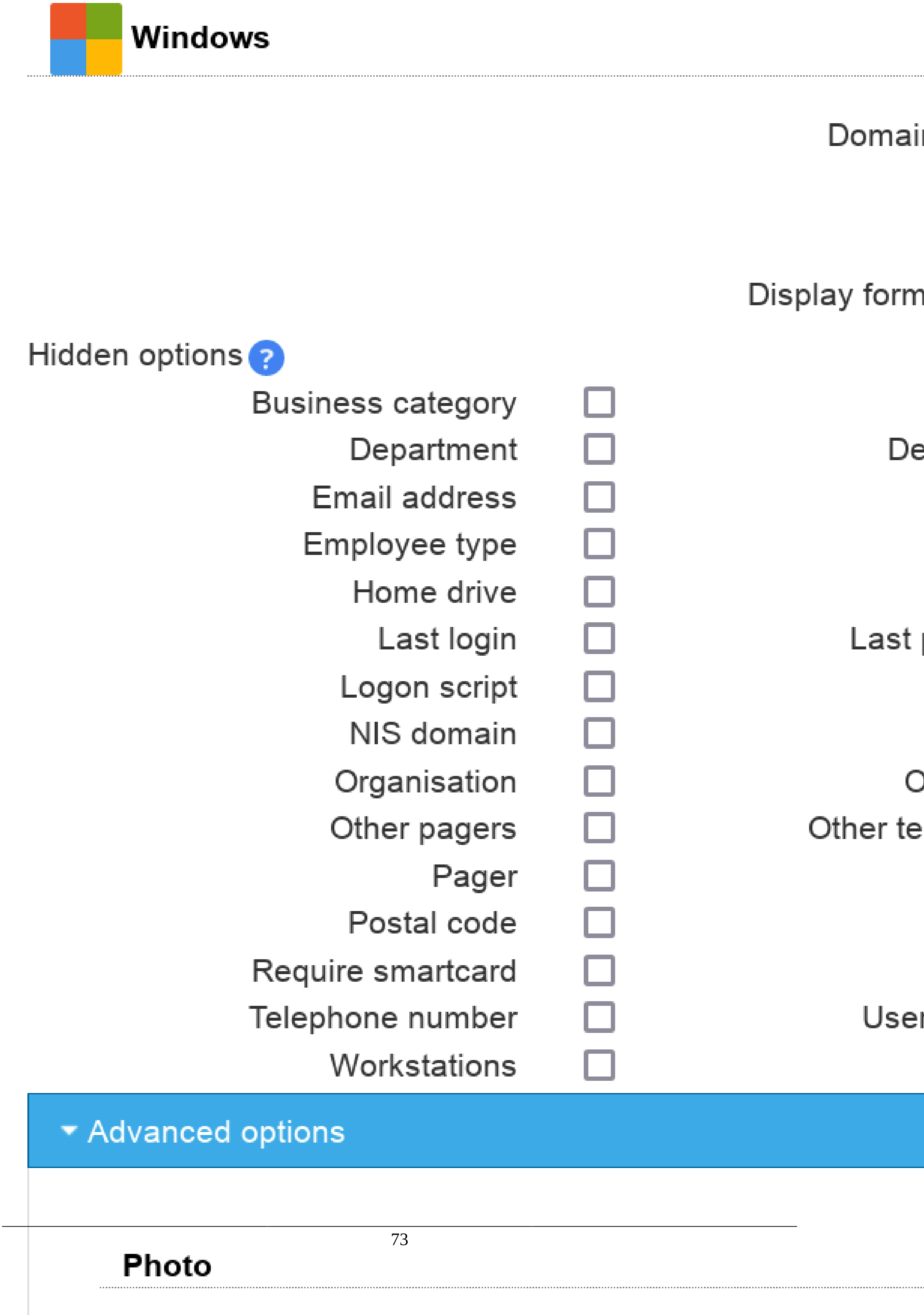
Selected modules:
- Windows (windowsUser)*

Available modules:
- Account (account)*
- Account locking (locking389ds)
- AD LDS (windowsLDSUser)*
- Asterisk (asteriskAccount)

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

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

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



Windows

Domai

Display form

Hidden options ?

Business category □

Department □

Email address □

Employee type □

Home drive □

Last login □

Logon script □

NIS domain □

Organisation □

Other pagers □

Pager □

Postal code □

Require smartcard □

Telephone number □

Workstations □

De

Last

O

Other te

User

▾ Advanced options

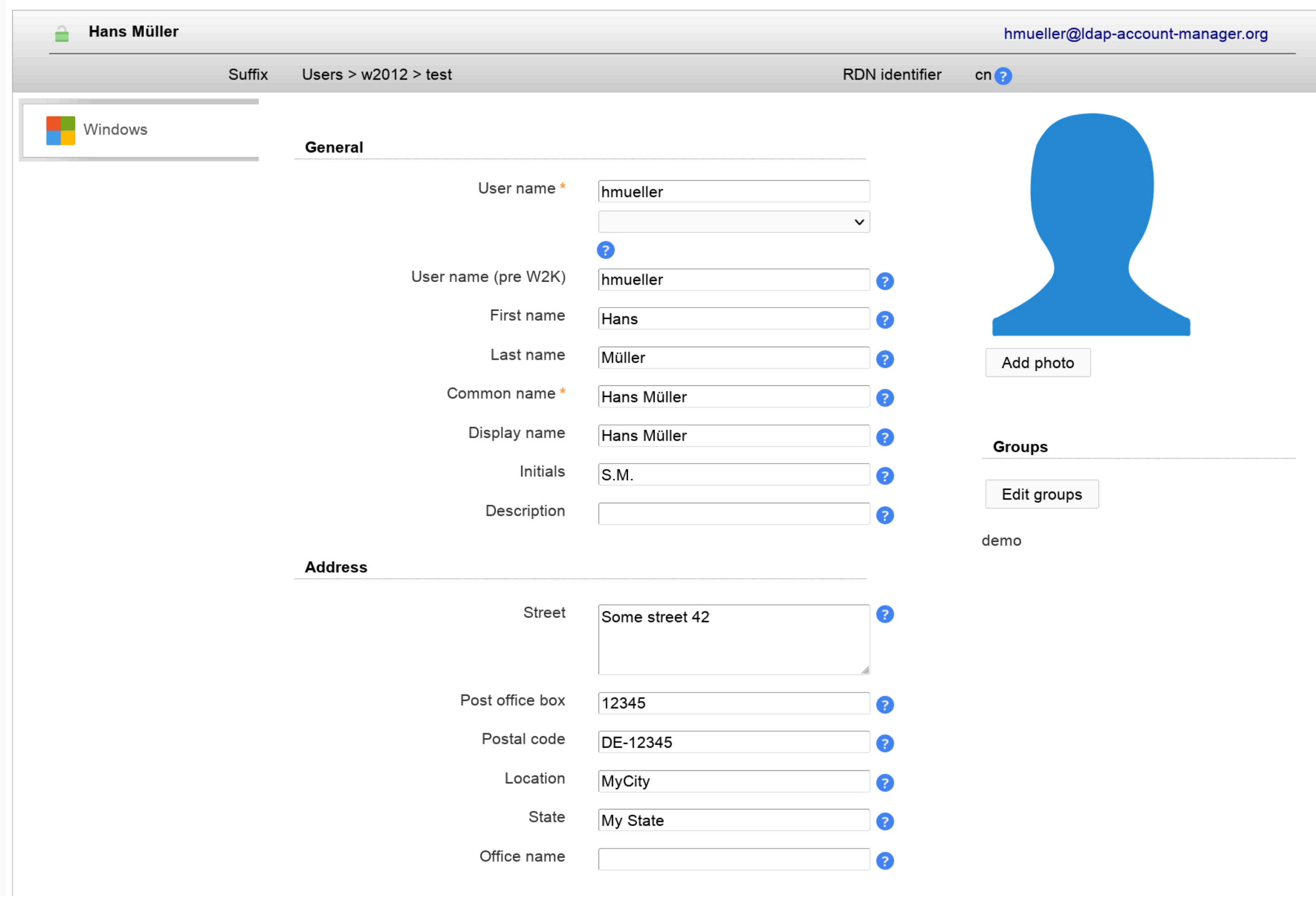
Photo

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.



Hans Müller hmueller@ldap-account-manager.org

Suffix Users > w2012 > test RDN identifier cn

General

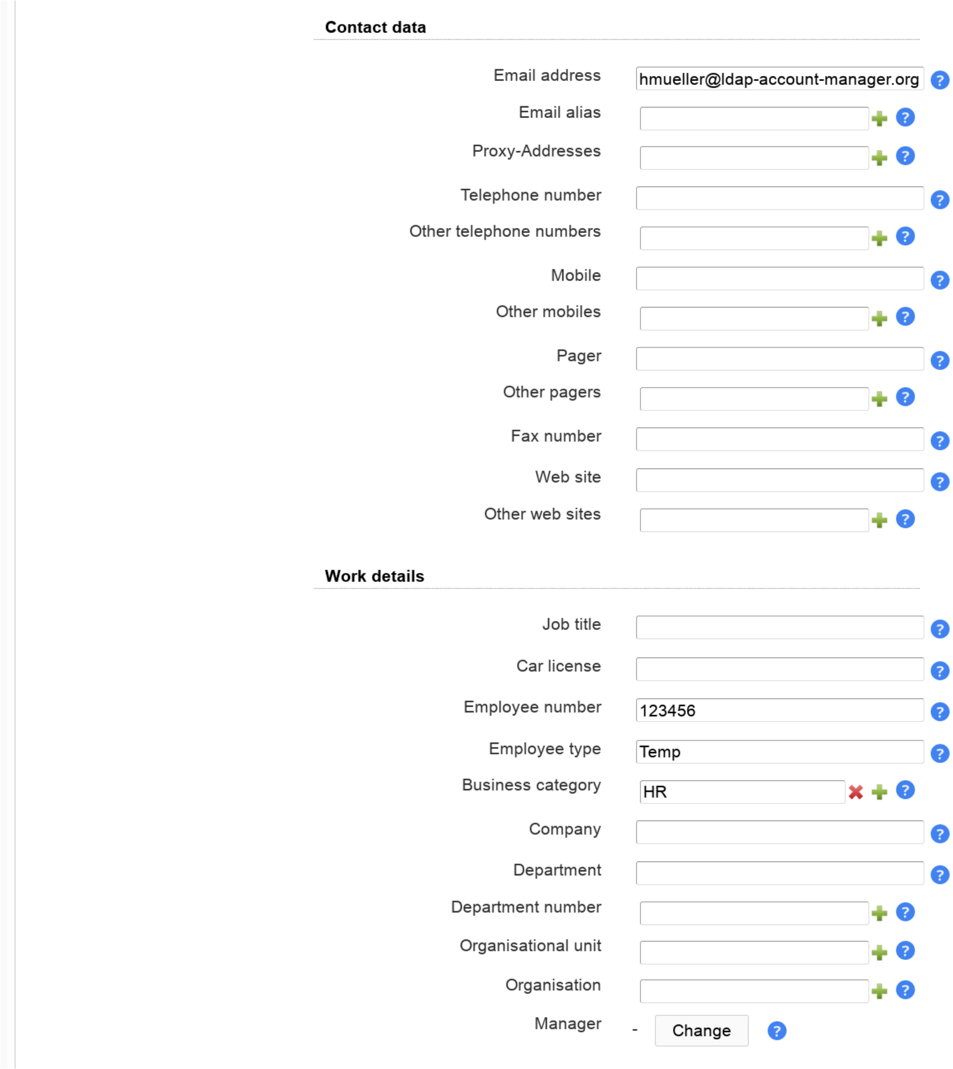
User name *	hmueller
User name (pre W2K)	hmueller
First name	Hans
Last name	Müller
Common name *	Hans Müller
Display name	Hans Müller
Initials	S.M.
Description	

Address

Street	Some street 42
Post office box	12345
Postal code	DE-12345
Location	MyCity
State	My State
Office name	

Groups

demo



Contact data

Email address	hmueller@ldap-account-manager.org
Email alias	
Proxy-Addresses	
Telephone number	
Other telephone numbers	
Mobile	
Other mobiles	
Pager	
Other pagers	
Fax number	
Web site	
Other web sites	

Work details

Job title	
Car license	
Employee number	123456
Employee type	Temp
Business category	HR
Company	
Department	
Department number	
Organisational unit	
Organisation	
Manager	- Change

Wildcards

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

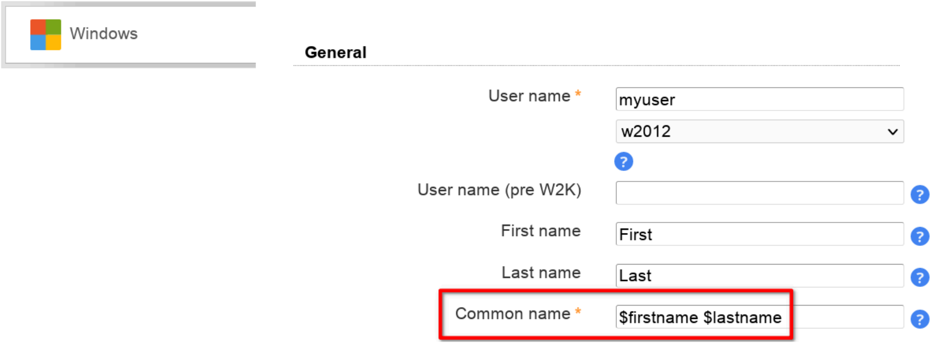
- $personaltitle: Personal title
- $firstname: First name
- $lastname: Last name
- $user: User name
- $commonname: Common name
- $email: Email address

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

- Common name
- Display name
- Email

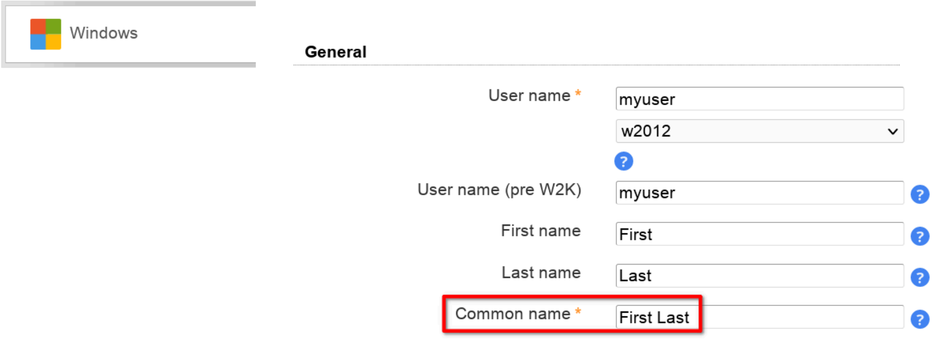
- Email alias
- Home directory
- Profile path
- Script path
- User name
- User name (pre W2K)

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



General

User name * myuser
w2012
User name (pre W2K)
First name First
Last name Last
Common name * $firstname $lastname

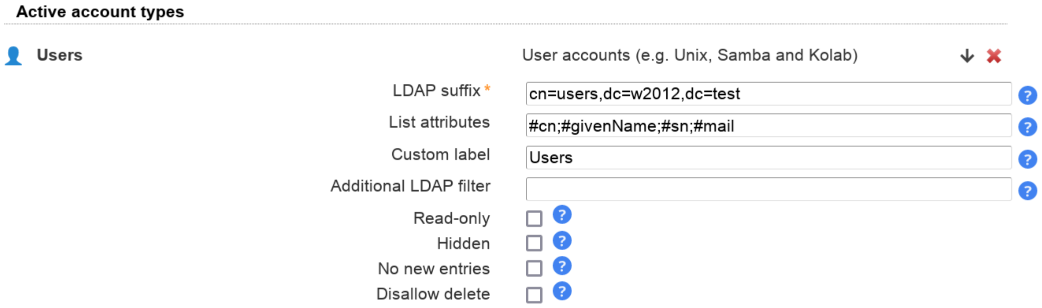


General

User name * myuser
w2012
User name (pre W2K) myuser
First name First
Last name Last
Common name * First Last

AD LDS (formerly ADAM) (LAM Pro)

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

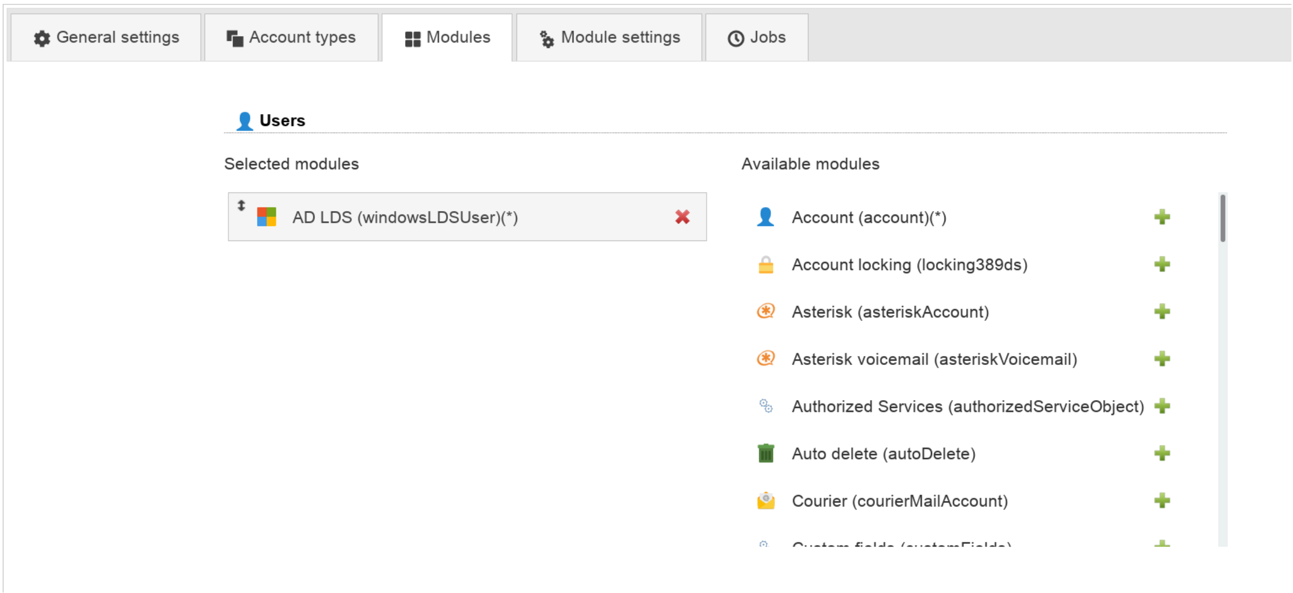


Active account types

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

LDAP suffix * cn=users,dc=w2012,dc=test
List attributes #cn;#givenName;#sn;#mail
Custom label Users
Additional LDAP filter
Read-only □
Hidden □
No new entries □
Disallow delete □

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



Users

Selected modules

AD LDS (windowsLDSUser)(*)

Available modules

Account (account)(*)

Account locking (locking389ds)

Asterisk (asteriskAccount)

Asterisk voicemail (asteriskVoicemail)

Authorized Services (authorizedServiceObject)

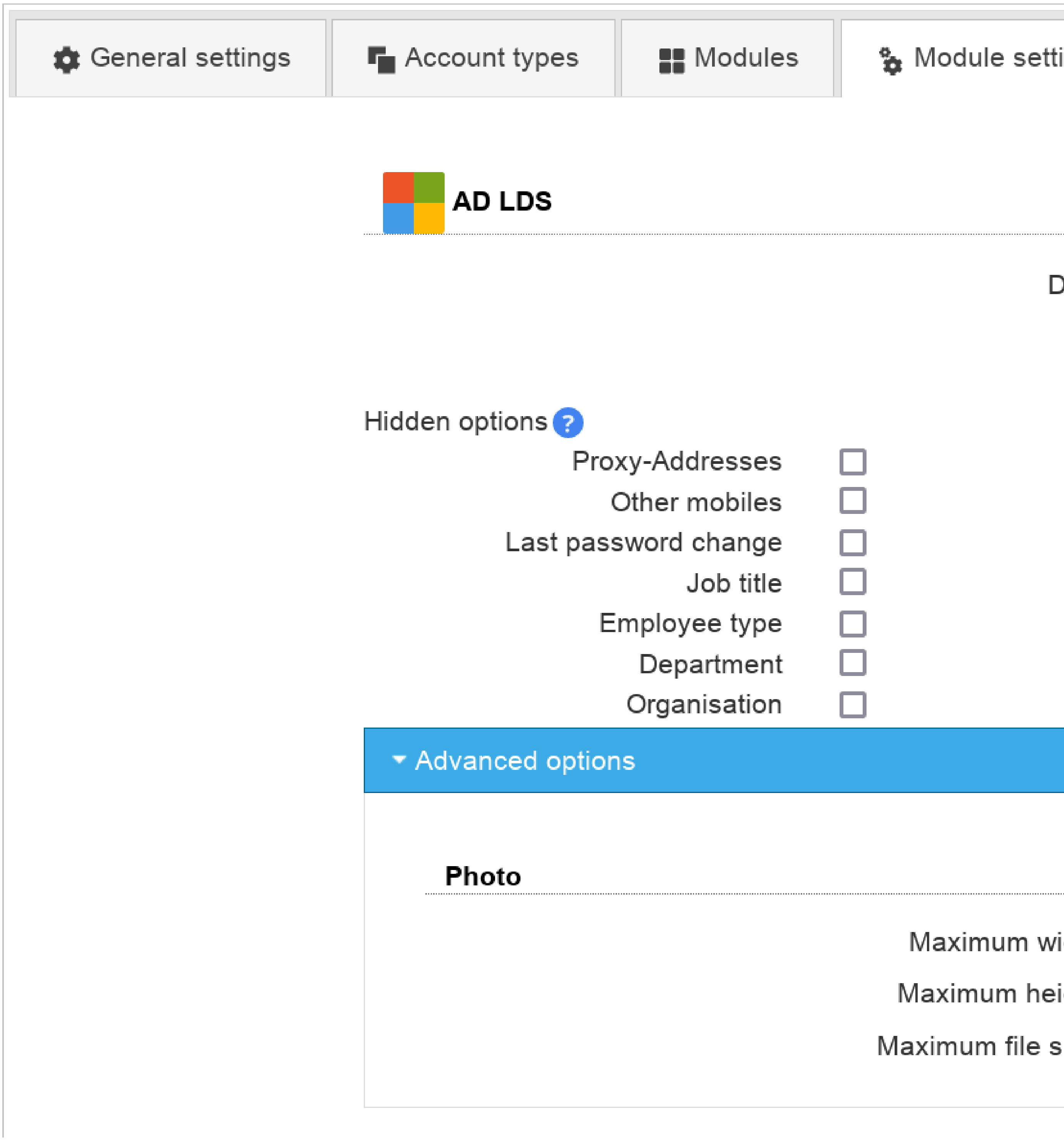
Auto delete (autoDelete)

Courier (courierMailAccount)

Custom fields (customFields)

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

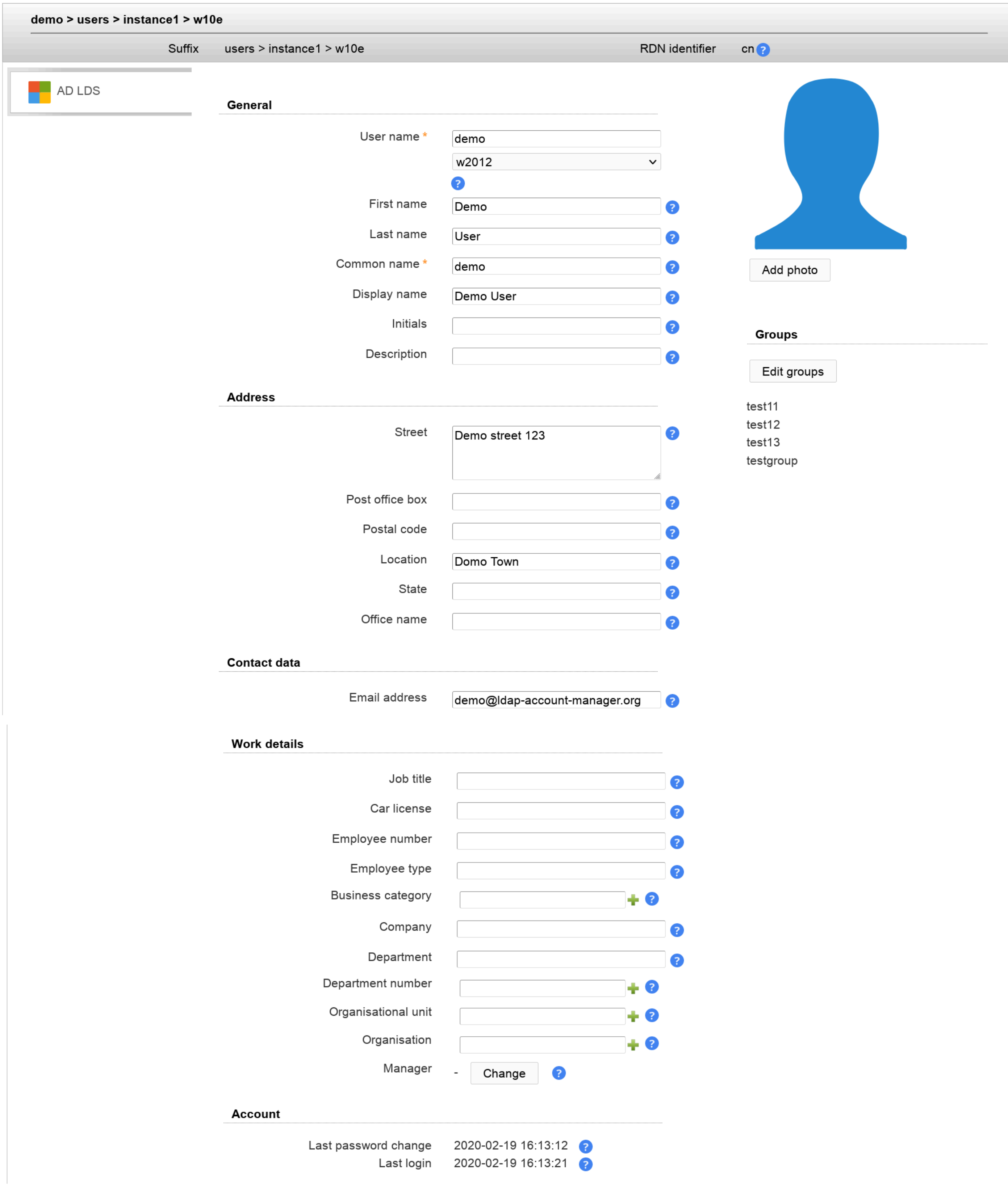
You can also set maximum values for user photos in advanced options.



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

Attention:

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



demo > users > instance1 > w10e

Suffix users > instance1 > w10e RDN identifier cn

General

User name *	demo w2012
First name	Demo
Last name	User
Common name *	demo
Display name	Demo User
Initials	
Description	

Address

Street	Demo street 123
Post office box	
Postal code	
Location	Domo Town
State	
Office name	

Contact data

Email address	demo@ldap-account-manager.org

Work details

Job title	
Car license	
Employee number	
Employee type	
Business category	
Company	
Department	
Department number	
Organisational unit	
Organisation	
Manager	-

Account

Last password change	2020-02-19 16:13:12
Last login	2020-02-19 16:13:21

Groups

test11
test12
test13
testgroup

Wildcards

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

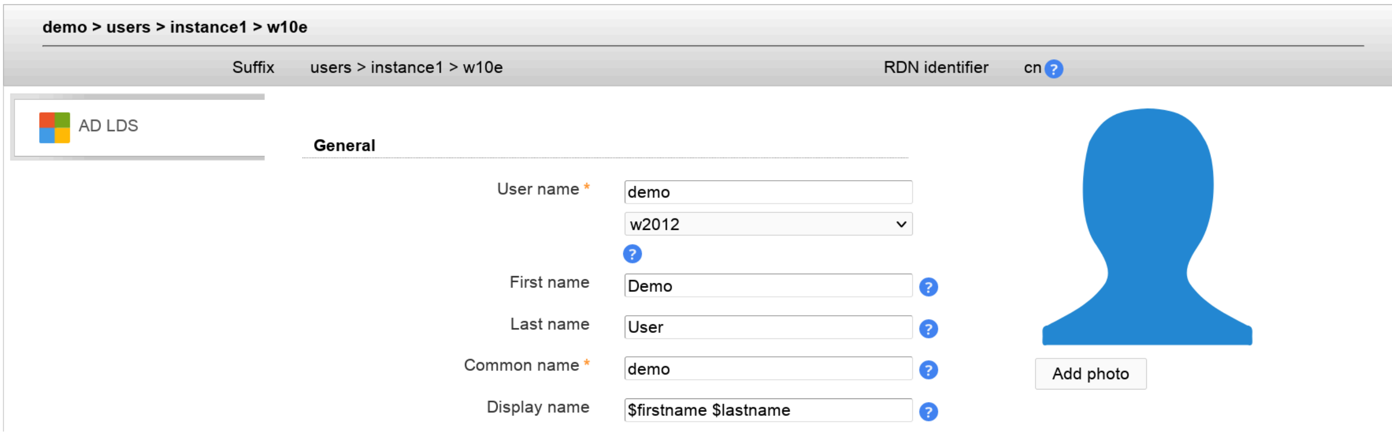
- $firstname: First name

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

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

- Common name
- Display name
- Email
- Email alias

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



demo > users > instance1 > w10e

Suffix: users > instance1 > w10e

RDN identifier: cn

General

User name *: demo

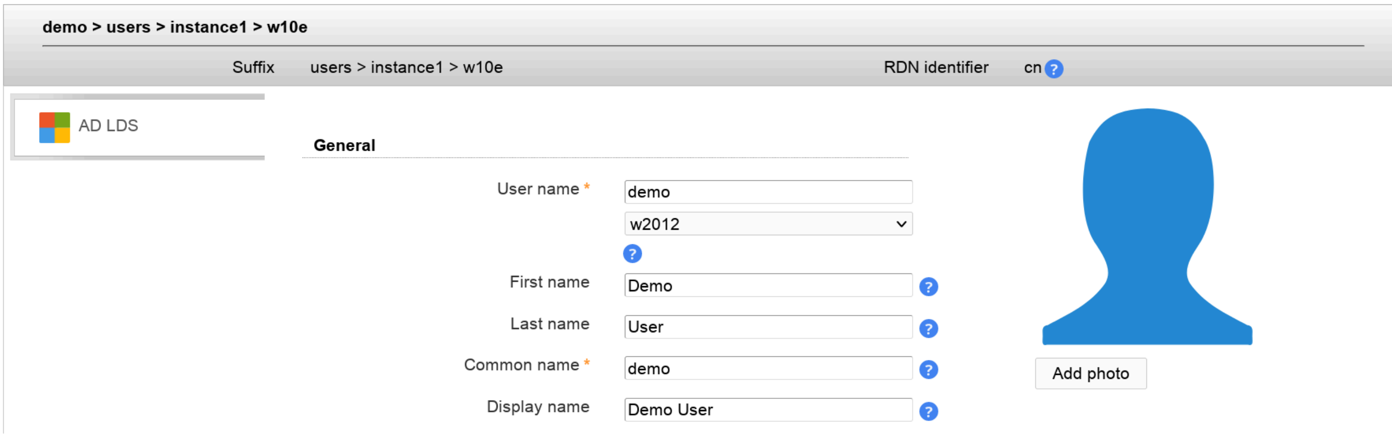
w2012

First name: Demo

Last name: User

Common name *: demo

Display name: $firstname $lastname



demo > users > instance1 > w10e

Suffix: users > instance1 > w10e

RDN identifier: cn

General

User name *: demo

w2012

First name: Demo

Last name: User

Common name *: demo

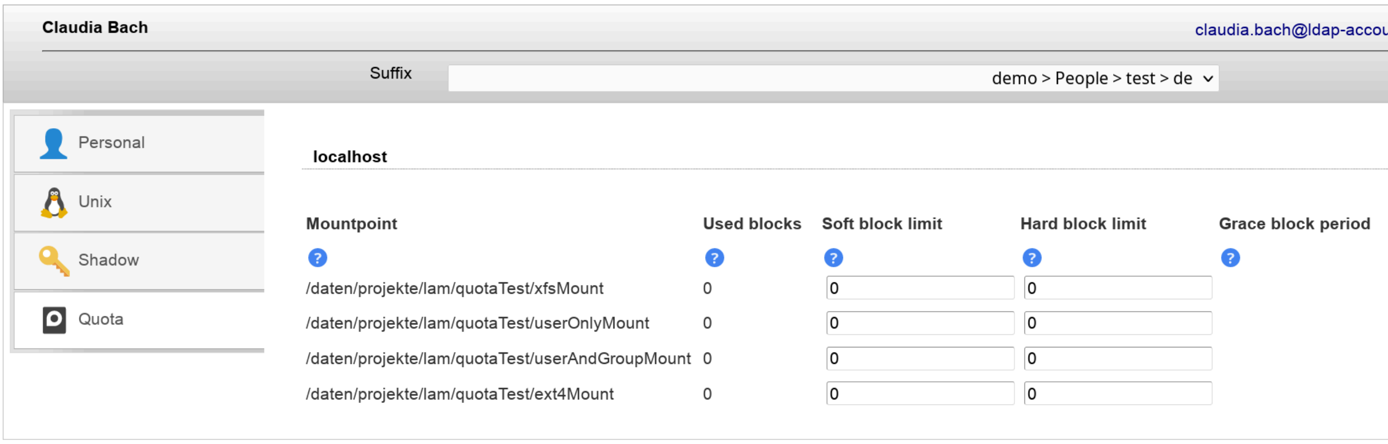
Display name: Demo User

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.



Suffix: demo > People > test > de

localhost

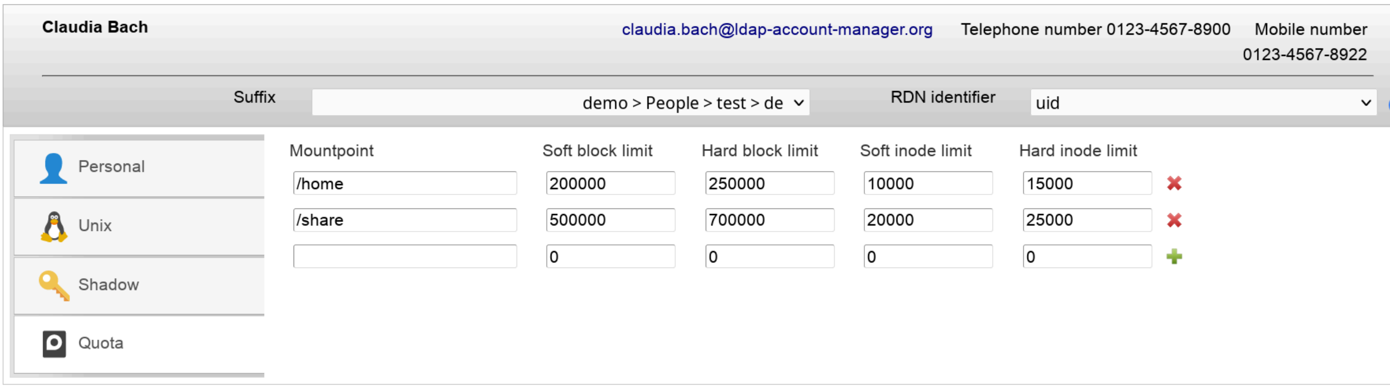
Mountpoint	Used blocks	Soft block limit	Hard block limit	Grace block period
/daten/projekte/lam/quotaTest/xfsMount	0	0	0	
/daten/projekte/lam/quotaTest/userOnlyMount	0	0	0	
/daten/projekte/lam/quotaTest/userAndGroupMount	0	0	0	
/daten/projekte/lam/quotaTest/ext4Mount	0	0	0	

Filesystem quota (LDAP)

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

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

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


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

Suffix: demo > People > test > de

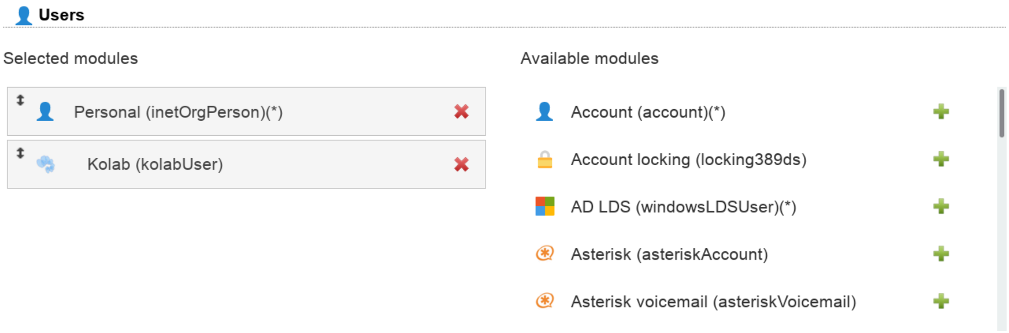
RDN identifier: uid

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.



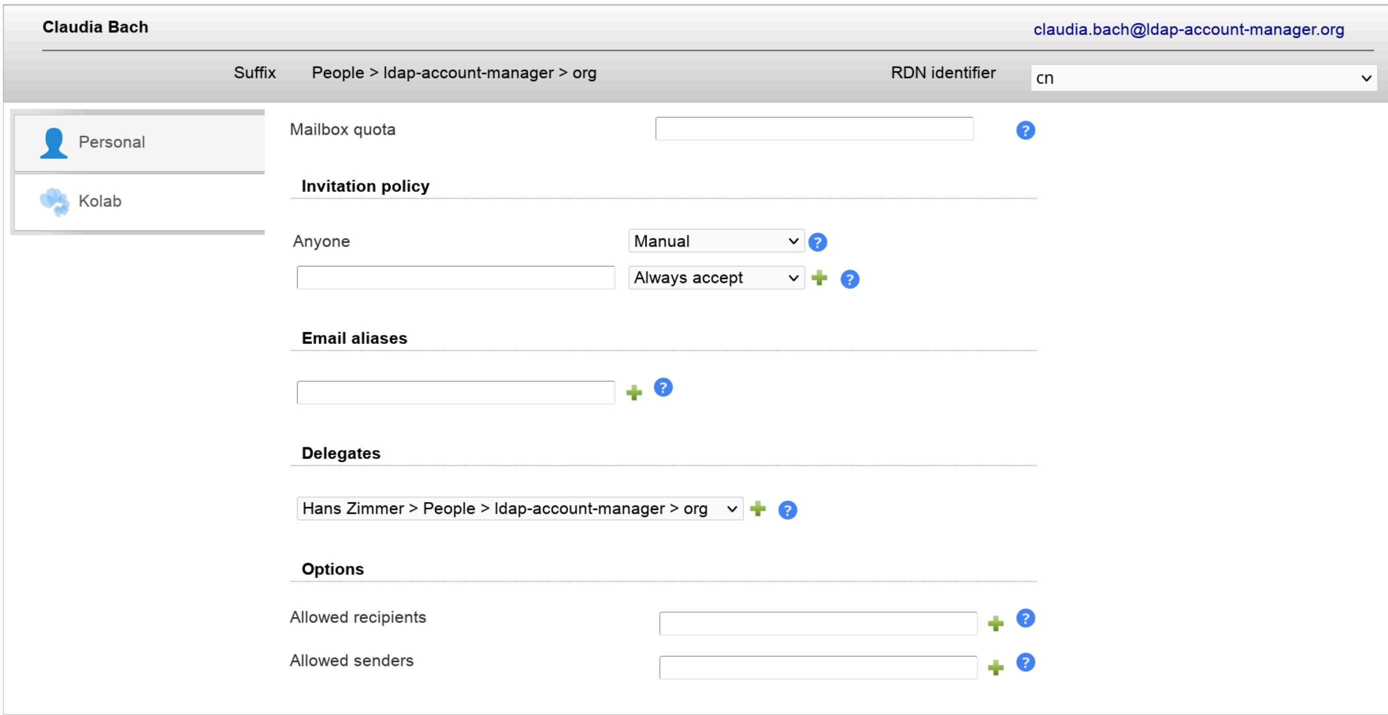
Selected modules

- Personal (inetOrgPerson)(*)
- Kolab (kolabUser)

Available modules

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

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



Claudia Bach

claudia.bach@ldap-account-manager.org

Suffix: People > ldap-account-manager > org

RDN identifier: cn

Mailbox quota:

Invitation policy

Anyone: Manual

Always accept

Email aliases

Delegates

Hans Zimmer > People > ldap-account-manager > org

Options

Allowed recipients:

Allowed senders:

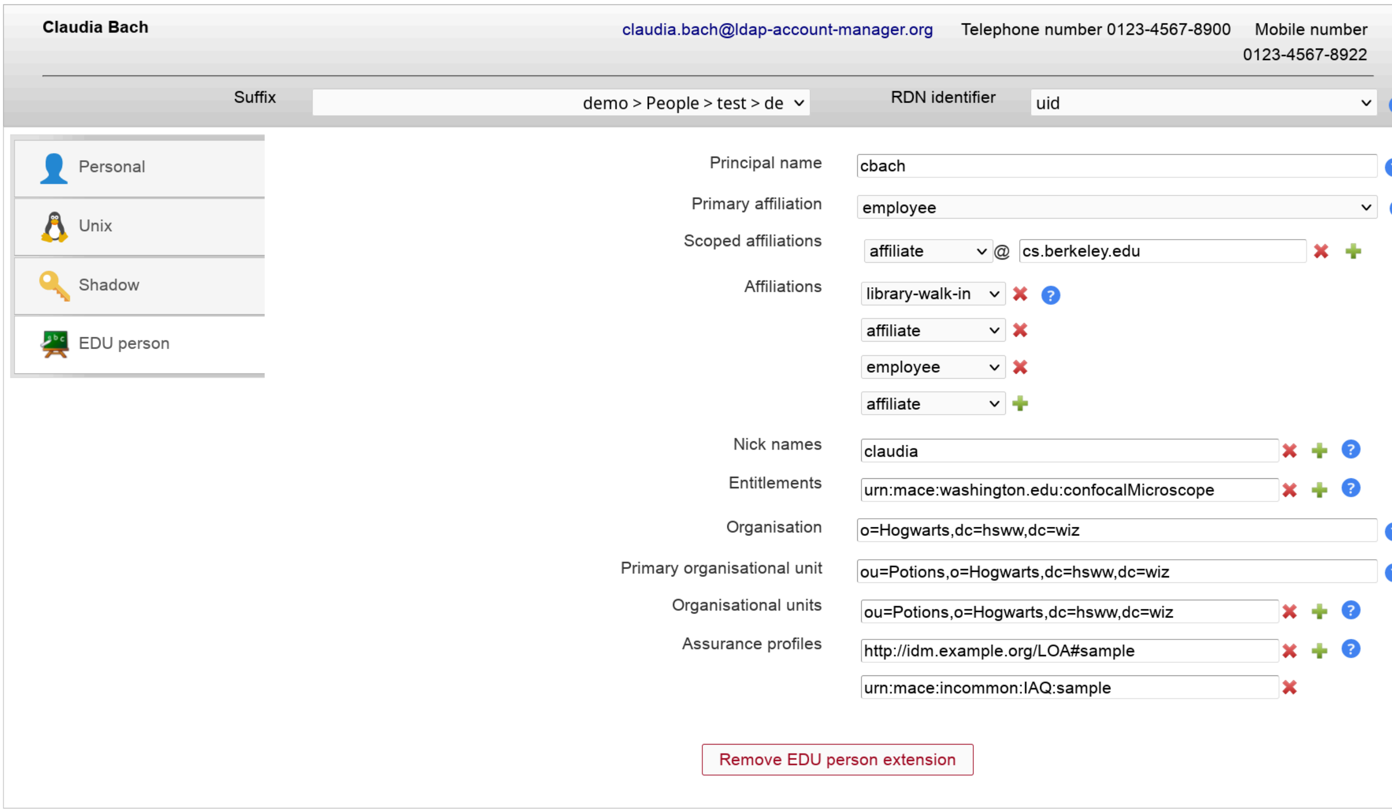
If you upgrade existing non-Kolab accounts please make sure that the account has an Unix password.

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.



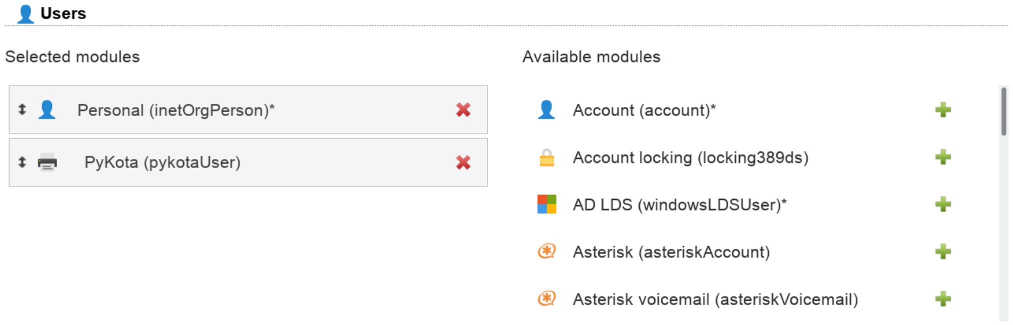
Claudia Bach claudia.bach@ldap-account-manager.org Telephone number 0123-4567-8900 Mobile number 0123-4567-8922

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

Principal name	cbach
Primary affiliation	employee
Scoped affiliations	affiliate @ cs.berkeley.edu
Affiliations	library-walk-in affiliate employee affiliate
Nick names	claudia
Entitlements	urn:mace:washington.edu:confocalMicroscope
Organisation	o=Hogwarts,dc=hsww,dc=wiz
Primary organisational unit	ou=Potions,o=Hogwarts,dc=hsww,dc=wiz
Organisational units	ou=Potions,o=Hogwarts,dc=hsww,dc=wiz
Assurance profiles	http://idm.example.org/LOA#sample urn:mace:incommon:IAQ:sample

PyKota

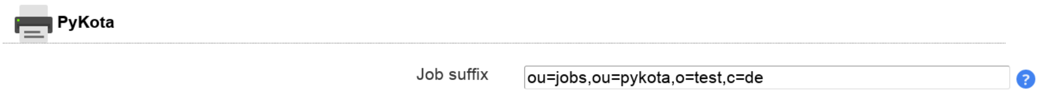
There are two LAM user modules depending if your user entries should be built on object class "pykotaObject" or a different structural object class (e.g. "inetOrgPerson"). For "pykotaObject" please select "PyKota (pykotaUserStructural(*))" and "PyKota (pykotaUser)" in all other cases.



Selected modules
- Personal (inetOrgPerson)*
- PyKota (pykotaUser)

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

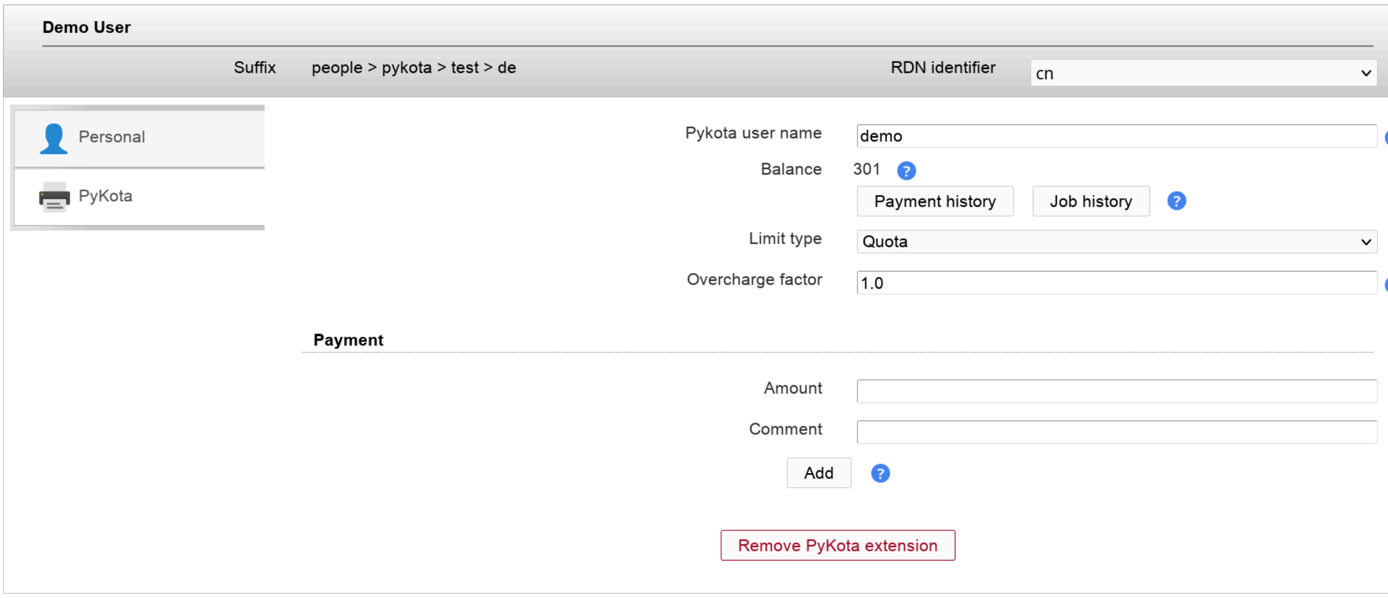
To display the job history please setup the job DN on tab "Module settings":



Job suffix: ou=jobs,ou=pykota,o=test,c=de

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

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



Demo User

Suffix people > pykota > test > de RDN identifier cn

Pykota user name	demo
Balance	301
	Payment history Job history
Limit type	Quota
Overcharge factor	1.0

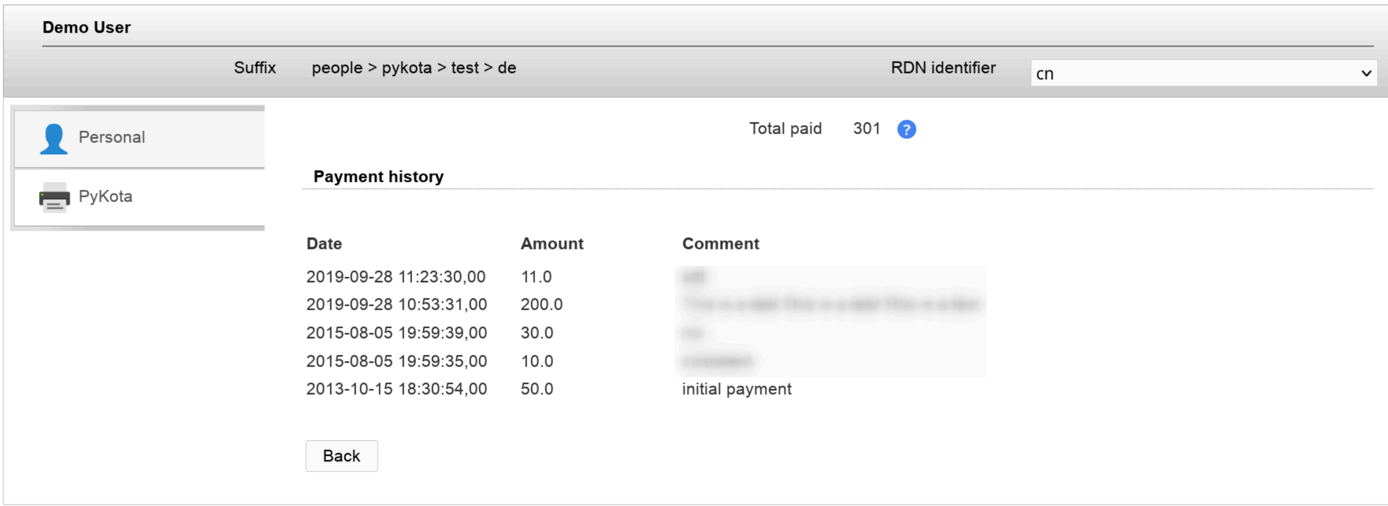
Payment

Amount	
Comment	

Add

Remove PyKota extension

You may also view the payment and job history.



Demo User

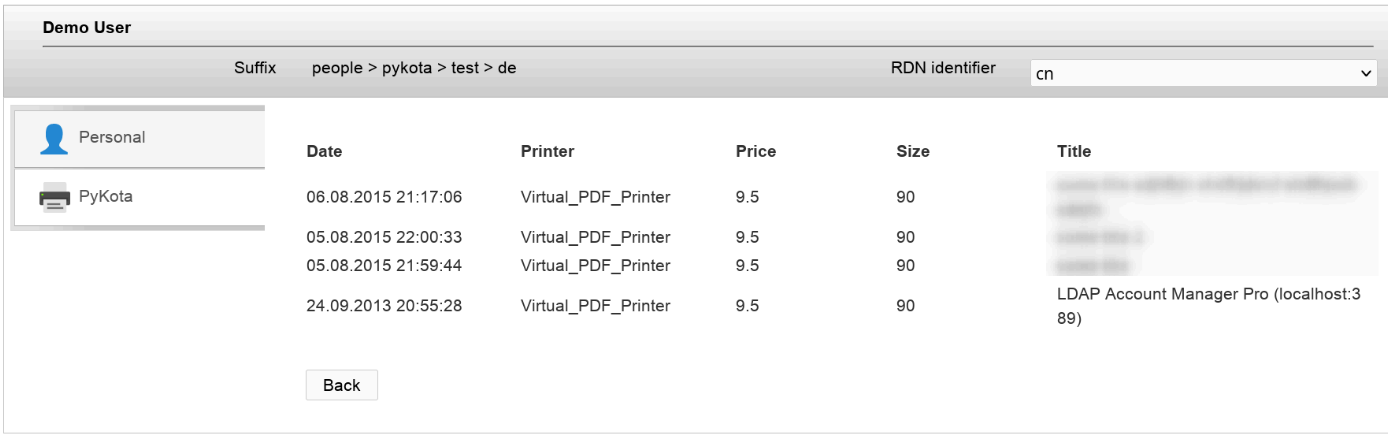
Suffix people > pykota > test > de RDN identifier cn

Total paid 301

Payment history

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

Back



Demo User

Suffix people > pykota > test > de RDN identifier cn

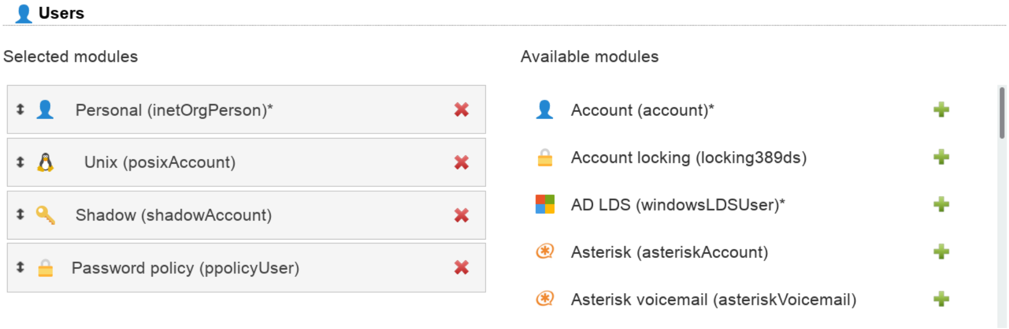
Date	Printer	Price	Size	Title
06.08.2015 21:17:06	Virtual_PDF_Printer	9.5	90	[redacted]
05.08.2015 22:00:33	Virtual_PDF_Printer	9.5	90	[redacted]
05.08.2015 21:59:44	Virtual_PDF_Printer	9.5	90	[redacted]
24.09.2013 20:55:28	Virtual_PDF_Printer	9.5	90	LDAP Account Manager Pro (localhost:389)

Back

Password policy (LAM Pro)

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

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



Users

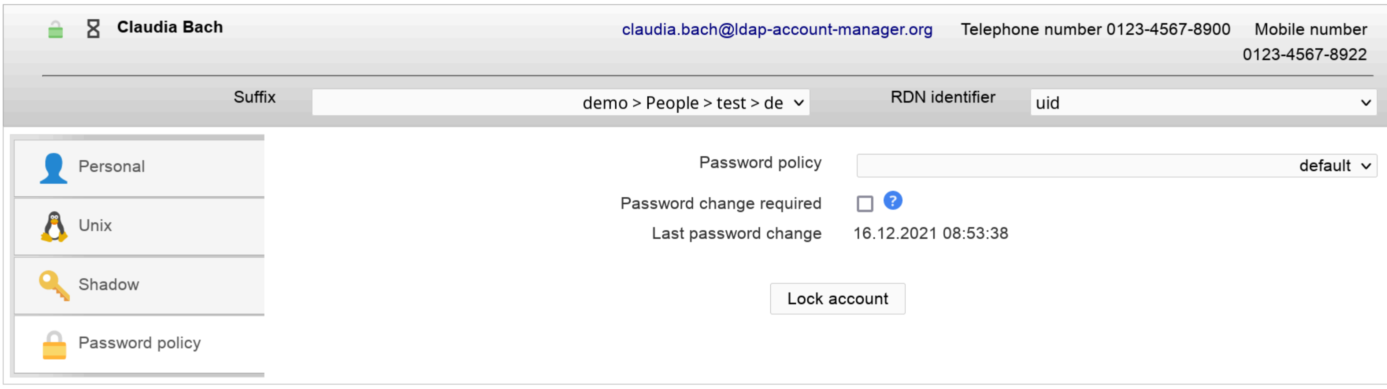
Selected modules

- Personal (inetOrgPerson)*
- Unix (posixAccount)
- Shadow (shadowAccount)
- Password policy (ppolicyUser)

Available modules

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

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



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

Suffix: demo > People > test > de

RDN identifier: uid

Password policy: default

Password change required ☐

Last password change 16.12.2021 08:53:38

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.

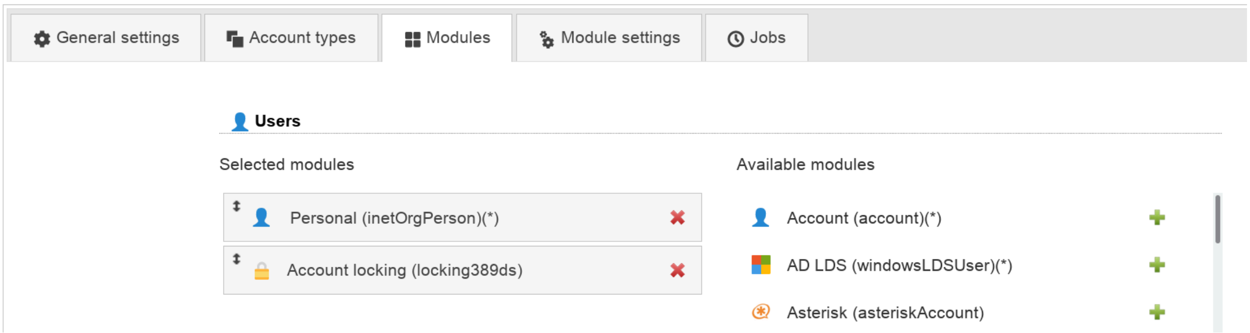
Account locking for 389ds (LAM Pro)

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)".



Users

Selected modules

- Personal (inetOrgPerson)(*)
- Account locking (locking389ds)

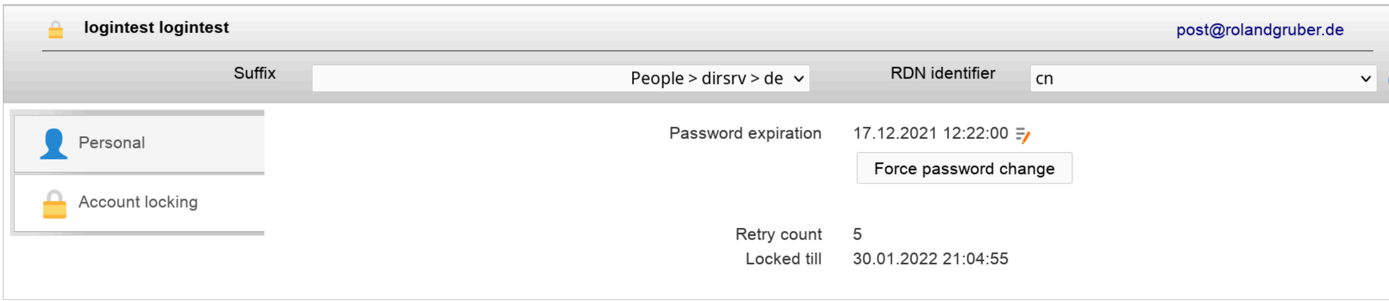
Available modules

- Account (account)(*)
- AD LDS (windowsLDSUser)(*)
- Asterisk (asteriskAccount)

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.



logintest logintest

post@rolandgruber.de

Suffix: People > dirsrv > de

RDN identifier: cn

Password expiration: 17.12.2021 12:22:00

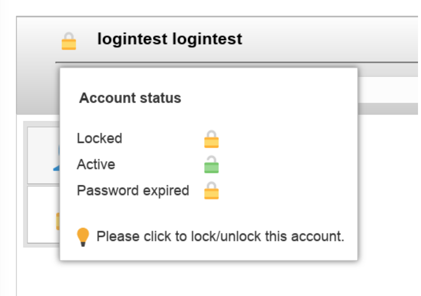
Retry count: 5

Locked till: 30.01.2022 21:04:55

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.



logintest logintest

Account status

Locked 🔒

Active 🔒

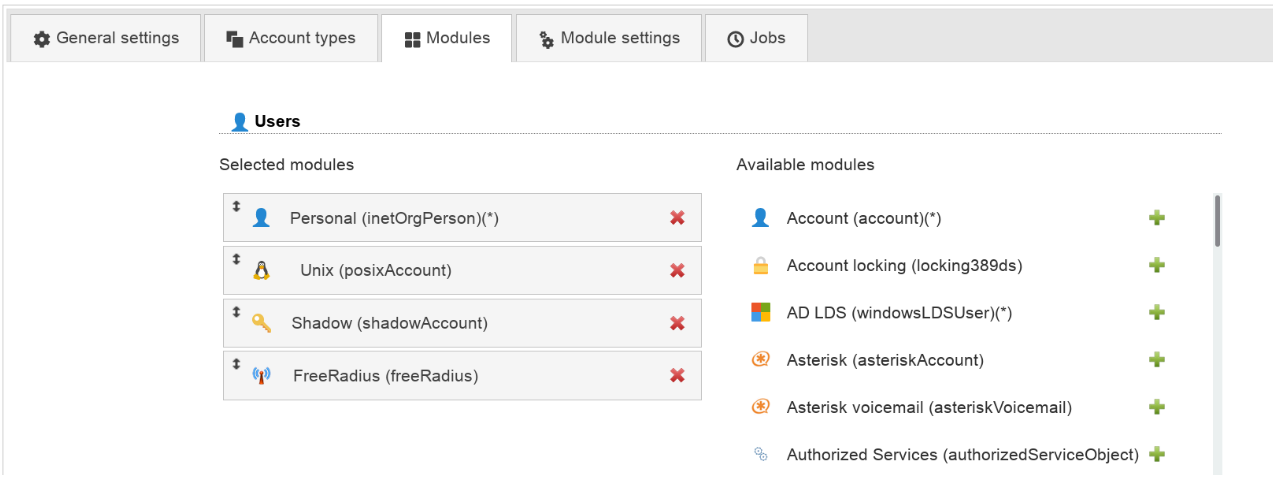
Password expired 🔒

Please click to lock/unlock this account.

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:



Users

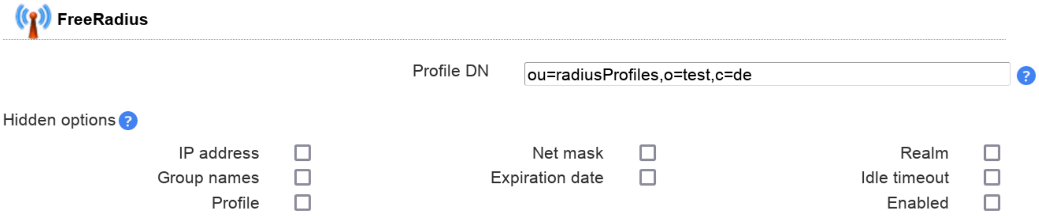
Selected modules

- Personal (inetOrgPerson)(*) ✖
- Unix (posixAccount) ✖
- Shadow (shadowAccount) ✖
- FreeRadius (freeRadius) ✖

Available modules

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

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".



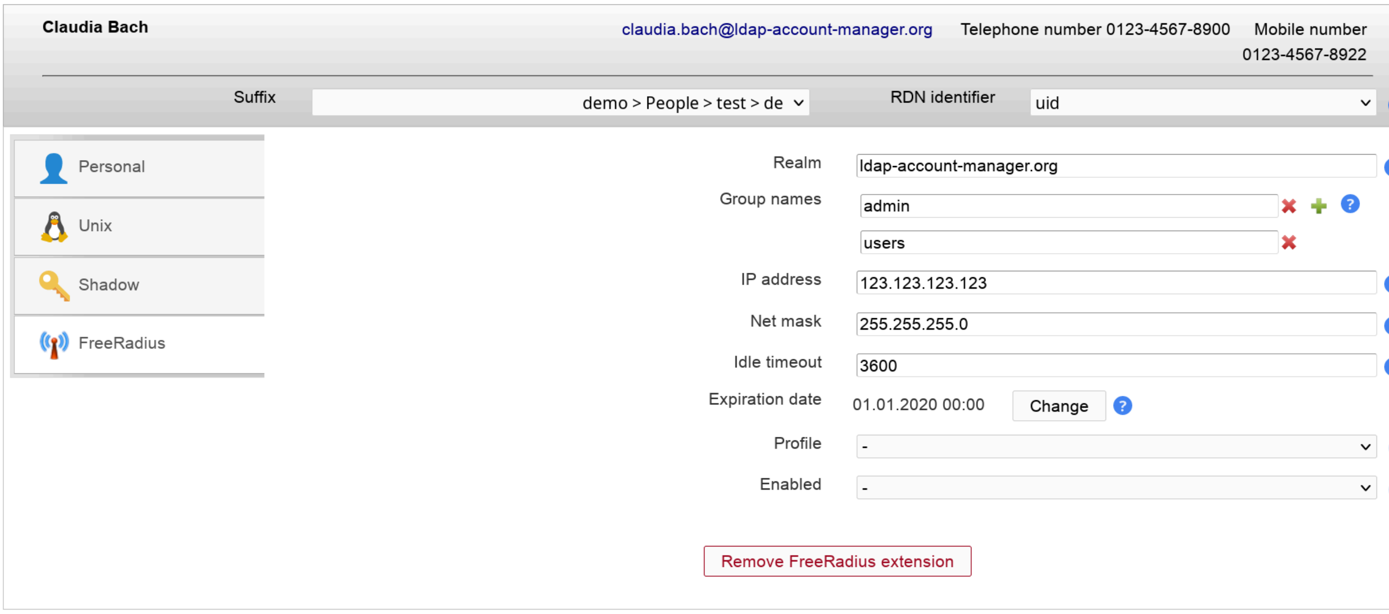
FreeRadius

Profile DN: ou=radiusProfiles,o=test,c=de

Hidden options

IP address	□	Net mask	□	Realm	□
Group names	□	Expiration date	□	Idle timeout	□
Profile	□			Enabled	□

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.



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

Realm: ldap-account-manager.org

Group names: admin, users

IP address: 123.123.123.123

Net mask: 255.255.255.0

Idle timeout: 3600

Expiration date: 01.01.2020 00:00 Change

Profile: -

Enabled: -

Remove FreeRadius extension

Heimdal Kerberos (LAM Pro)

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

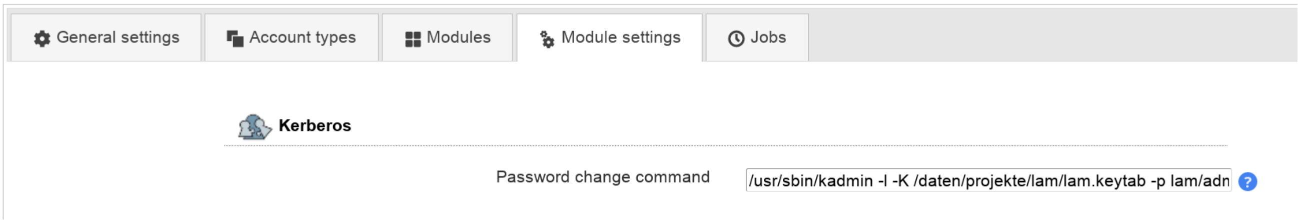
Setup password changing

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

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

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

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

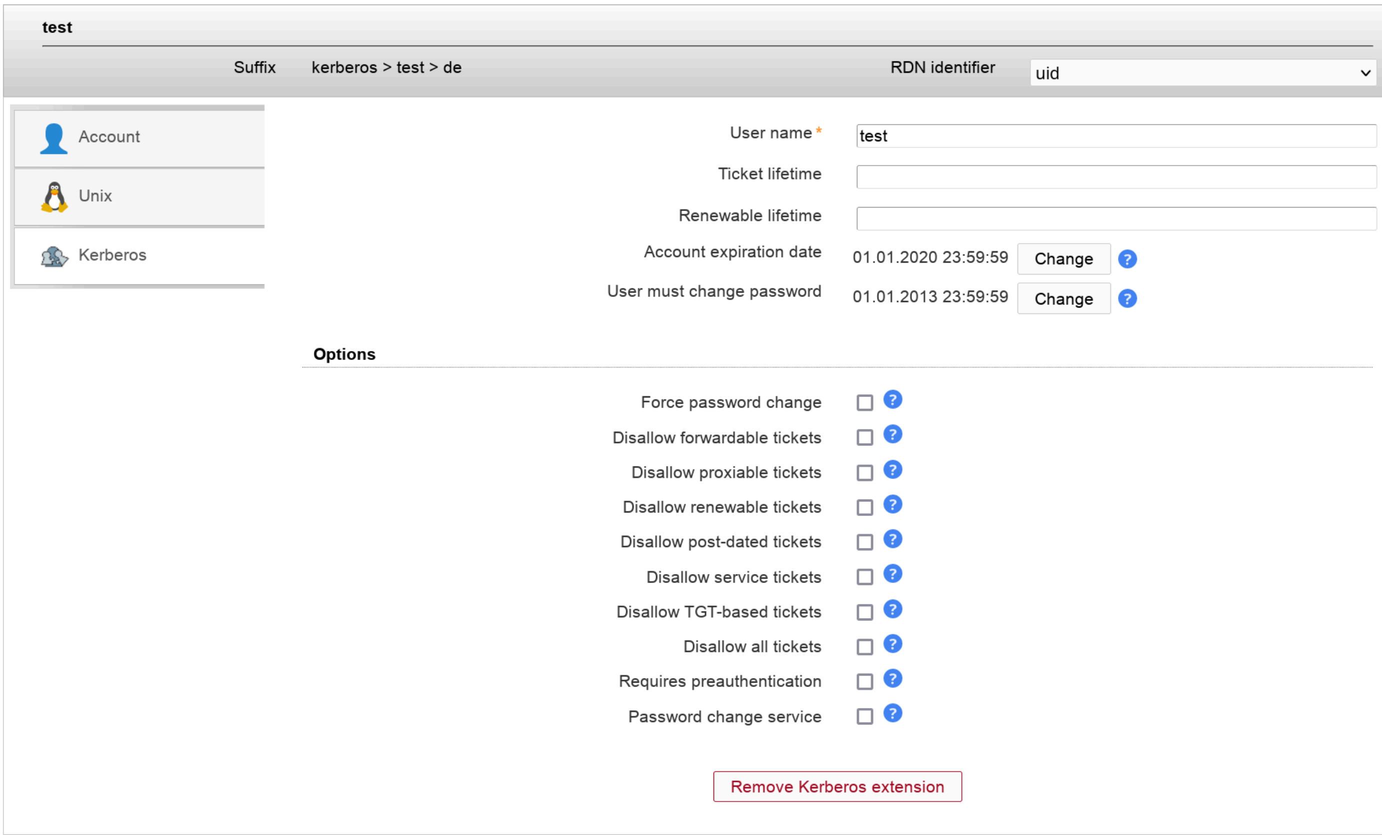


Kerberos

Password change command: /usr/sbin/kadmin -l -K /daten/projekte/lam/lam.keytab -p lam/adn

User management

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



test

Suffix: kerberos > test > de

RDN identifier: uid

User name *: test

Ticket lifetime:

Renewable lifetime:

Account expiration date: 01.01.2020 23:59:59

User must change password: 01.01.2013 23:59:59

Options

Force password change □

Disallow forwardable tickets □

Disallow proxiable tickets □

Disallow renewable tickets □

Disallow post-dated tickets □

Disallow service tickets □

Disallow TGT-based tickets □

Disallow all tickets □

Requires preauthentication □

Password change service □

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.

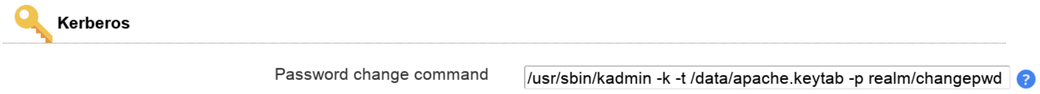
Keytabs may be created with the "ktutil" application.

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

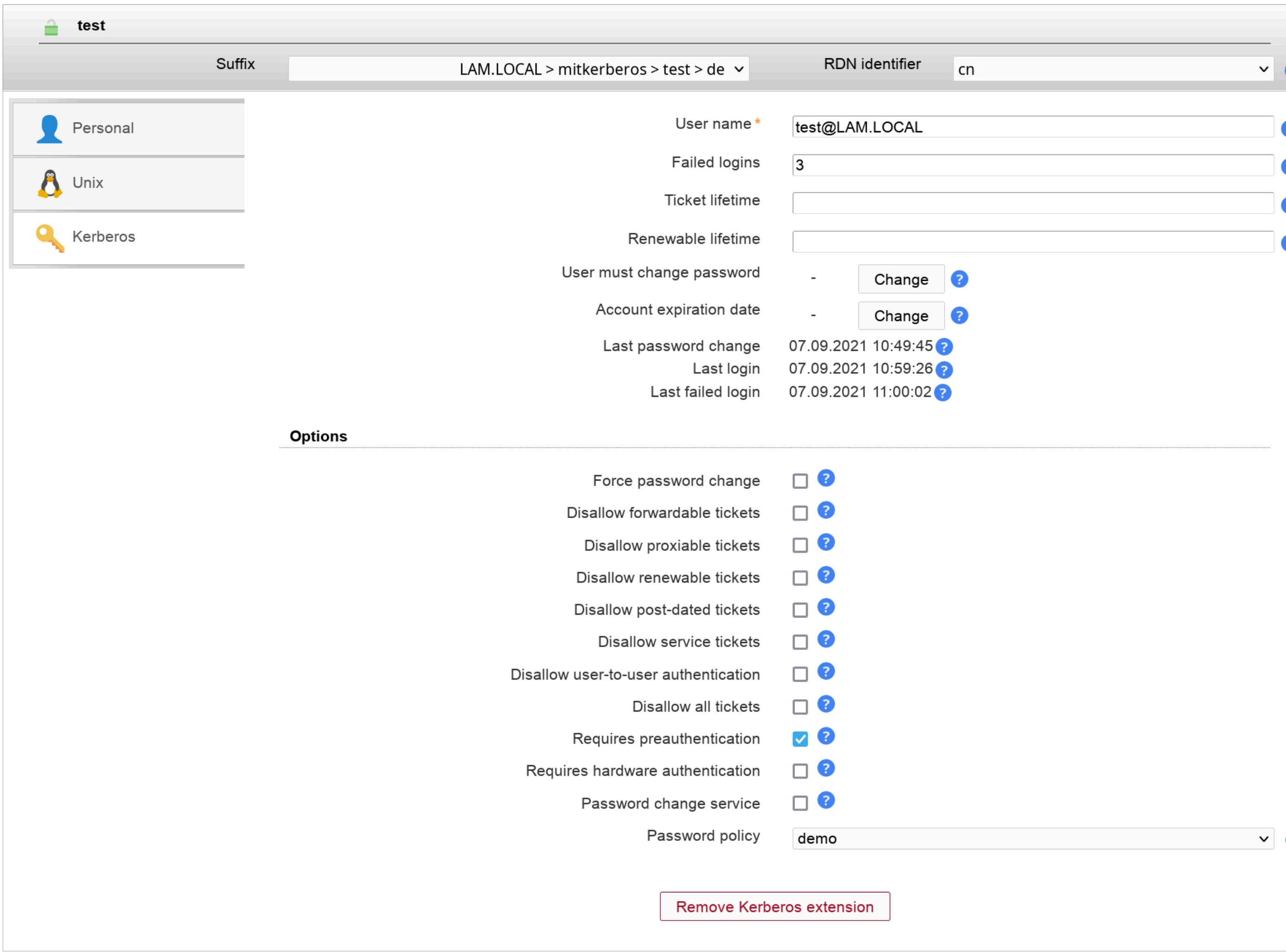


Kerberos

Password change command: /usr/sbin/kadmin -k -t /data/apache.keytab -p realm/changepwd

User management

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



test

Suffix: LAM.LOCAL > mitkerberos > test > de
RDN identifier: cn

User name *: test@LAM.LOCAL
Failed logins: 3
Ticket lifetime:
Renewable lifetime:
User must change password: - Change
Account expiration date: - Change
Last password change: 07.09.2021 10:49:45
Last login: 07.09.2021 10:59:26
Last failed login: 07.09.2021 11:00:02

Options

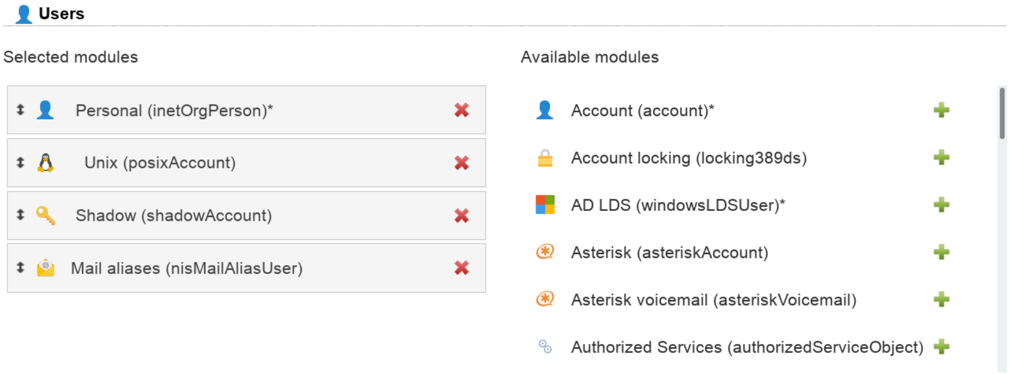
Force password change ☐
Disallow forwardable tickets ☐
Disallow proxiable tickets ☐
Disallow renewable tickets ☐
Disallow post-dated tickets ☐
Disallow service tickets ☐
Disallow user-to-user authentication ☐
Disallow all tickets ☐
Requires preauthentication ☑
Requires hardware authentication ☐
Password change service ☐
Password policy: demo

NIS mail aliases

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

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

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



Users

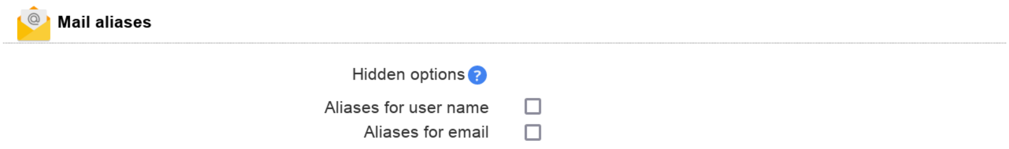
Selected modules

- Personal (inetOrgPerson)*
- Unix (posixAccount)
- Shadow (shadowAccount)
- Mail aliases (nisMailAliasUser)

Available modules

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

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



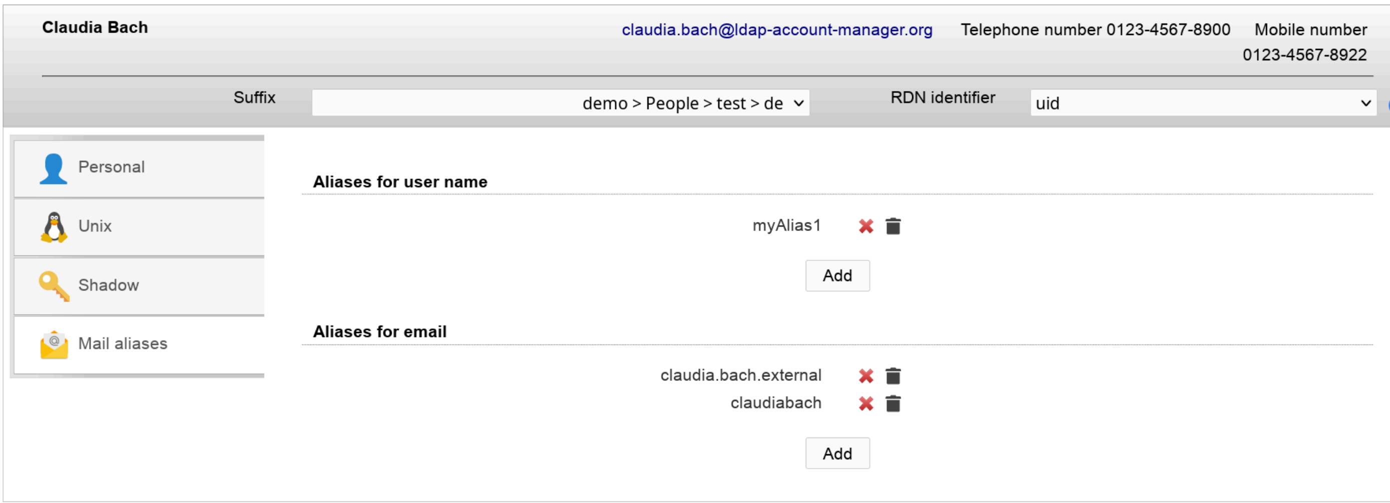
Mail aliases

Hidden options ?

Aliases for user name □
Aliases for email □

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

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



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

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

Aliases for user name

myAlias1 ✖ 🗑

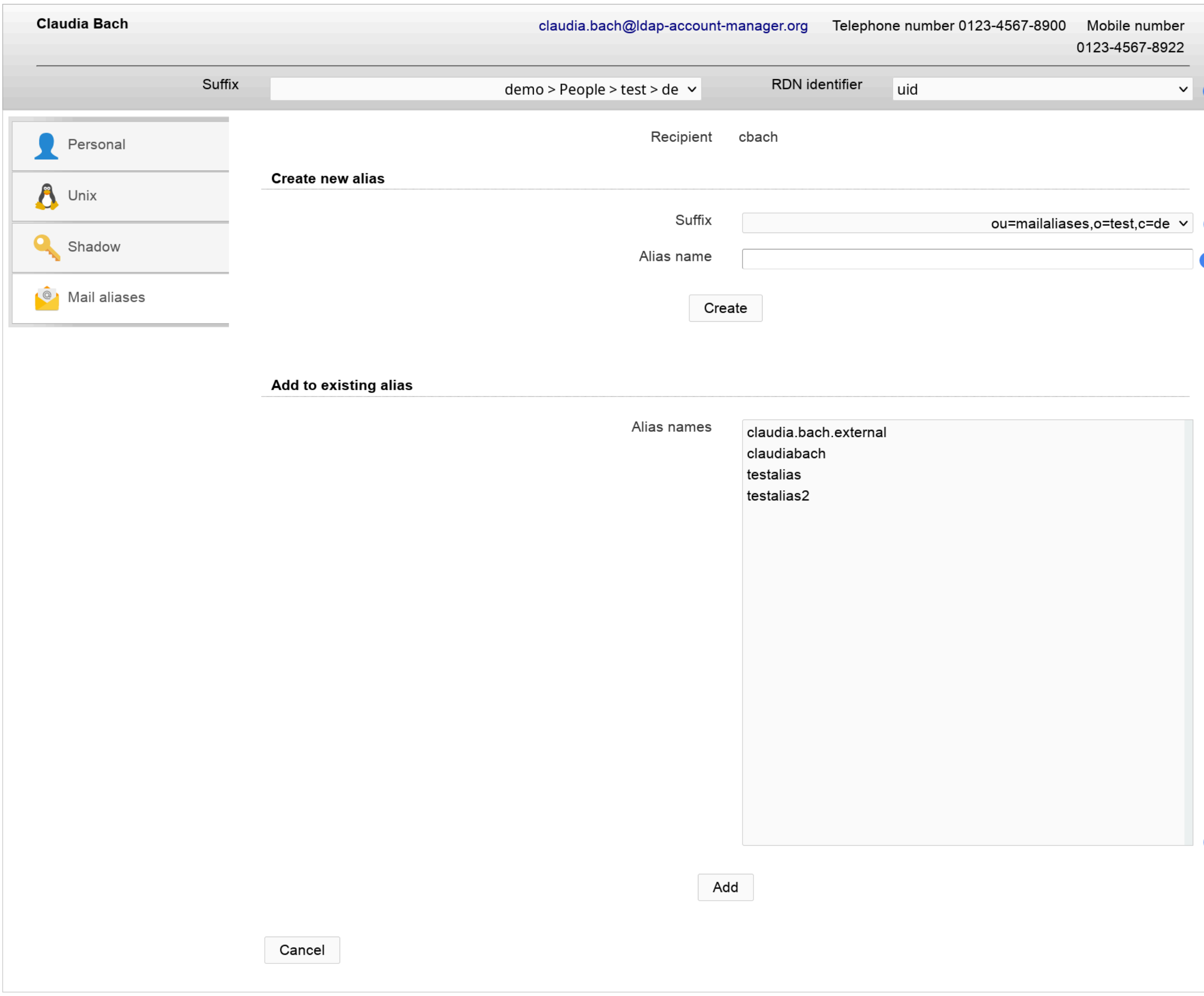
Add

Aliases for email

claudia.bach.external ✖ 🗑
claudiabach ✖ 🗑

Add

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



Claudia Bach

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

Suffix: demo > People > test > de

RDN identifier: uid

Recipient: cbach

Create new alias

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

Alias name:

Add to existing alias

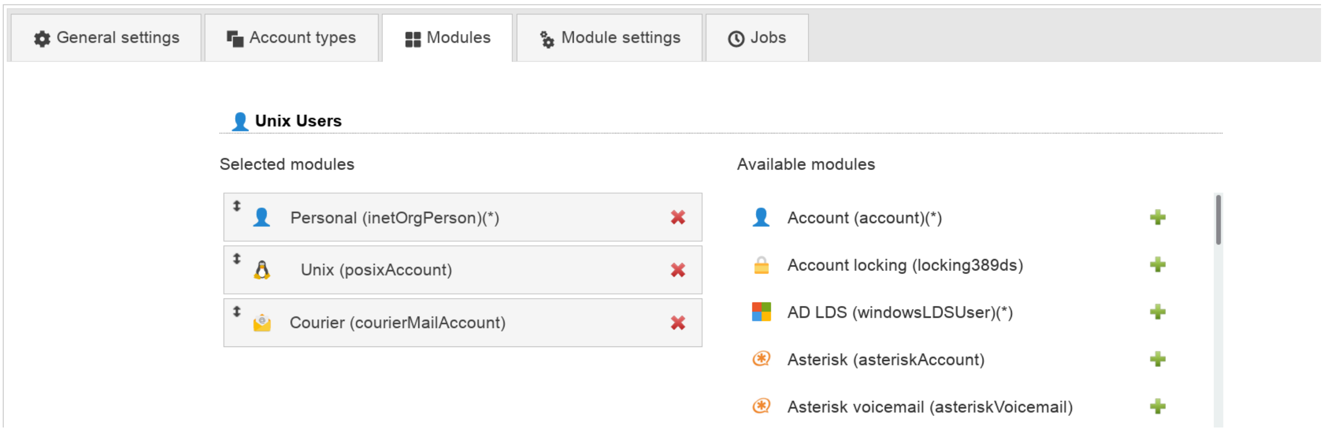
Alias names:
claudia.bach.external
claudiabach
testalias
testalias2

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.



Unix Users

Selected modules

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

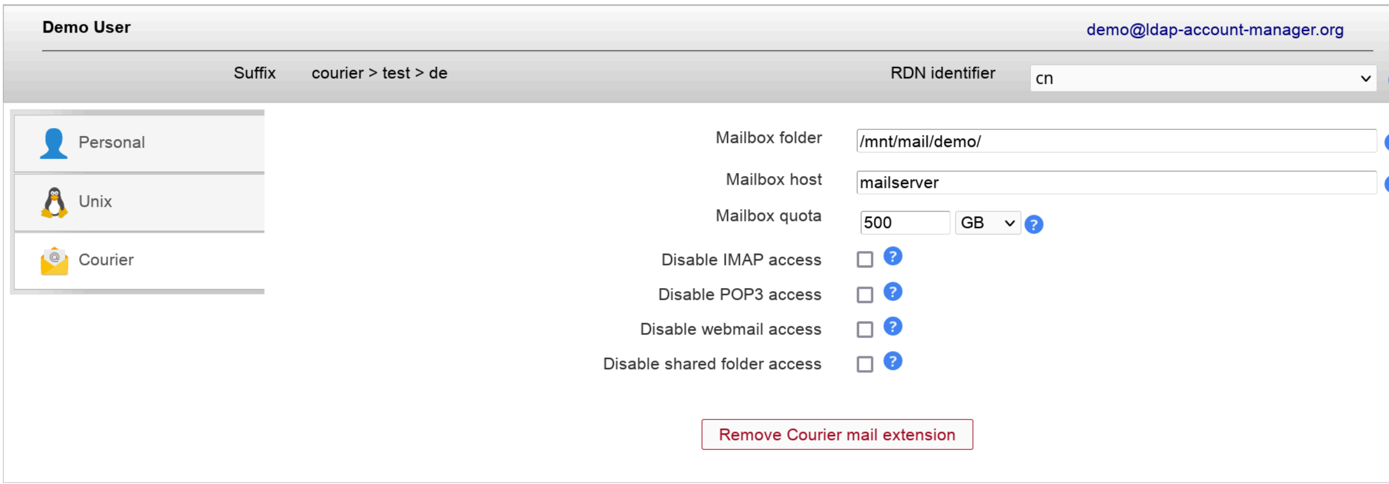
Available modules

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

Usage:

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

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



Suffix: courier > test > de

RDN identifier: cn

Mailbox folder: /mnt/mail/demo/

Mailbox host: mailserver

Mailbox quota: 500 GB

Disable IMAP access ☐

Disable POP3 access ☐

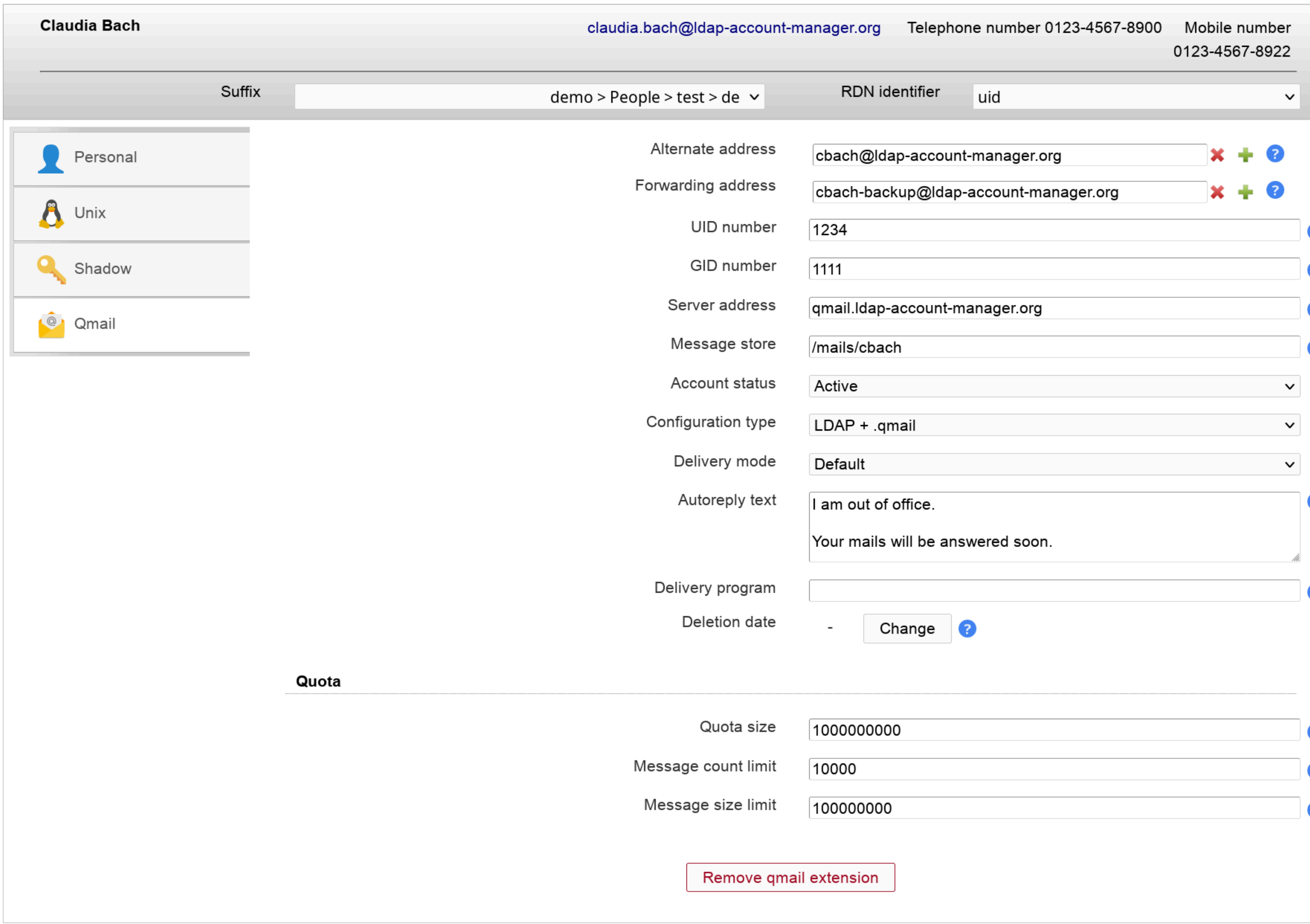
Disable webmail access ☐

Disable shared folder access ☐

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

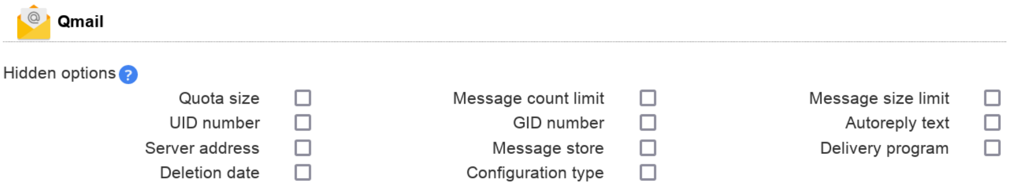
Suffix: demo > People > test > de
RDN identifier: uid

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	- Change

Quota

Quota size	1000000000
Message count limit	10000
Message size limit	100000000

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.



Qmail

Hidden options

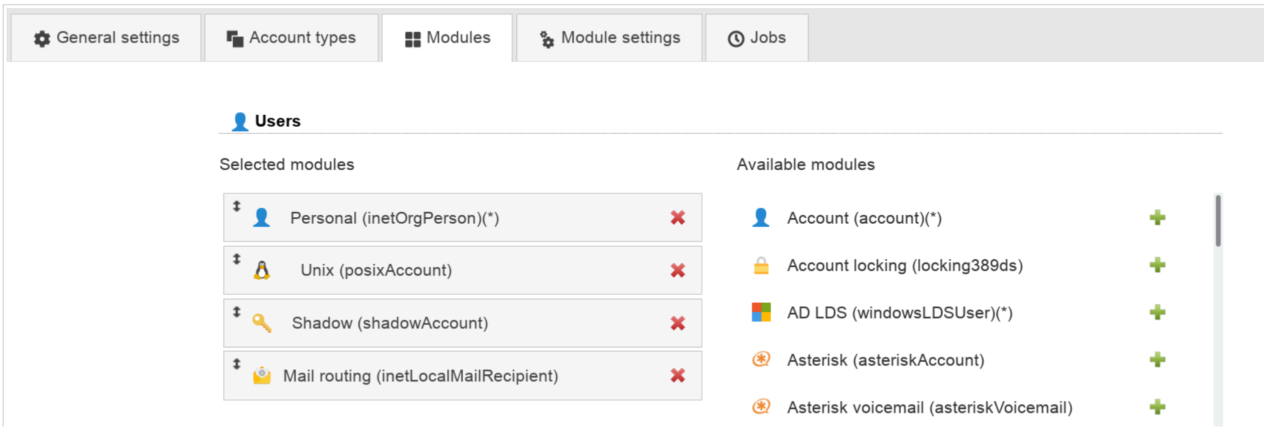
Quota size	☐	Message count limit	☐	Message size limit	☐
UID number	☐	GID number	☐	Autoreply text	☐
Server address	☐	Message store	☐	Delivery program	☐
Deletion date	☐	Configuration type	☐		

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.



Users

Selected modules

- Personal (inetOrgPerson)(*)
- Unix (posixAccount)
- Shadow (shadowAccount)
- Mail routing (inetLocalMailRecipient)

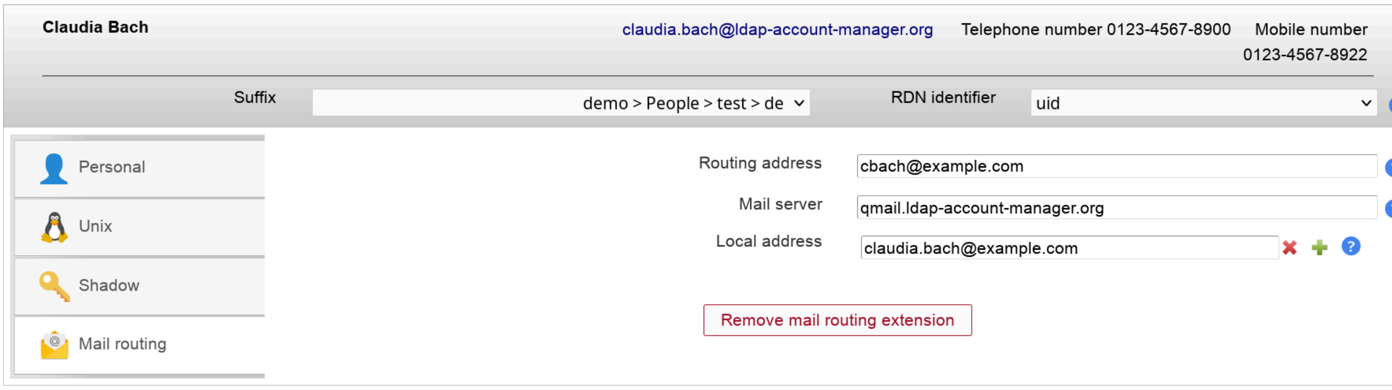
Available modules

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

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.



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

Routing address: cbach@example.com

Mail server: qmail.ldap-account-manager.org

Local address: claudia.bach@example.com

Wildcards

The module supports wildcards in the following input fields:

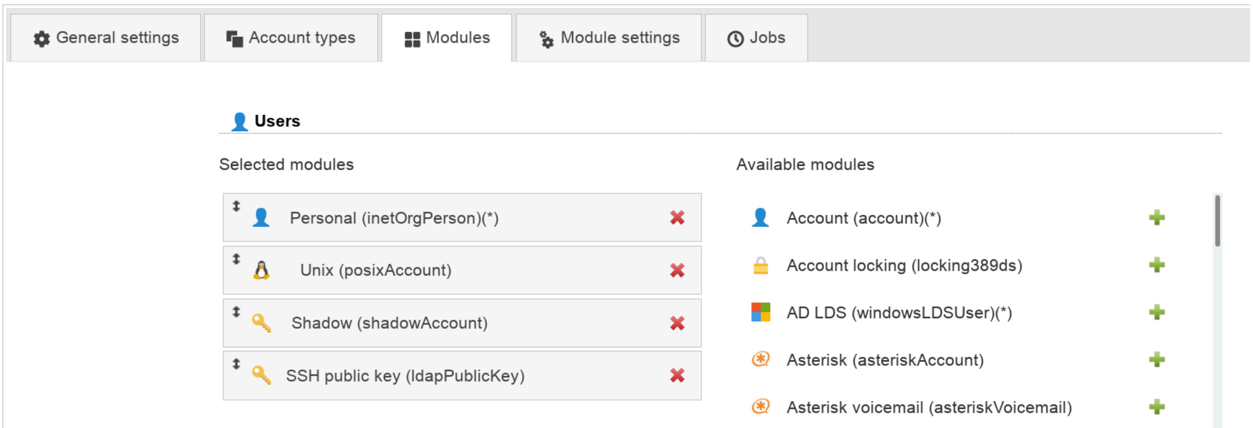
- Routing address
- Local address

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

SSH public keys

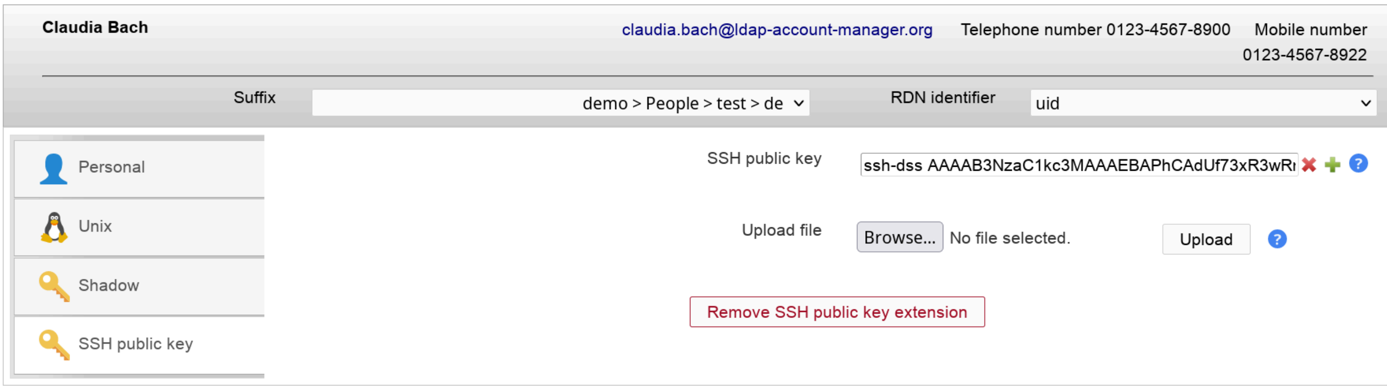
You can manage your public keys for SSH in LAM if you installed the LPK patch for SSH [http://code.google.com/p/openssh-lpk/] or setup AuthorizedKeysCommand (see below).

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



Selected modules:
- Personal (inetOrgPerson)(*)
- Unix (posixAccount)
- Shadow (shadowAccount)
- SSH public key (ldapPublicKey)

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



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

SSH public key: ssh-dss AAAAB3NzaC1kc3MAAAEBAPhCAdUf73xR3wRı

Upload file: No file selected.

Example for AuthorizedKeysCommand

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

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

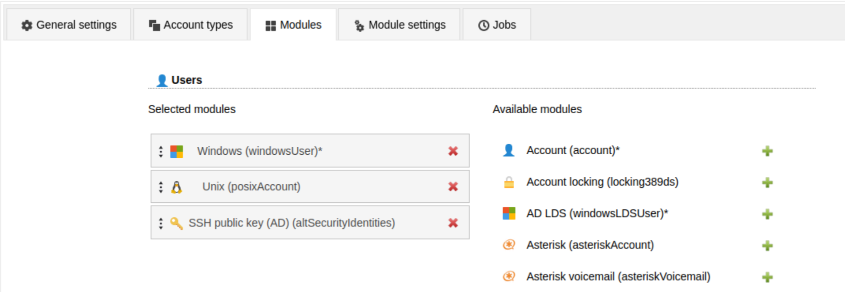
```
#!/bin/bash
uid=$1
server=ldap.domain.com
baseDN=ou=people,dc=example,dc=com
port=389
ldapsearch -x -h $server -p $port -b $baseDN -s sub "(&(objectclass=posixAccount)(uid=$uid))" | sed -n '/^ /{H;d};/sshPublicKey:
```

Now setup your sshd_config

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

SSH public keys (AD)

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



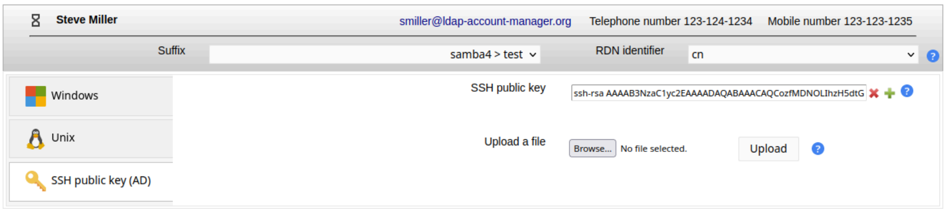
Users

Selected modules

- Windows (windowsUser)*
- Unix (posixAccount)
- SSH public key (AD) (altSecurityIdentities)

Available modules

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



Steve Miller smiller@ldap-account-manager.org Telephone number 123-124-1234 Mobile number 123-123-1235

Suffix: samba4 > test
RDN identifier: cn

SSH public key: ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAACAQCozfMDNOLIhzH5dtG

Upload a file: No file selected.

Example for AuthorizedKeysCommand

This will dynamically get the public key from LDAP.

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

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

Now setup your sshd_config

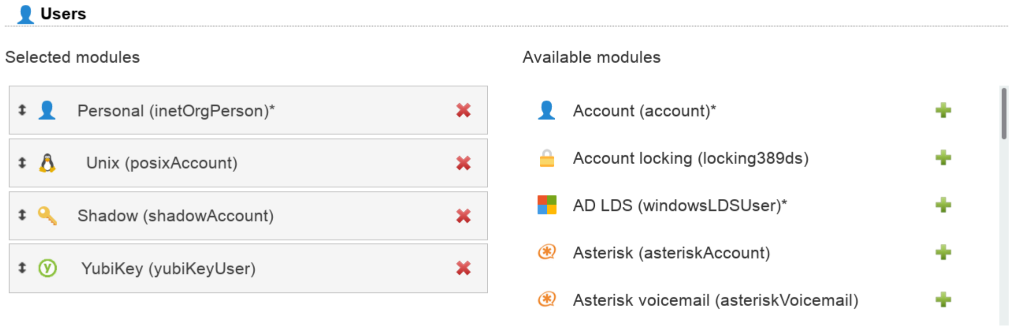
```
AuthorizedKeysCommand /usr/bin/ldapAuthSSH.sh
AuthorizedKeysCommandUser root
```

YubiKey

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

Configuration

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


Users

Selected modules

- Personal (inetOrgPerson)*
- Unix (posixAccount)
- Shadow (shadowAccount)
- YubiKey (yubiKeyUser)

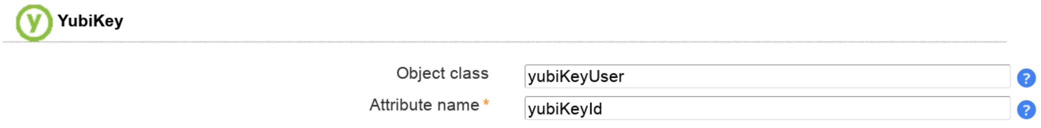
Available modules

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

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

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

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

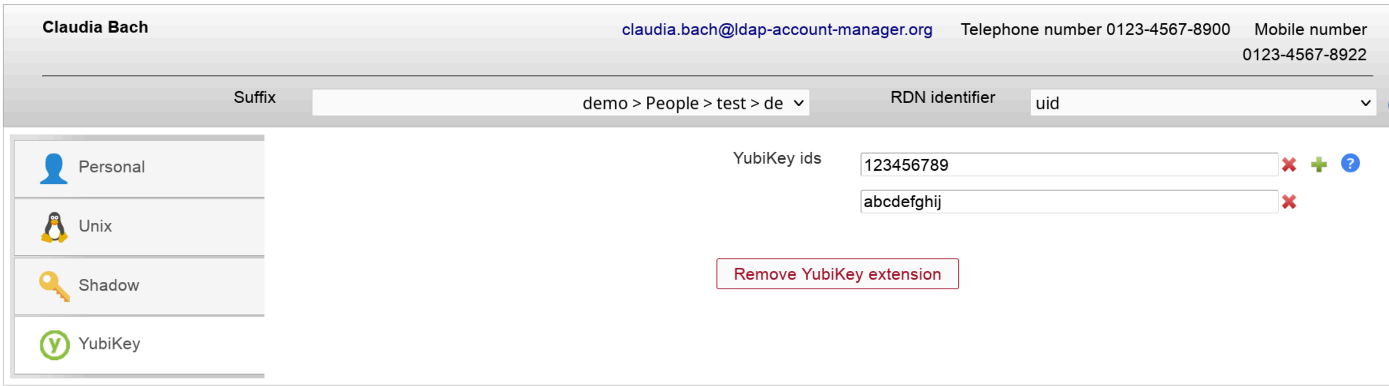


YubiKey

Object class: yubiKeyUser

Attribute name *: yubiKeyId

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



Claudia Bach

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

Suffix: demo > People > test > de

RDN identifier: uid

YubiKey ids: 123456789

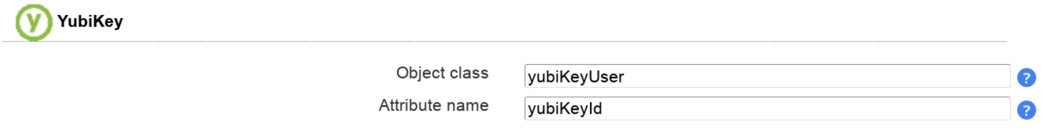
abcdefghij

Self Service (LAM Pro)

This will allow your users to update their own keys.

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

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

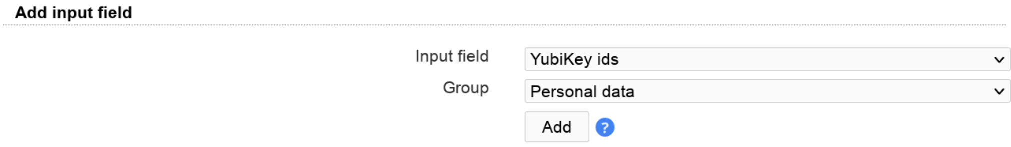


YubiKey

Object class: yubiKeyUser

Attribute name: yubiKeyId

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

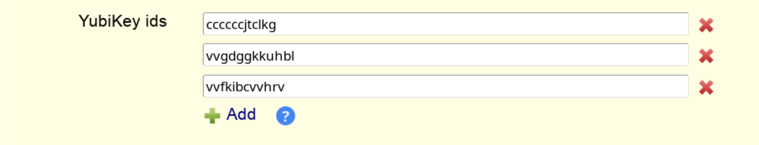


Add input field

Input field: YubiKey ids

Group: Personal data

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



YubiKey ids: ccccccjtclkg

vvgdggkkuhbl

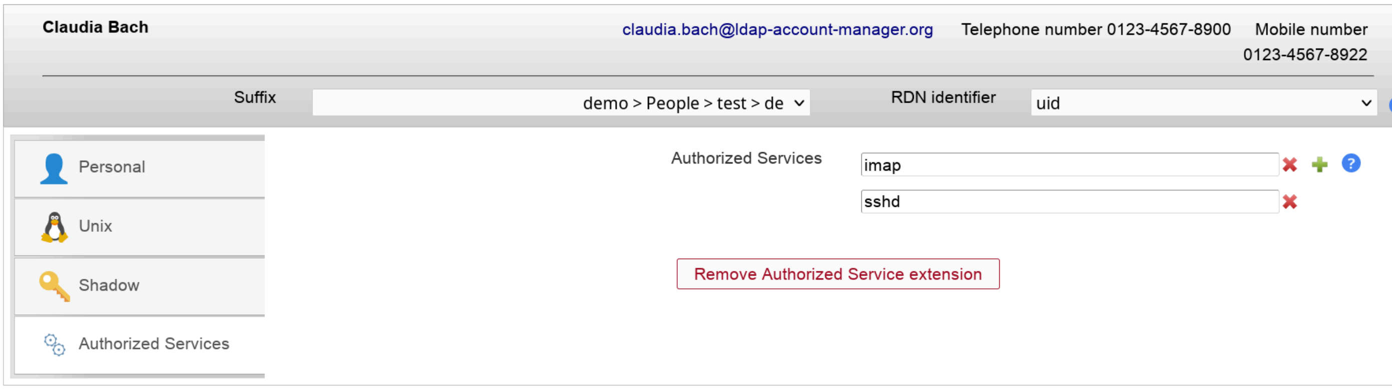
vvfkibcvvhrv

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.



Claudia Bach

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

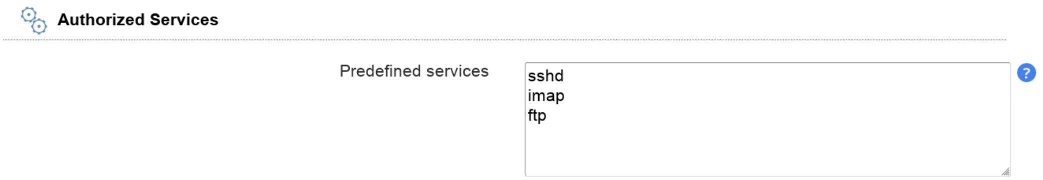
Suffix: demo > People > test > de

RDN identifier: uid

Authorized Services: imap

sshd

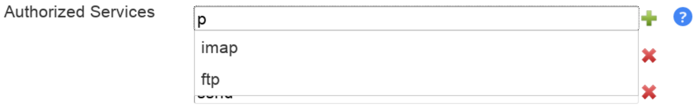
You can define a list of services in your LAM server profile that is used for autocompletion.



Authorized Services

Predefined services:
sshd
imap
ftp

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.

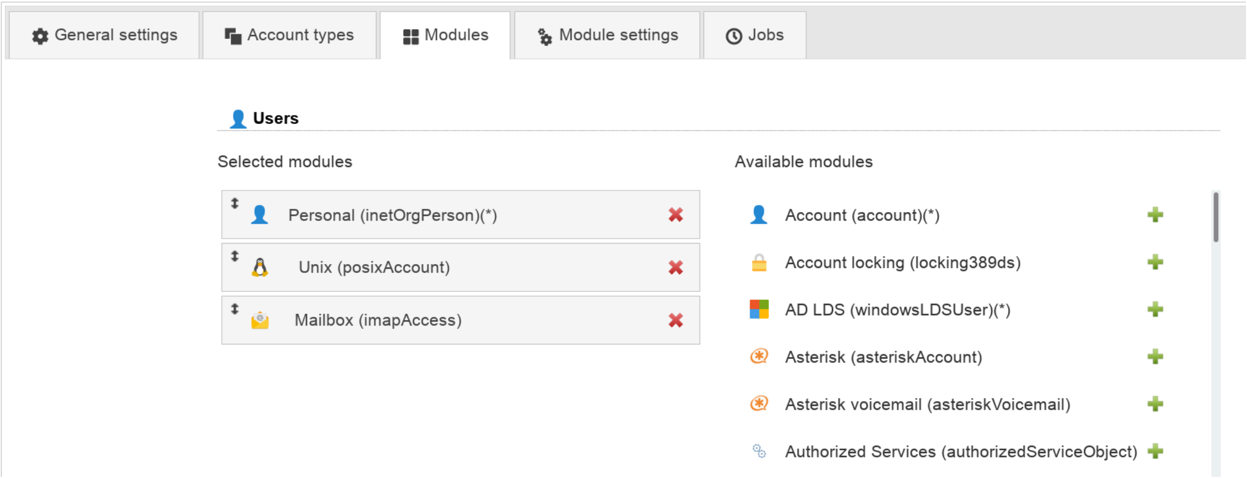


Authorized Services: p

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:



Users

Selected modules

- Personal (inetOrgPerson)(*)
- Unix (posixAccount)
- Mailbox (imapAccess)

Available modules

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

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

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

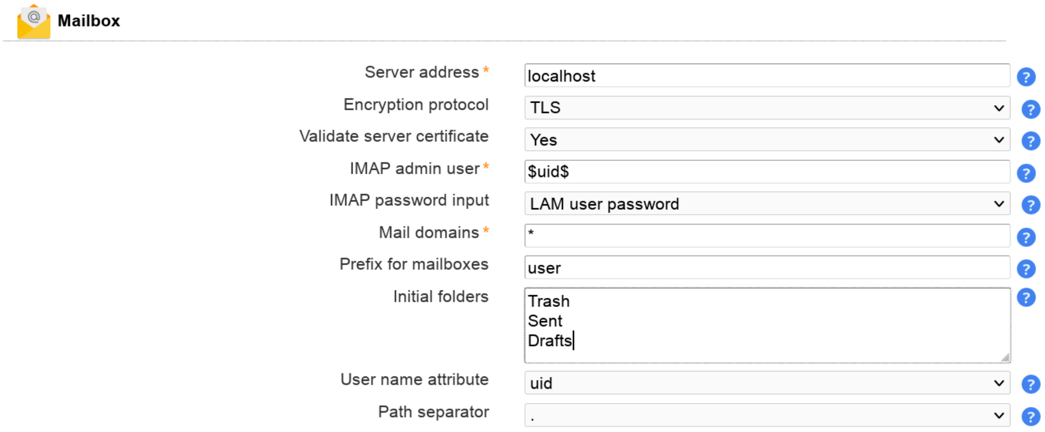
The mail domains specify for which accounts mailboxes may be created/deleted. E.g. if you enter "lam-demo.org" then mailboxes can be managed for "user@lam-demo.org" but not for "user@example.com". Use "*" for any domain.

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

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

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

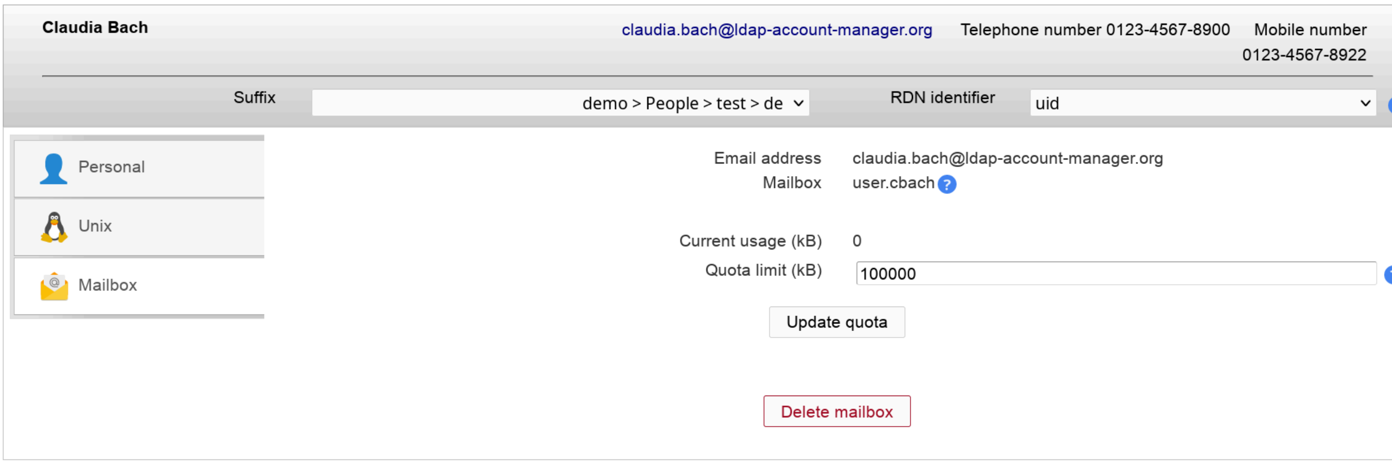
You can specify a list of initial folder names to create for new mailboxes. LAM will then create them with each new mailbox.


Mailbox

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

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

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


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

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

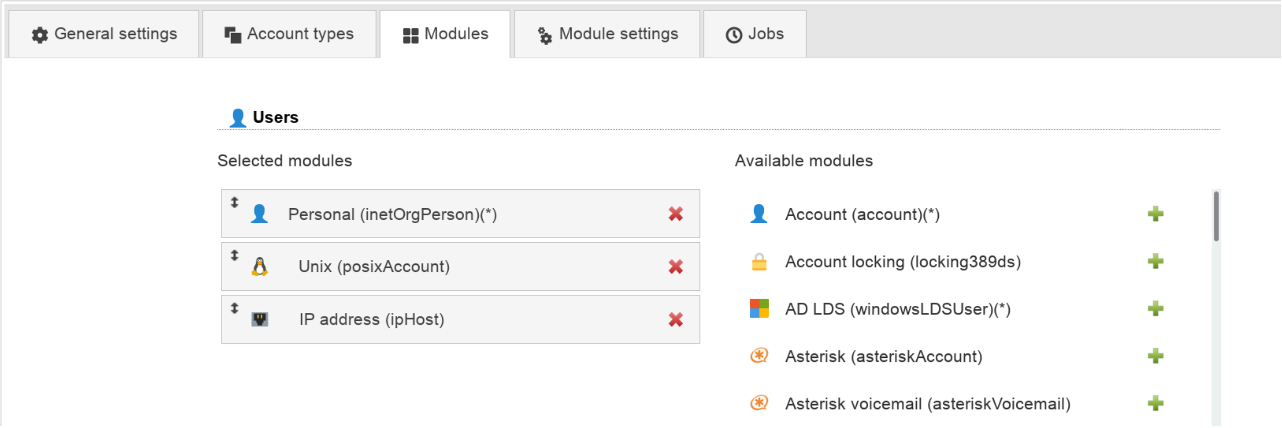
Email address: claudia.bach@ldap-account-manager.org
Mailbox: user.cbach

Current usage (kB): 0
Quota limit (kB): 100000

IP addresses (LAM Pro)

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

Configuration

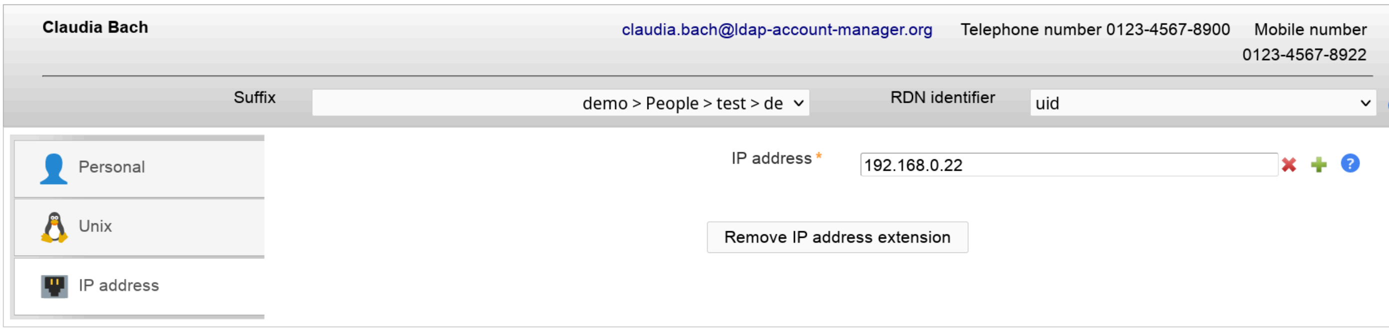


Users

Selected modules
- Personal (inetOrgPerson)(*)
- Unix (posixAccount)
- IP address (ipHost)

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

User editing


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

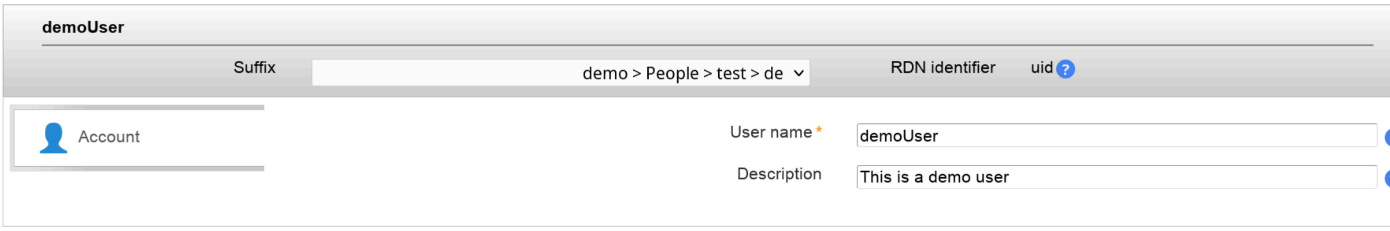
Suffix: demo > People > test > de
RDN identifier: uid

IP address *: 192.168.0.22

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.



demoUser

Suffix: demo > People > test > de

RDN identifier: uid

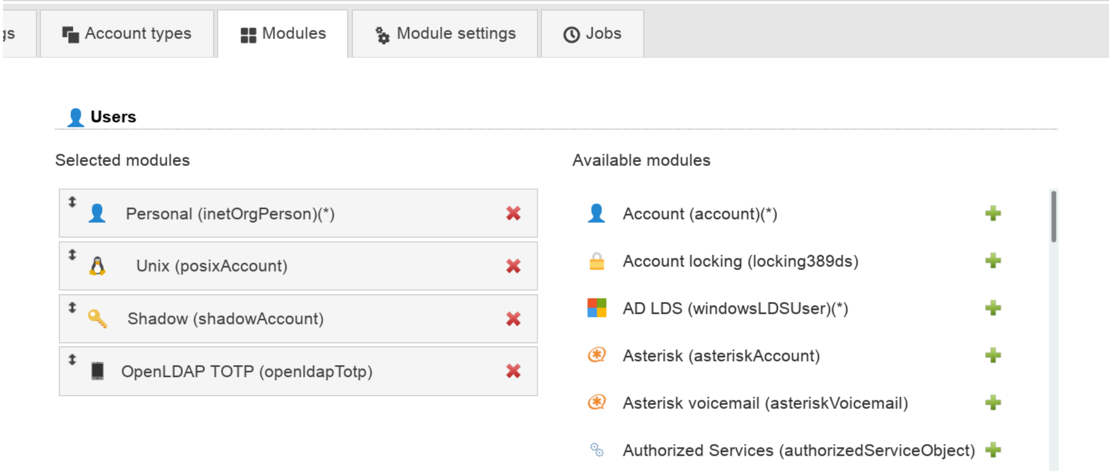
User name *: demoUser

Description: This is a demo user

OpenLDAP TOTP (LAM Pro)

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

For admin interface add the OpenLDAP TOTP module:



Selected modules

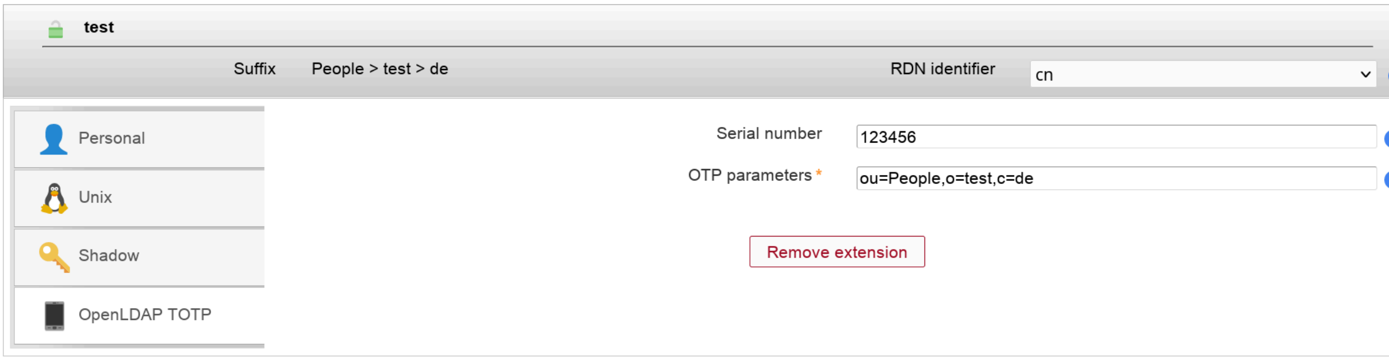
- Personal (inetOrgPerson)(*)
- Unix (posixAccount)
- Shadow (shadowAccount)
- OpenLDAP TOTP (openldapTotp)

Available modules

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

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

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



test

Suffix: People > test > de

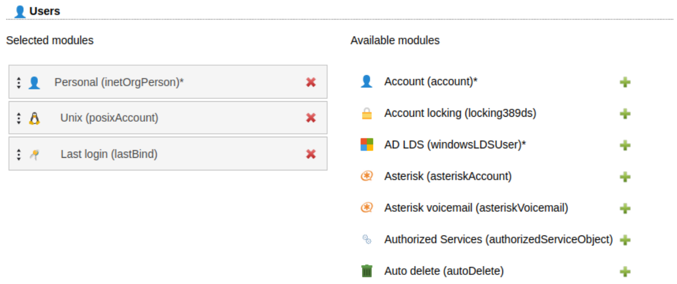
RDN identifier: cn

Serial number: 123456

OTP parameters *: ou=People,o=test,c=de

Last login (LAM Pro)

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



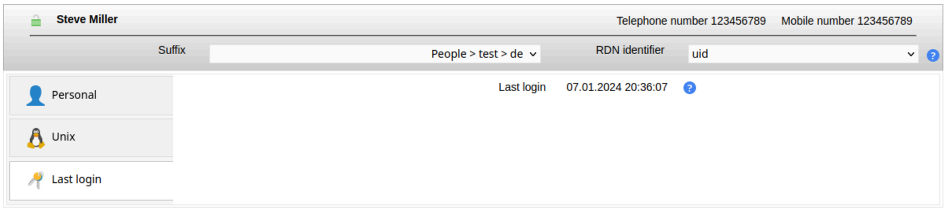
Users

Selected modules

- Personal (inetOrgPerson)*
- Unix (posixAccount)
- Last login (lastBind)

Available modules

- Account (account)*
- Account locking (locking389ds)
- AD LDS (windowsLDSUser)*
- Asterisk (asteriskAccount)
- Asterisk voicemail (asteriskVoicemail)
- Authorized Services (authorizedServiceObject)
- Auto delete (autoDelete)



Steve Miller — Telephone number 123456789 — Mobile number 123456789

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

Last login: 07.01.2024 20:36:07

TAK

The TAK [https://www.civtak.org/] module supports the Team Awareness Kit or Tactical Assault Kit (TAK) with the Android Team Awareness Kit (ATAK).

You can define callsigns, team roles and colors for users.

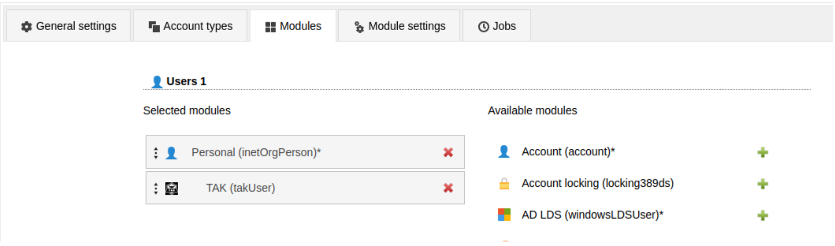
LDAP schema

The module expects that TAK users use the object class "takUser" and the attributes "takCallsign", "takRole" and "takColor". You can find matching schema files in /usr/share/ldap-account-manager/docs/schema (DEB/RPM) or docs/schema (tar.bz2). Please see the beginning of the files for installation instructions.

- OpenLDAP: tak-OpenLDAP.ldif
- Samba 4: tak-Samba4-attributes.ldif and tak-Samba4-objectClass.ldif
- Windows (AD): tak-Windows.ldif

Configuration

Add the TAK module for users in your server profile:



Users 1

Selected modules

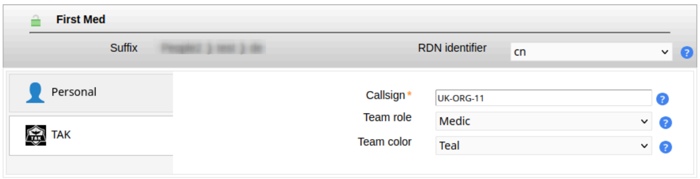
- Personal (inetOrgPerson)*
- TAK (takUser)

Available modules

- Account (account)*
- Account locking (locking389ds)
- AD LDS (windowsLDSUser)*

Now you can manage the TAK attributes for users.

LAM Pro users can add these attributes to the self-service profile if needed.



First Med

Suffix: [redacted] — RDN identifier: cn

Callsign*: UK-ORG-11

Team role: Medic

Team color: Teal

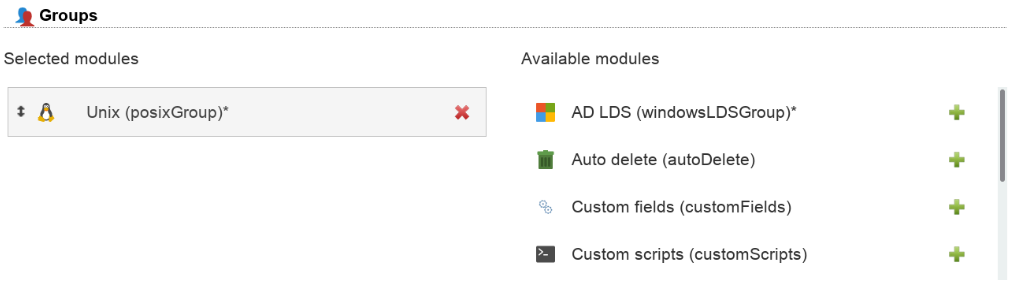
Groups

Unix

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

Configuration

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



Groups

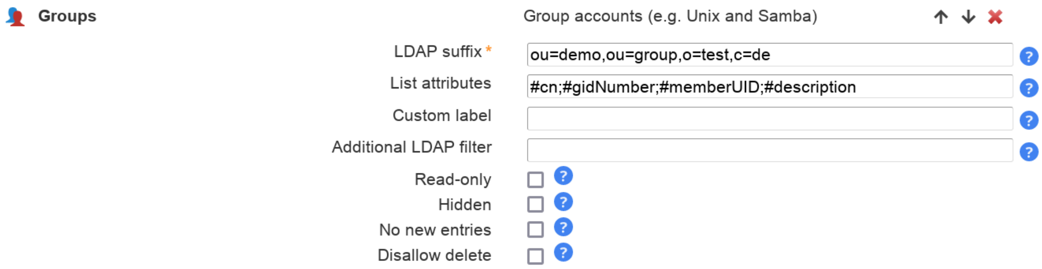
Selected modules

- Unix (posixGroup)*

Available modules

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

Virtual list attributes:



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

LDAP suffix*	ou=demo,ou=group,o=test,c=de
List attributes	#cn;#gidNumber;#memberUID;#description
Custom label	
Additional LDAP filter	
Read-only	□
Hidden	□
No new entries	□
Disallow delete	□

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

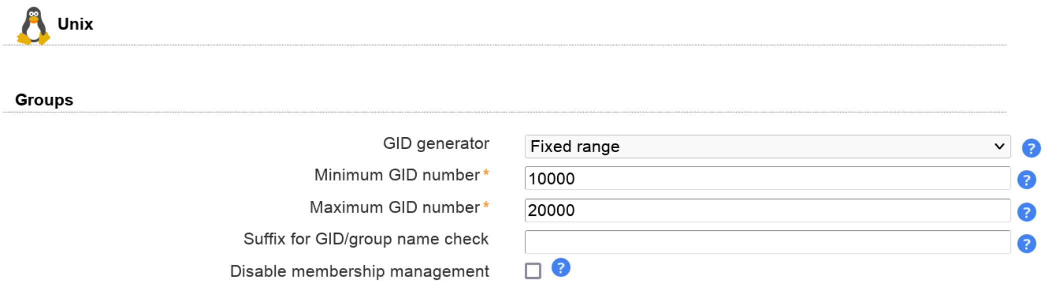
- memberuid_count: number of entries in attribute "memberuid"
- member_count: number of entries in attribute "member"
- uniqueMember_count: number of entries in attribute "uniquemember"
- owner_count: number of entries in attribute "owner"
- roleOccupant_count: number of entries in attribute "roleOccupant"

Module settings:

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

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

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

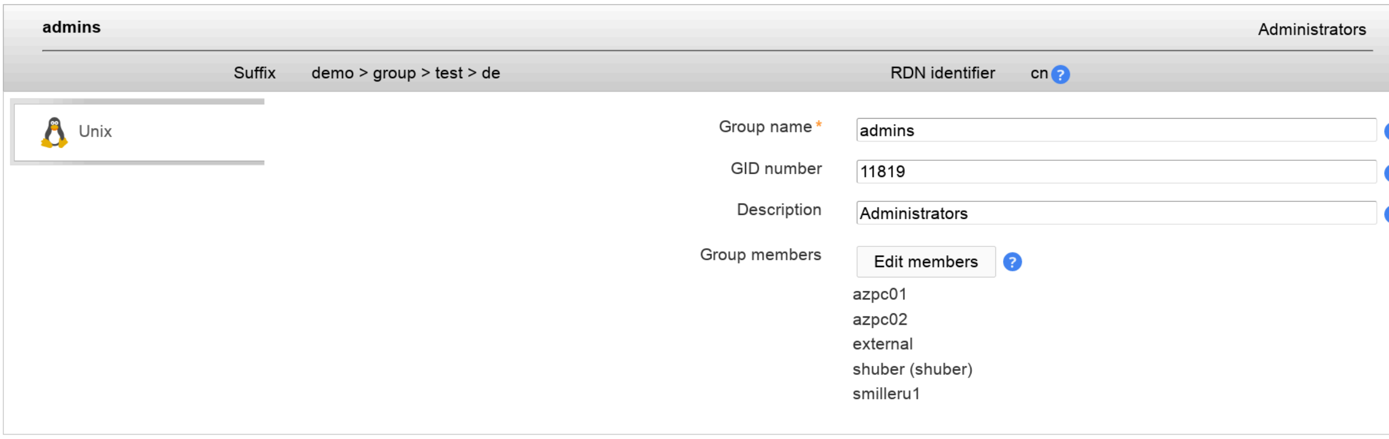


Unix

Groups

GID generator	Fixed range
Minimum GID number*	10000
Maximum GID number*	20000
Suffix for GID/group name check	
Disable membership management	□

Group management:

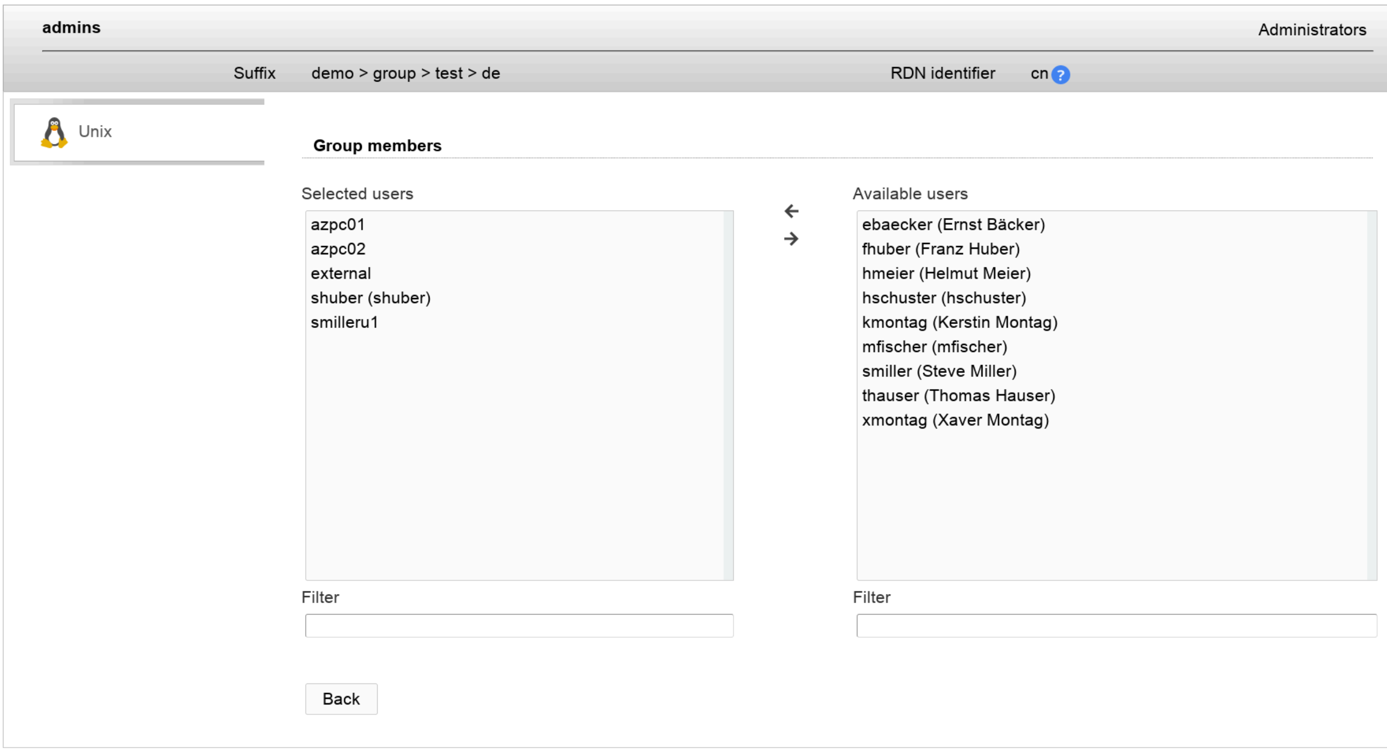


admins Administrators

Suffix demo > group > test > de RDN identifier cn

Group name*	admins
GID number	11819
Description	Administrators
Group members	Edit members azpc01 azpc02 external shuber (shuber) smilleru1

Group membership management:



admins Administrators

Suffix demo > group > test > de RDN identifier cn

Group members

Selected users	Available users
azpc01	ebaecker (Ernst Bäcker)
azpc02	fhuber (Franz Huber)
external	hmeier (Helmut Meier)
shuber (shuber)	hschuster (hschuster)
smilleru1	kmontag (Kerstin Montag)
	mfischer (mfischer)
	smiller (Steve Miller)
	thauser (Thomas Hauser)
	xmontag (Xaver Montag)

Filter Filter

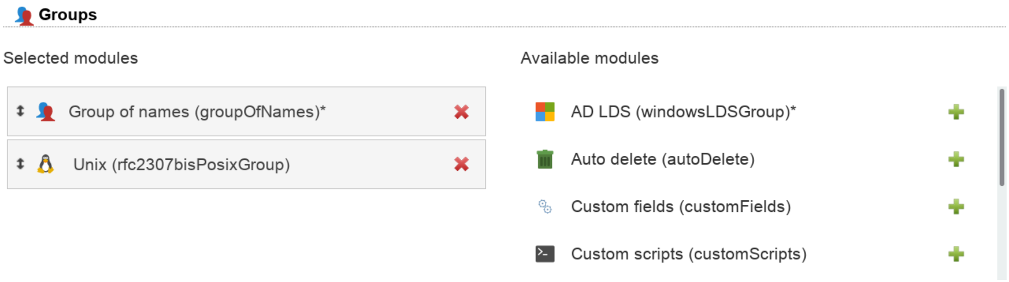
Unix groups with rfc2307bis schema (LAM Pro)

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

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

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

Module activation:



Groups

Selected modules

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

Available modules

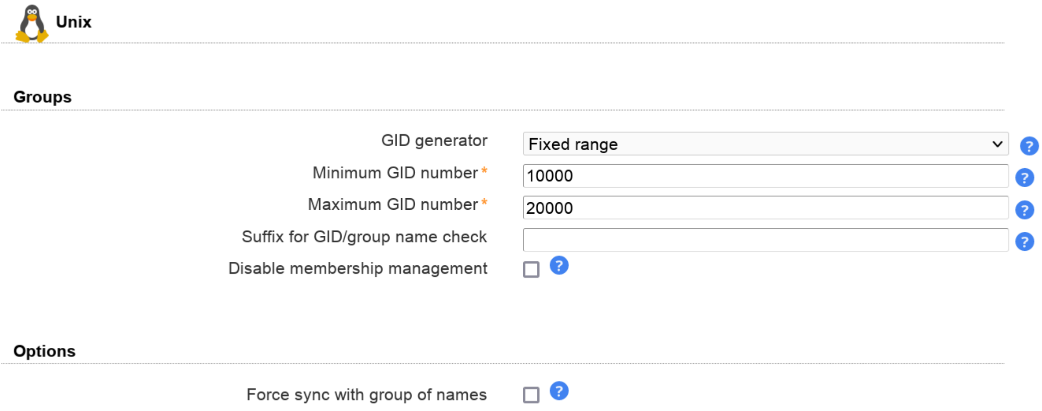
- AD LDS (windowsLDSGroup)*
- Auto delete (autoDelete)
- Custom fields (customFields)
- Custom scripts (customScripts)

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

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

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

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



Unix

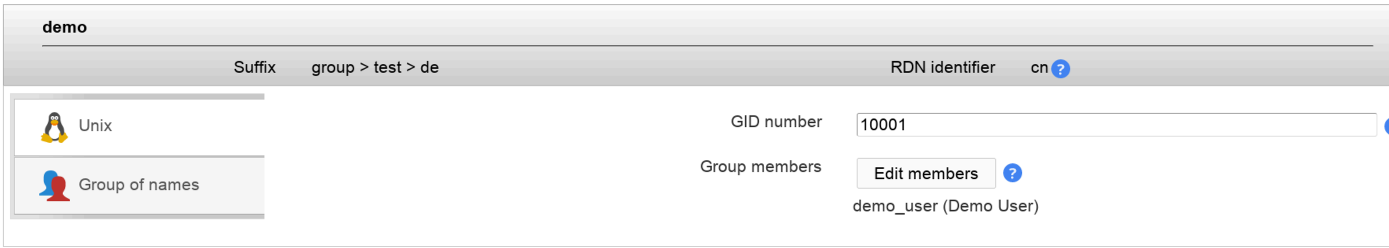
Groups

GID generator: Fixed range
Minimum GID number*: 10000
Maximum GID number*: 20000
Suffix for GID/group name check:
Disable membership management □

Options

Force sync with group of names □

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



demo

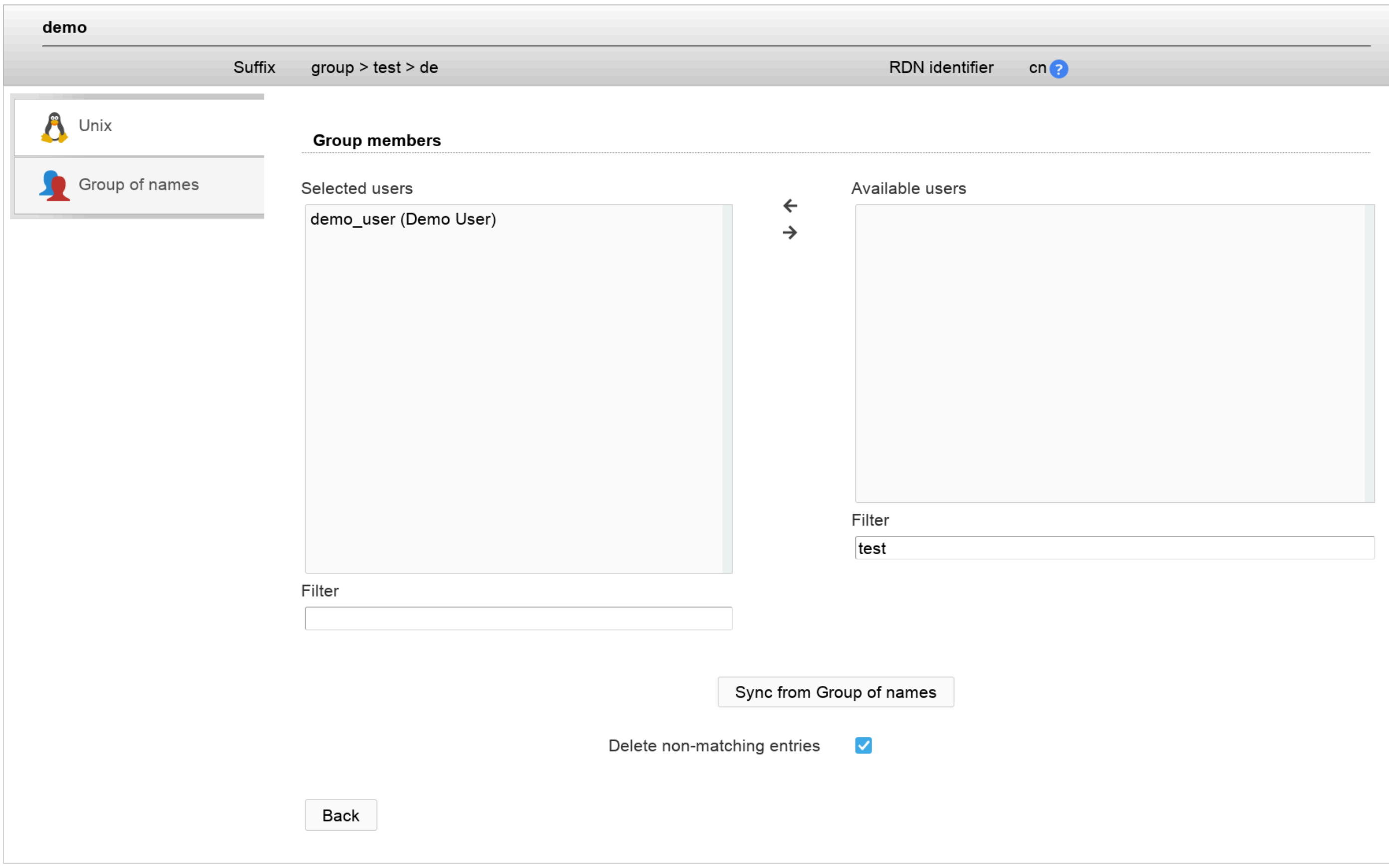
Suffix group > test > de RDN identifier cn

GID number 10001

Group members

demo_user (Demo User)

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



demo

Suffix group > test > de RDN identifier cn

Selected users

demo_user (Demo User)

Filter

Available users

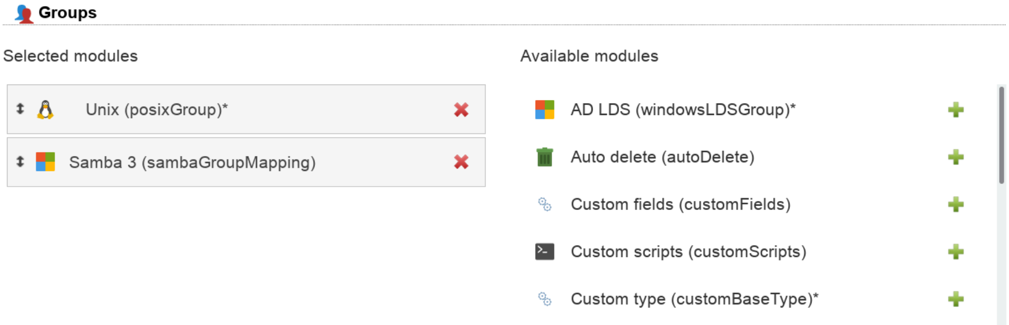
Filter test

Delete non-matching entries ☑

Samba 3

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

Module activation:



Groups

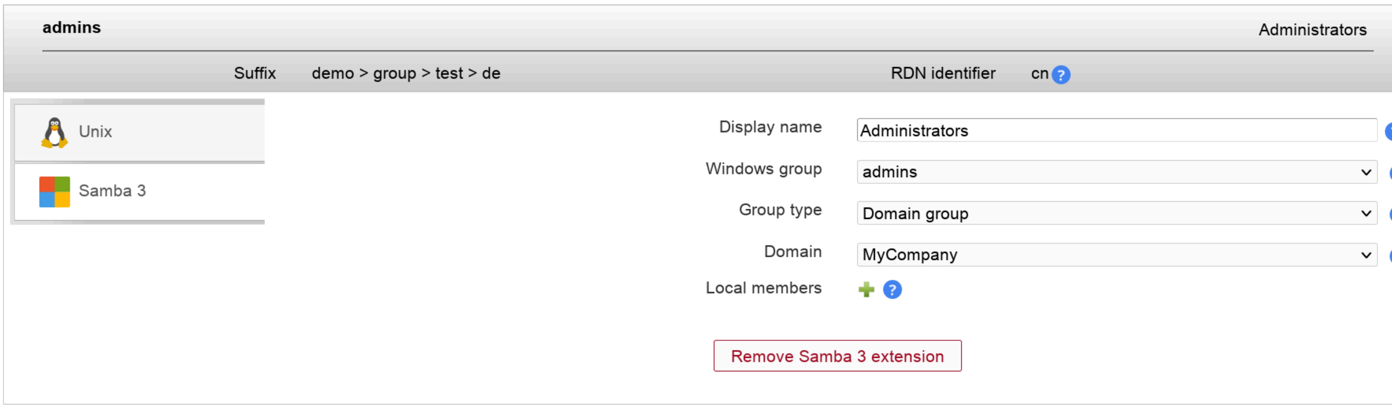
Selected modules

- Unix (posixGroup)*
- Samba 3 (sambaGroupMapping)

Available modules

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

Group editing:



admins — Administrators

Suffix: demo > group > test > de — RDN identifier: cn

Display name: Administrators

Windows group: admins

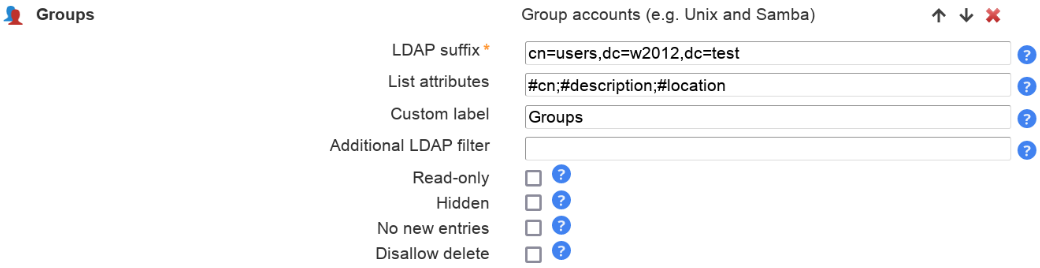
Group type: Domain group

Domain: MyCompany

Local members

Windows (Samba 4)

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



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

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

List attributes: #cn;#description;#location

Custom label: Groups

Additional LDAP filter:

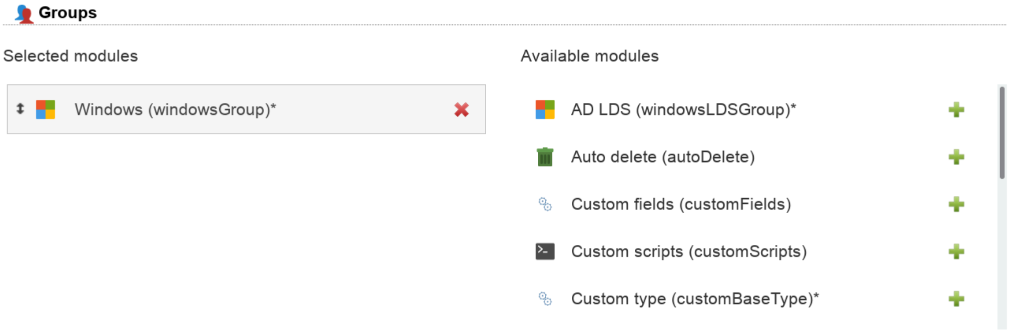
Read-only ☐

Hidden ☐

No new entries ☐

Disallow delete ☐

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



Groups

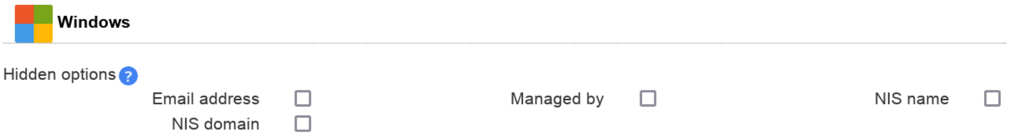
Selected modules:

- Windows (windowsGroup)*

Available modules:

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

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



Windows

Hidden options

Email address ☐ Managed by ☐ NIS name ☐

NIS domain ☐

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:

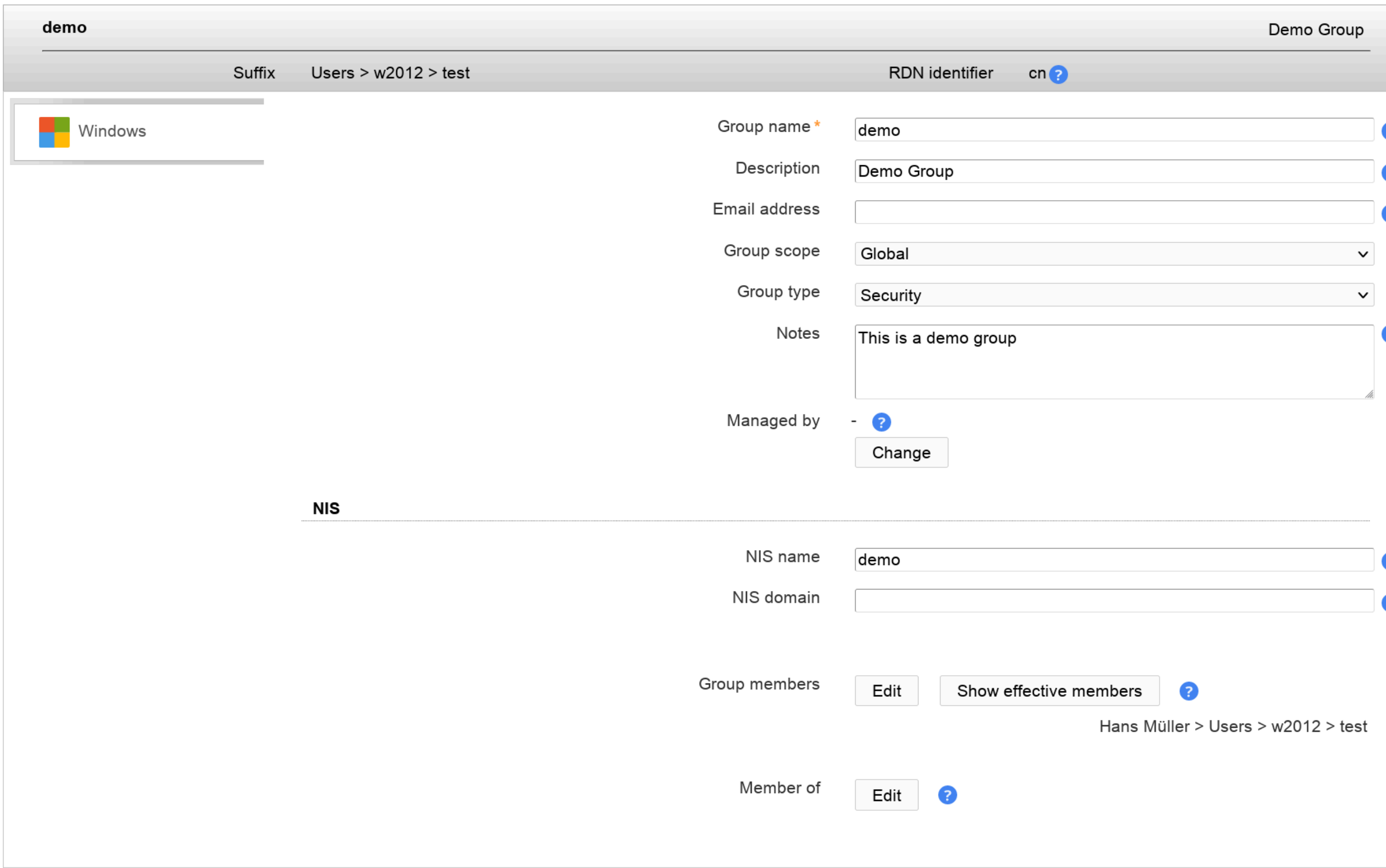
- Global: Use this for groups with frequent changes. Global groups are not replicated to other domains.

- 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.

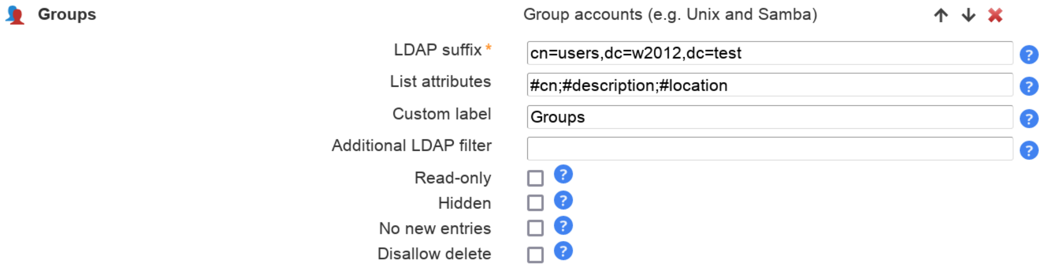


Suffix Users > w2012 > test
RDN identifier cn

Group name* demo
Description Demo Group
Email address
Group scope Global
Group type Security
Notes This is a demo group
Managed by -
NIS name demo
NIS domain
Group members Hans Müller > Users > w2012 > test
Member of

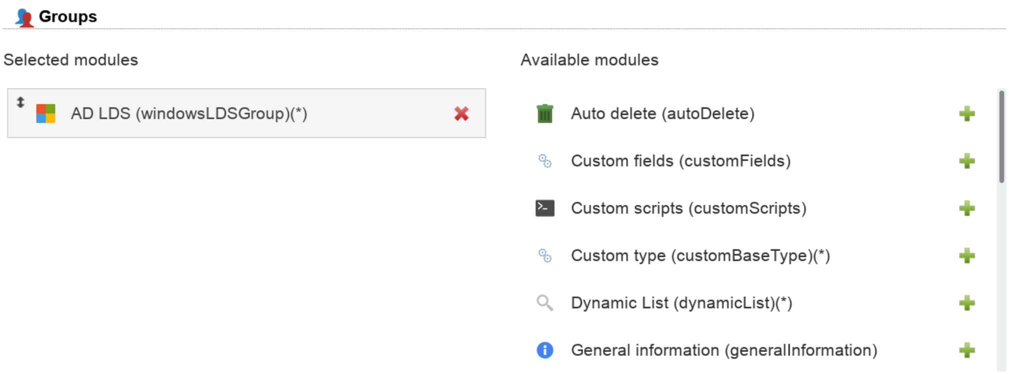
AD LDS (formerly ADAM) (LAM Pro)

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



LDAP suffix* cn=users,dc=w2012,dc=test
List attributes #cn;#description;#location
Custom label Groups
Additional LDAP filter
Read-only □
Hidden □
No new entries □
Disallow delete □

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



Groups

Selected modules

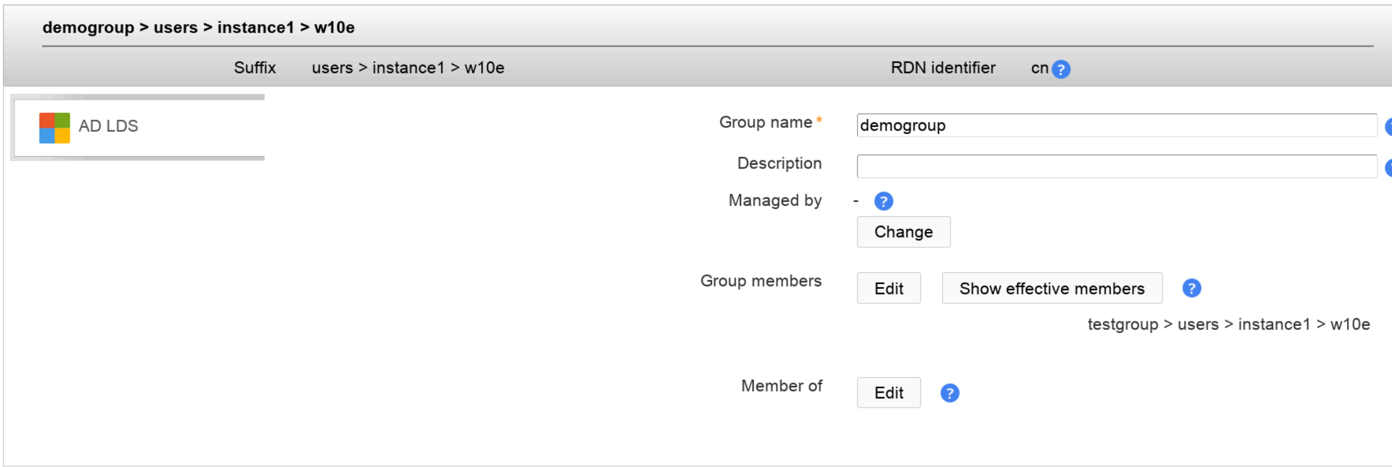
- AD LDS (windowsLDSGroup)(*)

Available modules

- Auto delete (autoDelete)
- Custom fields (customFields)
- Custom scripts (customScripts)
- Custom type (customBaseType)(*)
- Dynamic List (dynamicList)(*)
- General information (generalInformation)

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

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



demogroup > users > instance1 > w10e

Suffix users > instance1 > w10e RDN identifier cn

AD LDS

Group name * demogroup

Description

Managed by -

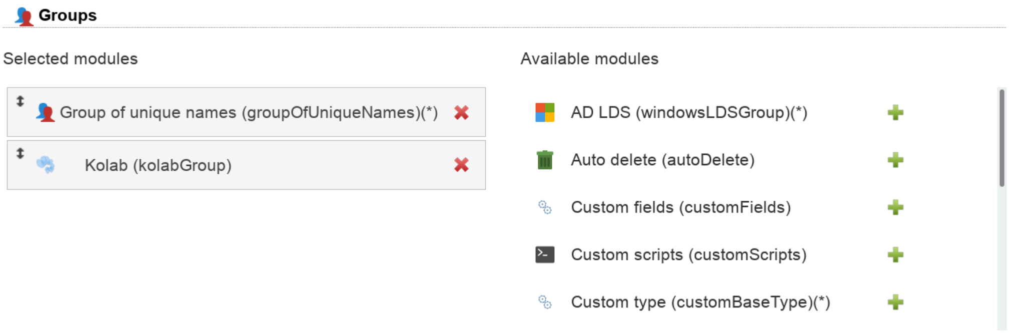
Group members

testgroup > users > instance1 > w10e

Member of

Kolab

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



Groups

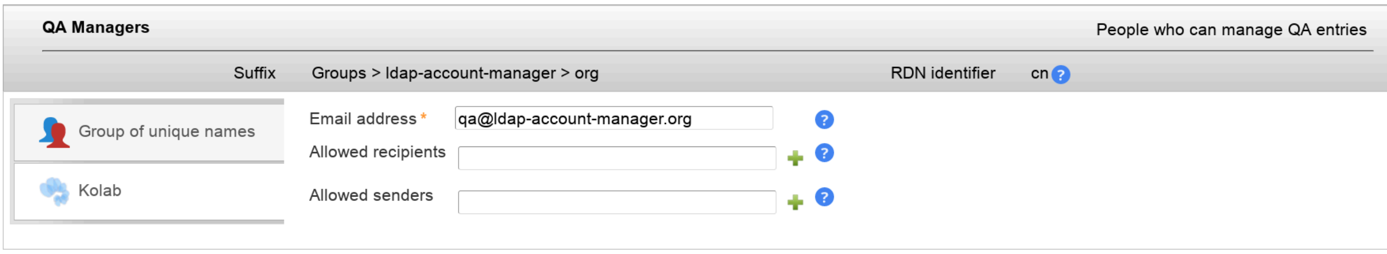
Selected modules

- Group of unique names (groupOfUniqueNames)(*)
- Kolab (kolabGroup)

Available modules

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

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



QA Managers — People who can manage QA entries

Suffix: Groups > ldap-account-manager > org — RDN identifier: cn

Email address *: qa@ldap-account-manager.org

Allowed recipients:

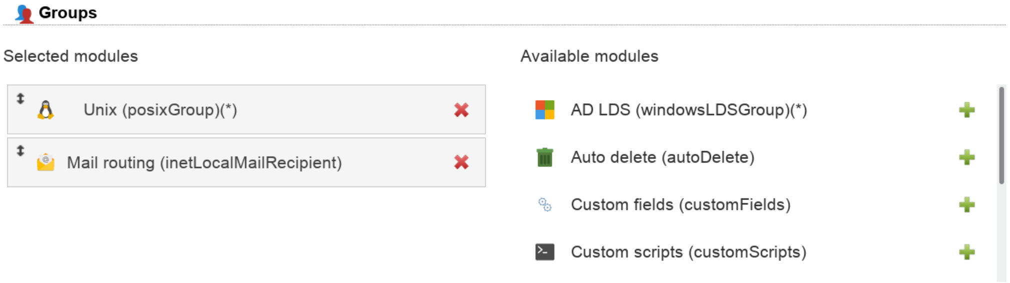
Allowed senders:

Mail routing

LAM supports to manage mail routing for group accounts.

Module activation:

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



Groups

Selected modules:

- Unix (posixGroup)(*)
- Mail routing (inetLocalMailRecipient)

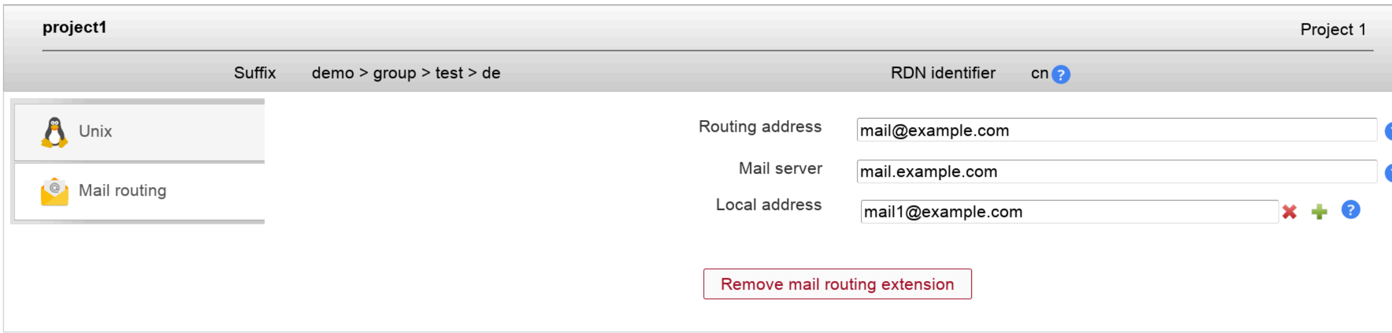
Available modules:

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

Usage:

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

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



project1 — Project 1

Suffix: demo > group > test > de — RDN identifier: cn

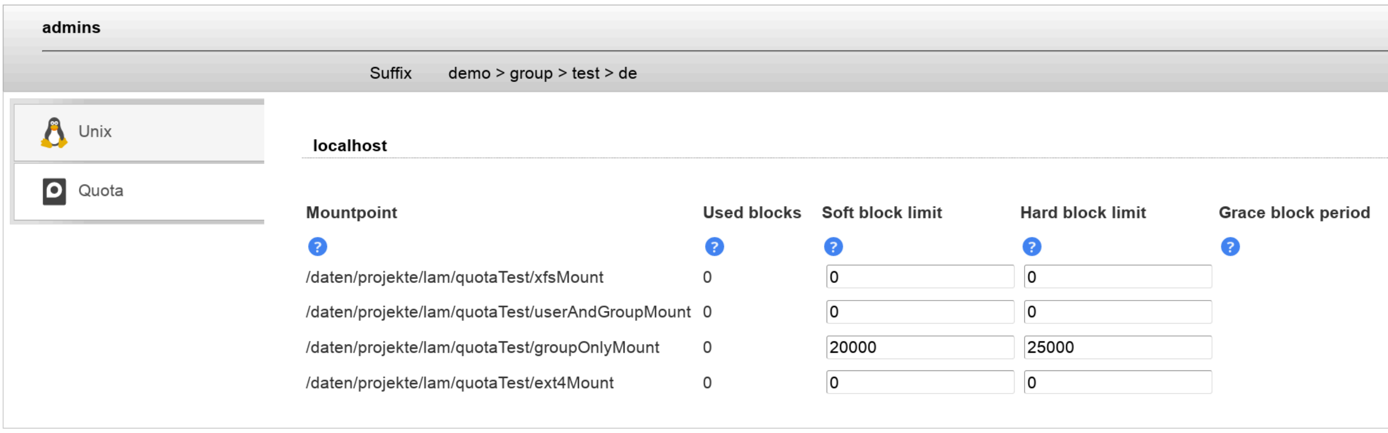
Routing address: mail@example.com

Mail server: mail.example.com

Local address: mail1@example.com

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.



Mountpoint	Used blocks	Soft block limit	Hard block limit	Grace block period
/daten/projekte/lam/quotaTest/xfsMount	0	0	0	
/daten/projekte/lam/quotaTest/userAndGroupMount	0	0	0	
/daten/projekte/lam/quotaTest/groupOnlyMount	0	20000	25000	
/daten/projekte/lam/quotaTest/ext4Mount	0	0	0	

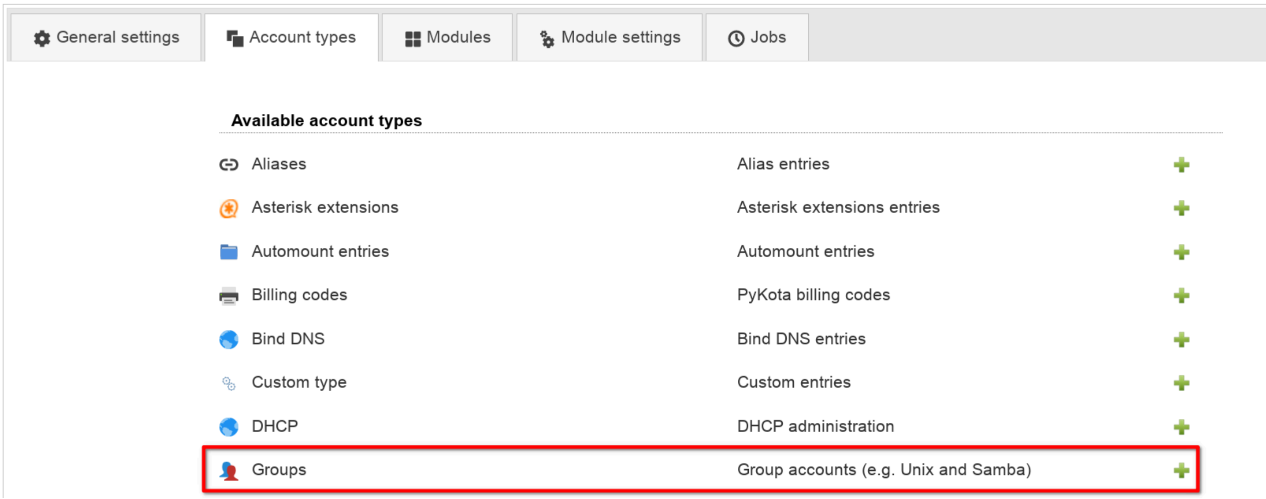
Dynamic lists (LAM Pro)

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

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

Configuration

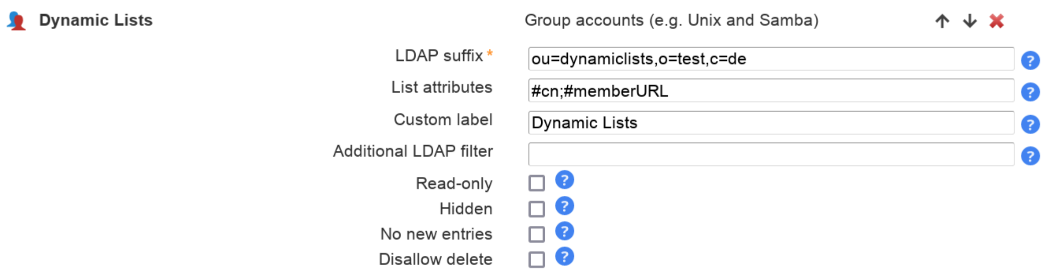
Add a new group account type and set a unique label for it.



Available account types

Aliases	Alias entries
Asterisk extensions	Asterisk extensions entries
Automount entries	Automount entries
Billing codes	PyKota billing codes
Bind DNS	Bind DNS entries
Custom type	Custom entries
DHCP	DHCP administration
Groups	Group accounts (e.g. Unix and Samba)

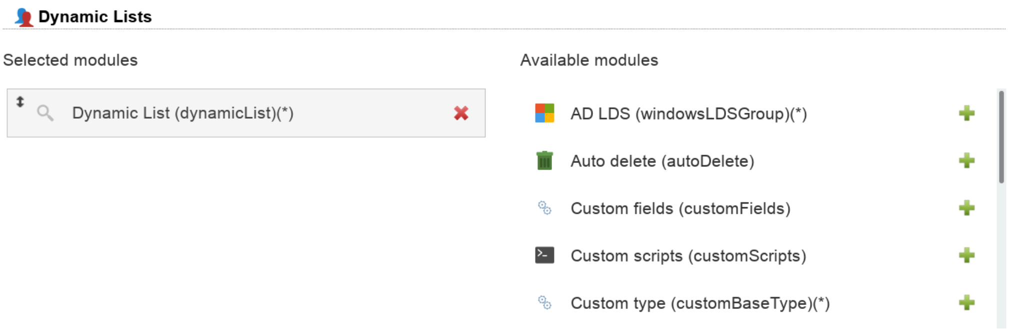
Do not forget to set proper "List attributes" to be shown on the overview page of all dynamic lists.



Dynamic Lists — Group accounts (e.g. Unix and Samba)

LDAP suffix *: ou=dynamiclists,o=test,c=de
List attributes: #cn;#memberURL
Custom label: Dynamic Lists
Additional LDAP filter:
Read-only □
Hidden □
No new entries □
Disallow delete □

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



Dynamic Lists

Selected modules

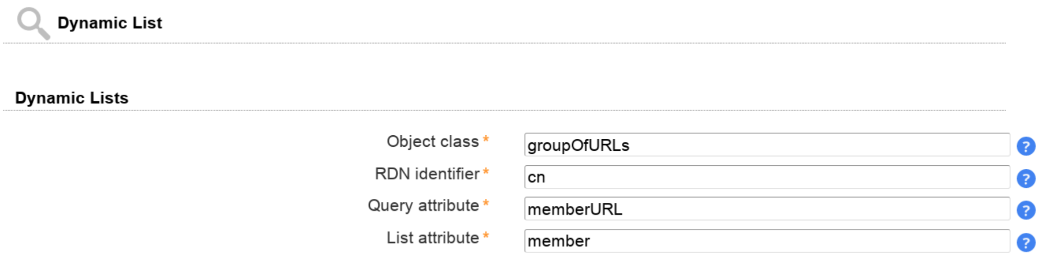
- Dynamic List (dynamicList)(*)

Available modules

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

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

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



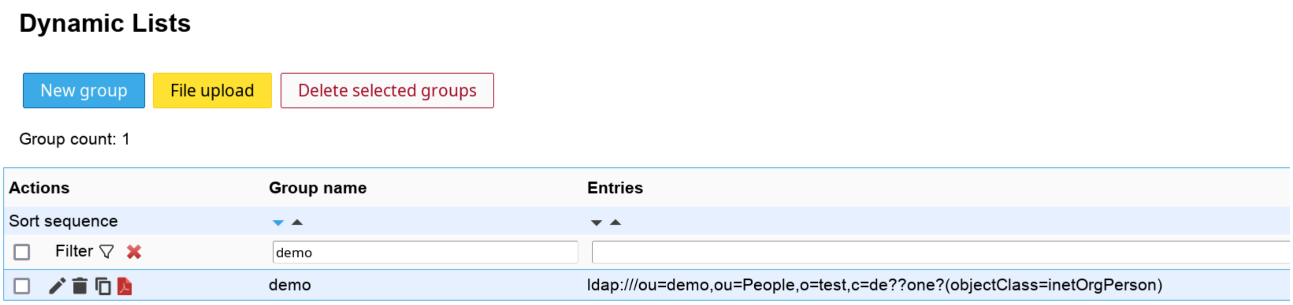
Dynamic List

Dynamic Lists

Object class *	groupOfURLs
RDN identifier *	cn
Query attribute *	memberURL
List attribute *	member

Usage

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



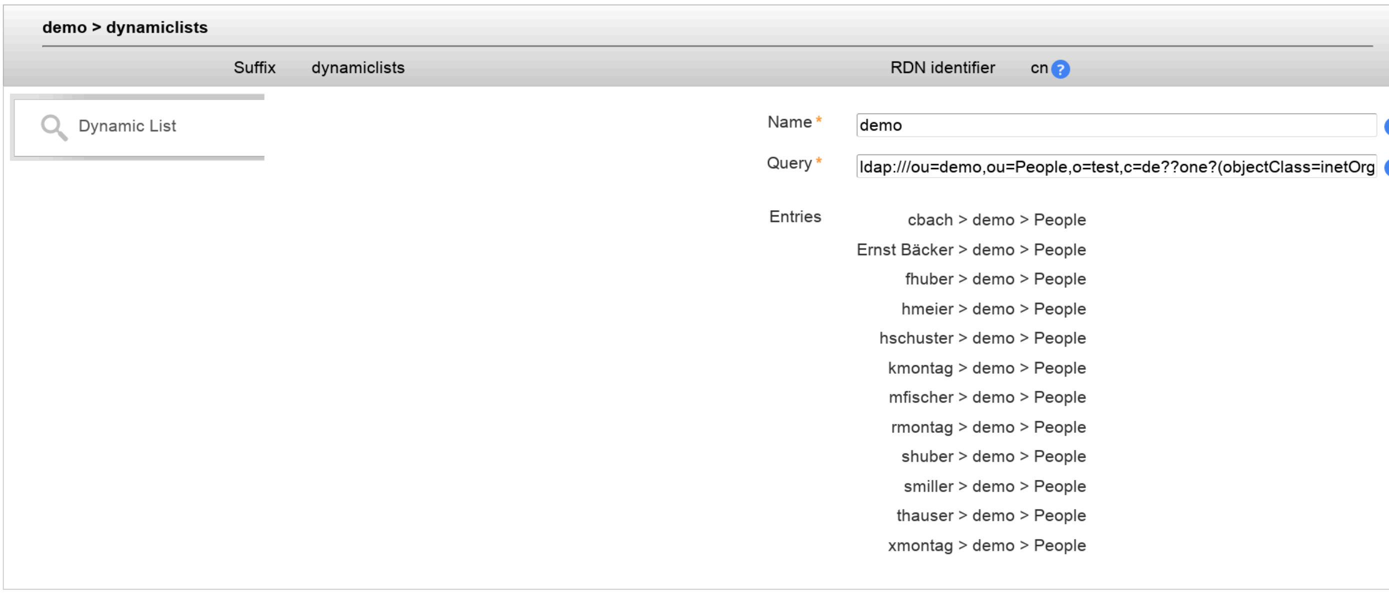
Dynamic Lists

New group | File upload | Delete selected groups

Group count: 1

Actions	Group name	Entries
Sort sequence		
□ Filter	demo	
□	demo	ldap:///ou=demo,ou=People,o=test,c=de??one?(objectClass=inetOrgPerson)

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



demo > dynamiclists

Suffix dynamiclists RDN identifier cn

Dynamic List

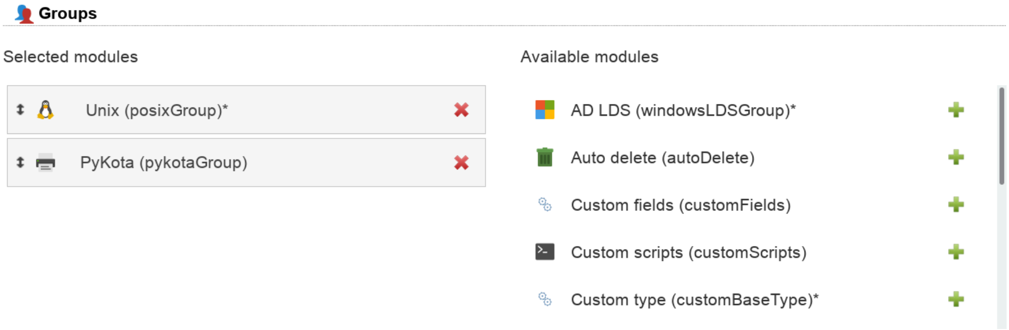
Name * demo

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

Entries
cbach > demo > People
Ernst Bäcker > demo > People
fhuber > demo > People
hmeier > demo > People
hschuster > demo > People
kmontag > demo > People
mfischer > demo > People
rmontag > demo > People
shuber > demo > People
smiller > demo > People
thauser > demo > People
xmontag > demo > People

PyKota

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

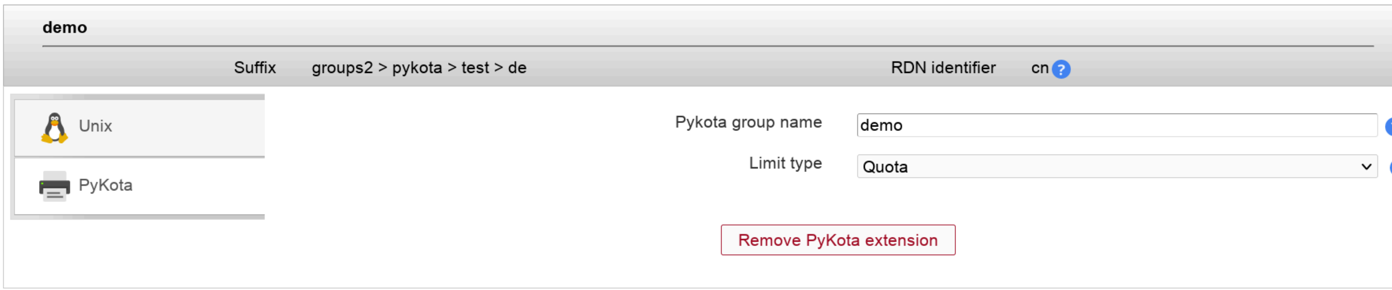


Groups

Selected modules
- Unix (posixGroup)*
- PyKota (pykotaGroup)

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

Now you can add the PyKota extension to your groups.



demo

Suffix groups2 > pykota > test > de RDN identifier cn

Unix
PyKota

Pykota group name demo

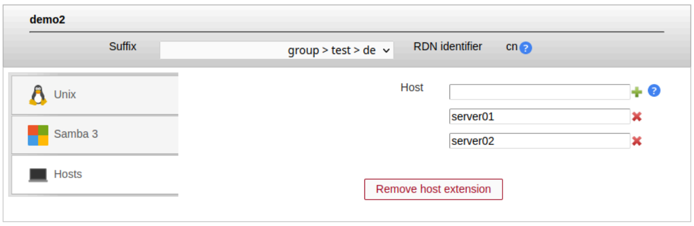
Limit type Quota

Remove PyKota extension

Hosts

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

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



demo2

Suffix: group > test > de

RDN identifier: cn

Host: server01, server02

Password policy (LAM Pro)

See password policy for users.

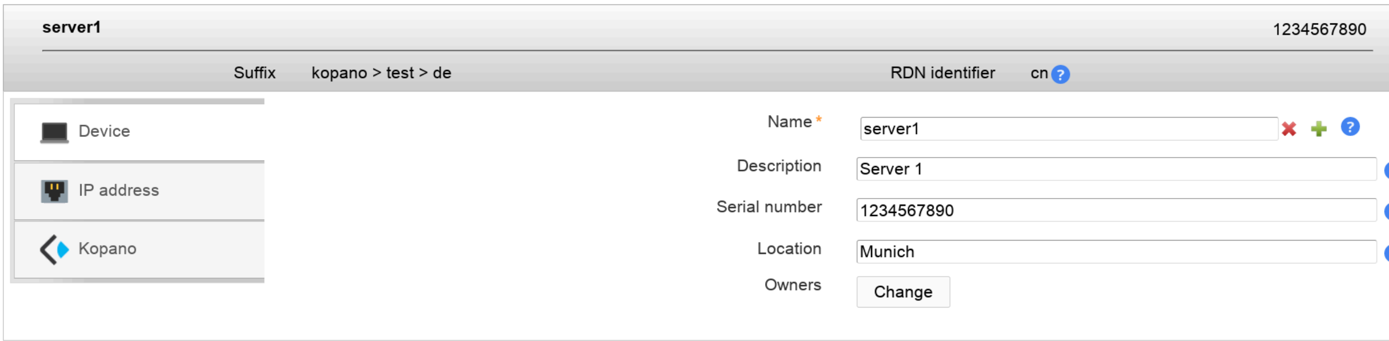
Hosts

Account

Please see the description here.

Device (LAM Pro)

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



server1 1234567890

Suffix: kopano > test > de

RDN identifier: cn

Name*: server1

Description: Server 1

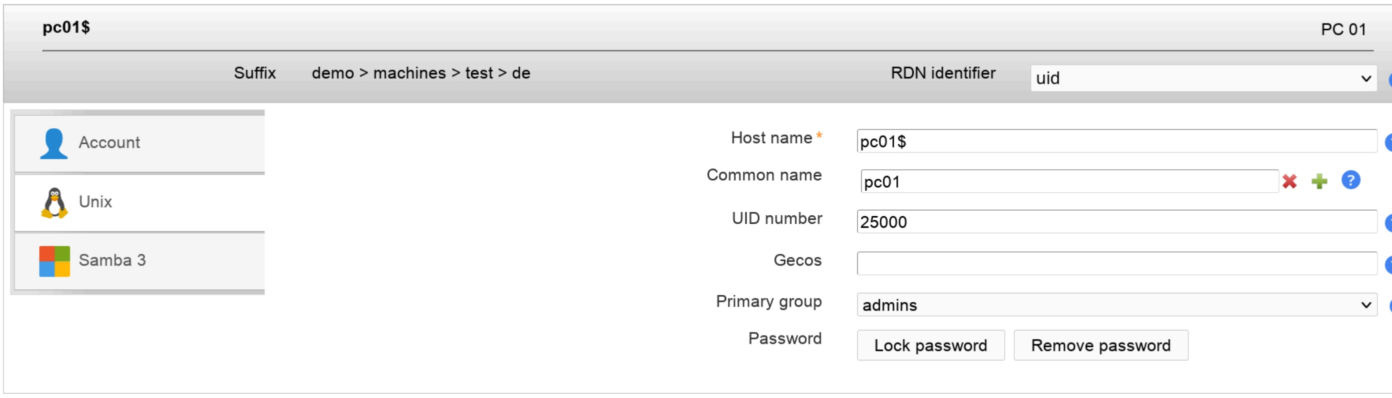
Serial number: 1234567890

Location: Munich

Owners

Samba 3

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



pc01$ PC 01

Suffix: demo > machines > test > de

RDN identifier: uid

Host name*: pc01$

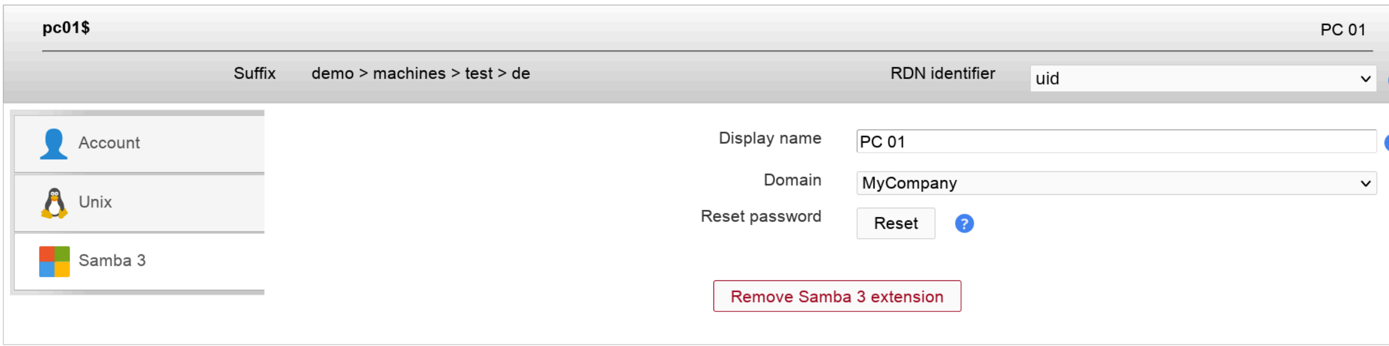
Common name: pc01

UID number: 25000

Gecos:

Primary group: admins

Password



pc01$ PC 01

Suffix demo > machines > test > de RDN identifier uid

Account
Unix
Samba 3

Display name PC 01

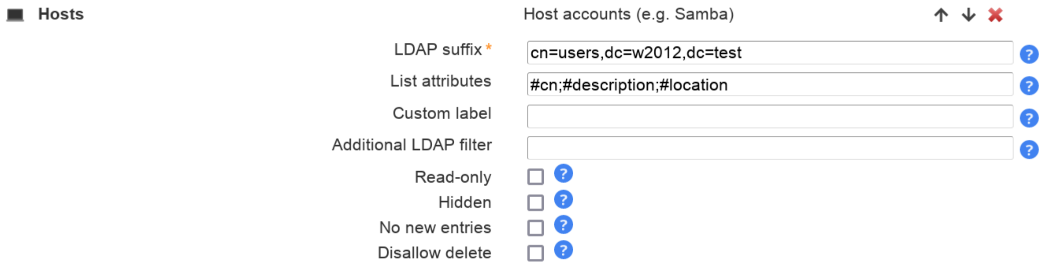
Domain MyCompany

Reset password Reset

Remove Samba 3 extension

Windows (Samba 4)

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



Hosts Host accounts (e.g. Samba)

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

List attributes #cn;#description;#location

Custom label

Additional LDAP filter

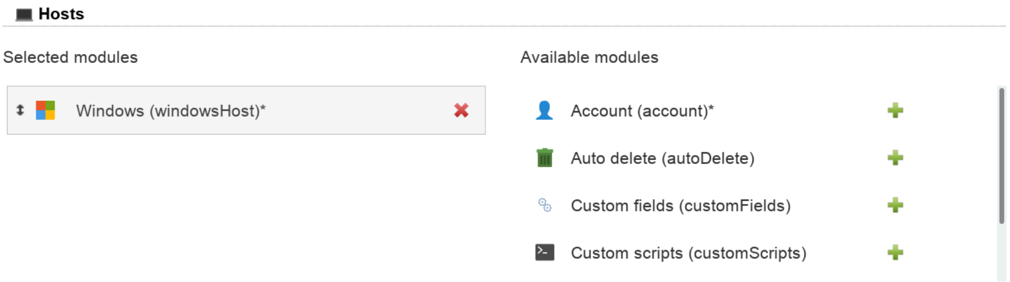
Read-only ☐

Hidden ☐

No new entries ☐

Disallow delete ☐

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



Hosts

Selected modules

Windows (windowsHost)*

Available modules

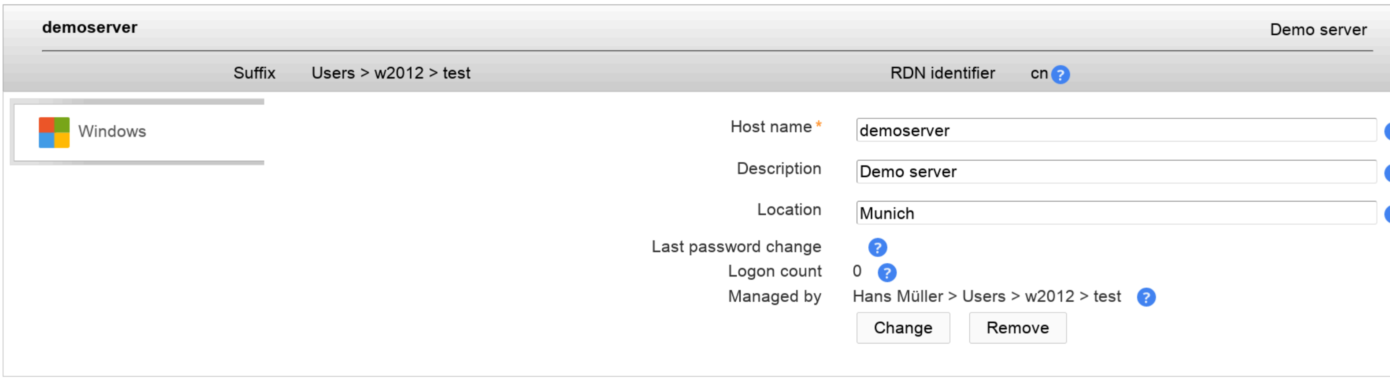
Account (account)*

Auto delete (autoDelete)

Custom fields (customFields)

Custom scripts (customScripts)

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



demoserver Demo server

Suffix Users > w2012 > test RDN identifier cn

Windows

Host name * demoserver

Description Demo server

Location Munich

Last password change

Logon count 0

Managed by Hans Müller > Users > w2012 > test

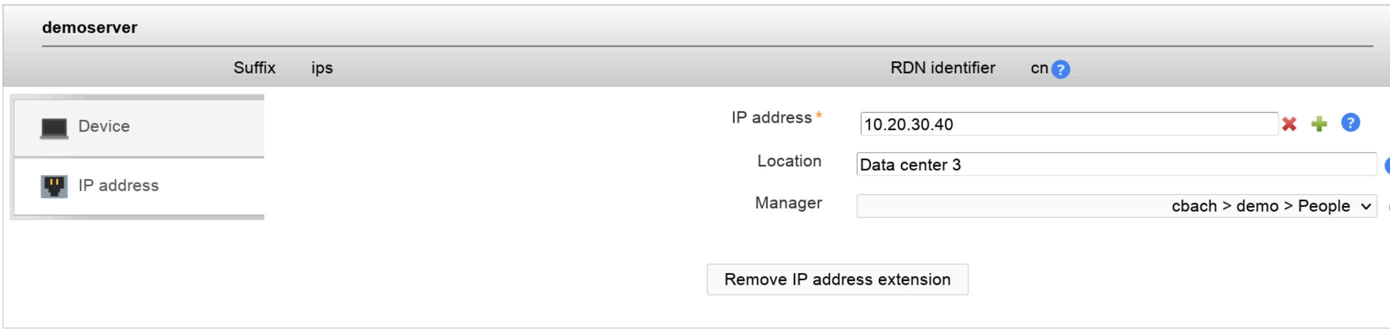
Change Remove

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.



demoserver

Suffix: ips

RDN identifier: cn

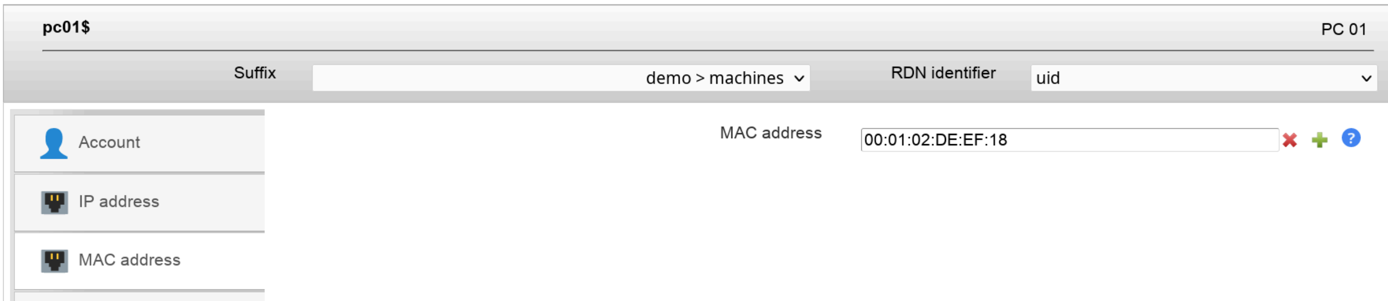
IP address*: 10.20.30.40

Location: Data center 3

Manager: cbach > demo > People

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.



pc01$

PC 01

Suffix: demo > machines

RDN identifier: uid

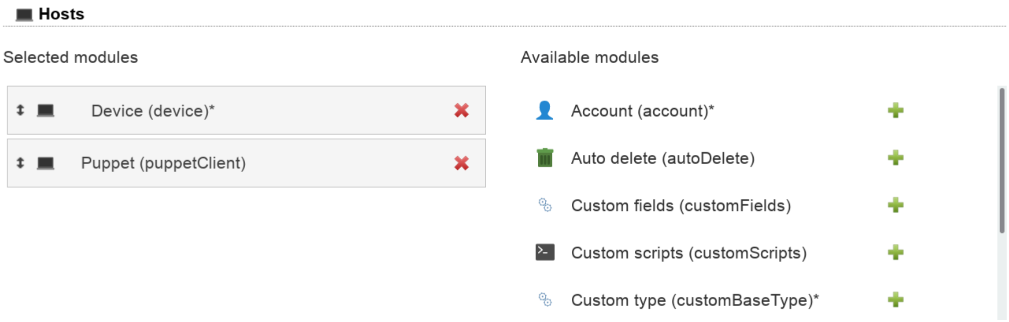
MAC address: 00:01:02:DE:EF:18

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.



Hosts

Selected modules

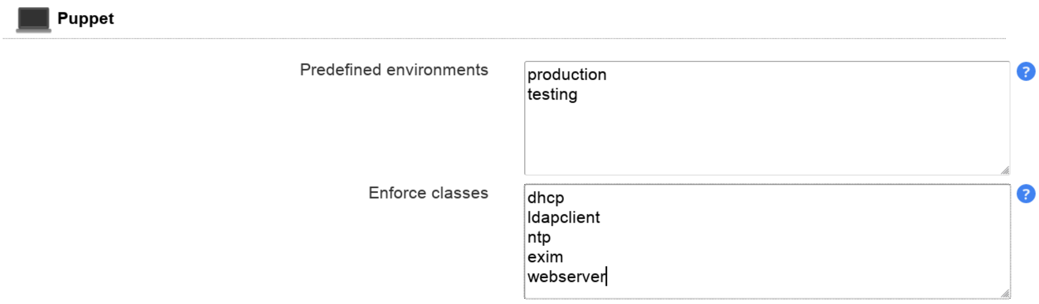
- Device (device)*
- Puppet (puppetClient)

Available modules

- Account (account)*
- Auto delete (autoDelete)
- Custom fields (customFields)
- Custom scripts (customScripts)
- Custom type (customBaseType)*

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

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



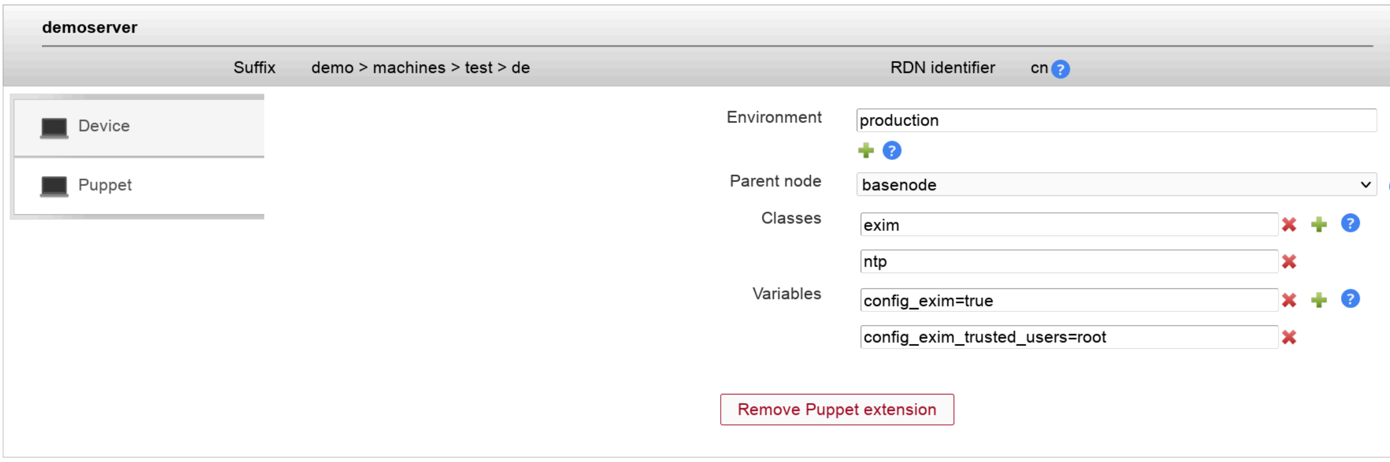
Puppet

Predefined environments: production
testing

Enforce classes: dhcp
ldapclient
ntp
exim
webserver

Editing nodes

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



demoserver

Suffix: demo > machines > test > de

RDN identifier: cn

Environment: production

Parent node: basenode

Classes: exim
ntp

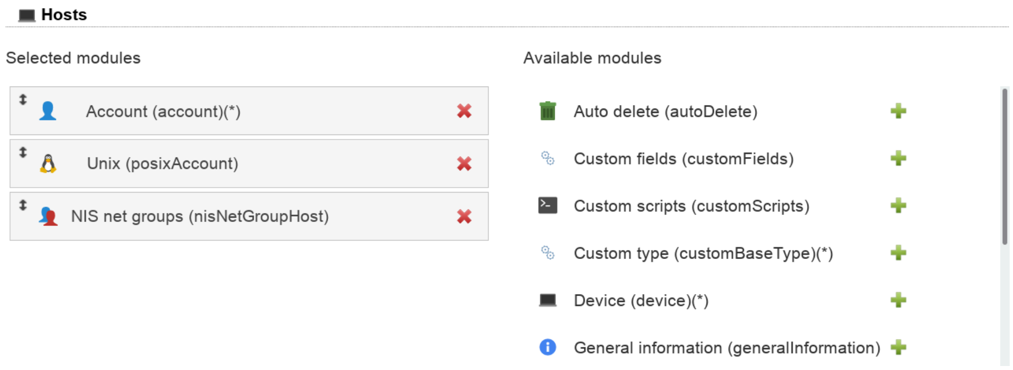
Variables: config_exim=true
config_exim_trusted_users=root

NIS net groups

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

Configuration

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



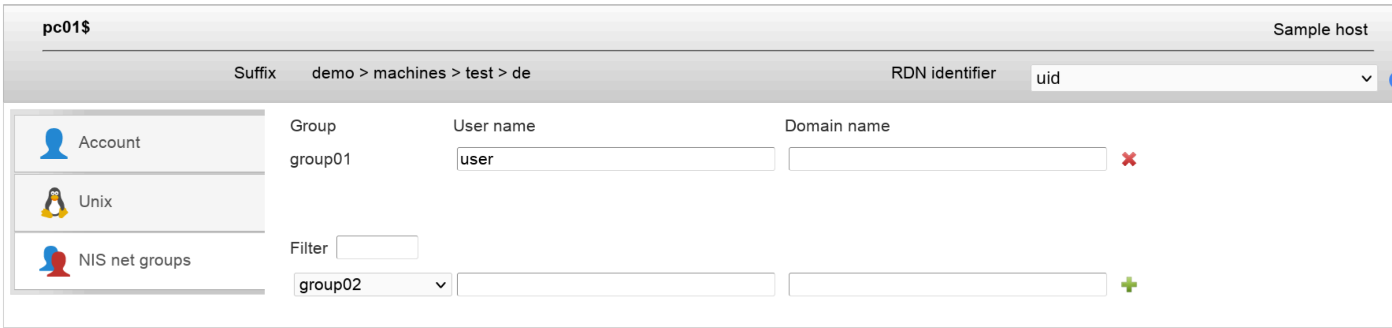
Hosts

Selected modules:
- Account (account)(*)
- Unix (posixAccount)
- NIS net groups (nisNetGroupHost)

Available modules:
- Auto delete (autoDelete)
- Custom fields (customFields)
- Custom scripts (customScripts)
- Custom type (customBaseType)(*)
- Device (device)(*)
- General information (generalInformation)

Host editing

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



pc01$ Sample host

Suffix demo > machines > test > de RDN identifier uid

Group	User name	Domain name
group01	user	

Filter

group02

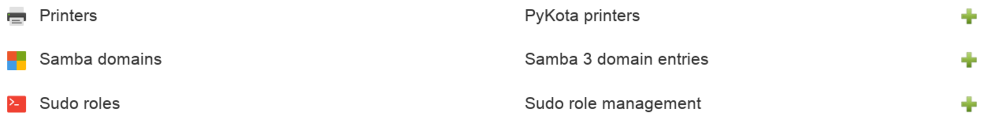
Password policy (LAM Pro)

See password policy for users.

Samba 3 domains

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

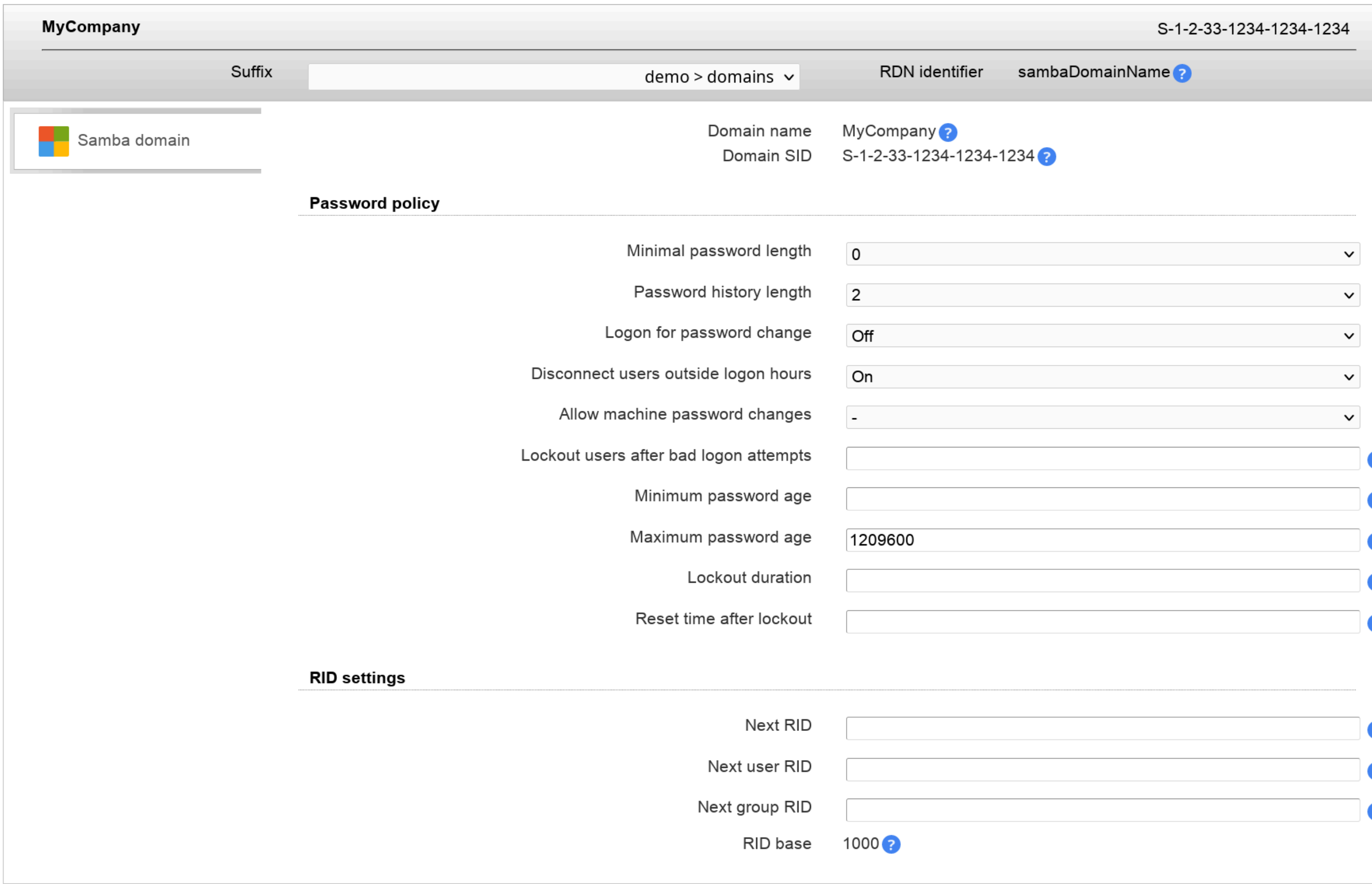
Please activate the account type "Samba domains" in your LAM server profile. Please notice that Samba by default uses the LDAP root for domain objects (e.g. dc=example,dc=com).



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

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

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



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

Suffix	demo > domains	RDN identifier	sambaDomainName

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

Password policy

Minimal password length	0
Password history length	2
Logon for password change	Off
Disconnect users outside logon hours	On
Allow machine password changes	-
Lockout users after bad logon attempts	
Minimum password age	
Maximum password age	1209600
Lockout duration	
Reset time after lockout	

RID settings

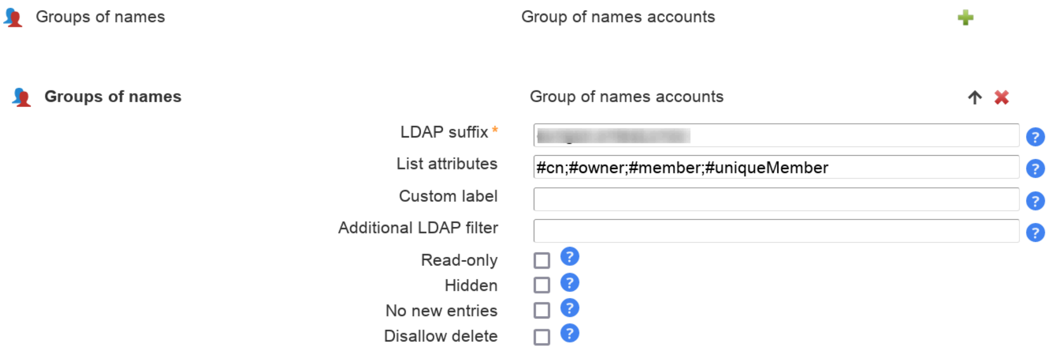
Next RID	
Next user RID	
Next group RID	
RID base	1000

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

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

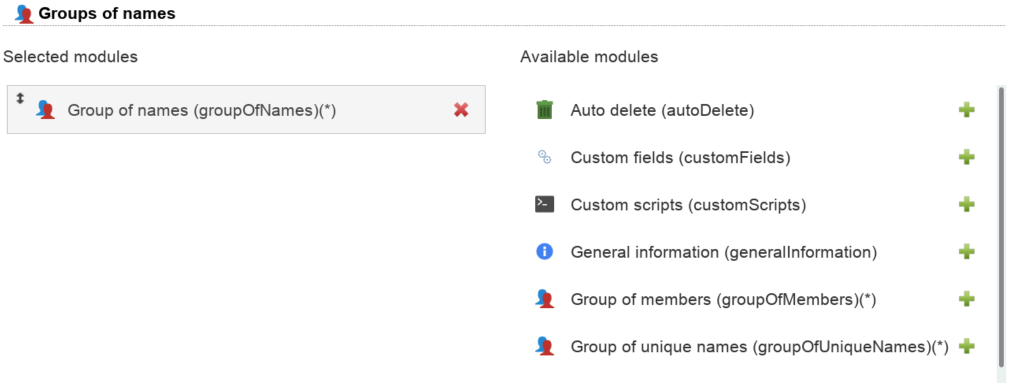
Configuration:

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".



LDAP suffix *	[redacted]
List attributes	#cn;#owner;#member;#uniqueMember
Custom label	
Additional LDAP filter	
Read-only	□
Hidden	□
No new entries	□
Disallow delete	□

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



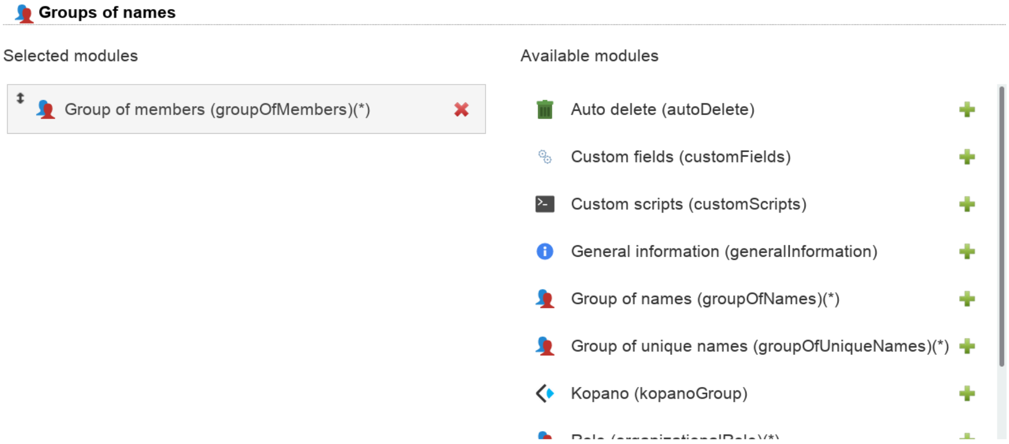
Groups of names

Selected modules

- Group of names (groupOfNames)(*)

Available modules

- Auto delete (autoDelete)
- Custom fields (customFields)
- Custom scripts (customScripts)
- General information (generalInformation)
- Group of members (groupOfMembers)(*)
- Group of unique names (groupOfUniqueNames)(*)



Groups of names

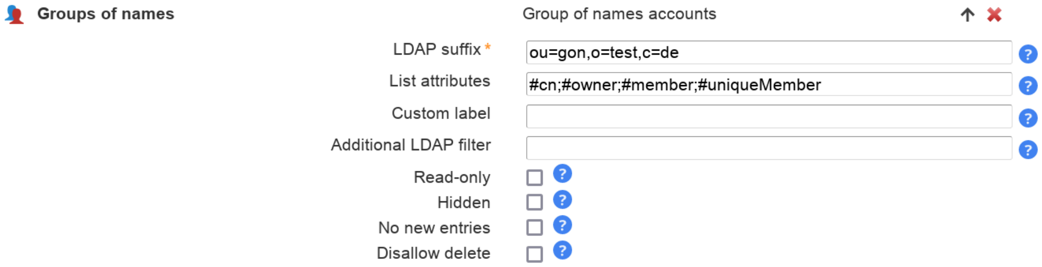
Selected modules

- Group of members (groupOfMembers)(*)

Available modules

- Auto delete (autoDelete)
- Custom fields (customFields)
- Custom scripts (customScripts)
- General information (generalInformation)
- Group of names (groupOfNames)(*)
- Group of unique names (groupOfUniqueNames)(*)
- Kopano (kopanoGroup)
- Role (organizationalRole)(*)

Virtual list attributes:



Groups of names

Group of names accounts

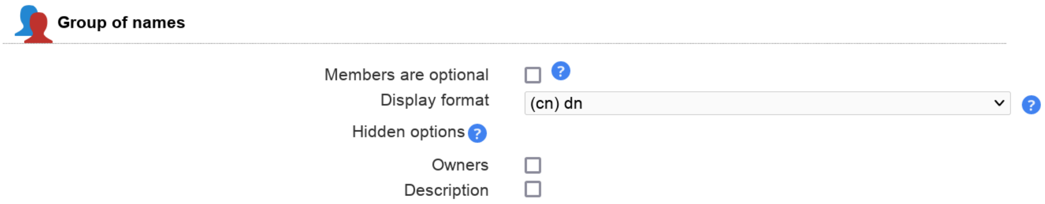
LDAP suffix *	ou=gon,o=test,c=de
List attributes	#cn;#owner;#member;#uniqueMember
Custom label	
Additional LDAP filter	
Read-only	□
Hidden	□
No new entries	□
Disallow delete	□

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

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

Module settings:

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



Group of names

Members are optional □

Display format: (cn) dn

Hidden options

Owners □

Description □

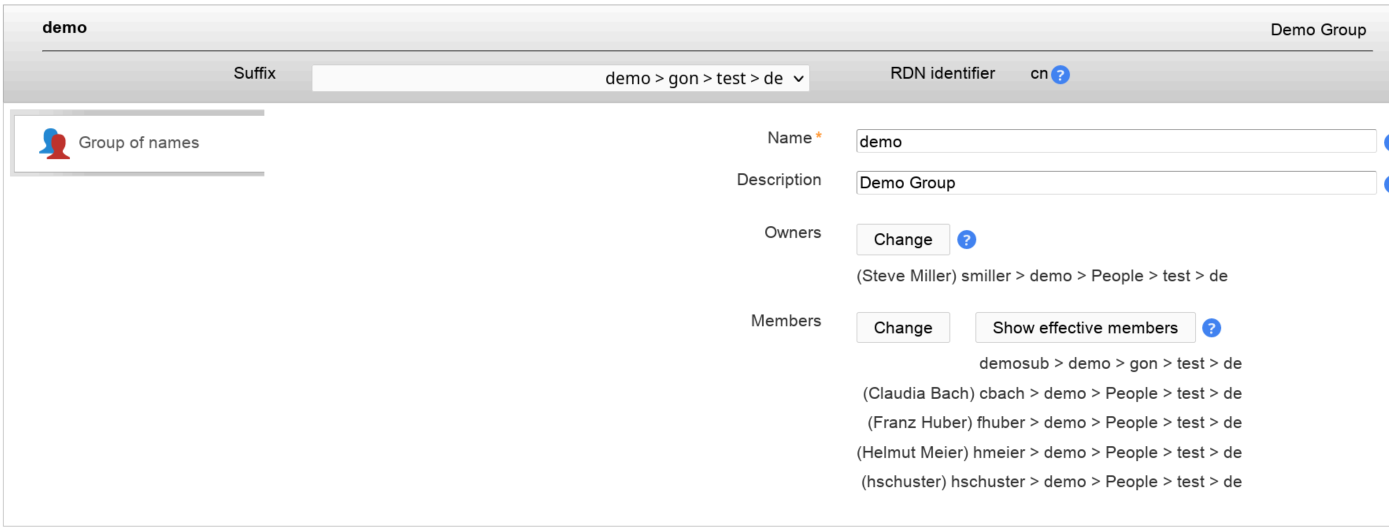
Group management:

Group of (unique) names have four basic attributes:

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

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

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



demo — Demo Group

Suffix: demo > gon > test > de

RDN identifier: cn

Name*: demo

Description: Demo Group

Owners: Change

(Steve Miller) smiller > demo > People > test > de

Members: Change | Show effective members

demosub > demo > gon > test > de
(Claudia Bach) cbach > demo > People > test > de
(Franz Huber) fhuber > demo > People > test > de
(Helmut Meier) hmeier > demo > People > test > de
(hschuster) hschuster > demo > People > test > de

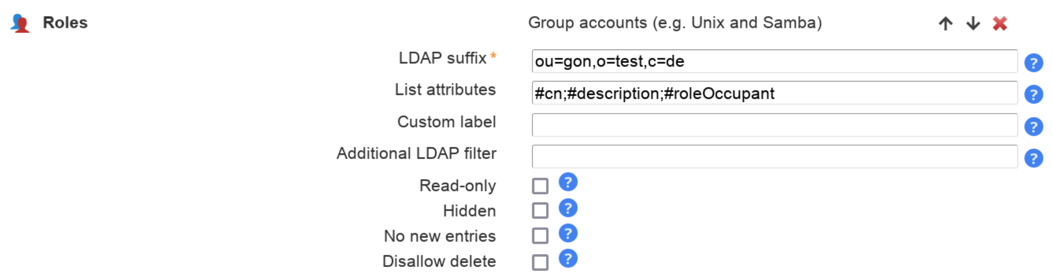
Organizational roles (LAM Pro)

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

Configuration:

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

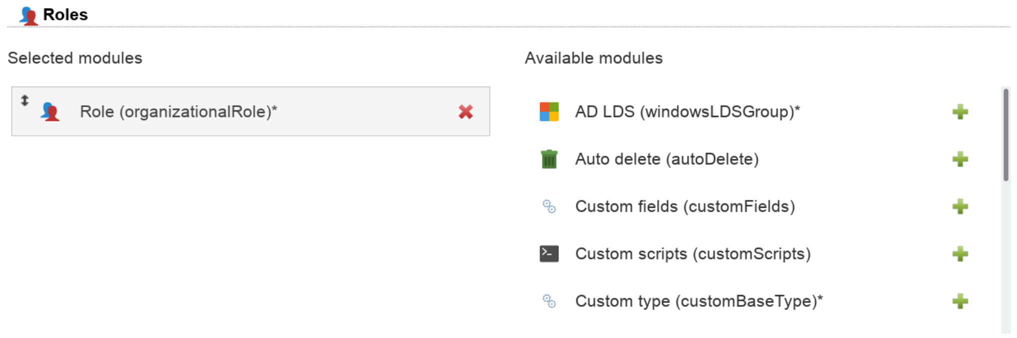
Groups — Group accounts (e.g. Unix and Samba)



Roles — Group accounts (e.g. Unix and Samba)

LDAP suffix *	ou=gon,o=test,c=de
List attributes	#cn;#description;#roleOccupant
Custom label	
Additional LDAP filter	
Read-only	□
Hidden	□
No new entries	□
Disallow delete	□

Then add the module "Role (organizationalRole)".



Roles

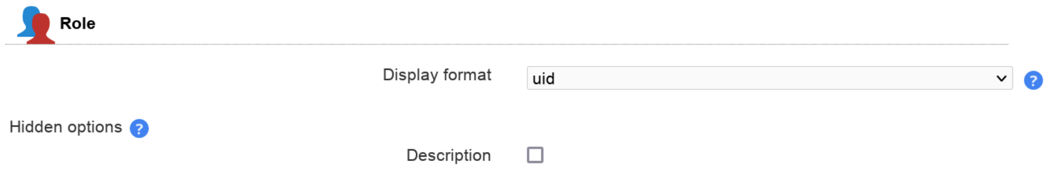
Selected modules

- Role (organizationalRole)*

Available modules

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

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



Role

Display format	uid

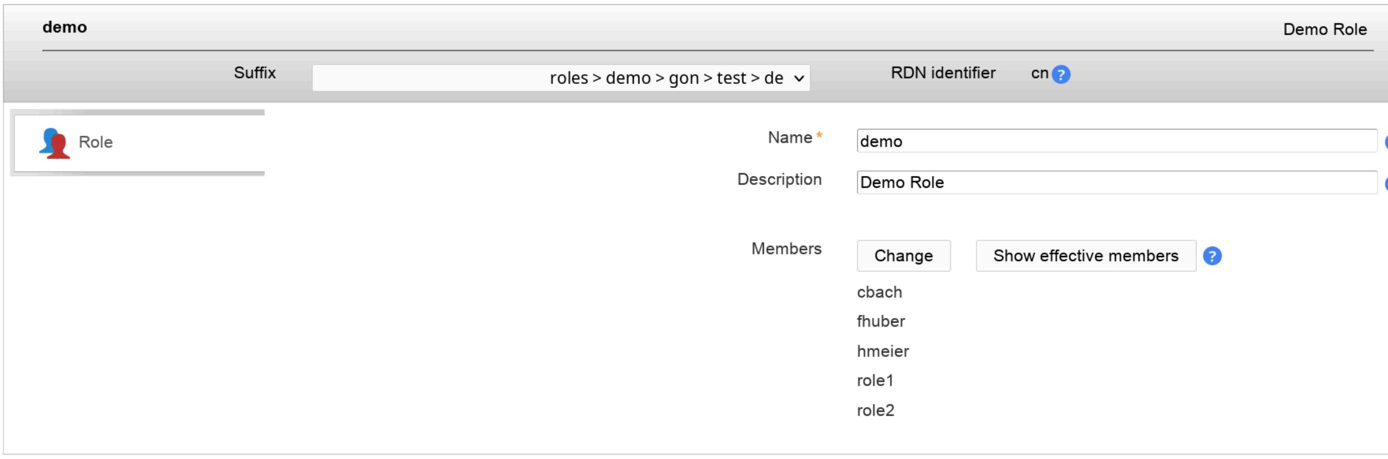
Hidden options

Description	□

Role management:

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

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



demo — Demo Role

Suffix: roles > demo > gon > test > de — RDN identifier: cn

Role

Name *	demo
Description	Demo Role

Members

cbach
fhuber
hmeier
role1
role2

Simple Security Object (LAM Pro)

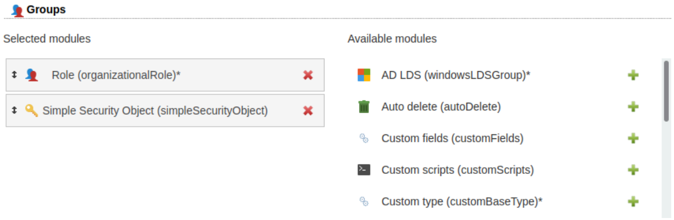
This allows to add passwords to LDAP entries which do not support passwords by other object classes. E.g. passwords can be added to organizational roles.

The simple security object module can be added to the following account types: users, groups, group of names and hosts

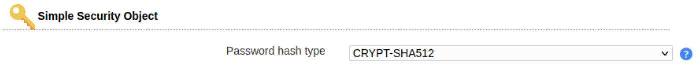
Attention: simple security objects require a password to be set. If you choose LDAP_EXOP as password hash then no new LDAP entries can be created. The reason is that EXOP requires to set the password on an already existing account (but simpleSecurityObject requires to set it in first place). So no password is set at the initial account creation which will then fail.

Configuration:

Add the Simple Security Object module to your account type.

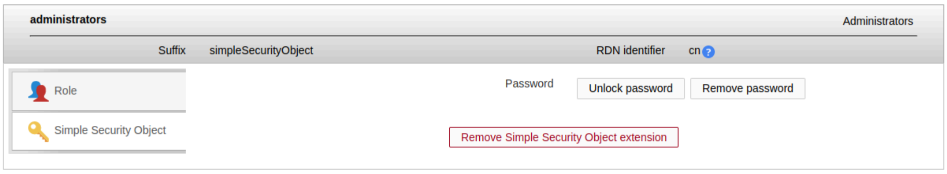

Groups
Selected modules
Role (organizationalRole)*
Simple Security Object (simpleSecurityObject)
Available modules
AD LDS (windowsLDSGroup)*
Auto delete (autoDelete)
Custom fields (customFields)
Custom scripts (customScripts)
Custom type (customBaseType)*

Next configure the password hash type to use (module settings tab).



Password hash type CRYPT-SHA512

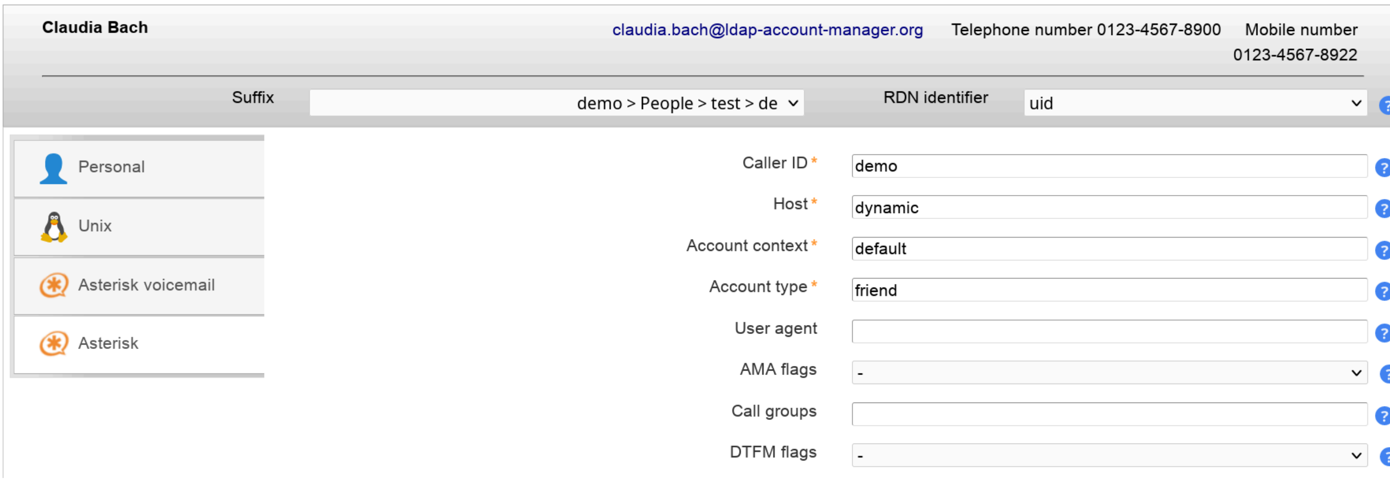
Now you can add a password to your entries by adding the extension to an entry.



Asterisk

LAM includes large support for Asterisk. You can add Asterisk extensions (including voicemail) to your users and also manage Asterisk extensions.

The Asterisk support for users can be added by selecting the Asterisk and Asterisk voicemail modules for users in your LAM server profile. This will add the following tabs to your user accounts.

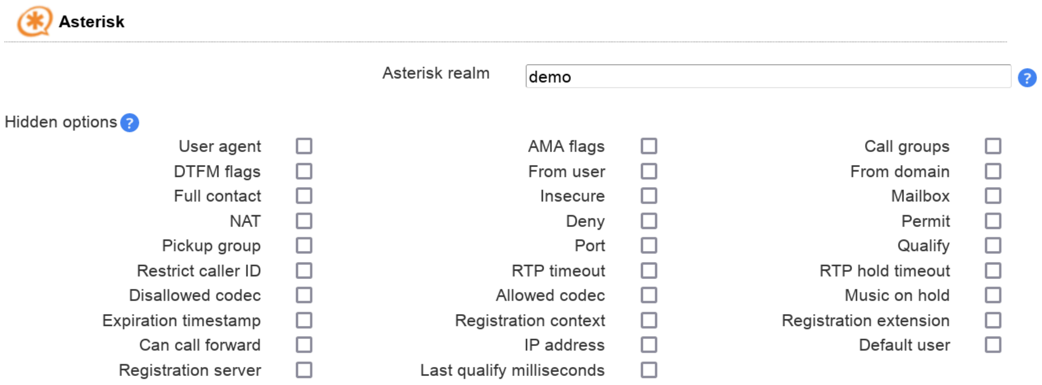


Claudia Bach claudia.bach@ldap-account-manager.org Telephone number 0123-4567-8900 Mobile number 0123-4567-8922

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

Caller ID *: demo
Host *: dynamic
Account context *: default
Account type *: friend
User agent:
AMA flags: -
Call groups:
DTFM flags: -

The Asterisk module allows to edit a large amount of attributes. Therefore, you can hide unused fields. Please edit you server profile (Module settings) to do so.



Asterisk

Asterisk realm: demo

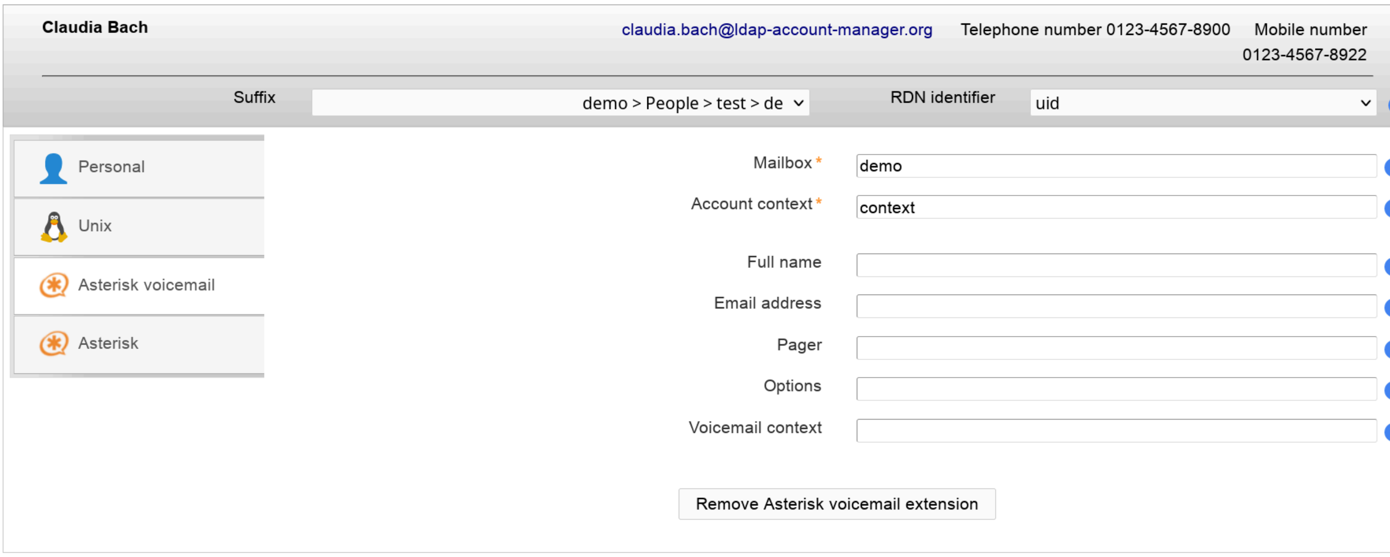
Hidden options

User agent ☐
DTFM flags ☐
Full contact ☐
NAT ☐
Pickup group ☐
Restrict caller ID ☐
Disallowed codec ☐
Expiration timestamp ☐
Can call forward ☐
Registration server ☐

AMA flags ☐
From user ☐
Insecure ☐
Deny ☐
Port ☐
RTP timeout ☐
Allowed codec ☐
Registration context ☐
IP address ☐
Last qualify milliseconds ☐

Call groups ☐
From domain ☐
Mailbox ☐
Permit ☐
Qualify ☐
RTP hold timeout ☐
Music on hold ☐
Registration extension ☐
Default user ☐

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



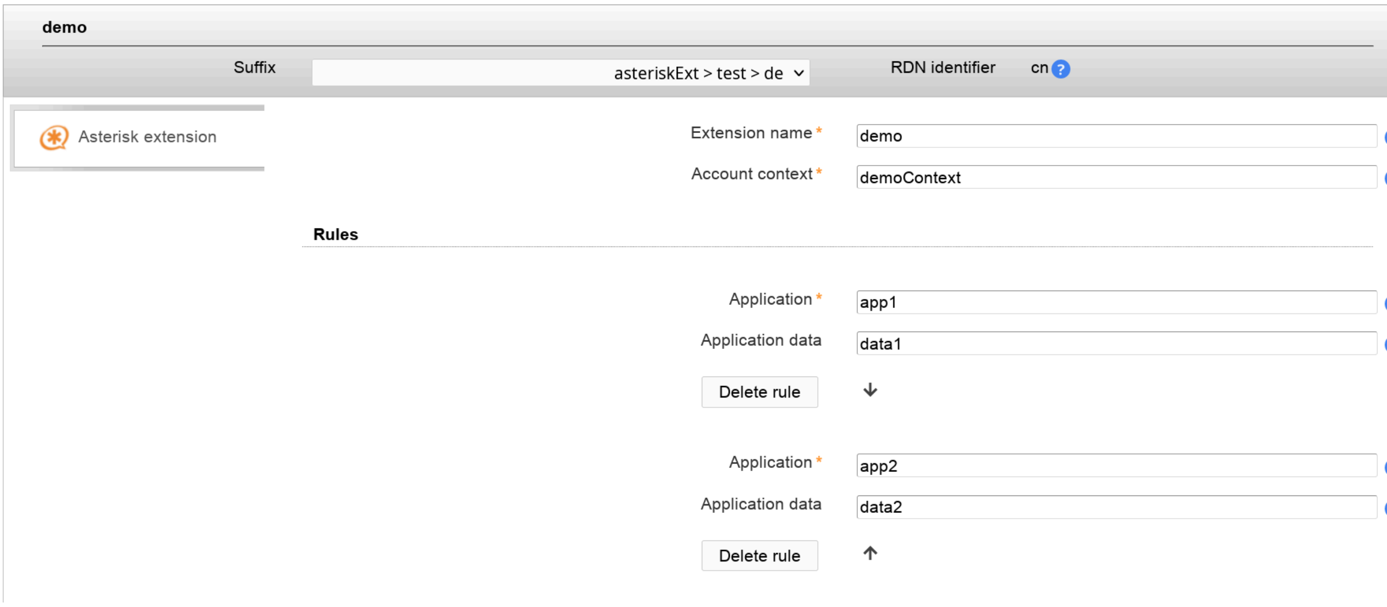
Claudia Bach claudia.bach@ldap-account-manager.org Telephone number 0123-4567-8900 Mobile number 0123-4567-8922

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

Mailbox *: demo
Account context *: context
Full name:
Email address:
Pager:
Options:
Voicemail context:

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

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.

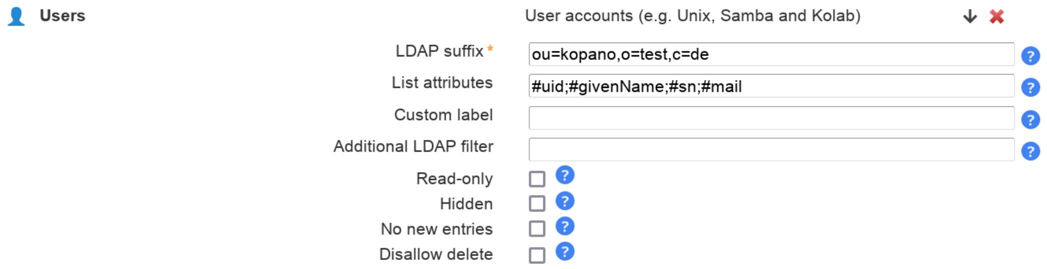
Users

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.



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

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

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

Custom label:

Additional LDAP filter:

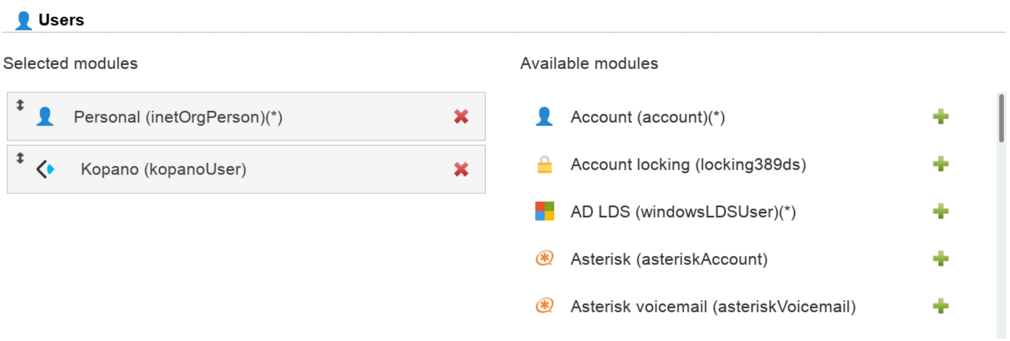
Read-only ☐

Hidden ☐

No new entries ☐

Disallow delete ☐

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



Users

Selected modules

- Personal (inetOrgPerson)(*) ✖
- Kopano (kopanoUser) ✖

Available modules

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

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

Attention: LAM Pro uses the Kopano OpenLDAP schema by default. This schema fits for OpenLDAP, OpenDJ, Apache Directory server and other common LDAP servers. If you run Samba 4 or Active Directory then you need to switch the schema to "Active Directory" on the module settings tab.

You can hide options that you do not need. E.g. if you do not want to manage quotas per user then you can hide these options.

Examples for your Kopano ldap.cfg:

"Send as" attribute: dn

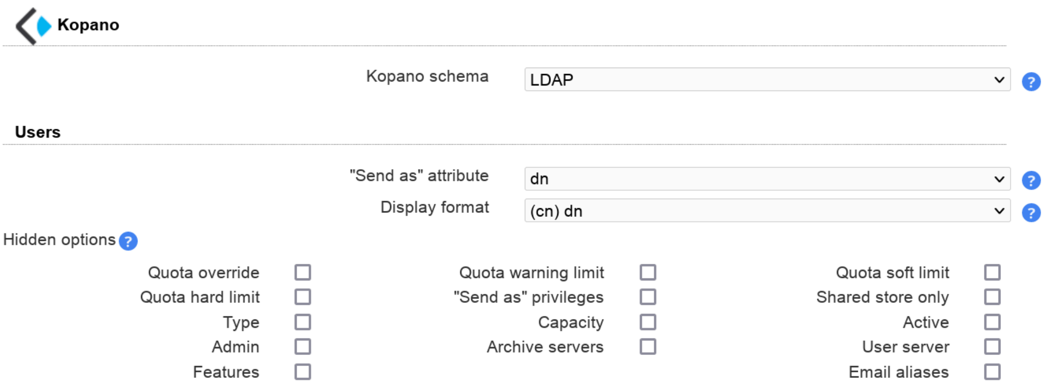
ldap_user_sendas_attribute_type = dn

"Send as" attribute: uid

ldap_user_sendas_attribute_type = text

ldap_user_sendas_relation_attribute = uid

Attention: If the Active Directory schema is used then LAM will always use dn and ignore this setting.



Kopano

Kopano schema: LDAP

Users

"Send as" attribute: dn

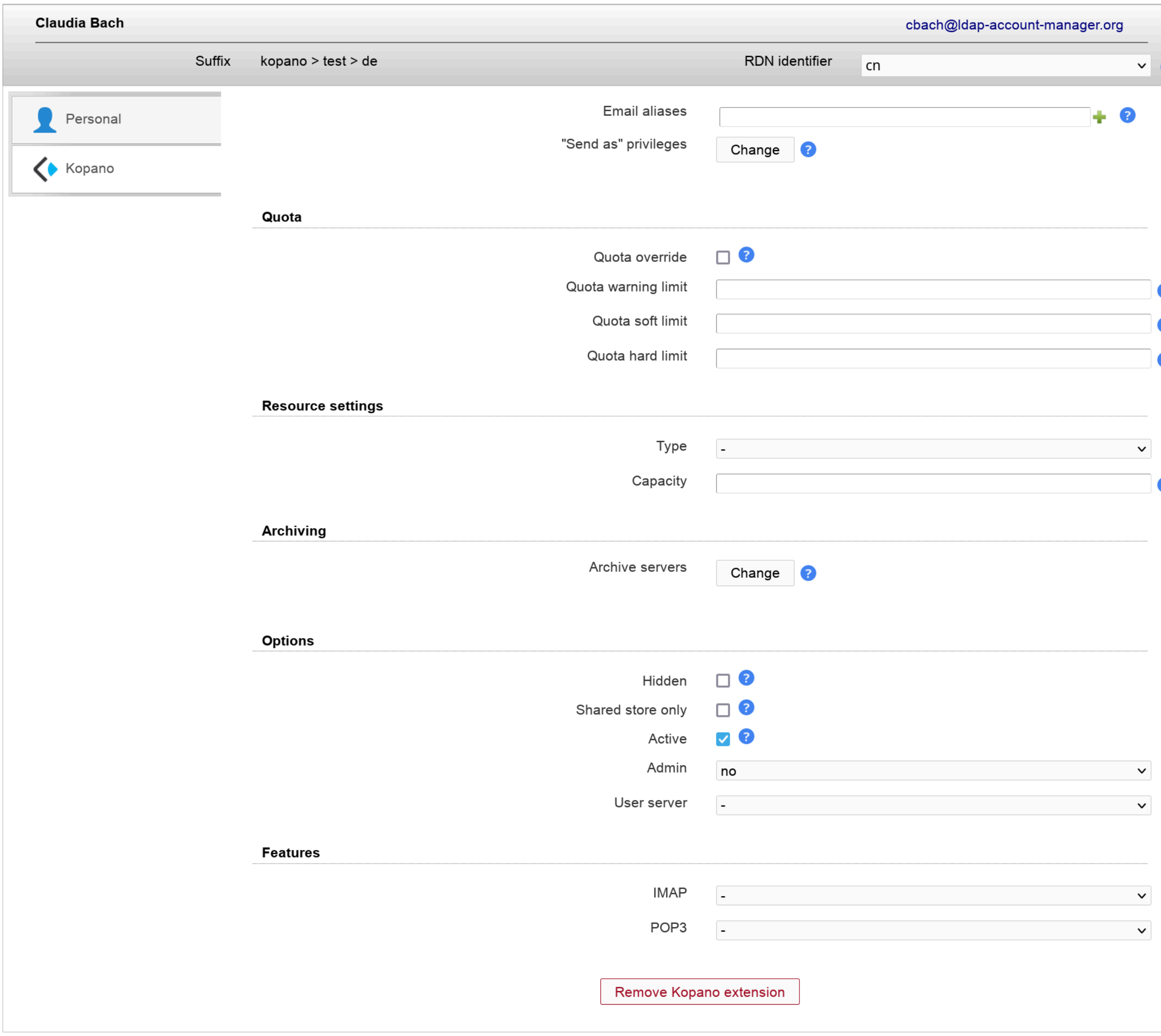
Display format: (cn) dn

Hidden options

- Quota override ☐
- Quota hard limit ☐
- Type ☐
- Admin ☐
- Features ☐
- Quota warning limit ☐
- "Send as" privileges ☐
- Capacity ☐
- Archive servers ☐
- Quota soft limit ☐
- Shared store only ☐
- Active ☐
- User server ☐
- Email aliases ☐

Usage

LAM Pro will now display the Kopano tab on your users. This includes email settings, quotas and some options (e.g. hide from address book). You can also set the resource type and capacity for meeting rooms and equipment. The Kopano extension can be added and removed at any time for every user.



Claudia Bach cbach@ldap-account-manager.org

Suffix kopano > test > de RDN identifier cn

Email aliases

"Send as" privileges

Quota

Quota override □

Quota warning limit

Quota soft limit

Quota hard limit

Resource settings

Type -

Capacity

Archiving

Archive servers

Options

Hidden □

Shared store only □

Active ☑

Admin no

User server -

Features

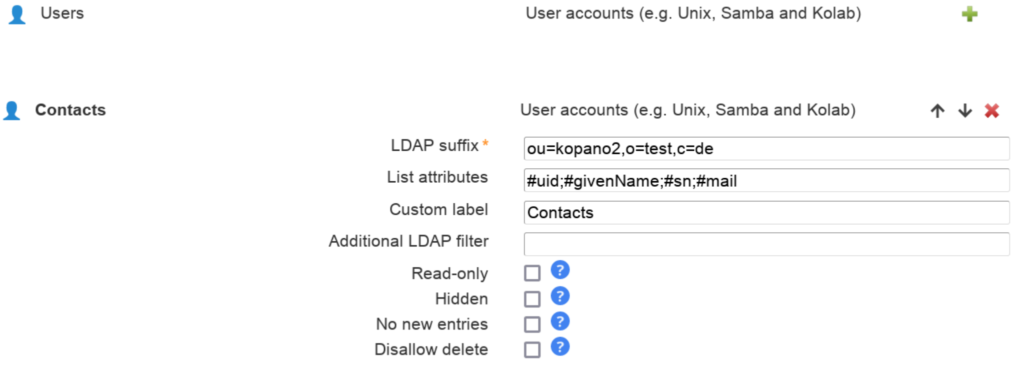
IMAP -

POP3 -

Contacts

Configuration

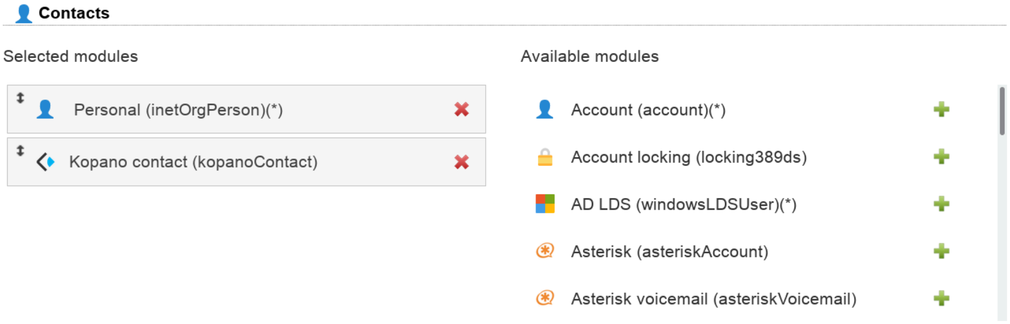
The configuration is similar to users. Instead of the Kopano user module please select the contact module.



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

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

LDAP suffix *	ou=kopano2,o=test,c=de
List attributes	#uid;#givenName;#sn;#mail
Custom label	Contacts
Additional LDAP filter	
Read-only	□
Hidden	□
No new entries	□
Disallow delete	□



Contacts

Selected modules

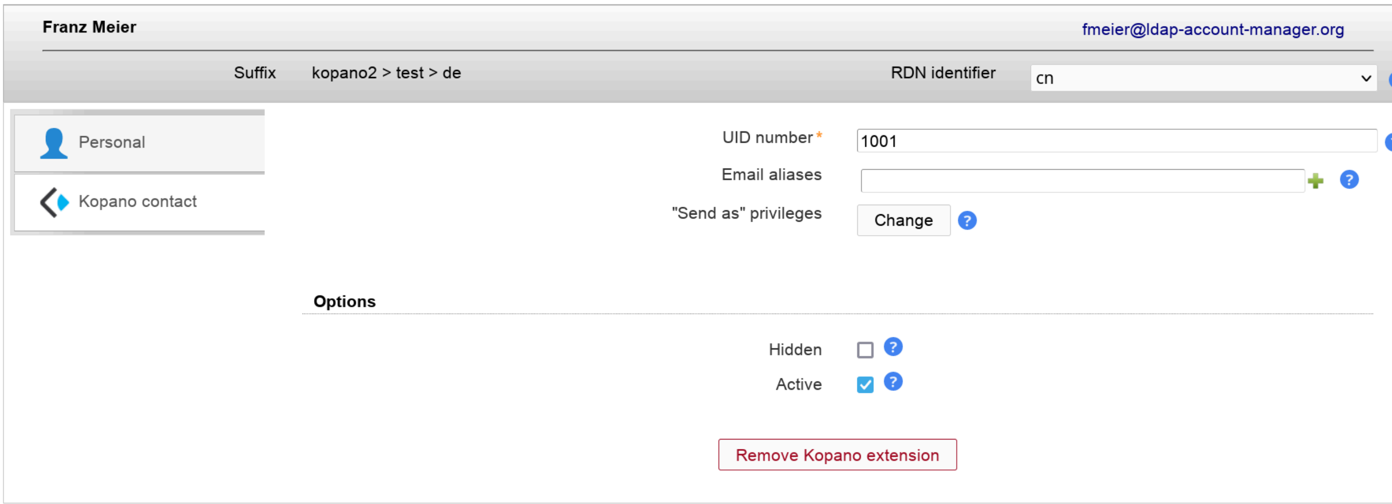
- Personal (inetOrgPerson)(*)
- Kopano contact (kopanoContact)

Available modules

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

Usage

LAM Pro will now display the Kopano contact tab on your users. The Kopano extension can be added and removed at any time for every user.



Franz Meier fmeier@ldap-account-manager.org

Suffix kopano2 > test > de RDN identifier cn

UID number* 1001

Email aliases

"Send as" privileges Change

Options

Hidden □

Active ☑

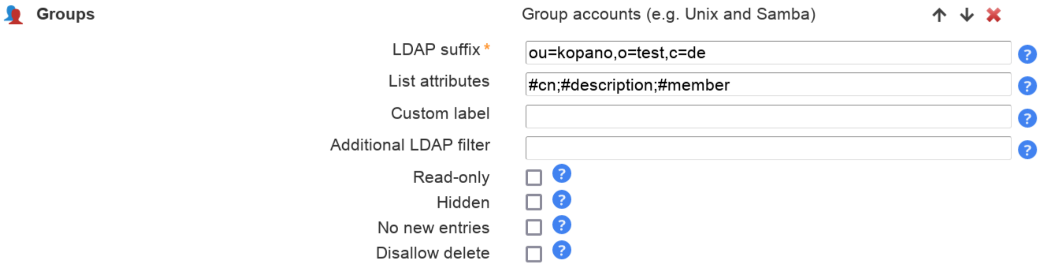
Groups

Configuration

To enable Kopano support for groups please activate the Kopano module for the group account type in you server profile:

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

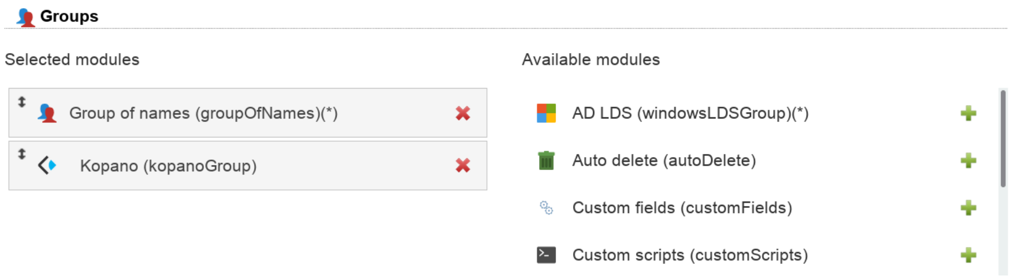
Adjust the suffix and list attributes to your needs.



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

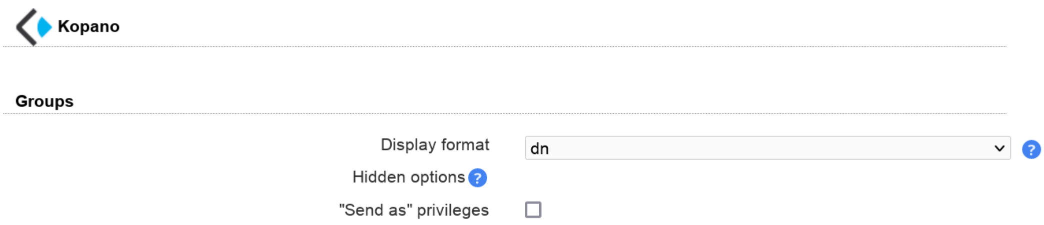
Selected modules

- Group of names (groupOfNames)(*) ✖
- Kopano (kopanoGroup) ✖

Available modules

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

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



Kopano

Groups

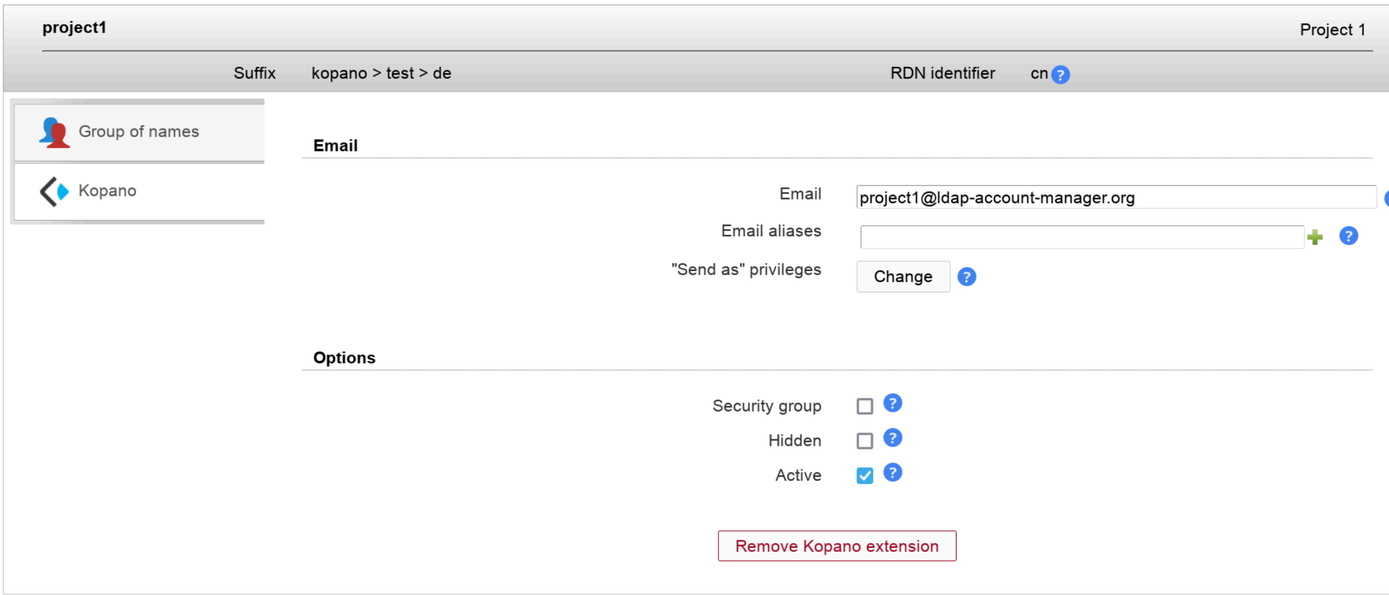
Display format: dn

Hidden options

"Send as" privileges ☐

Usage

LAM Pro will now display the Kopano tab on your groups. The Kopano extension can be added and removed at any time for every group.



project1 Project 1

Suffix: kopano > test > de   RDN identifier: cn

Email

Email: project1@ldap-account-manager.org

Email aliases:

"Send as" privileges: Change

Options

Security group ☐

Hidden ☐

Active ☑

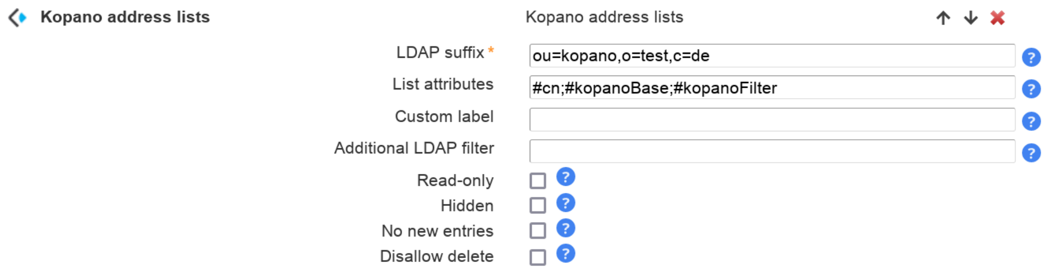
Address lists

Configuration

To enable Kopano support for address lists please activate the Kopano address list account type in you server profile (tab account types):

Kopano address lists   Kopano address lists ➕

Adjust the suffix and list attributes to your needs.



Kopano address lists

Kopano address lists

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

List attributes #cn;#kopanoBase;#kopanoFilter

Custom label

Additional LDAP filter

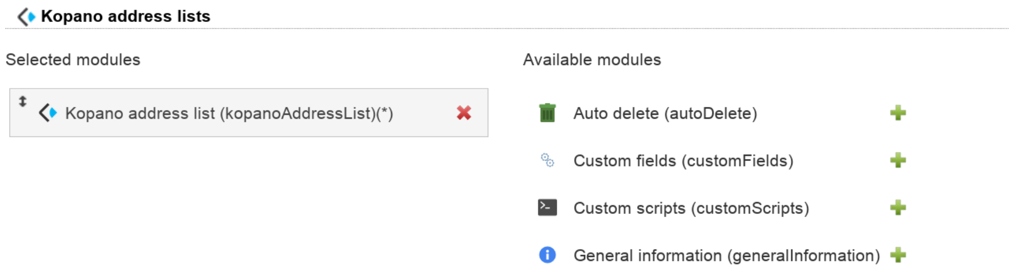
Read-only □

Hidden □

No new entries □

Disallow delete □

Then select the Kopano address list module (tab Modules).



Kopano address lists

Selected modules

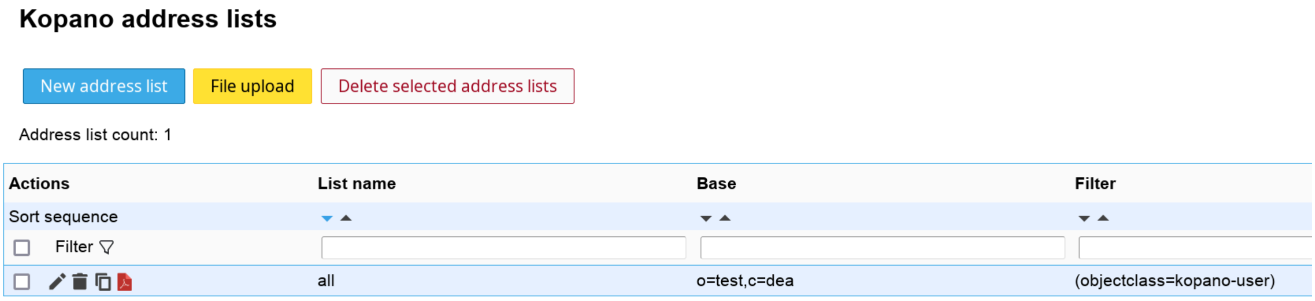
- Kopano address list (kopanoAddressList)(*)

Available modules

- Auto delete (autoDelete)
- Custom fields (customFields)
- Custom scripts (customScripts)
- General information (generalInformation)

Usage

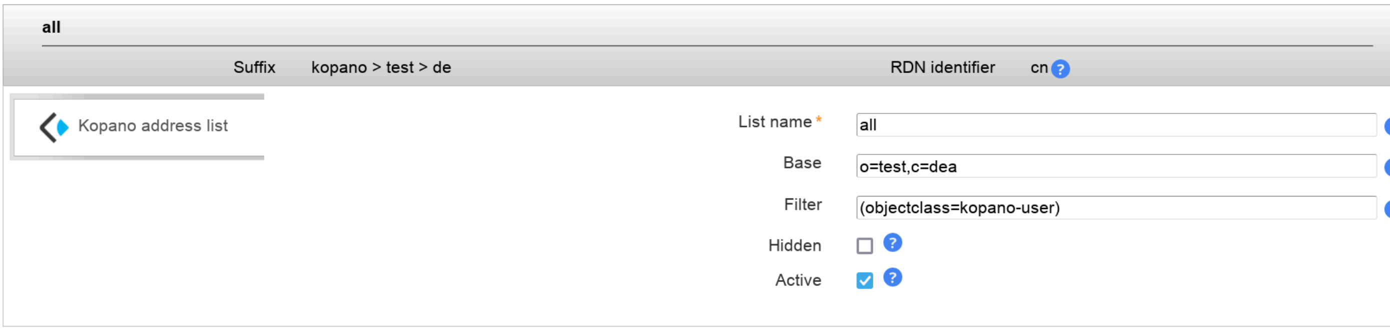
LAM Pro will now display the Kopano address list tab.



Kopano address lists

Address list count: 1

Actions	List name	Base	Filter
Sort sequence			
□ Filter			
□	all	o=test,c=dea	(objectclass=kopano-user)



all

Suffix kopano > test > de

RDN identifier cn

List name * all

Base o=test,c=dea

Filter (objectclass=kopano-user)

Hidden □

Active ☑

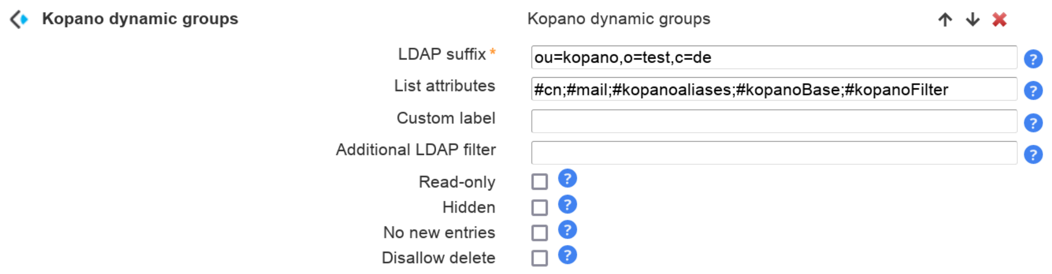
Dynamic groups

Configuration

To enable Kopano support for dynamic groups please activate the Kopano dynamic group account type in you 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 * ou=kopano,o=test,c=de

List attributes #cn;#mail;#kopanoaliases;#kopanoBase;#kopanoFilter

Custom label

Additional LDAP filter

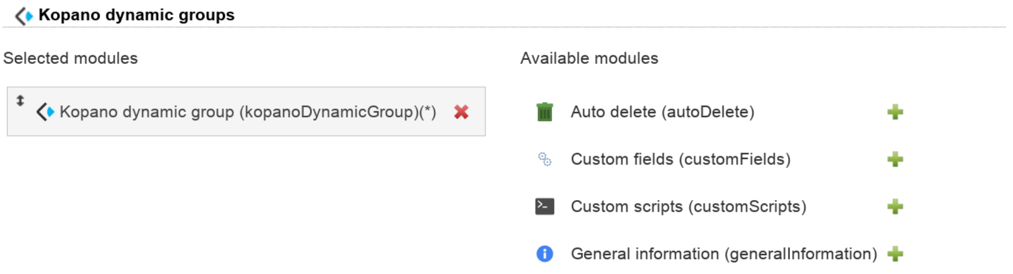
Read-only □

Hidden □

No new entries □

Disallow delete □

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



Kopano dynamic groups

Selected modules

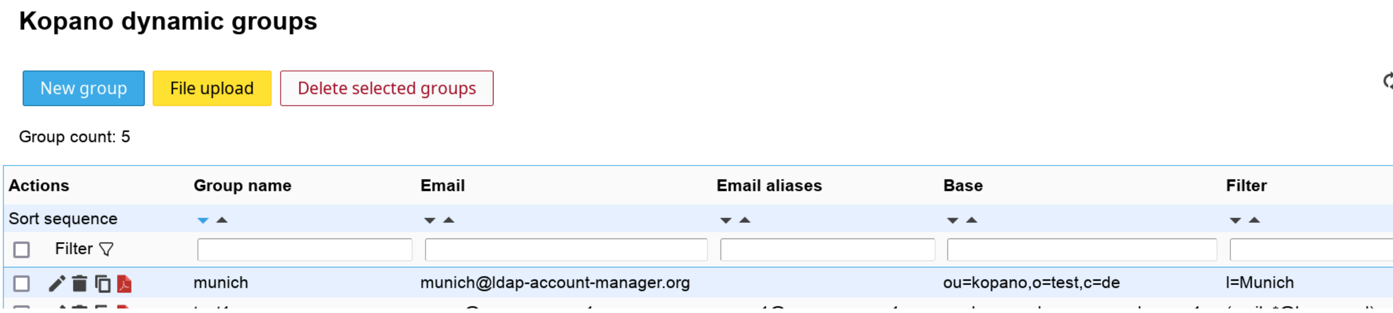
- Kopano dynamic group (kopanoDynamicGroup)(*)

Available modules

- Auto delete (autoDelete)
- Custom fields (customFields)
- Custom scripts (customScripts)
- General information (generalInformation)

Usage

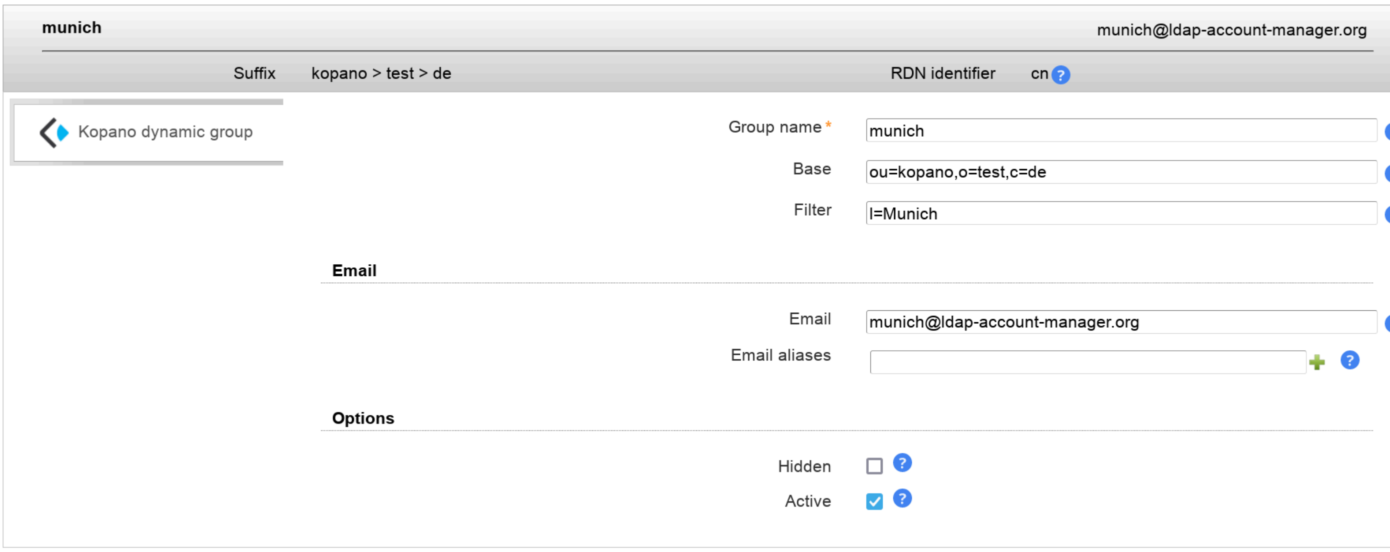
LAM Pro will now display the Kopano address list tab.



Kopano dynamic groups

Group count: 5

Actions	Group name	Email	Email aliases	Base	Filter
Sort sequence	▼ ▲	▼ ▲	▼ ▲	▼ ▲	▼ ▲
□ Filter					
□	munich	munich@ldap-account-manager.org		ou=kopano,o=test,c=de	l=Munich



munich munich@ldap-account-manager.org

Suffix kopano > test > de RDN identifier cn

Group name * munich

Base ou=kopano,o=test,c=de

Filter l=Munich

Email

Email munich@ldap-account-manager.org

Email aliases

Options

Hidden □

Active ☑

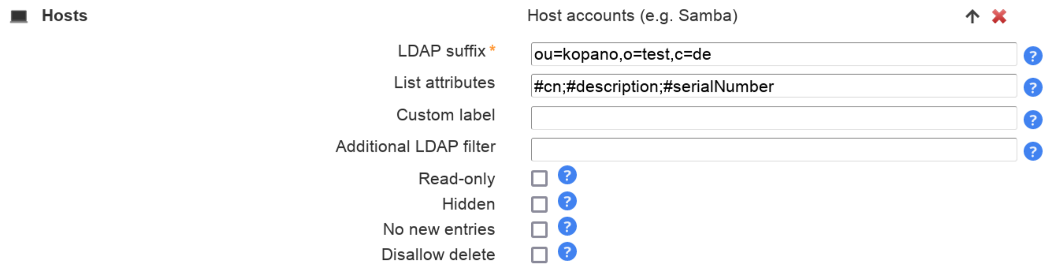
Servers

Configuration

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

Hosts — Host accounts (e.g. Samba)

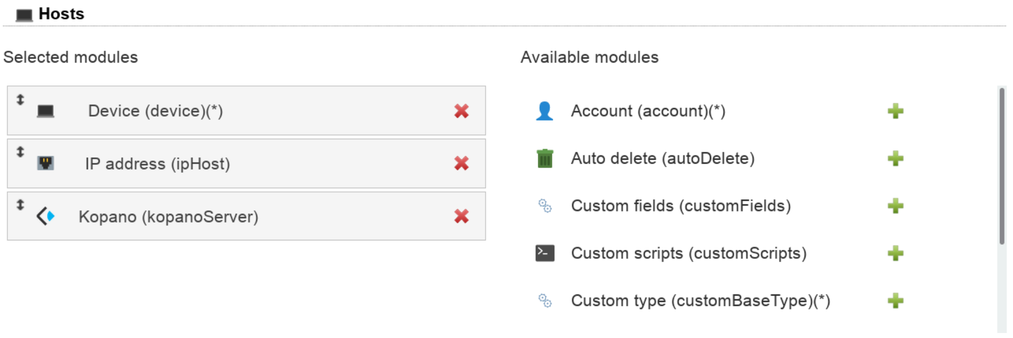
Adjust the suffix and list attributes to your needs.



Hosts — Host accounts (e.g. Samba)

LDAP suffix *	ou=kopano,o=test,c=de
List attributes	#cn;#description;#serialNumber
Custom label	
Additional LDAP filter	
Read-only	□
Hidden	□
No new entries	□
Disallow delete	□

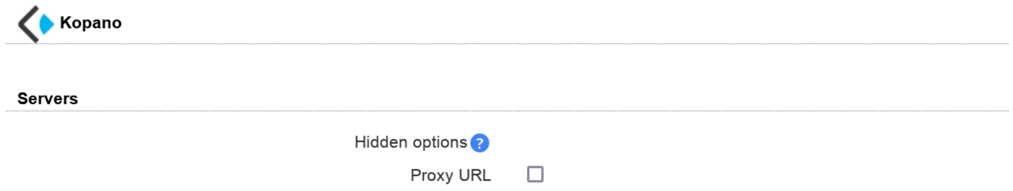
Then select the Kopano server module (tab Modules).



Hosts

Selected modules	Available modules
Device (device)(*)	Account (account)(*)
IP address (ipHost)	Auto delete (autoDelete)
Kopano (kopanoServer)	Custom fields (customFields)
	Custom scripts (customScripts)
	Custom type (customBaseType)(*)

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



Kopano

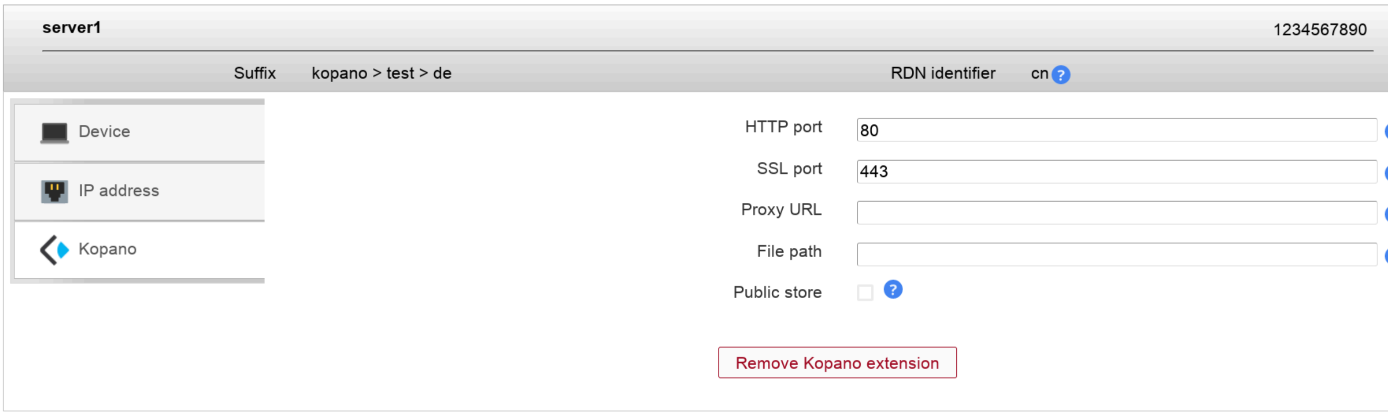
Servers

Hidden options

Proxy URL □

Usage

LAM Pro will now display the Kopano tab on your hosts. The Kopano extension can be added and removed at any time for every server.



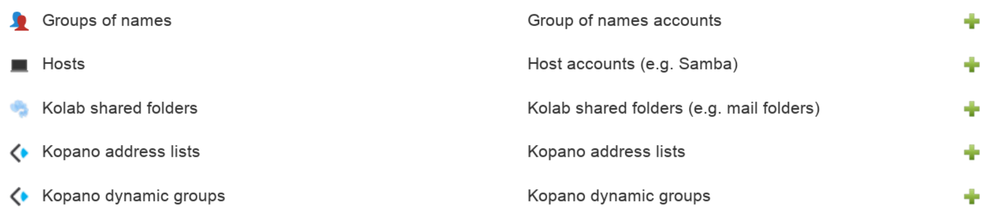
server1 1234567890

Suffix kopano > test > de RDN identifier cn

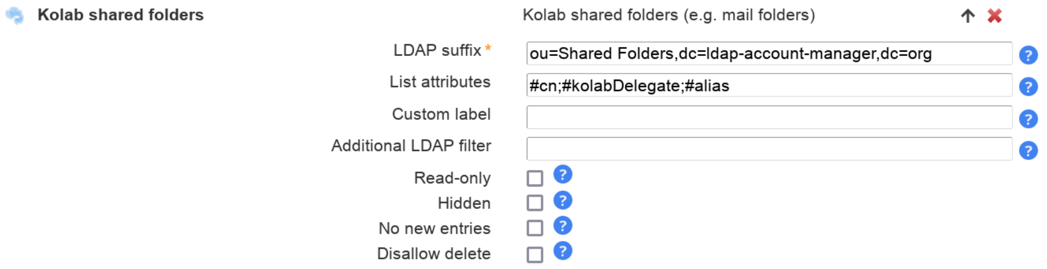
HTTP port	80
SSL port	443
Proxy URL	
File path	
Public store	□

Kolab shared folders

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



Groups of names	Group of names accounts	✚
Hosts	Host accounts (e.g. Samba)	✚
Kolab shared folders	Kolab shared folders (e.g. mail folders)	✚
Kopano address lists	Kopano address lists	✚
Kopano dynamic groups	Kopano dynamic groups	✚



Kolab shared folders Kolab shared folders (e.g. mail folders)

LDAP suffix * ou=Shared Folders,dc=ldap-account-manager,dc=org

List attributes #cn;#kolabDelegate;#alias

Custom label

Additional LDAP filter

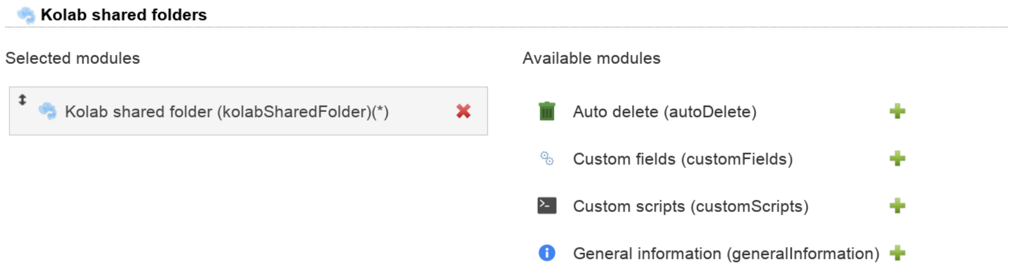
Read-only □

Hidden □

No new entries □

Disallow delete □

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



Kolab shared folders

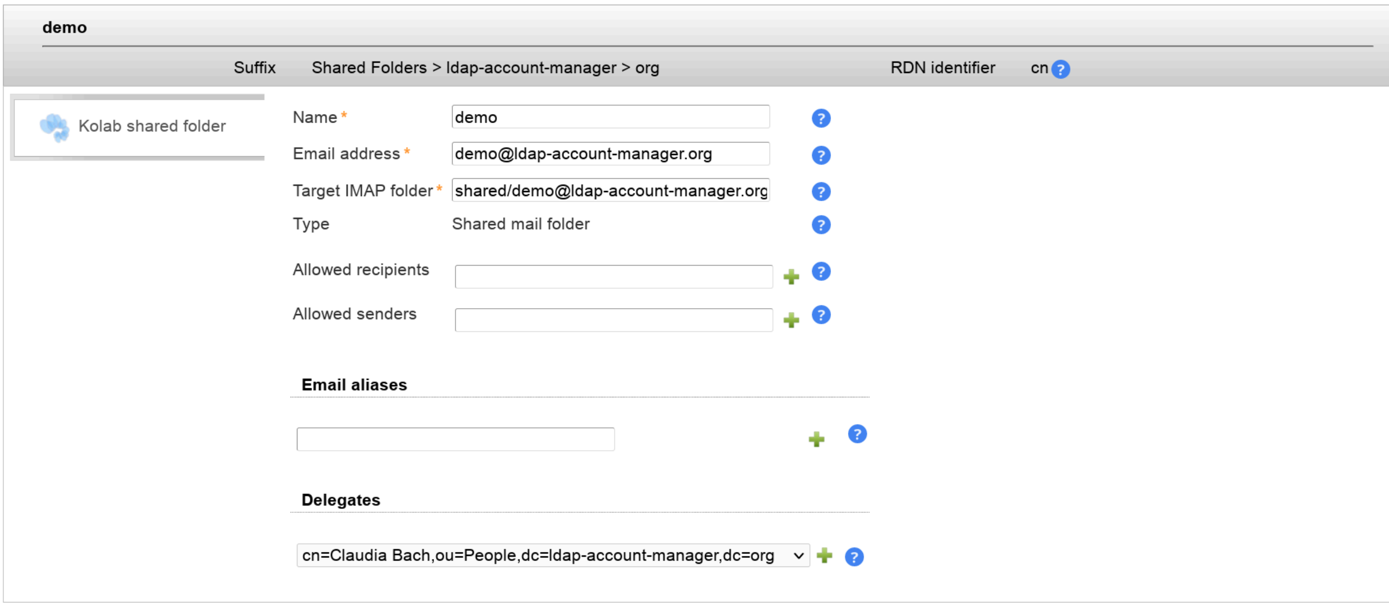
Selected modules

- Kolab shared folder (kolabSharedFolder)(*)

Available modules

- Auto delete (autoDelete) ✚
- Custom fields (customFields) ✚
- Custom scripts (customScripts) ✚
- General information (generalInformation) ✚

Now you can start to add shared folders inside LAM.



demo

Suffix Shared Folders > ldap-account-manager > org RDN identifier cn

Kolab shared folder

Name * demo

Email address * demo@ldap-account-manager.org

Target IMAP folder * shared/demo@ldap-account-manager.org

Type Shared mail folder

Allowed recipients

Allowed senders

Email aliases

Delegates

cn=Claudia Bach,ou=People,dc=ldap-account-manager,dc=org

DHCP

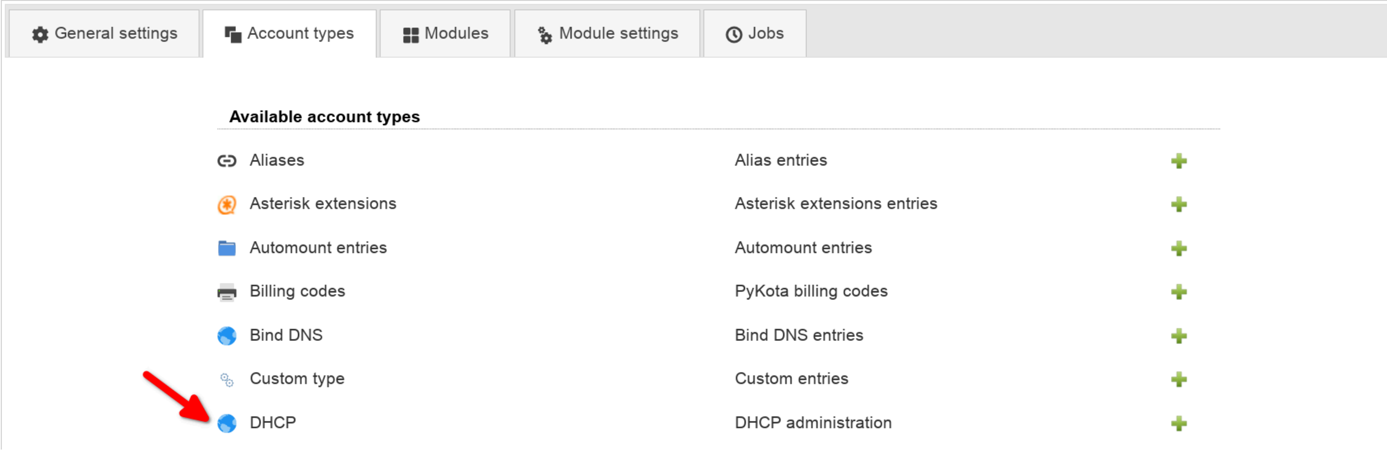
You can manage your DHCP server with LAM. It supports to manage subnets, fixed IP entries, IP ranges and DDNS.

Configuration

The DHCP management can be activated by adding the account type DHCP to your server profile. Please also add the DHCP modules.

LAM requires that you use an LDAP entry with the object class "dhcpService" or "dhcpServer" as suffix for this account type. If the "dhcpServer" entry points to a "dhcpService" entry via "dhcpServiceDN" then you need to use the DN of the "dhcpService" entry as LDAP suffix for DHCP.

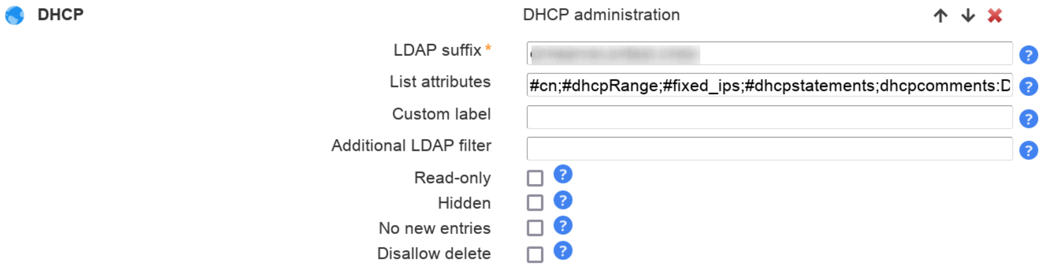
Add account type:



Available account types

Aliases	Alias entries	✚
Asterisk extensions	Asterisk extensions entries	✚
Automount entries	Automount entries	✚
Billing codes	PyKota billing codes	✚
Bind DNS	Bind DNS entries	✚
Custom type	Custom entries	✚
DHCP	DHCP administration	✚

Set suffix:



DHCP DHCP administration

LDAP suffix * [redacted]

List attributes #cn;#dhcpRange;#fixed_ips;#dhcpstatements;dhcpcomments:D

Custom label

Additional LDAP filter

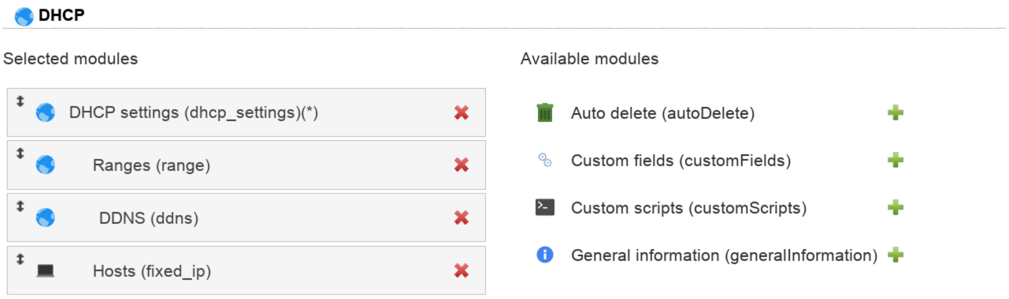
Read-only □

Hidden □

No new entries □

Disallow delete □

Add modules:



DHCP

Selected modules

- DHCP settings (dhcp_settings)(*) ✖
- Ranges (range) ✖
- DDNS (ddns) ✖
- Hosts (fixed_ip) ✖

Available modules

- Auto delete (autoDelete) ✚
- Custom fields (customFields) ✚
- Custom scripts (customScripts) ✚
- General information (generalInformation) ✚

Example server entry:

```
dn: cn=server,ou=dhcp,dc=ldap-account-manager,dc=org

objectclass: dhcpServer

objectclass: dhcpOptions

objectclass: top

cn: server

dhcpcomments: My DHCP server

dhcpoption: domain-name "ldap-account-manager.org"

dhcpoption: domain-name-servers 192.168.1.1

dhcpoption: routers 192.168.1.1

dhcpoption: netbios-name-servers 192.168.1.1

dhcpoption: subnet-mask 255.255.255.0

dhcpoption: 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";
```

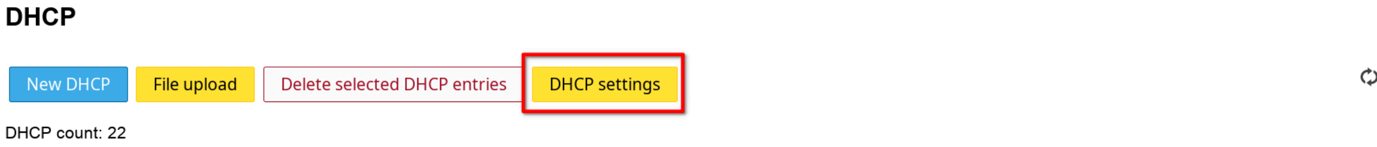
slapd.conf changes:

```
include /etc/ldap/schema/dhcp.schema
```

```
index dhcpHWAddress eq

index dhcpClassData eq
```

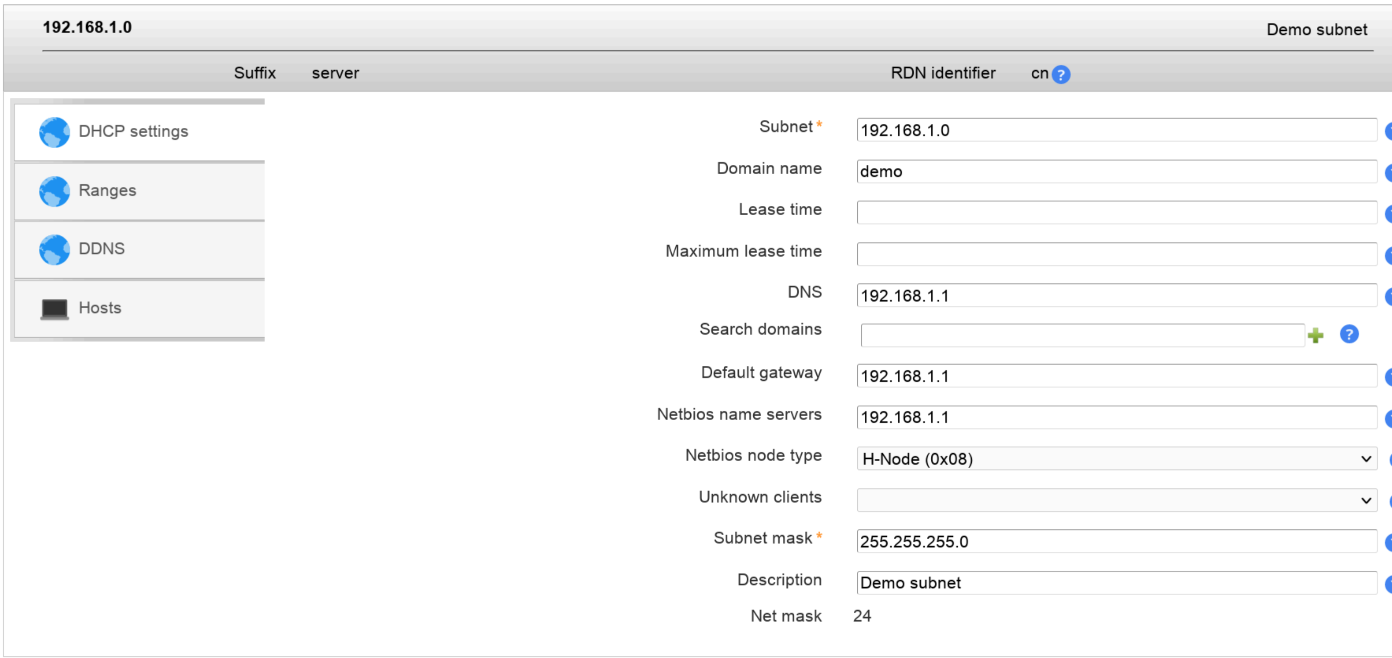
Run slapindex to rebuild the index.

You can manage the settings of your DHCP service/server entry:



DHCP count: 22

You can easily create new subnet entries.

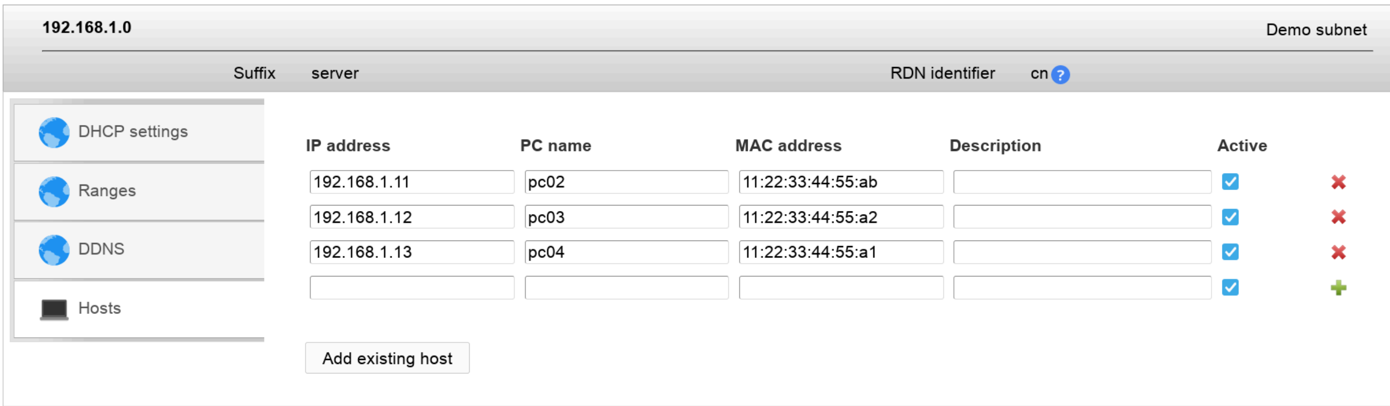


192.168.1.0 — Demo subnet

Suffix: server — RDN identifier: cn

Subnet*	192.168.1.0
Domain name	demo
Lease time	
Maximum lease time	
DNS	192.168.1.1
Search domains	
Default gateway	192.168.1.1
Netbios name servers	192.168.1.1
Netbios node type	H-Node (0x08)
Unknown clients	
Subnet mask*	255.255.255.0
Description	Demo subnet
Net mask	24

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



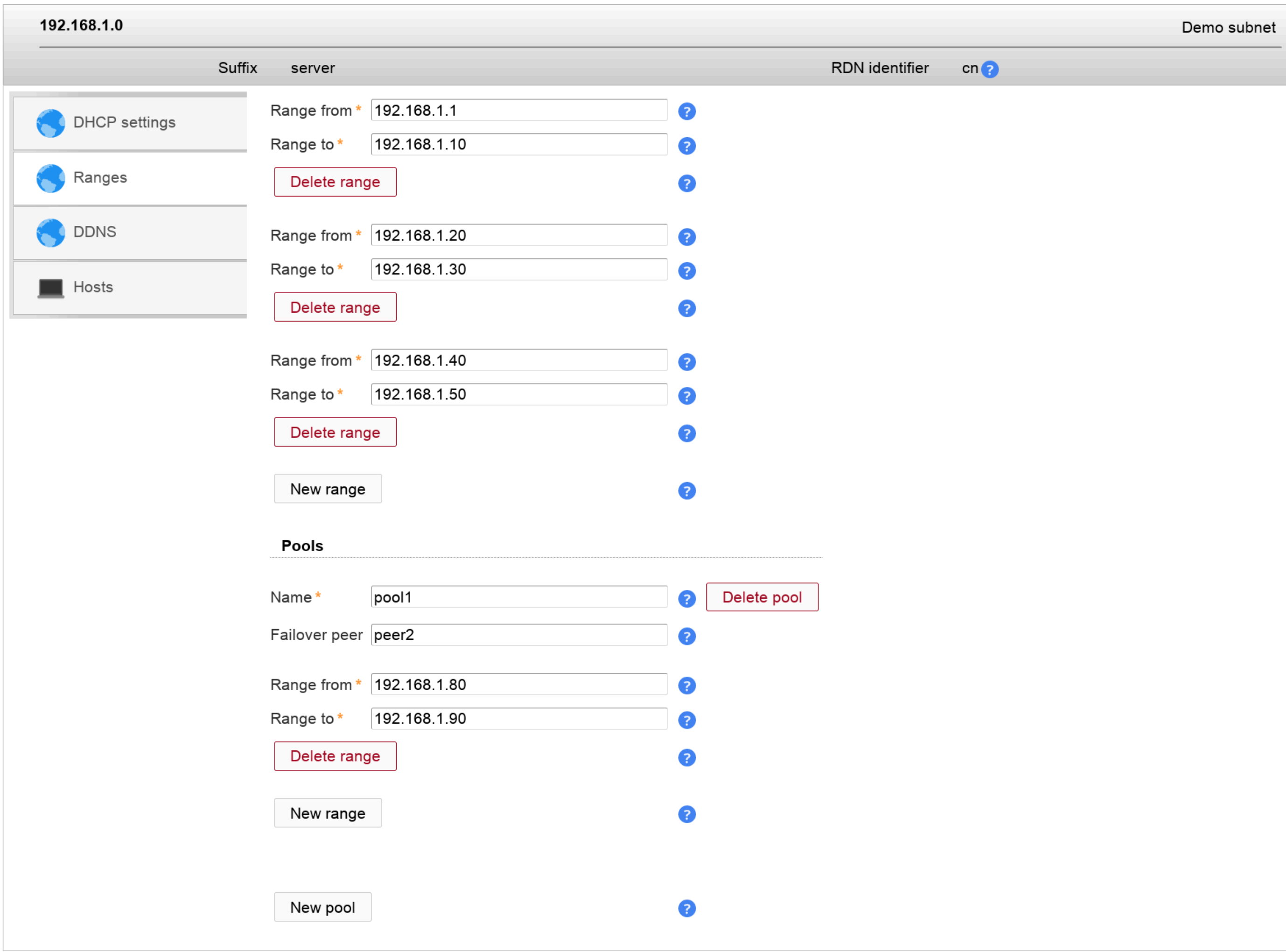
192.168.1.0 — Demo subnet

Suffix: server — RDN identifier: cn

IP address	PC name	MAC address	Description	Active	
192.168.1.11	pc02	11:22:33:44:55:ab		☑	✖
192.168.1.12	pc03	11:22:33:44:55:a2		☑	✖
192.168.1.13	pc04	11:22:33:44:55:a1		☑	✖
				☑	+

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.



Suffix: server

RDN identifier: cn

Range from *: 192.168.1.1
Range to *: 192.168.1.10

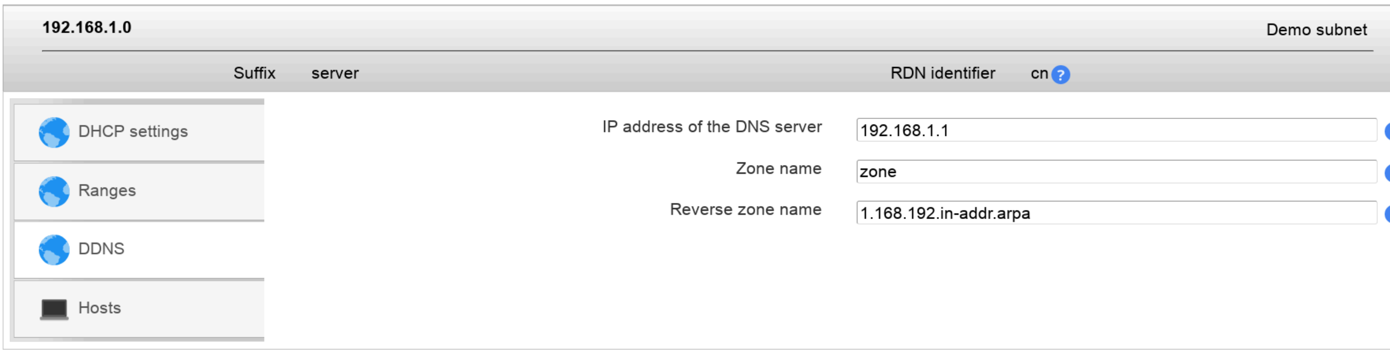
Range from *: 192.168.1.20
Range to *: 192.168.1.30

Range from *: 192.168.1.40
Range to *: 192.168.1.50

Name *: pool1
Failover peer: peer2

Range from *: 192.168.1.80
Range to *: 192.168.1.90

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



Suffix: server

RDN identifier: cn

IP address of the DNS server: 192.168.1.1

Zone name: zone

Reverse zone name: 1.168.192.in-addr.arpa

Bind dyndb-ldap (LAM Pro)

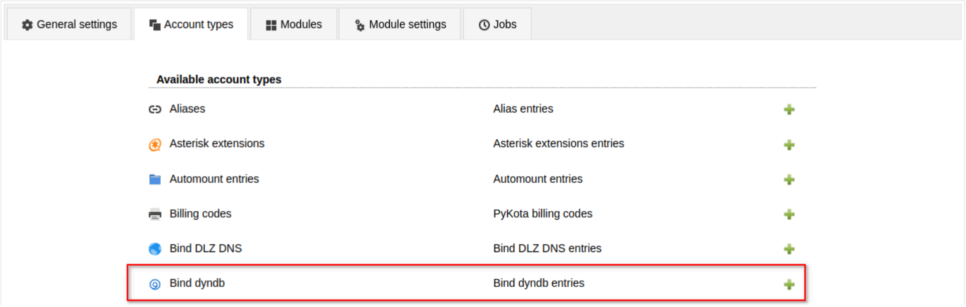
The bind-dyndb-ldap [https://pagure.io/bind-dyndb-ldap] plugin for Bind [https://www.isc.org/bind/] allows you to manage DNS entries in LDAP. Please install the bind-dyndb-ldap schema file on your LDAP server. It is part of the bind-dyndb-ldap download. LAM Pro can manage DNS zones and the following record types:

- A/AAAA: IP addresses
- CNAME: alias names

- DNAME: delegation name
- MX: mail servers
- NS: name servers
- PTR: reverse DNS entries
- SRV: service entries
- TXT: text records

Configuration

Please open your LAM server profile configuration and add two instances of the "Bind dyndb" account type. One for records and one for zones.



Available account types

Aliases	Alias entries	+
Asterisk extensions	Asterisk extensions entries	+
Automount entries	Automount entries	+
Billing codes	PyKota billing codes	+
Bind DLZ DNS	Bind DLZ DNS entries	+
Bind dyndb	Bind dyndb entries	+

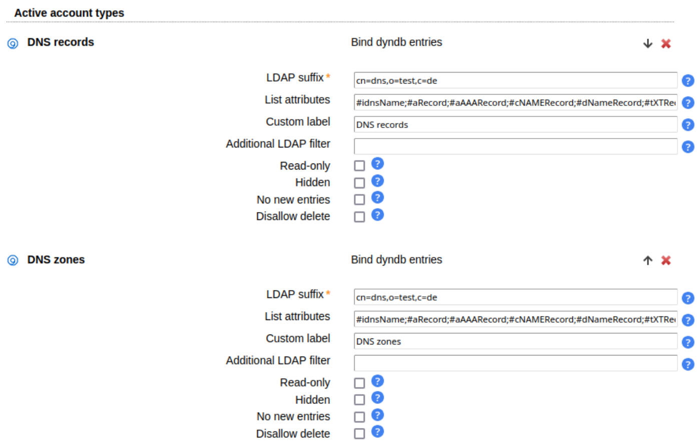
The recommended settings are as follows. Please adapt if needed.

DNS records:

- LDAP suffix: if you manage a single domain then use the DN of the zone entry. If you manage multiple domains then use the DN under which they are stored (e.g. the "nsContainer").
- List attributes: #idnsName;#aRecord;#aAAARecord;#cNAMERecord;#dNameRecord;#tXTRecord;#mxrecord;#srvrecord;#ptrrecord;#dnsttl
- Custom label: DNS records

DNS zones:

- LDAP suffix: use the DN under which the domains are stored (e.g. the "nsContainer").
- List attributes: #idnsName;#aRecord;#aAAARecord;#cNAMERecord;#dNameRecord;#tXTRecord;#idnssoaserial
- Custom label: DNS zones



Active account types

DNS records — Bind dyndb entries

LDAP suffix * cn=dns,o=test,c=de

List attributes #idnsName;#aRecord;#aAAARecord;#cNAMERecord;#dNameRecord;#tXTRe

Custom label DNS records

Additional LDAP filter

Read-only □

Hidden □

No new entries □

Disallow delete □

DNS zones — Bind dyndb entries

LDAP suffix * cn=dns,o=test,c=de

List attributes #idnsName;#aRecord;#aAAARecord;#cNAMERecord;#dNameRecord;#tXTRe

Custom label DNS zones

Additional LDAP filter

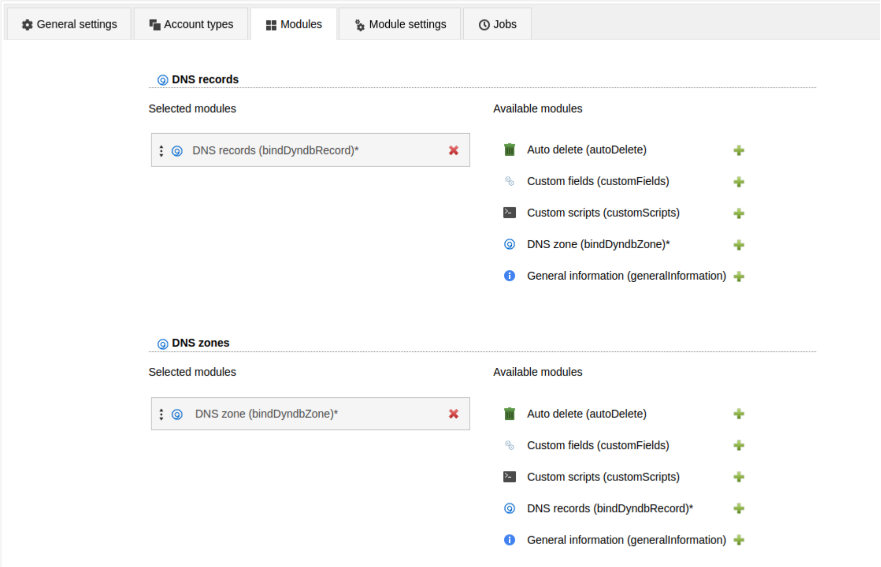
Read-only □

Hidden □

No new entries □

Disallow delete □

Next, switch to the modules tab. Here, select DNS records for your record type and DNS zone for your zone type. Then you can save the server profile and login to LAM.



DNS records

Selected modules: DNS records (bindDyndbRecord)*

Available modules:

- Auto delete (autoDelete)
- Custom fields (customFields)
- Custom scripts (customScripts)
- DNS zone (bindDyndbZone)*
- General information (generalInformation)

DNS zones

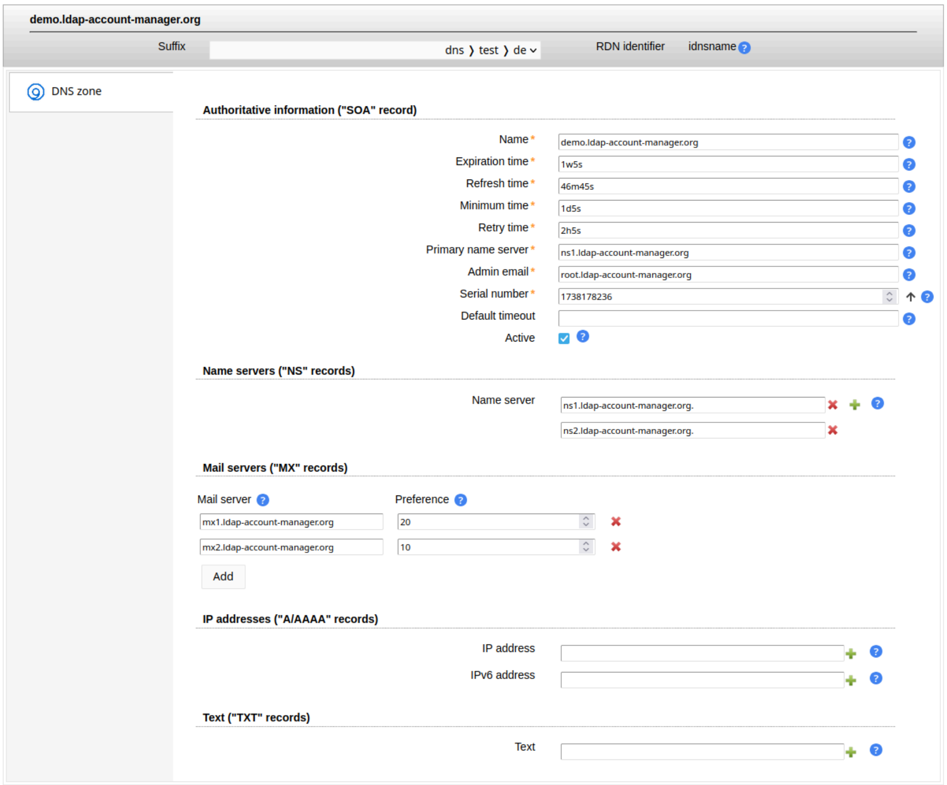
Selected modules: DNS zone (bindDyndbZone)*

Available modules:

- Auto delete (autoDelete)
- Custom fields (customFields)
- Custom scripts (customScripts)
- DNS records (bindDyndbRecord)*
- General information (generalInformation)

DNS zones

This allows you to manage your DNS zones (SOA+NS records). You can e.g. specify timeouts and name servers.



demo.ldap-account-manager.org

Suffix: dns ❭ test ❭ de — RDN identifier: idnsname

Authoritative information ("SOA" record)

Name *	demo.ldap-account-manager.org
Expiration time *	1w5s
Refresh time *	46m45s
Minimum time *	1d5s
Retry time *	2h5s
Primary name server *	ns1.ldap-account-manager.org
Admin email *	root.ldap-account-manager.org
Serial number *	1738178236
Default timeout	
Active	☑

Name servers ("NS" records)

Name server	ns1.ldap-account-manager.org.
	ns2.ldap-account-manager.org.

Mail servers ("MX" records)

Mail server	Preference
mx1.ldap-account-manager.org	20
mx2.ldap-account-manager.org	10

IP addresses ("A/AAAA" records)

IP address	
IPv6 address	

Text ("TXT" records)

Text	

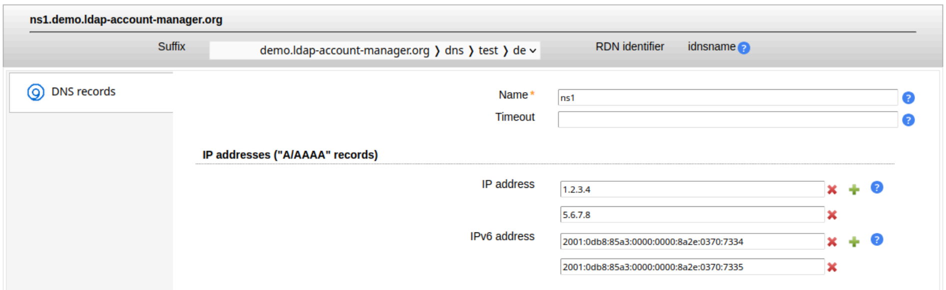
DNS entries

LAM supports the following DNS record types:

- A/AAAA: IP addresses
- CNAME: alias names
- DNAME: delegation name
- MX: mail servers
- PTR: reverse DNS entries
- SRV: service entries
- TXT: text records

IP addresses (A/AAAA)

Here you can enter IPv4 (A) or IPv6 (AAAA) addresses for a DNS name.



ns1.demo.ldap-account-manager.org

Suffix: demo.ldap-account-manager.org ❭ dns ❭ test ❭ de — RDN identifier: idnsname

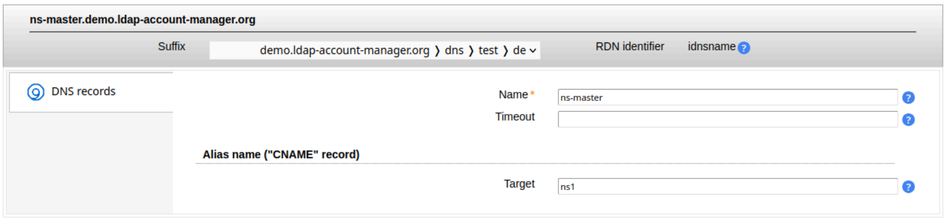
Name *	ns1
Timeout	

IP addresses ("A/AAAA" records)

IP address	1.2.3.4
	5.6.7.8
IPv6 address	2001:0db8:85a3:0000:0000:8a2e:0370:7334
	2001:0db8:85a3:0000:0000:8a2e:0370:7335

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.



ns-master.demo.ldap-account-manager.org

Suffix: demo.ldap-account-manager.org ❭ dns ❭ test ❭ de

RDN identifier: idnsname

Name*: ns-master

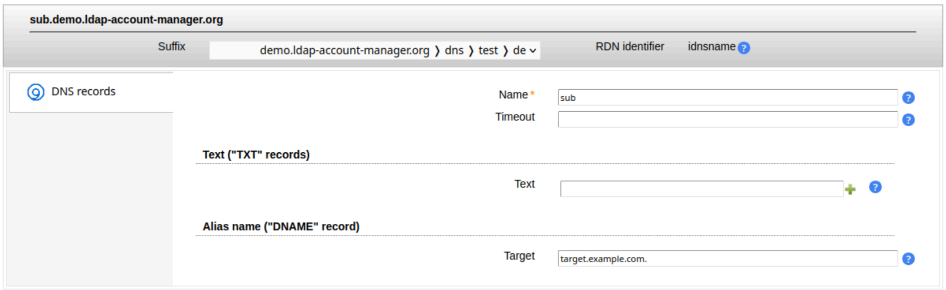
Timeout:

Alias name ("CNAME" record)

Target: ns1

Alias names (DNAME)

You can delegate a DNS zone to a different server.



sub.demo.ldap-account-manager.org

Suffix: demo.ldap-account-manager.org ❭ dns ❭ test ❭ de

RDN identifier: idnsname

Name*: sub

Timeout:

Text ("TXT" records)

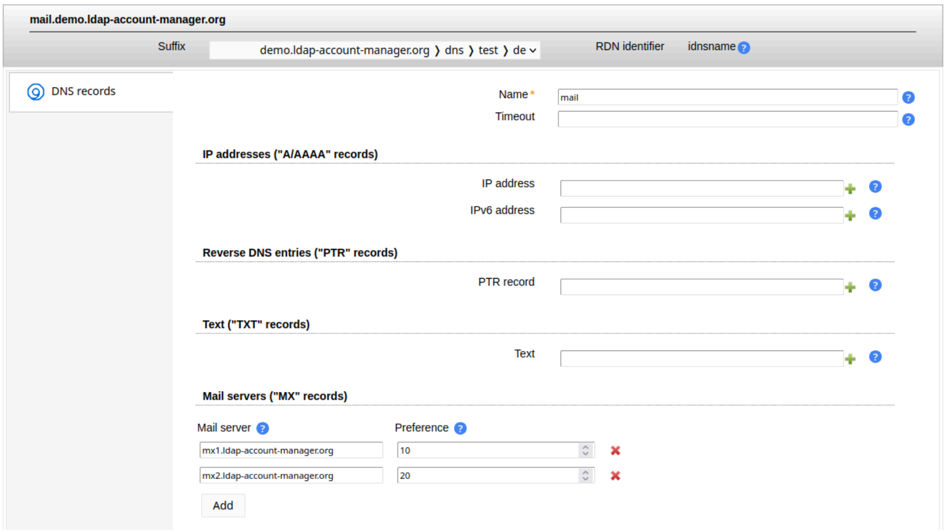
Text:

Alias name ("DNAME" record)

Target: target.example.com.

Mail servers (MX)

The mail server entries define where mails to a domain should be delivered. The server with the lowest preference has the highest priority.



mail.demo.ldap-account-manager.org

Suffix: demo.ldap-account-manager.org ❭ dns ❭ test ❭ de

RDN identifier: idnsname

Name*: mail

Timeout:

IP addresses ("A/AAAA" records)

IP address:

IPv6 address:

Reverse DNS entries ("PTR" records)

PTR record:

Text ("TXT" records)

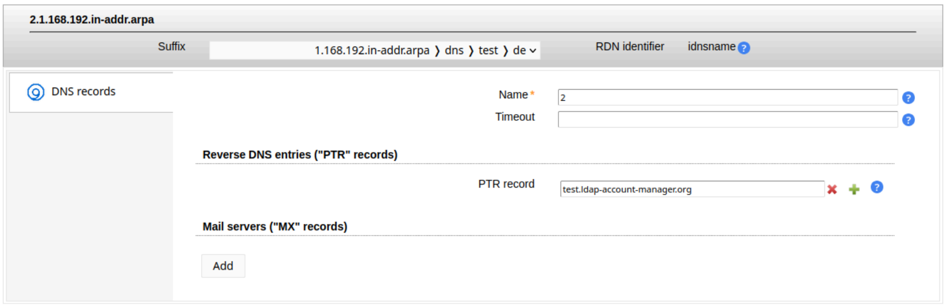
Text:

Mail servers ("MX" records)

Mail server	Preference
mx1.ldap-account-manager.org	10
mx2.ldap-account-manager.org	20

Reverse DNS entries (PTR)

Reverse DNS entries are important when you need to find the DNS name that is associated with a given IP address. Reverse DNS entries are stored in a separate DNS zone.



2.1.168.192.in-addr.arpa

Suffix: 1.168.192.in-addr.arpa ❯ dns ❯ test ❯ de

RDN identifier: idnsname

DNS records

Name*: 2

Timeout:

Reverse DNS entries ("PTR" records)

PTR record: test.ldap-account-manager.org

Mail servers ("MX" records)

Add

Services (SRV)

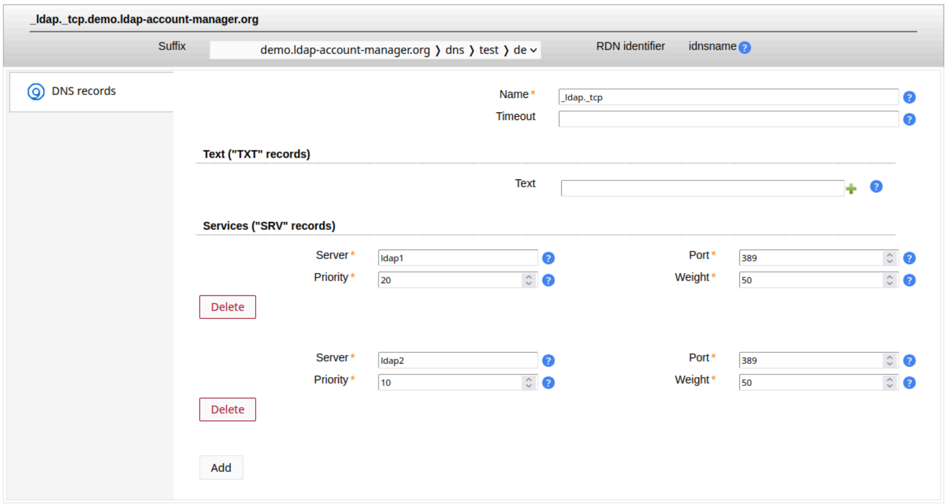
Service records can be used to specify which servers provide common services such as LDAP. Please note that the host name must be _SERVICE._PROTOCOL (e.g. _ldap._tcp).

Priority: The priority of the target host, lower value means more preferred.

Weight: A relative weight for records with the same priority. E.g. weights 20 and 80 for a service will result in 20% queries to the one server and 80% to the other.

Port: The port number that is used for your service.

Server: DNS name where service can be reached (relative without or absolute with dot at the end).



_ldap._tcp.demo.ldap-account-manager.org

Suffix: demo.ldap-account-manager.org ❯ dns ❯ test ❯ de

RDN identifier: idnsname

DNS records

Name*: _ldap._tcp

Timeout:

Text ("TXT" records)

Text:

Services ("SRV" records)

Server*: ldap1
Priority*: 20
Port*: 389
Weight*: 50

Delete

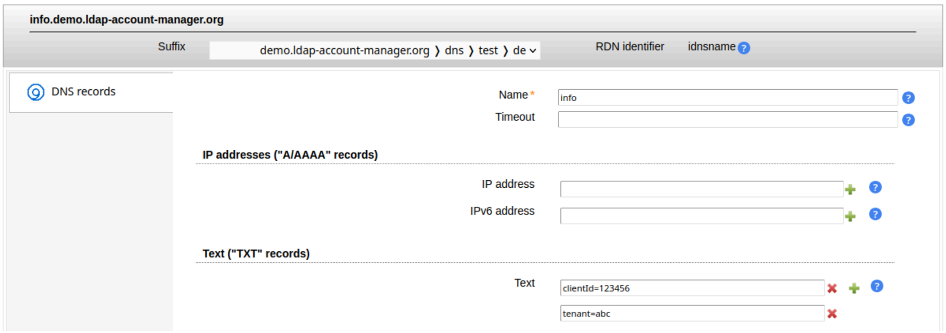
Server*: ldap2
Priority*: 10
Port*: 389
Weight*: 50

Delete

Add

Text records (TXT)

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



info.demo.ldap-account-manager.org

Suffix: demo.ldap-account-manager.org ❯ dns ❯ test ❯ de

RDN identifier: idnsname

DNS records

Name*: info

Timeout:

IP addresses ("A/AAAA" records)

IP address:

IPv6 address:

Text ("TXT" records)

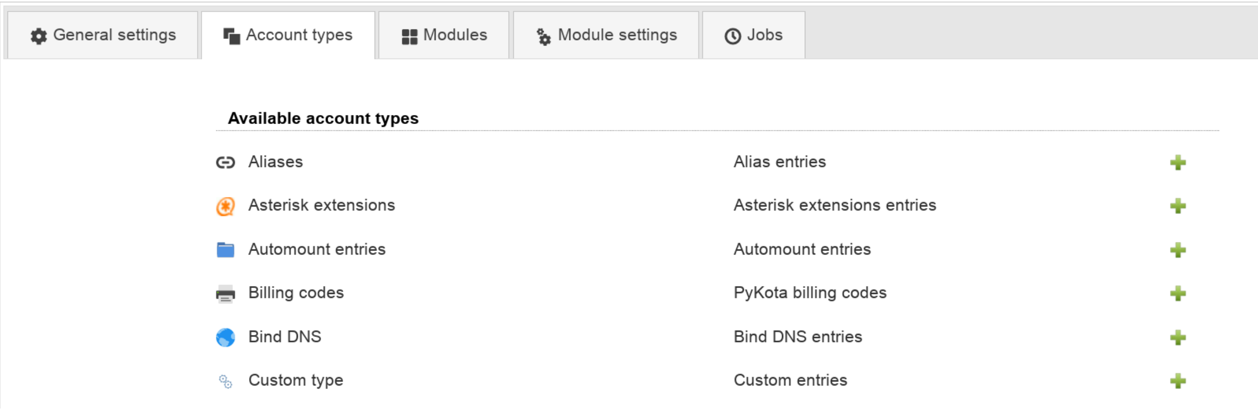
Text: clientId=123456
tenant=abc

Bind DLZ (LAM Pro)

Bind DLZ [http://bind-dlz.sourceforge.net] is an extension to the DNS server Bind [http://www.isc.org/software/bind] that allows to store DNS entries inside LDAP. Please install the Bind DLZ schema file on your LDAP server. It is part of the Bind download. You can also get it from Bind's git repository [https://gitlab.isc.org/isc-projects/bind9/blob/master/contrib/dlz/modules/ldap/testing/dlz.schema].

Configuration

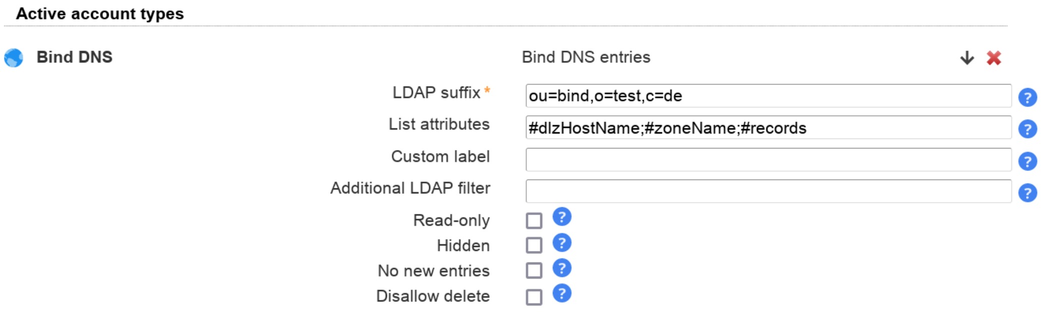
First, you need to add the Bind DNS account type and the Bind DLZ module:



Available account types

Aliases	Alias entries	➕
Asterisk extensions	Asterisk extensions entries	➕
Automount entries	Automount entries	➕
Billing codes	PyKota billing codes	➕
Bind DNS	Bind DNS entries	➕
Custom type	Custom entries	➕

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



Active account types

Bind DNS Bind DNS entries

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

List attributes #dlzHostName;#zoneName;#records

Custom label

Additional LDAP filter

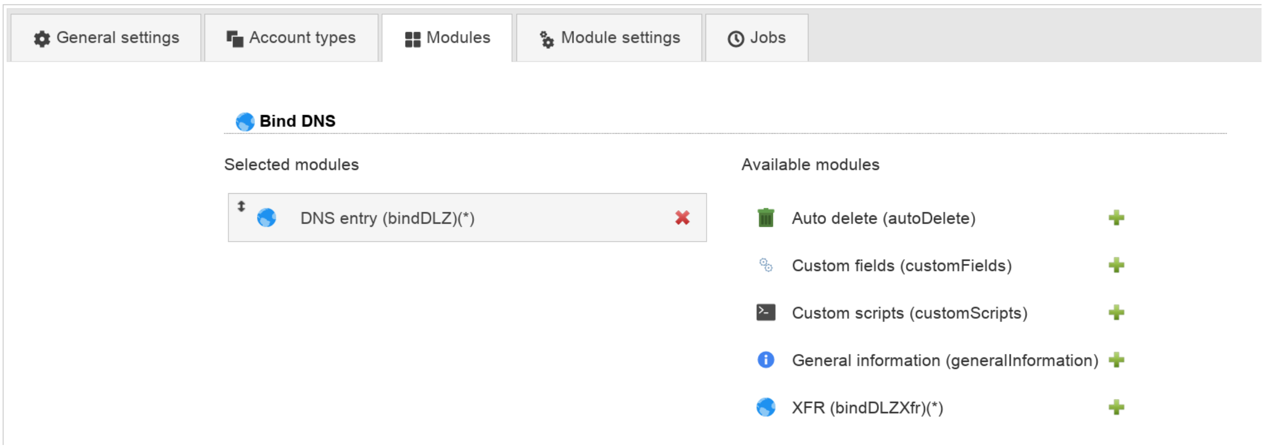
Read-only □

Hidden □

No new entries □

Disallow delete □

For regular entry management use "DNS entry (bindDLZ)(*)" module.



Bind DNS

Selected modules

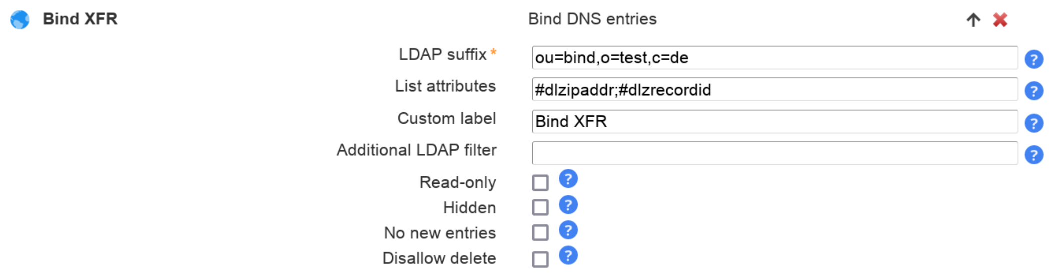
- DNS entry (bindDLZ)(*) ✖

Available modules

- Auto delete (autoDelete) ➕
- Custom fields (customFields) ➕
- Custom scripts (customScripts) ➕
- General information (generalInformation) ➕
- XFR (bindDLZXfr)(*) ➕

XFR

If you want to edit XFR entries please add a second account type for XFR. Recommended list attributes are "#dlzipaddr;#dlzrecordid".

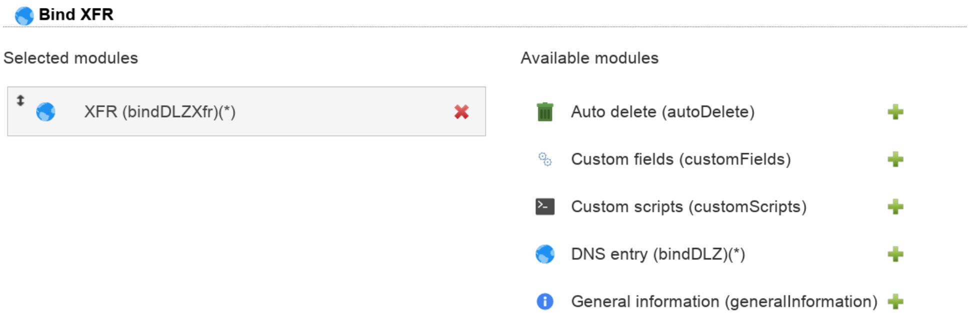


Bind XFR

Bind DNS entries

LDAP suffix *	ou=bind,o=test,c=de
List attributes	#dlzipaddr;#dlzrecordid
Custom label	Bind XFR
Additional LDAP filter	
Read-only	□
Hidden	□
No new entries	□
Disallow delete	□

Now use the "XFR (bindDLZXfr)(*)" module for this account type.



Bind XFR

Selected modules

- XFR (bindDLZXfr)(*)

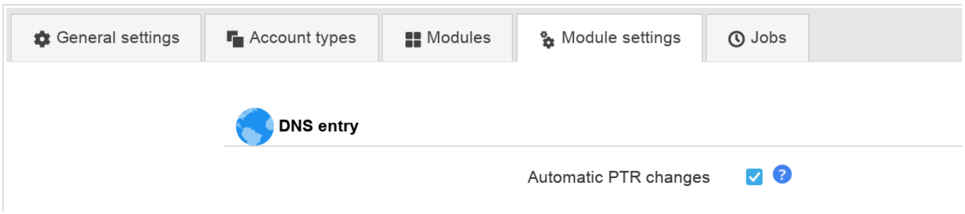
Available modules

- Auto delete (autoDelete)
- Custom fields (customFields)
- Custom scripts (customScripts)
- DNS entry (bindDLZ)(*)
- General information (generalInformation)

Automatic PTR management

LAM can automatically create/delete PTR entries for the entered IPv4/6 records. You can enable this feature on the module settings tab.

PTR records will get the same TTL as IP records. Please note that you need to have matching reverse zones (".in-addr.arpa"/".ip6.arpa") under the same suffix as your other DNS entries.



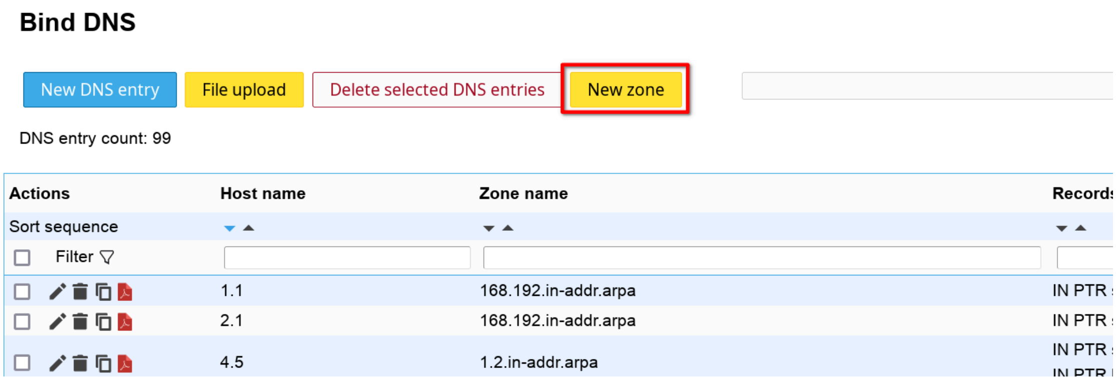
DNS entry

Automatic PTR changes ☑

Zone management

If you do not yet have a DNS zone then LAM can create one for you. In list view switch the suffix to an organizational unit DN. Now you will see a button "New zone".

This will create the zone container entry and a default DNS entry "@" for authoritative information. Now switch the suffix to your new zone and start adding DNS entries.



Bind DNS

DNS entry count: 99

Actions	Host name	Zone name	Record
Sort sequence	▼ ▲	▼ ▲	▼ ▲
☐ Filter ▽			
☐	1.1	168.192.in-addr.arpa	IN PTR
☐	2.1	168.192.in-addr.arpa	IN PTR
☐	4.5	1.2.in-addr.arpa	IN PTR IN PTR

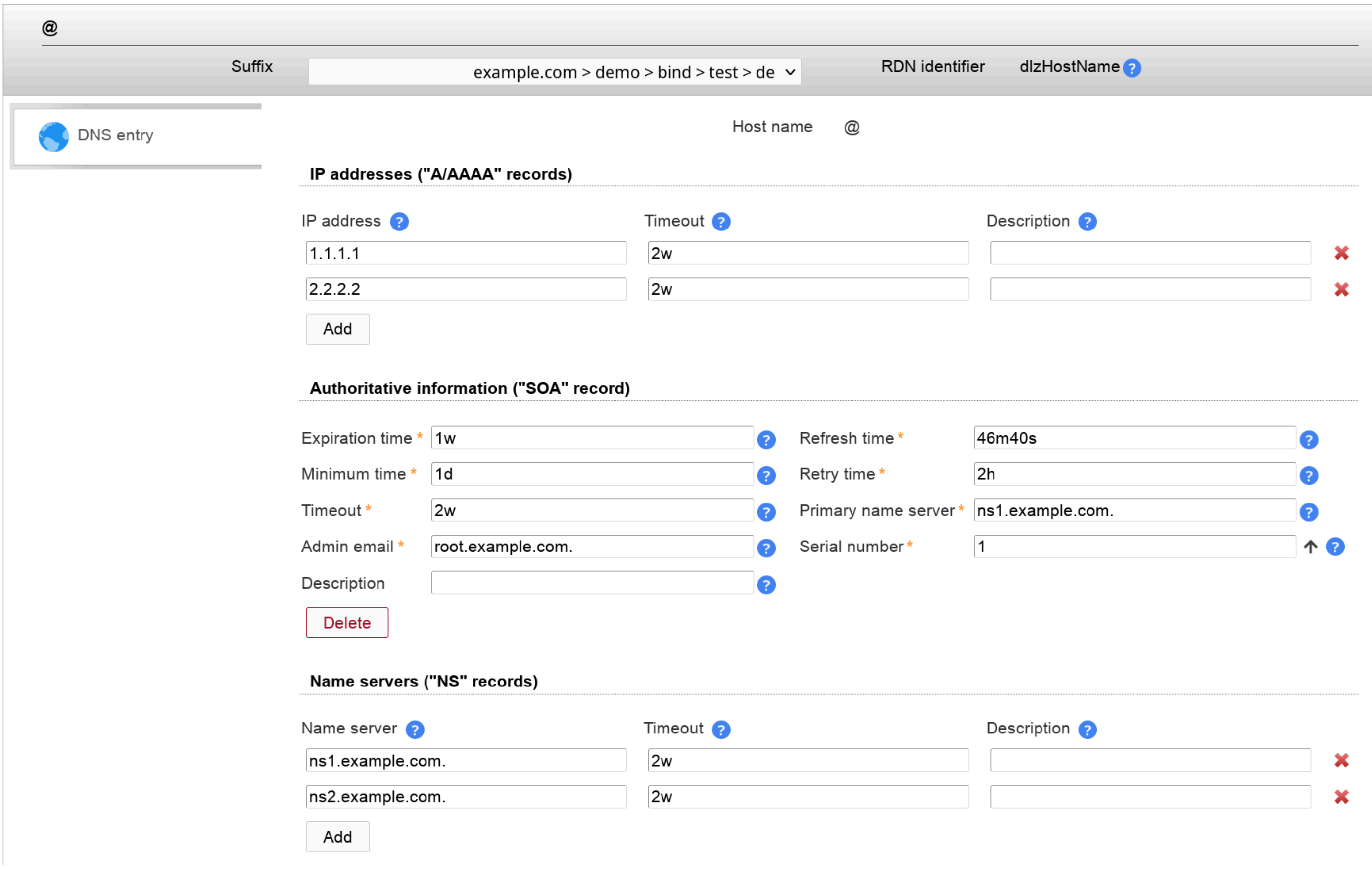
DNS entries

LAM supports the following DNS record types:

- SOA: authoritative information
- NS: name servers
- A/AAAA: IP addresses
- PTR: reverse DNS entries
- CNAME: alias names
- MX: mail servers
- TXT: text records
- SRV: service entries

Authoritative (SOA) and name server (NS) records

Here you can manage general information about the zone like timeouts and name servers. Please note that name servers must be inserted in a special format (dot at the end).



@

Suffix: example.com > demo > bind > test > de
RDN identifier: dlzHostName

DNS entry

Host name: @

IP addresses ("A/AAAA" records)

IP address	Timeout	Description
1.1.1.1	2w	
2.2.2.2	2w	

Add

Authoritative information ("SOA" record)

Expiration time *	1w	Refresh time *	46m40s
Minimum time *	1d	Retry time *	2h
Timeout *	2w	Primary name server *	ns1.example.com.
Admin email *	root.example.com.	Serial number *	1
Description			

Delete

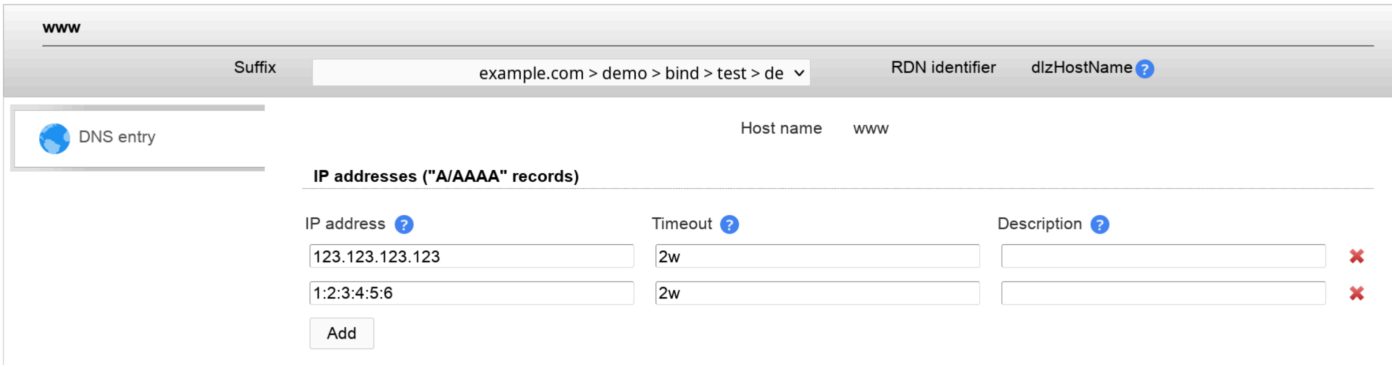
Name servers ("NS" records)

Name server	Timeout	Description
ns1.example.com.	2w	
ns2.example.com.	2w	

Add

IP addresses (A/AAAA)

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



www

Suffix: example.com > demo > bind > test > de
RDN identifier: dlzHostName

DNS entry

Host name: www

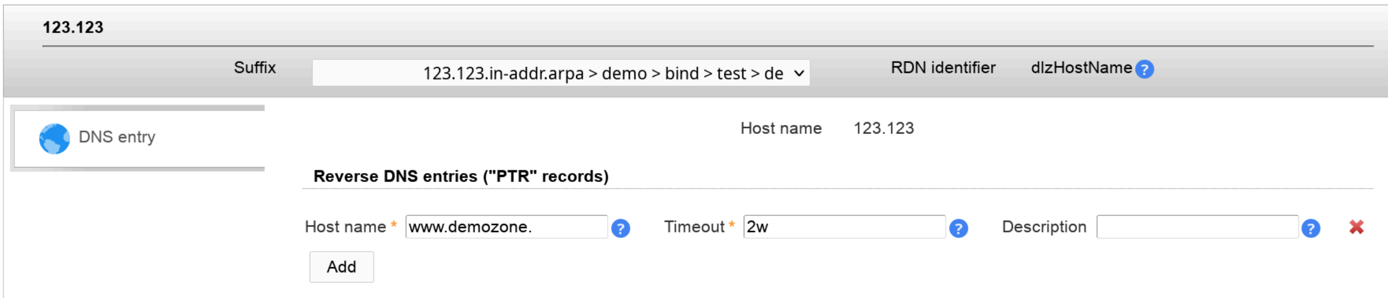
IP addresses ("A/AAAA" records)

IP address	Timeout	Description
123.123.123.123	2w	
1:2:3:4:5:6	2w	

Add

Reverse DNS entries

Reverse DNS entries are important when you need to find the DNS name that is associated with a given IP address. Reverse DNS entries are stored in a separate DNS zone.



123.123

Suffix: 123.123.in-addr.arpa > demo > bind > test > de

RDN identifier: dlzHostName

Host name: 123.123

Reverse DNS entries ("PTR" records)

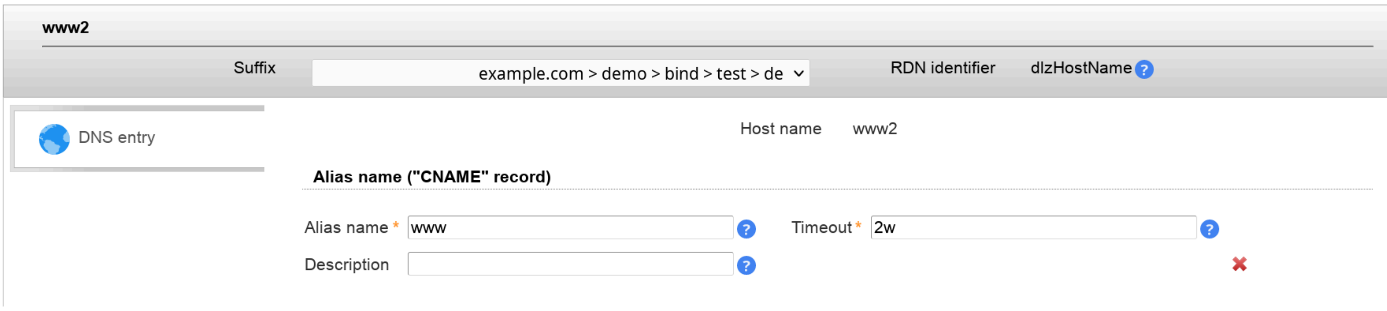
Host name *: www.demozone.

Timeout *: 2w

Description:

Alias names (CNAME)

Sometimes a DNS entry should simply point to a different DNS entry (e.g. for migrations). This can be done by adding an alias name.



www2

Suffix: example.com > demo > bind > test > de

RDN identifier: dlzHostName

Host name: www2

Alias name ("CNAME" record)

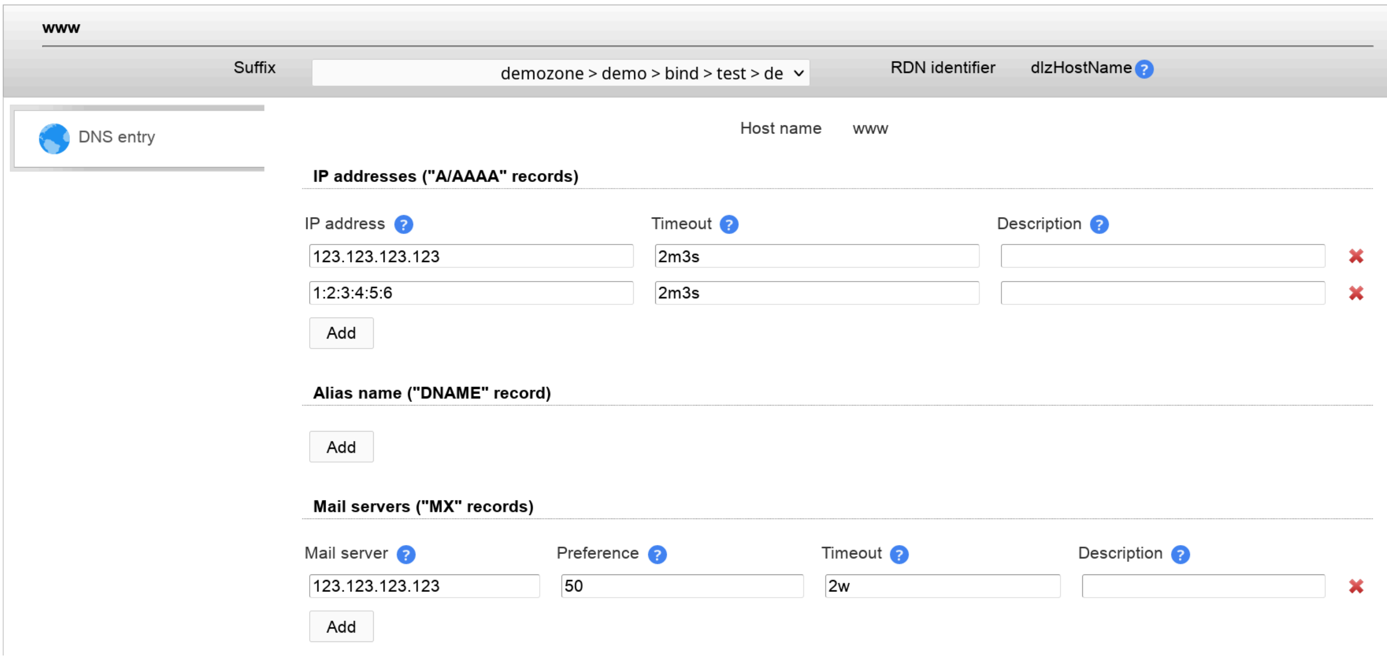
Alias name *: www

Timeout *: 2w

Description:

Mail servers (MX)

The mail server entries define where mails to a domain should be delivered. The server with the lowest preference has the highest priority.



www

Suffix: demozone > demo > bind > test > de

RDN identifier: dlzHostName

Host name: www

IP addresses ("A/AAAA" records)

IP address	Timeout	Description
123.123.123.123	2m3s	
1:2:3:4:5:6	2m3s	

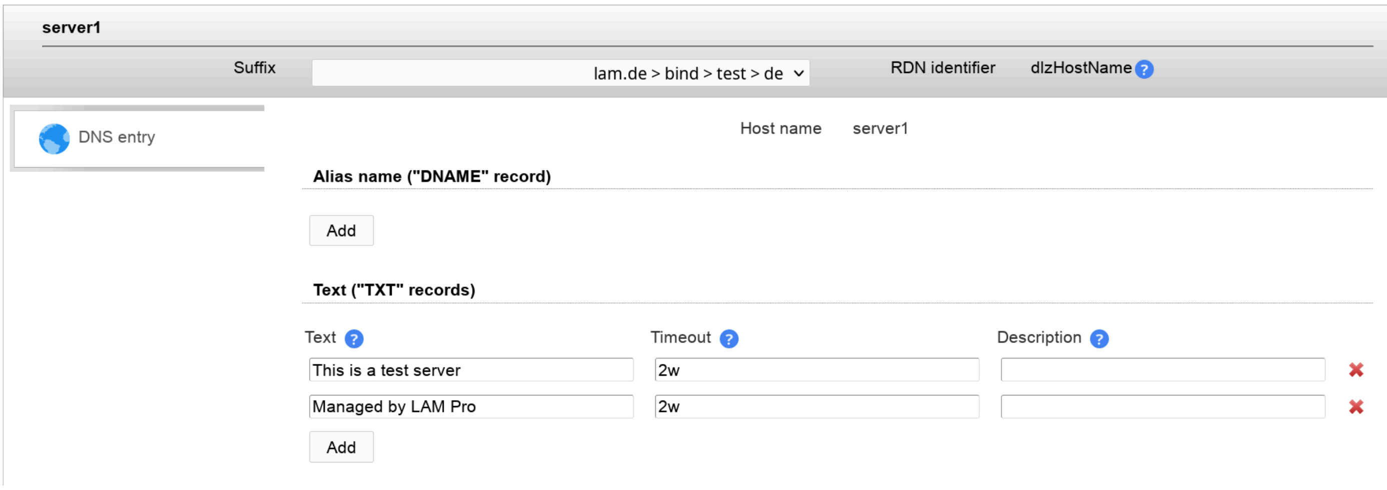
Alias name ("DNAME" record)

Mail servers ("MX" records)

Mail server	Preference	Timeout	Description
123.123.123.123	50	2w	

Text records (TXT)

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



server1

Suffix: lam.de > bind > test > de

RDN identifier: dlzHostName

Host name: server1

Alias name ("DNAME" record)

Text ("TXT" records)

Text	Timeout	Description
This is a test server	2w	
Managed by LAM Pro	2w	

Services (SRV)

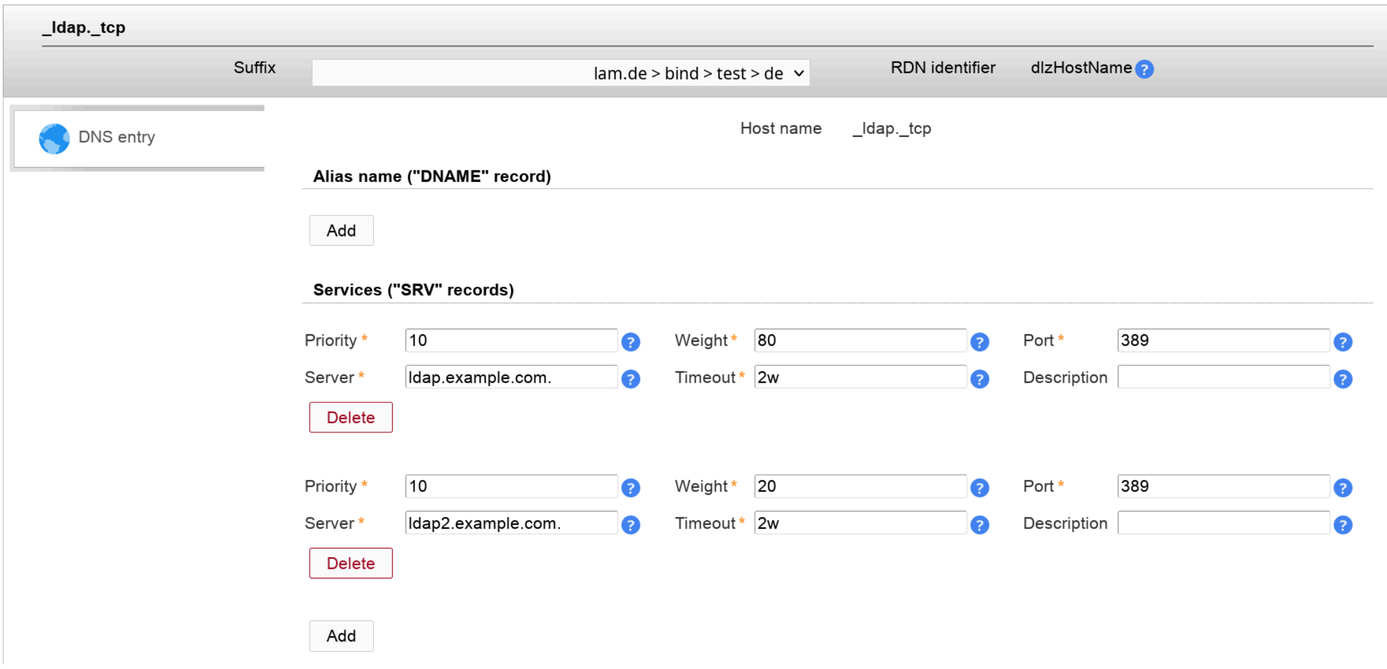
Service records can be used to specify which servers provide common services such as LDAP. Please note that the host name must be _SERVICE._PROTOCOL (e.g. _ldap._tcp).

Priority: The priority of the target host, lower value means more preferred.

Weight: A relative weight for records with the same priority. E.g. weights 20 and 80 for a service will result in 20% queries to the one server and 80% to the other.

Port: The port number that is used for your service.

Server: DNS name where service can be reached (with dot at the end).



_ldap._tcp

Suffix: lam.de > bind > test > de

RDN identifier: dlzHostName

Host name: _ldap._tcp

Alias name ("DNAME" record)

Services ("SRV" records)

Priority *: 10
Weight *: 80
Port *: 389
Server *: ldap.example.com.
Timeout *: 2w
Description:

Priority *: 10
Weight *: 20
Port *: 389
Server *: ldap2.example.com.
Timeout *: 2w
Description:

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.ns1.example.com (1 360000 3600 3600000 370000)
	IN	NS	ns1.example.com.
	IN	NS	ns2.example.com.
	IN	MX	10 mail1.example.com
	IN	MX	20 mail2.example.com
foo	IN	A	123.123.123.100
foo2	IN	CNAME	foo.example.com
bar	IN	A	123.123.123.101
	IN	AAAA	1:2:3:4:5

Please check that you have an existing zone entry that can be used for the file upload. See above to create a new zone.

Hint: If you use the function above to create a new zone then please skip the "@" entry in the CSV file below. LAM creates this entry with sample data.

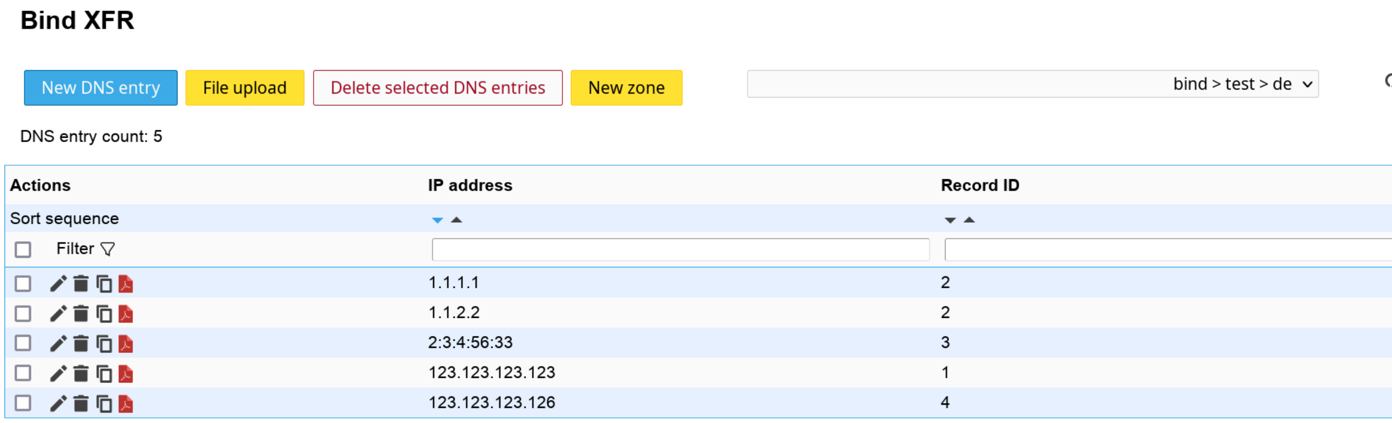
In this example we assume that the following zone entry exists:

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

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

XFR entries

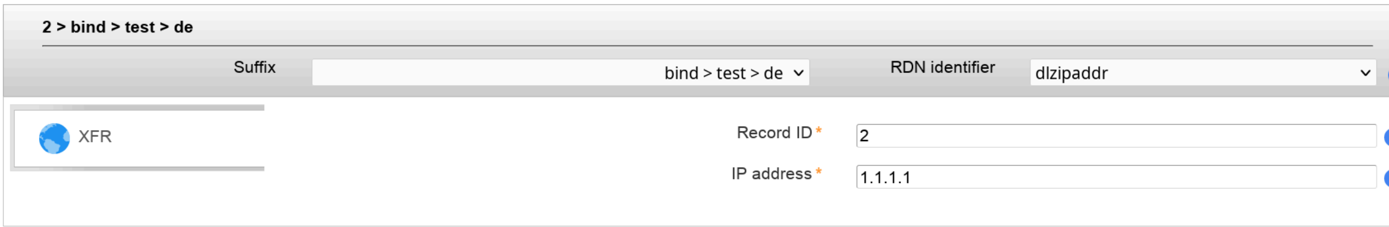
You can manage the XFR entries in the second tab that you configured before.



DNS entry count: 5

Actions	IP address	Record ID
Sort sequence		
□ Filter		
□	1.1.1.1	2
□	1.1.2.2	2
□	2:3:4:56:33	3
□	123.123.123.123	1
□	123.123.123.126	4

For each XFR entry you can set a record ID and the IP address.



2 > bind > test > de

Suffix: bind > test > de

RDN identifier: dlzipaddr

XFR

Record ID*: 2

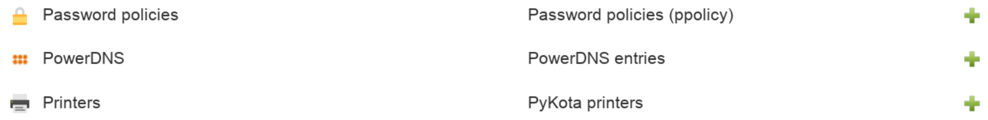
IP address*: 1.1.1.1

PowerDNS (LAM Pro)

This module allows to manage DNS entries for the PowerDNS name server.

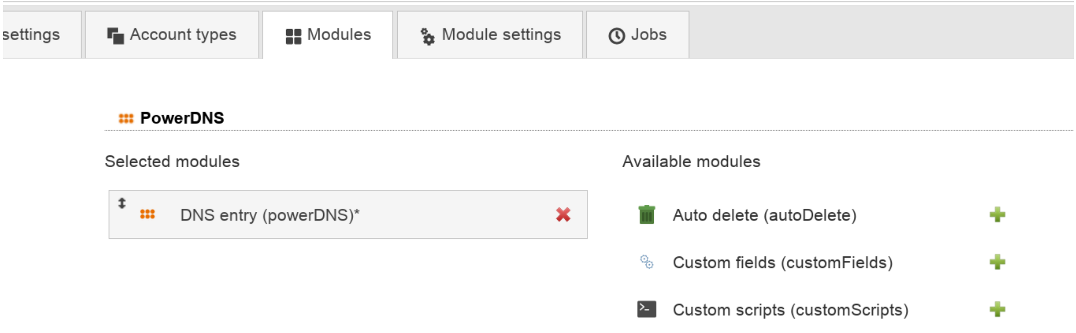
Configuration

First, add the PowerDNS account type to your server profile:



Password policies	Password policies (ppolicy)	✚
PowerDNS	PowerDNS entries	✚
Printers	PyKota printers	✚

Second, add the PowerDNS module to the new account type:



PowerDNS

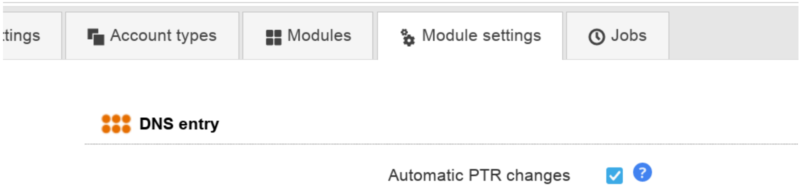
Selected modules

- DNS entry (powerDNS)* ✖

Available modules

- Auto delete (autoDelete) ✚
- Custom fields (customFields) ✚
- Custom scripts (customScripts) ✚

Third, activate automatic generation of PTR entries if needed. This is only required if you did not configure PowerDNS itself to generate PTR entries dynamically.



DNS entry

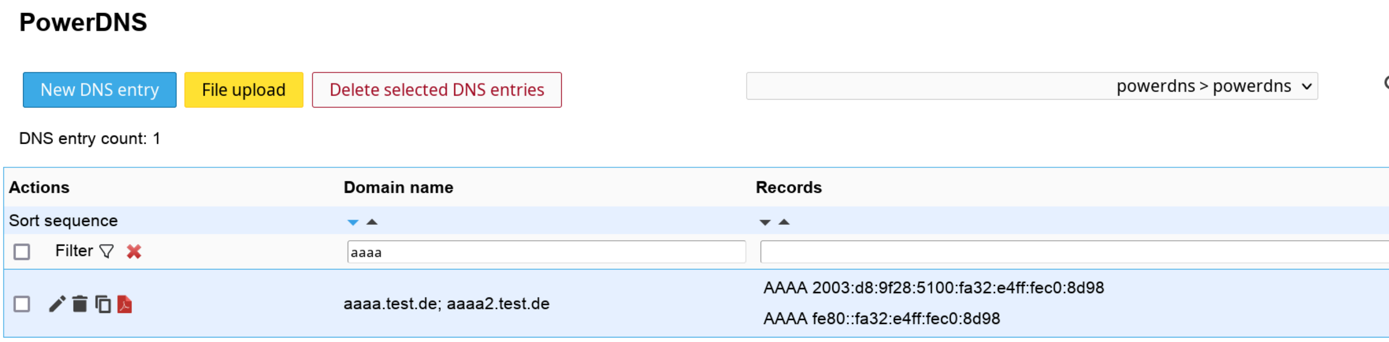
Automatic PTR changes ☑

Manage DNS entries

Now you can manage your DNS entries inside LAM.

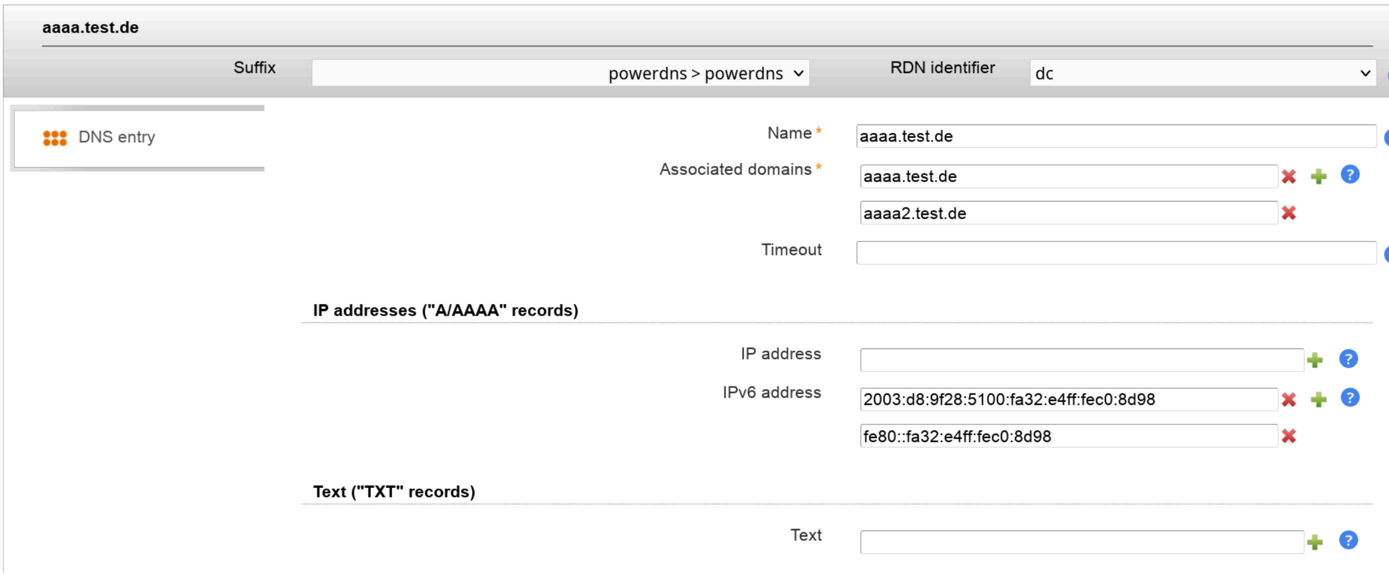
LAM supports the following record types:

- A
- AAAA
- CNAME
- DNAME
- MX
- NS
- PTR
- SOA
- SRV
- TXT



DNS entry count: 1

Actions	Domain name	Records
Filter	aaaa	
☐	aaaa.test.de; aaaa2.test.de	AAAA 2003:d8:9f28:5100:fa32:e4ff:fec0:8d98 AAAA fe80::fa32:e4ff:fec0:8d98

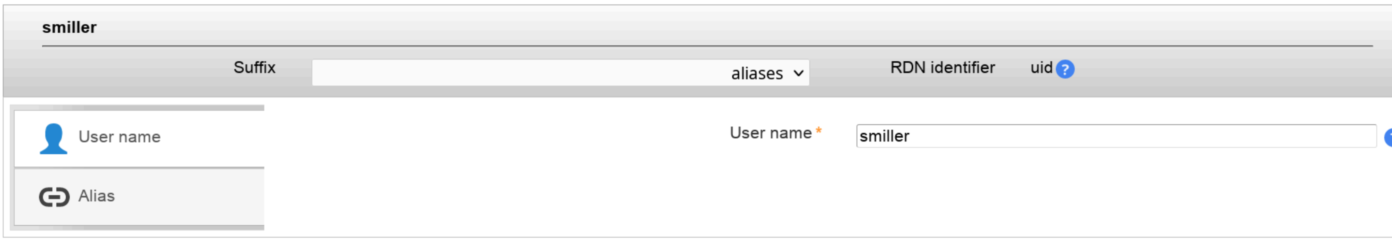


Suffix	powerdns > powerdns
RDN identifier	dc
Name *	aaaa.test.de
Associated domains *	aaaa.test.de aaaa2.test.de
Timeout	
IP address	
IPv6 address	2003:d8:9f28:5100:fa32:e4ff:fec0:8d98 fe80::fa32:e4ff:fec0:8d98
Text	

Aliases (LAM Pro)

Some applications use the object class "alias" to link LDAP entries to other parts of the LDAP tree. Activate the account type "Aliases" in your LAM server profile to use this account type.

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

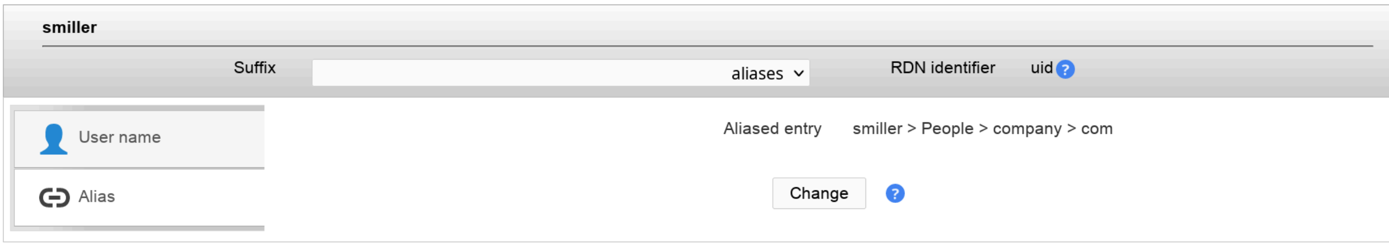


smiller

Suffix: aliases

RDN identifier: uid

User name *: smiller



smiller

Suffix: aliases

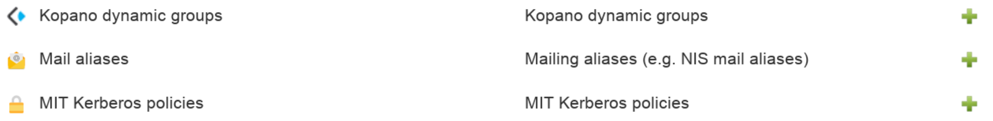
RDN identifier: uid

Aliased entry: smiller > People > company > com

Mail aliases

You can manage mail aliases (e.g. for NIS) inside LAM. This can be used to replace local /etc/aliases files with LDAP.

To activate this type please add "Mail aliases" in your LAM server profile:



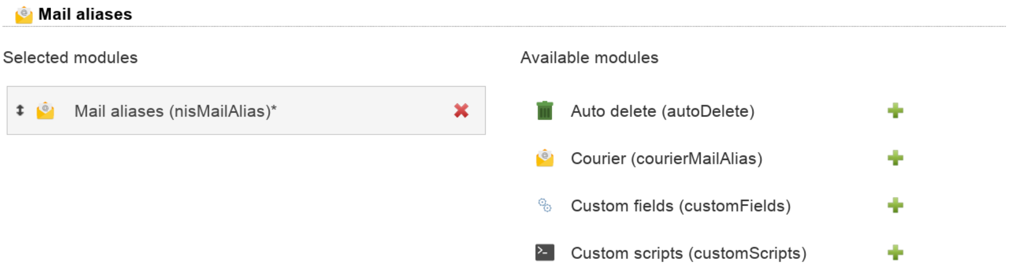
Kopano dynamic groups	Kopano dynamic groups	✚
Mail aliases	Mailing aliases (e.g. NIS mail aliases)	✚
MIT Kerberos policies	MIT Kerberos policies	✚

NIS mail aliases

Note: Use the mail alias user module to manage mail aliases on user pages.

All accounts of this type are based on the "nisMailAlias" object class and may have "cn" and "rfc822MailMember" attributes.

You need to select the Mail aliases module on the next tab.



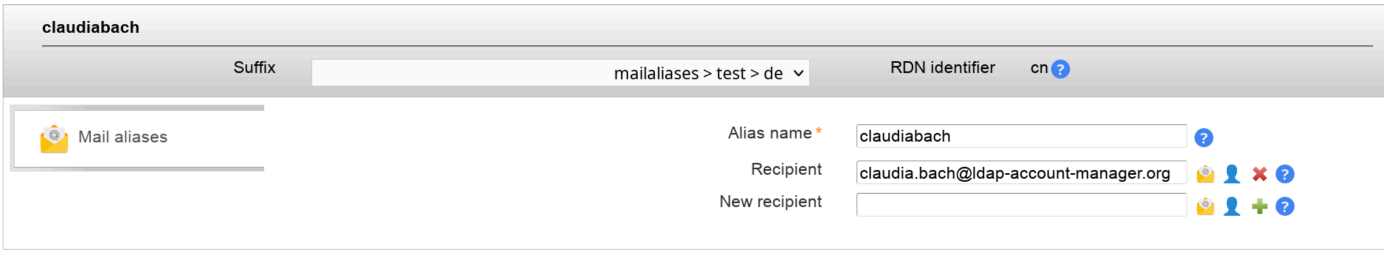
Mail aliases

Selected modules:
- Mail aliases (nisMailAlias)* ✖

Available modules:
- Auto delete (autoDelete) ✚
- Courier (courierMailAlias) ✚
- Custom fields (customFields) ✚
- Custom scripts (customScripts) ✚

The mail aliases will then appear as separate tab inside LAM. You may then manage the aliases with their names and recipient addresses.

There are mail/user icons that allow to select a mail address/user name from the existing users.



claudiabach

Suffix: mailaliases > test > de

RDN identifier: cn

Mail aliases

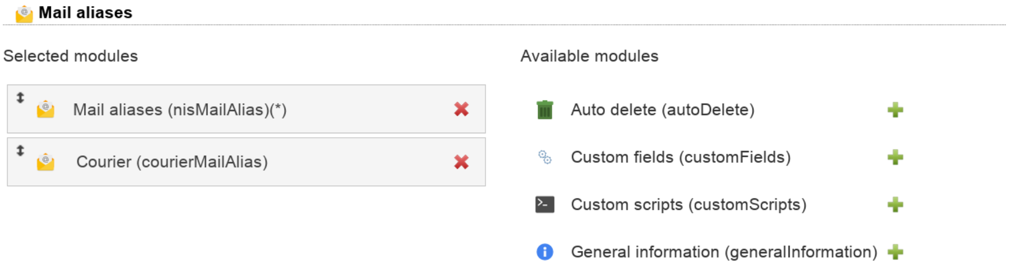
Alias name *: claudiabach

Recipient: claudia.bach@ldap-account-manager.org

New recipient:

Courier mail aliases

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



Mail aliases

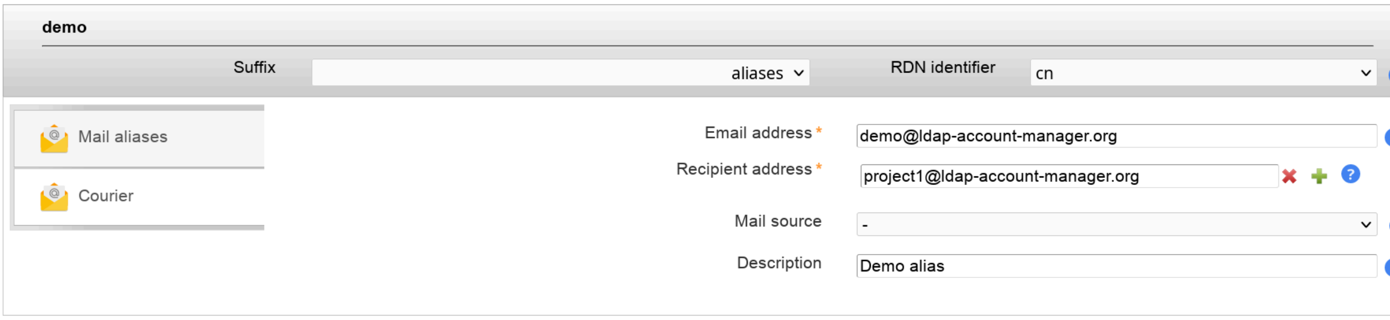
Selected modules

- Mail aliases (nisMailAlias)(*)
- Courier (courierMailAlias)

Available modules

- Auto delete (autoDelete)
- Custom fields (customFields)
- Custom scripts (customScripts)
- General information (generalInformation)

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



demo

Suffix: aliases

RDN identifier: cn

Mail aliases

Courier

Email address *: demo@ldap-account-manager.org

Recipient address *: project1@ldap-account-manager.org

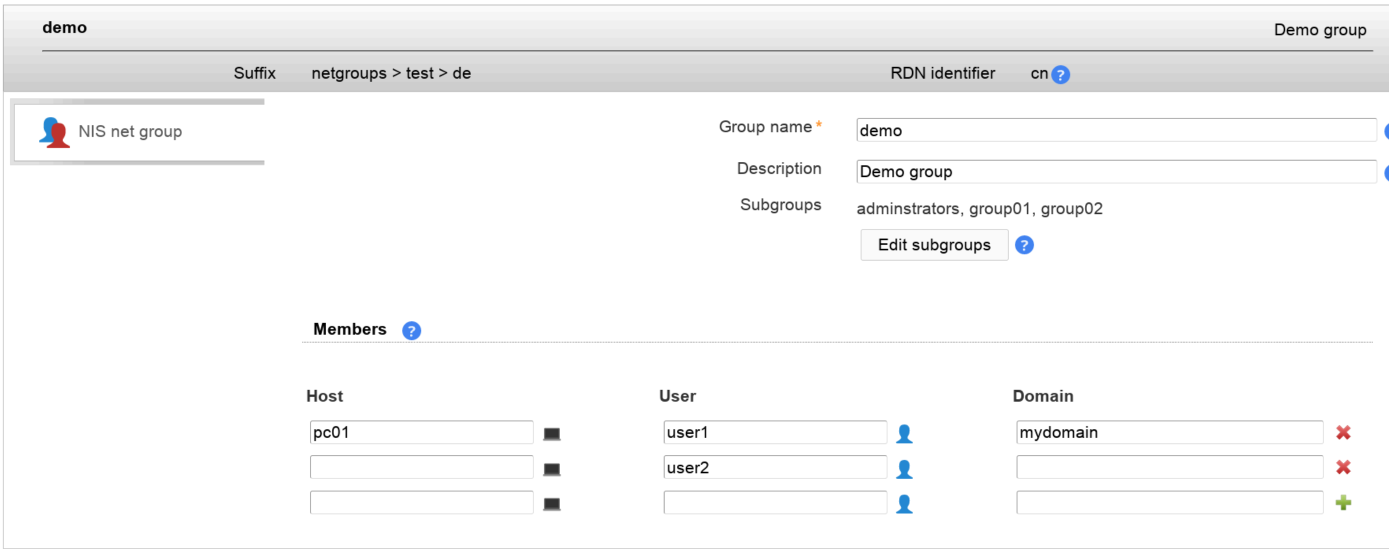
Mail source: -

Description: Demo alias

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.



demo Demo group

Suffix netgroups > test > de RDN identifier cn

Group name * demo

Description Demo group

Subgroups adminstrators, group01, group02

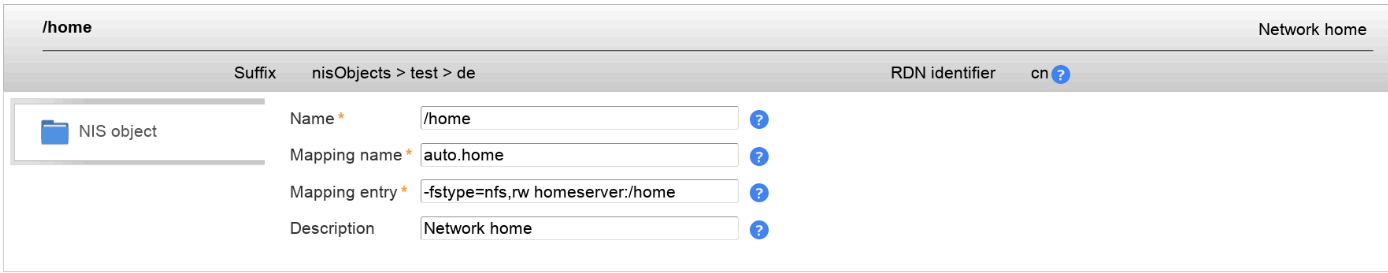
Members

Host	User	Domain
pc01	user1	mydomain
	user2	

NIS objects (LAM Pro)

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

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



/home Network home

Suffix nisObjects > test > de RDN identifier cn

Name * /home

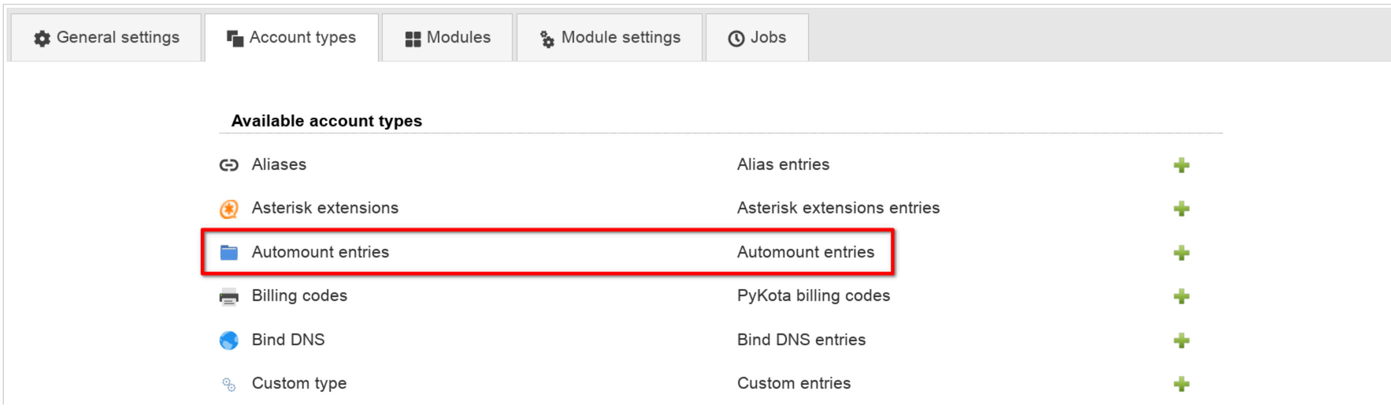
Mapping name * auto.home

Mapping entry * -fstype=nfs,rw homeserver:/home

Description Network home

Automount objects (LAM Pro)

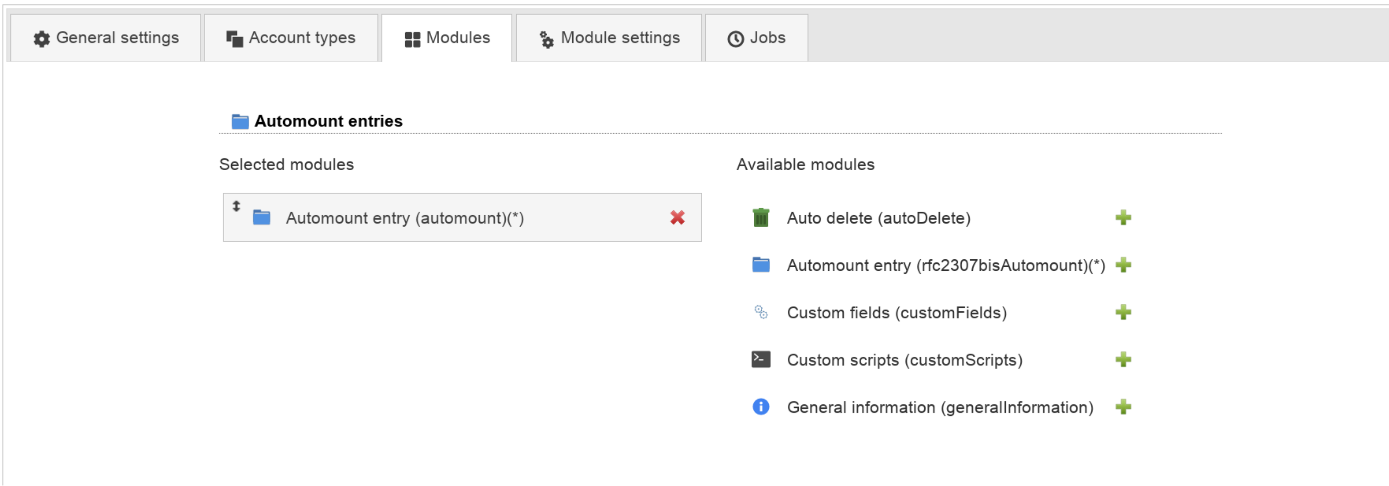
LAM Pro allows you to manage automount entries. Please activate the account type "Automount objects" in your LAM Pro server profile.



Available account types

Aliases	Alias entries	✚
Asterisk extensions	Asterisk extensions entries	✚
Automount entries	Automount entries	✚
Billing codes	PyKota billing codes	✚
Bind DNS	Bind DNS entries	✚
Custom type	Custom entries	✚

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)".



Automount entries

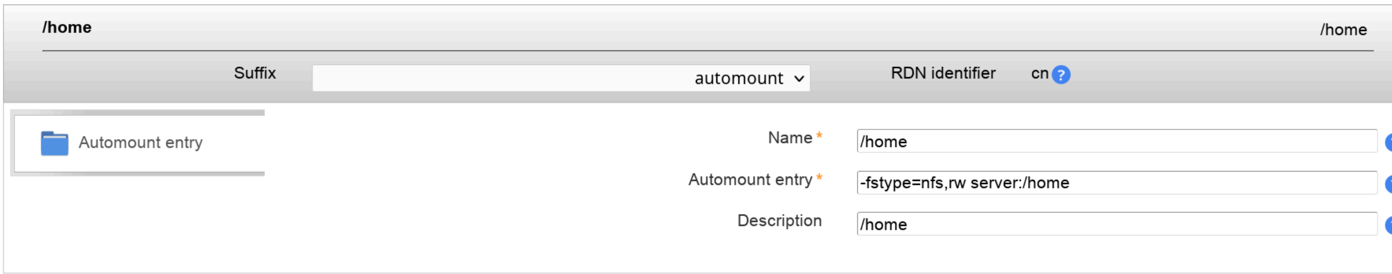
Selected modules

- Automount entry (automount)(*)

Available modules

- Auto delete (autoDelete)
- Automount entry (rfc2307bisAutomount)(*)
- Custom fields (customFields)
- Custom scripts (customScripts)
- General information (generalInformation)

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.



Suffix: automount
RDN identifier: cn

Name *: /home
Automount entry *: -fstype=nfs,rw server:/home
Description: /home

Please see the following external HowTos for more information on automounting and LDAP:

- AutofsLDAP [https://help.ubuntu.com/community/AutofsLDAP]
- Automount über LDAP (German) [http://www.pro-linux.de/artikel/2/760/automount-ueber-ldap.html]

Oracle databases (LAM Pro)

Oracle allows to manage connection data that is stored in tnsnames.ora to be stored in an LDAP directory.

Initial setup

LDAP server setup:

You will need to install the correct Oracle LDAP schema files on your LDAP server. If you run no Oracle LDAP server then you can get them (oidbase.schema, oidnet.schema, oidrdbms.schema, alias.schema) e.g. from here [http://www.idevelopment.info/data/Oracle/DBA_tips/LDAP/LDAP_8.shtml].

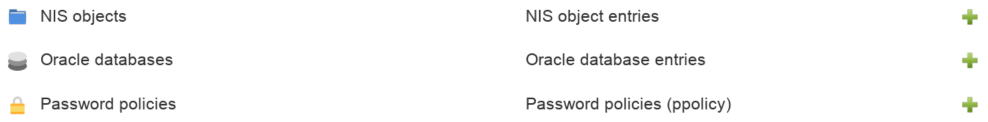
Next you need to create the root entry for Oracle. It should look like this:

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

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

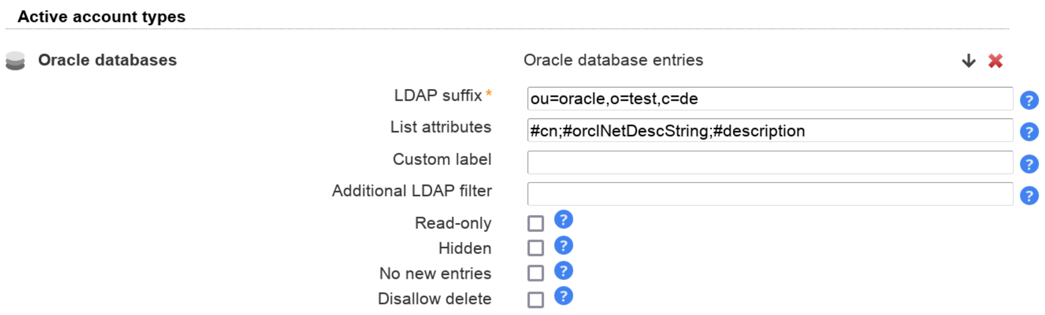
LAM setup:

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



NIS objects	NIS object entries	✚
Oracle databases	Oracle database entries	✚
Password policies	Password policies (ppolicy)	✚

In case you manage a single Oracle context just enter the cn=OracleContext entry as LDAP suffix. If you manage multiple Oracle context entries then set the LDAP suffix to a parent entry of them.

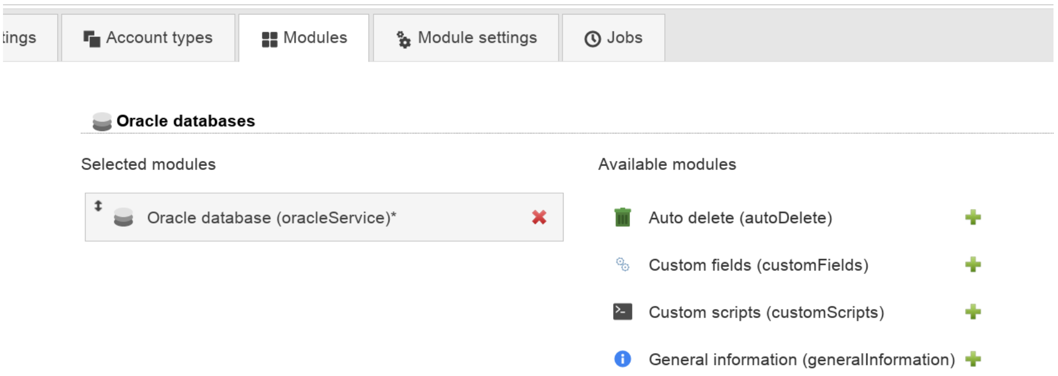


Active account types

Oracle databases Oracle database entries

LDAP suffix *	ou=oracle,o=test,c=de
List attributes	#cn;#orclNetDescString;#description
Custom label	
Additional LDAP filter	
Read-only	□
Hidden	□
No new entries	□
Disallow delete	□

Next, add the Oracle module:



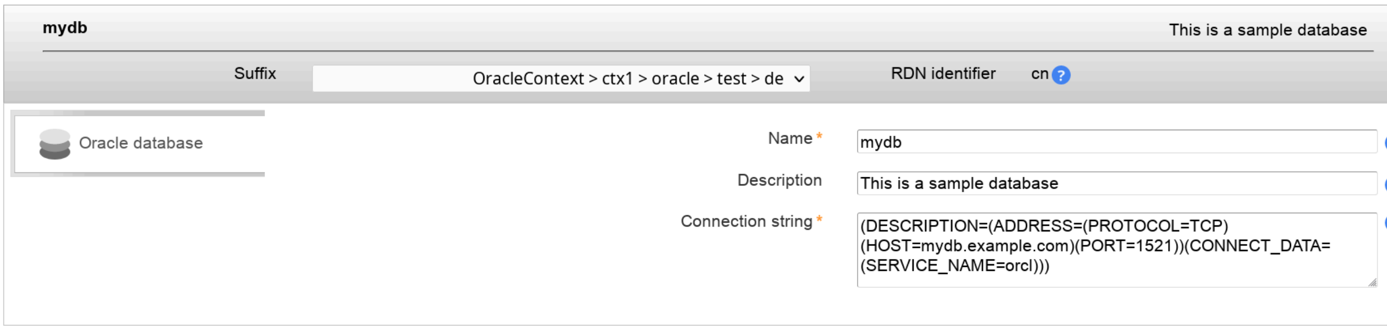
Oracle databases

Selected modules	Available modules
Oracle database (oracleService)*	Auto delete (autoDelete)
	Custom fields (customFields)
	Custom scripts (customScripts)
	General information (generalInformation)

Now you can login to LAM and start to add database entries.

Managing database entries

Each database has a service name, the connection string and an optional description.



mydb This is a sample database

Suffix OracleContext > ctx1 > oracle > test > de RDN identifier cn

Name *	mydb
Description	This is a sample database
Connection string *	(DESCRIPTION=(ADDRESS=(PROTOCOL=TCP)(HOST=mydb.example.com)(PORT=1521))(CONNECT_DATA=(SERVICE_NAME=orcl)))

Database client setup for LDAP

You need to activate the LDAP adapter to make the database tools reading LDAP. Edit network/admin/sqlnet.ora like this:

```
NAMES.DIRECTORY_PATH= (TNSNAMES, LDAP)
```

Then add a file called ldap.ora next to your sqlnet.ora and set the LDAP server and DN suffix where cn=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
```

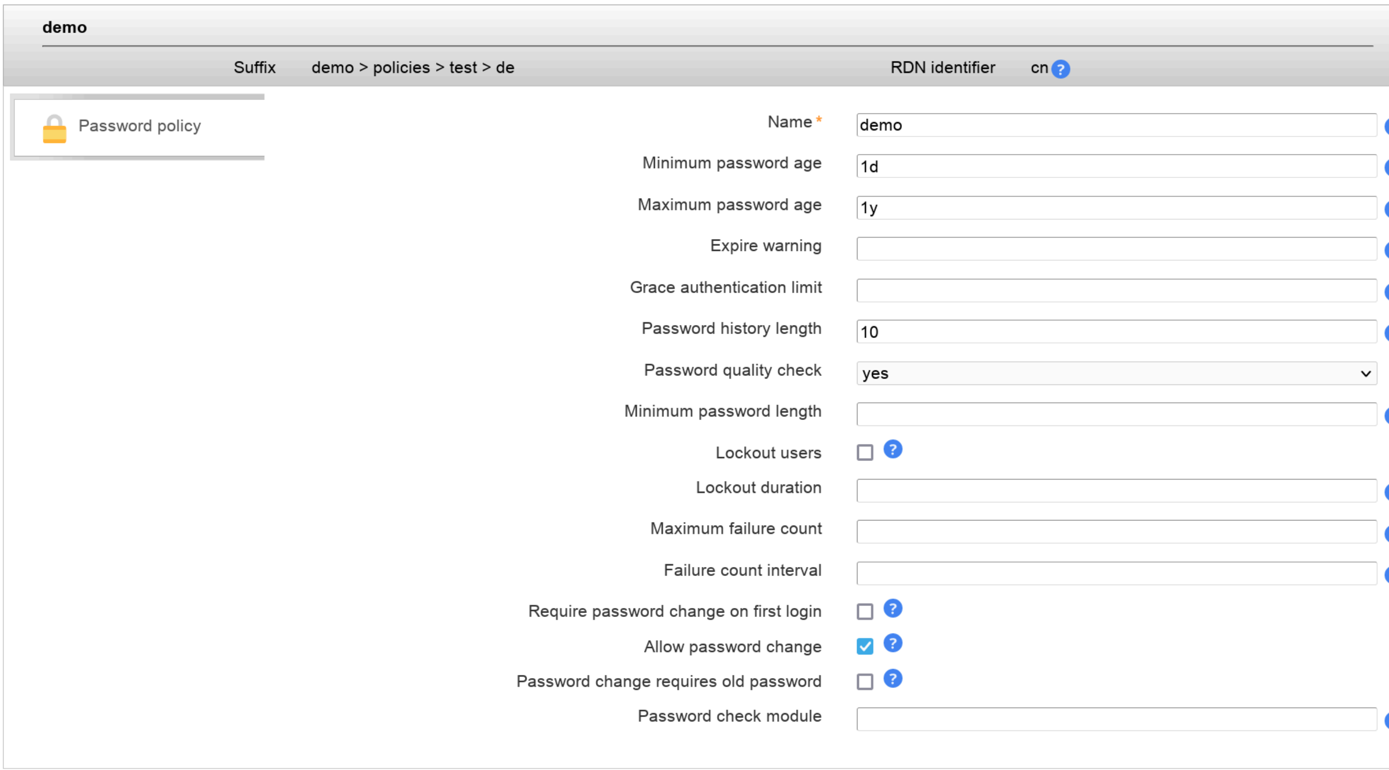
This will allow e.g. tnsping to get the connection data from LDAP:

```
[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=
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".



demo

Suffix demo > policies > test > de RDN identifier cn

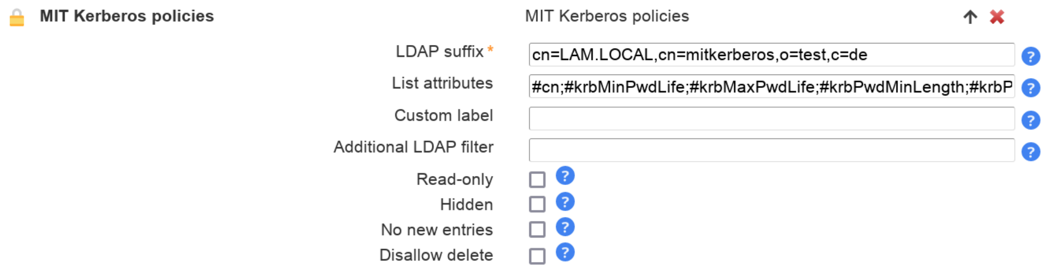
Name*	demo
Minimum password age	1d
Maximum password age	1y
Expire warning	
Grace authentication limit	
Password history length	10
Password quality check	yes
Minimum password length	
Lockout users	□
Lockout duration	
Maximum failure count	
Failure count interval	
Require password change on first login	□
Allow password change	☑
Password change requires old password	□
Password check module	

You will need to add the ppolicy schema to your OpenLDAP configuration and activate the ppolicy [http://linux.die.net/man/5/slapo-ppolicy] overlay module in slapd.conf to use this feature.

MIT Kerberos policies (LAM Pro)

Please add the account type "MIT Kerberos policies" on tab "Account types" in your server profile and setup the LDAP suffix where printers are stored.

MIT Kerberos policies MIT Kerberos policies ✚



MIT Kerberos policies MIT Kerberos policies

LDAP suffix * cn=LAM.LOCAL,cn=mitkerberos,o=test,c=de

List attributes #cn;#krbMinPwdLife;#krbMaxPwdLife;#krbPwdMinLength;#krbP

Custom label

Additional LDAP filter

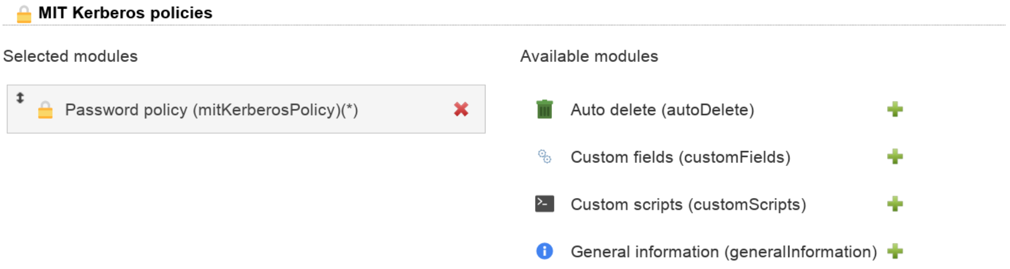
Read-only □

Hidden □

No new entries □

Disallow delete □

Then add the "Password policy (mitKerberosPolicy)" module on tab "Account modules".



MIT Kerberos policies

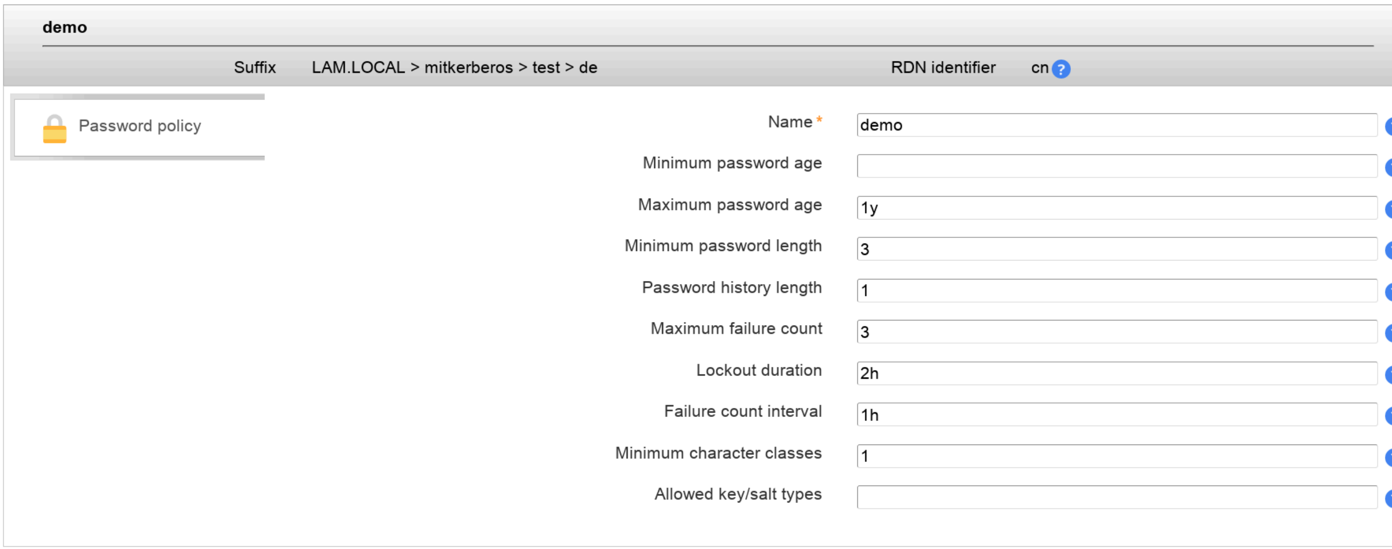
Selected modules

- Password policy (mitKerberosPolicy)(*)

Available modules

- Auto delete (autoDelete) ✚
- Custom fields (customFields) ✚
- Custom scripts (customScripts) ✚
- General information (generalInformation) ✚

Now login to LAM and you will see the MIT Kerberos policies tab. Here you can manage the different policies.



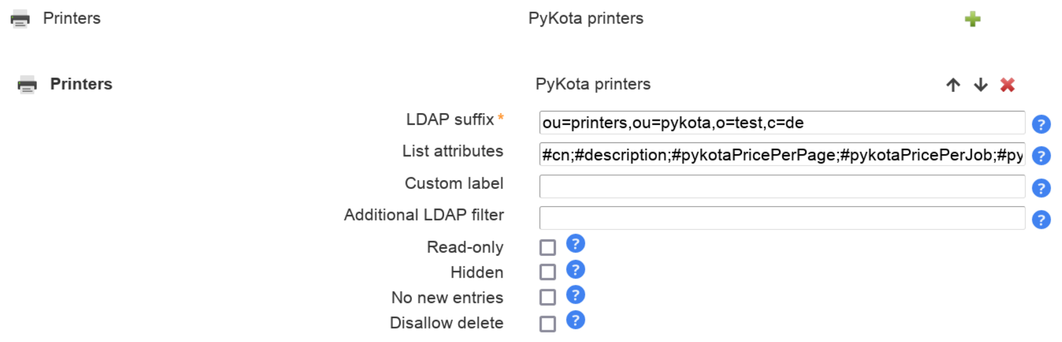
demo

Suffix LAM.LOCAL > mitkerberos > test > de RDN identifier cn

Name *	demo
Minimum password age	
Maximum password age	1y
Minimum password length	3
Password history length	1
Maximum failure count	3
Lockout duration	2h
Failure count interval	1h
Minimum character classes	1
Allowed key/salt types	

PyKota printers

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

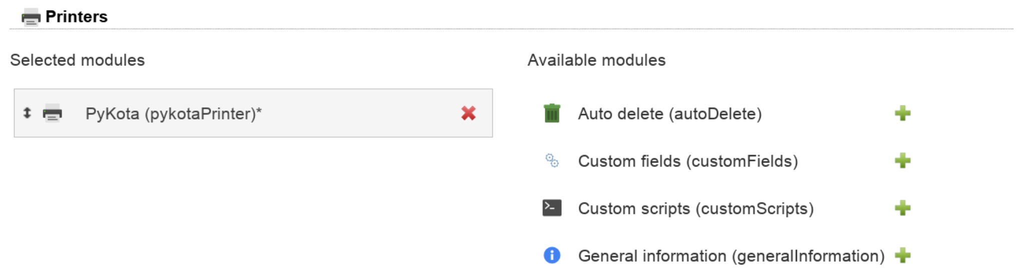


Printers — PyKota printers

Printers — PyKota printers

LDAP suffix *	ou=printers,ou=pykota,o=test,c=de
List attributes	#cn;#description;#pykotaPricePerPage;#pykotaPricePerJob;#py
Custom label	
Additional LDAP filter	
Read-only	□
Hidden	□
No new entries	□
Disallow delete	□

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



Printers

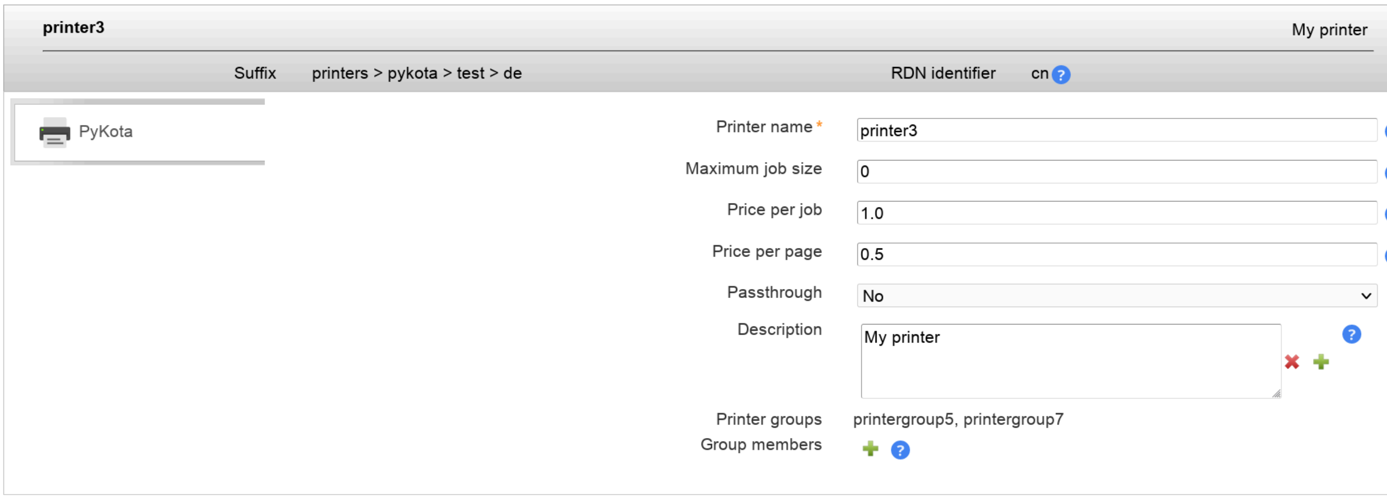
Selected modules

- PyKota (pykotaPrinter)*

Available modules

- Auto delete (autoDelete)
- Custom fields (customFields)
- Custom scripts (customScripts)
- General information (generalInformation)

Next you can start managing printers inside LAM. Here you can setup the costs for a print job. LAM will also show if the printer is member of any printer groups.

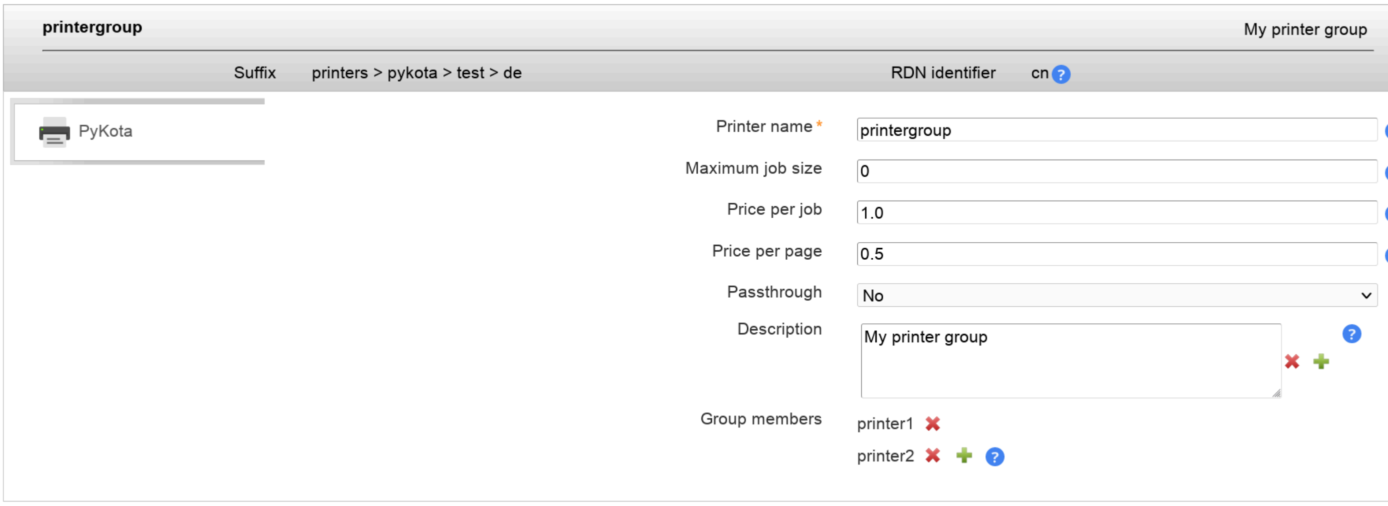


printer3 — My printer

Suffix printers > pykota > test > de — RDN identifier cn

Printer name *	printer3
Maximum job size	0
Price per job	1.0
Price per page	0.5
Passthrough	No
Description	My printer
Printer groups	printergroup5, printergroup7
Group members	

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



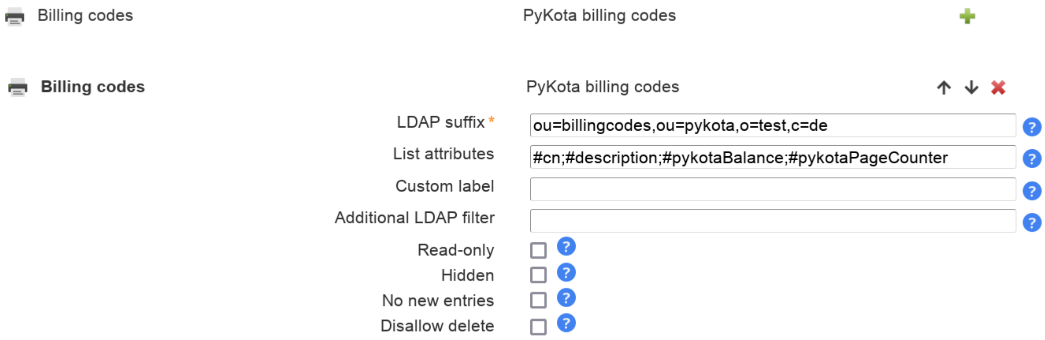
printergroup My printer group

Suffix printers > pykota > test > de RDN identifier cn

Printer name *	printergroup
Maximum job size	0
Price per job	1.0
Price per page	0.5
Passthrough	No
Description	My printer group
Group members	printer1 printer2

PyKota billing codes

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

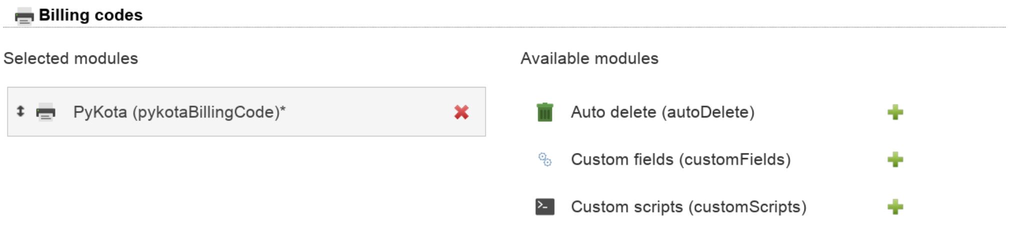


Billing codes PyKota billing codes

Billing codes PyKota billing codes

LDAP suffix *	ou=billingcodes,ou=pykota,o=test,c=de
List attributes	#cn;#description;#pykotaBalance;#pykotaPageCounter
Custom label	
Additional LDAP filter	
Read-only	□
Hidden	□
No new entries	□
Disallow delete	□

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



Billing codes

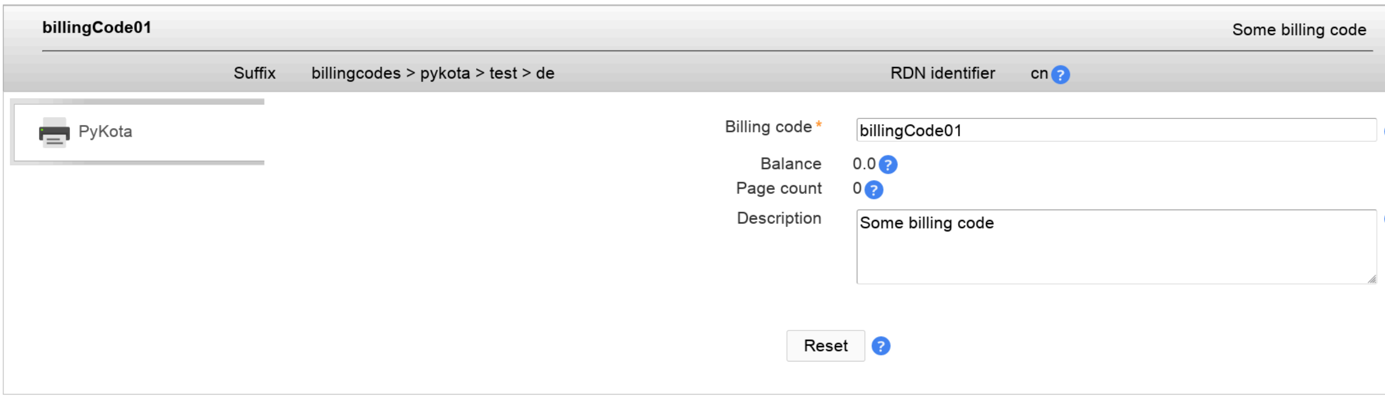
Selected modules

- PyKota (pykotaBillingCode)*

Available modules

- Auto delete (autoDelete)
- Custom fields (customFields)
- Custom scripts (customScripts)

Now login to LAM and you will see the billing code tab where you can manage your entries. If jobs were printed with a billing code then you will also see the balance and page count.



billingCode01 Some billing code

Suffix billingcodes > pykota > test > de RDN identifier cn

PyKota

Billing code *	billingCode01
Balance	0.0
Page count	0
Description	Some billing code

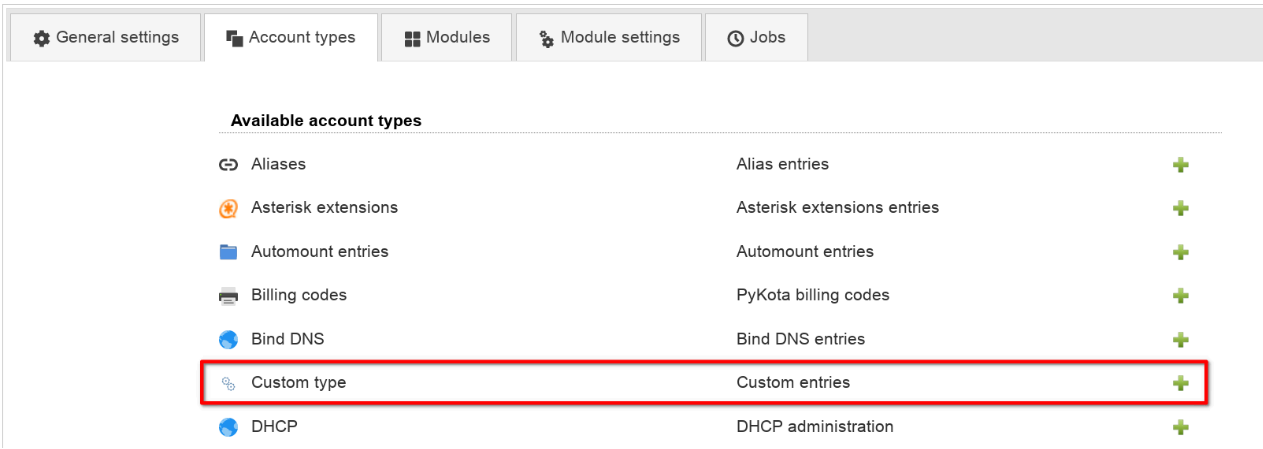
Custom types (LAM Pro)

This account type allows you to manage any type of LDAP entries. This is e.g. needed if you define your own structural object classes or LAM does not yet provide a module for a structural object class.

Always use this together with Custom fields to specify the LDAP attributes.

Configuration

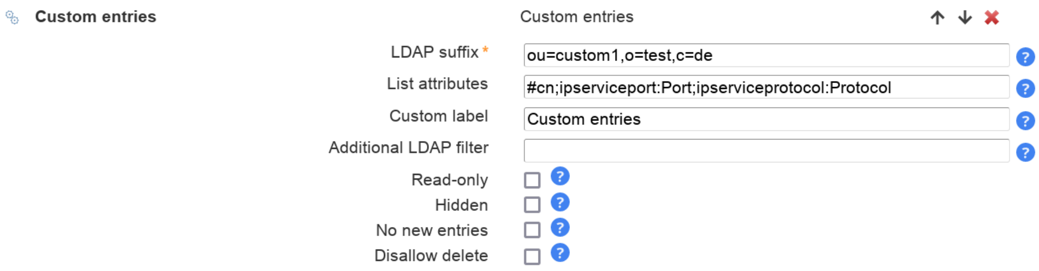
Add a custom account type in your server profile (you can also add multiple if needed).



Available account types

Aliases	Alias entries	+
Asterisk extensions	Asterisk extensions entries	+
Automount entries	Automount entries	+
Billing codes	PyKota billing codes	+
Bind DNS	Bind DNS entries	+
Custom type	Custom entries	+
DHCP	DHCP administration	+

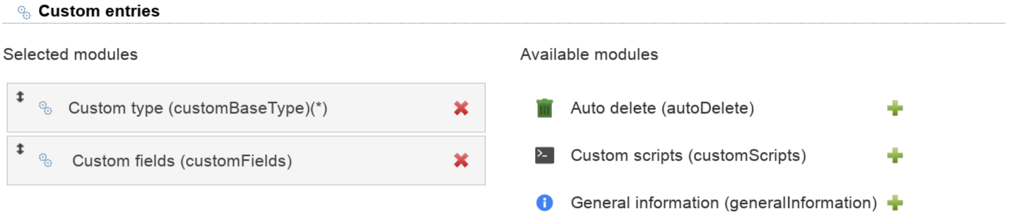
Then specify the root DN where the entries should be stored. Also provide the attributes to show in list view and a unique label for your entries.



Custom entries Custom entries

LDAP suffix *	ou=custom1,o=test,c=de
List attributes	#cn;ipserviceport:Port;ipserviceprotocol:Protocol
Custom label	Custom entries
Additional LDAP filter	
Read-only	□
Hidden	□
No new entries	□
Disallow delete	□

On tab modules add the custom type module. You will also need the Custom fields module to manage the attributes.



Custom entries

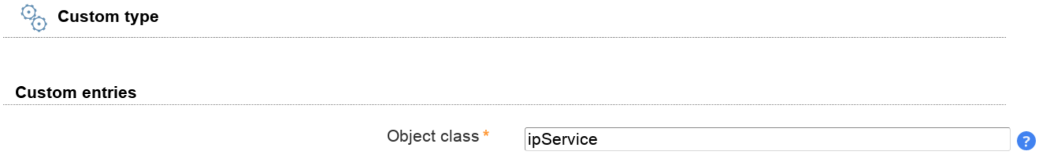
Selected modules

- Custom type (customBaseType)(*)
- Custom fields (customFields)

Available modules

- Auto delete (autoDelete)
- Custom scripts (customScripts)
- General information (generalInformation)

Finally, switch to tab Module settings. Here you need to specify the structural object class. Also configure the Custom fields module to manage all your attributes.



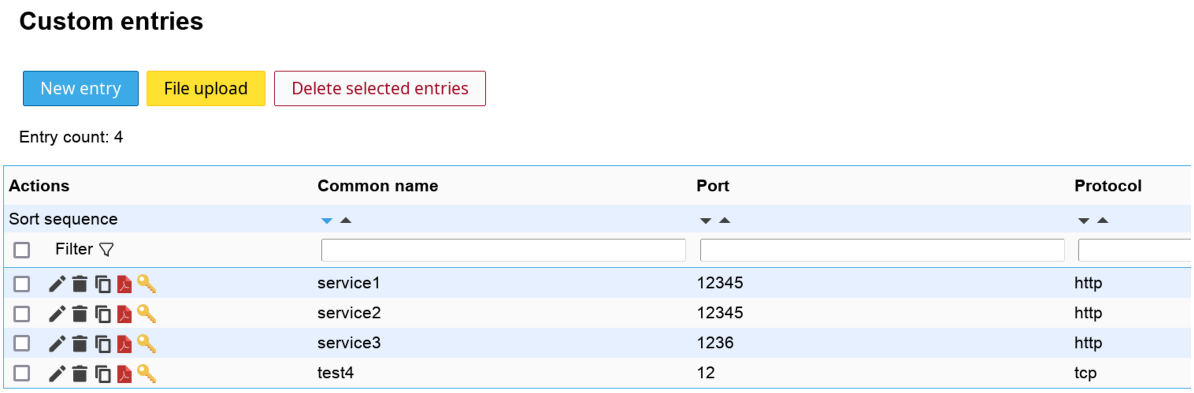
Custom type

Custom entries

Object class * ipService

Manage your entries

You can now login to LAM and will see one tab for each configured custom type.



Custom entries

Entry count: 4

Actions	Common name	Port	Protocol
Sort sequence	▼▲	▼▲	▼▲
□ Filter			
□	service1	12345	http
□	service2	12345	http
□	service3	1236	http
□	test4	12	tcp

Custom fields (LAM Pro)

This module allows you to manage LDAP attributes that are not covered by the other LAM modules (e.g. if you use a custom LDAP schema). You can fully define how your input fields look like:

- Label
- LDAP attribute name
- Unique name for field
- Help text
- Read-only display
- Field type: text, password, text area, checkbox, radio buttons, select list, file upload, LDAP date (and time), constant
- Validation via regular expression
- Error message if validation fails

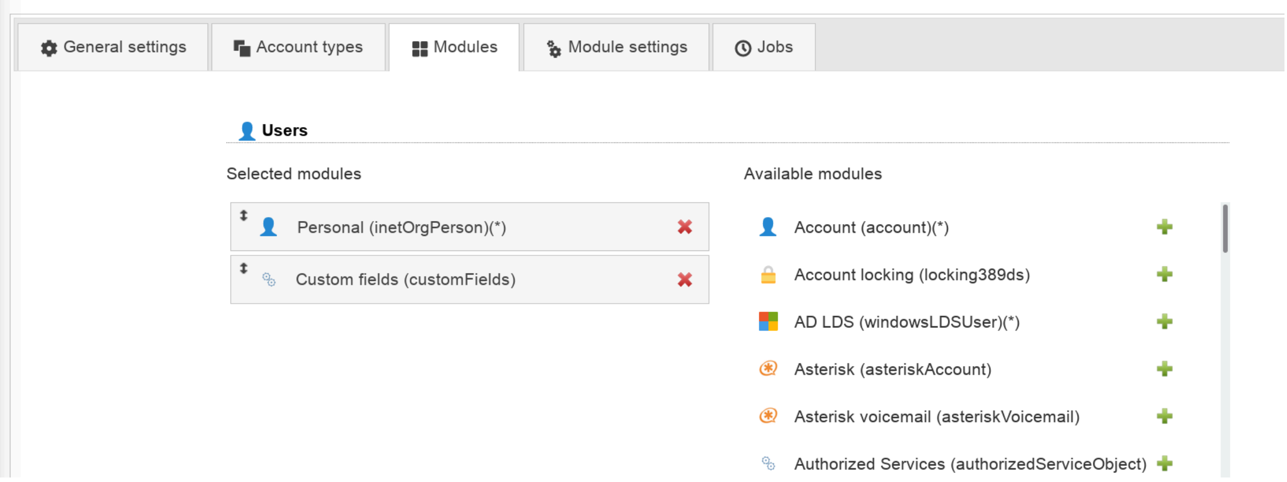
Limitations:

Custom fields cannot manage

- structural object classes (supported by Custom types)
- attributes that require validation rules across multiple attributes or cannot be described by a simple regular expression

Activating the custom fields module:

You may specify custom fields for all of your account types. Please enter tab "Modules" in your server profile. Now activate the "Custom fields (customFields)" module for all needed account types.



Users

Selected modules

- Personal (inetOrgPerson)(*)
- Custom fields (customFields)

Available modules

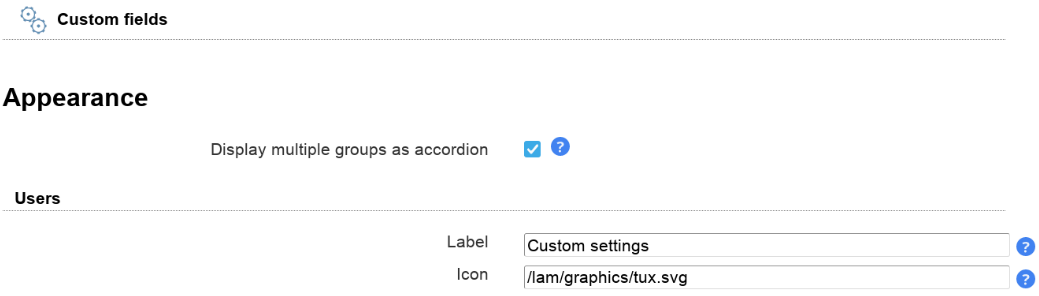
- Account (account)(*)
- Account locking (locking389ds)
- AD LDS (windowsLDSUser)(*)
- Asterisk (asteriskAccount)
- Asterisk voicemail (asteriskVoicemail)
- Authorized Services (authorizedServiceObject)

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: Custom settings

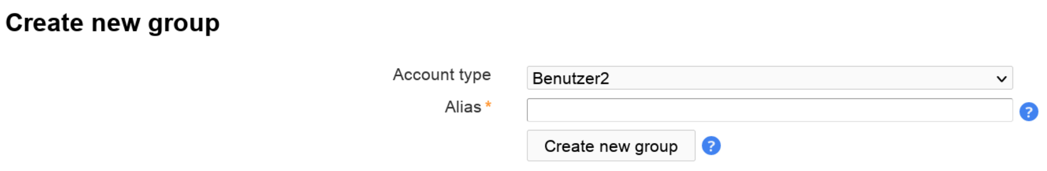
Icon: /lam/graphics/tux.svg

Defining groups:

All input fields are divided into groups. A group may contain one or more object classes and allows you to add/ remove a certain set of input fields.

E.g. you may define two groups - "My application A" and "My application B" - that manage different LDAP attributes and object classes. This way you will be able to control both attribute sets independently.

To create a group please edit your server profile and switch to tab "Module settings". You will see the section "Custom fields" which allows you to add new groups. Now select your account type (e.g. Users) and specify an alias for your group. This alias will be printed as group header when you later edit an account in the admin interface.



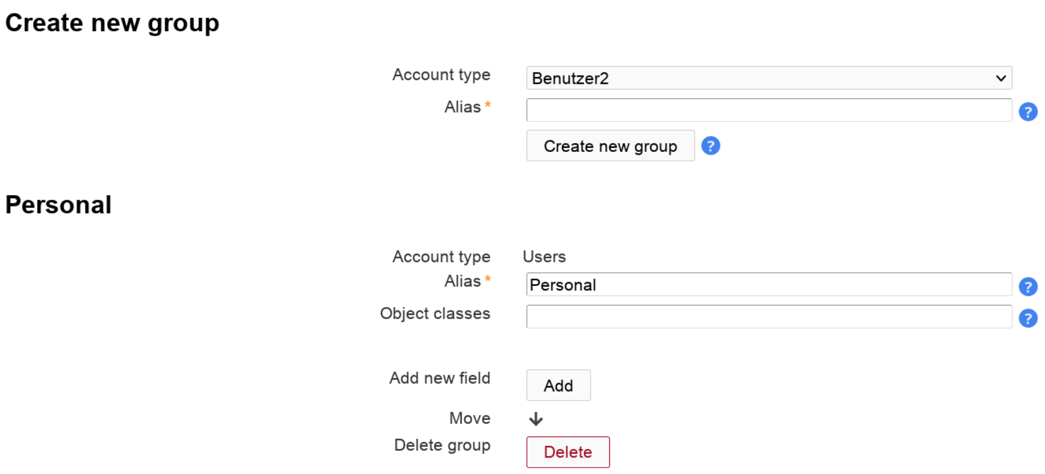
Create new group

Account type: Benutzer2

Alias *

After you created your new group you can setup the managed object classes. If you specify any object classes then you will later be able to add/remove a complete set of attributes including their object classes.

Skipping the object classes field is only useful if you want to manage some attributes that are not yet supported by LAM but there is already a LAM module that manages the object class.



Create new group

Account type: Benutzer2

Alias *

Personal

Account type: Users

Alias *: Personal

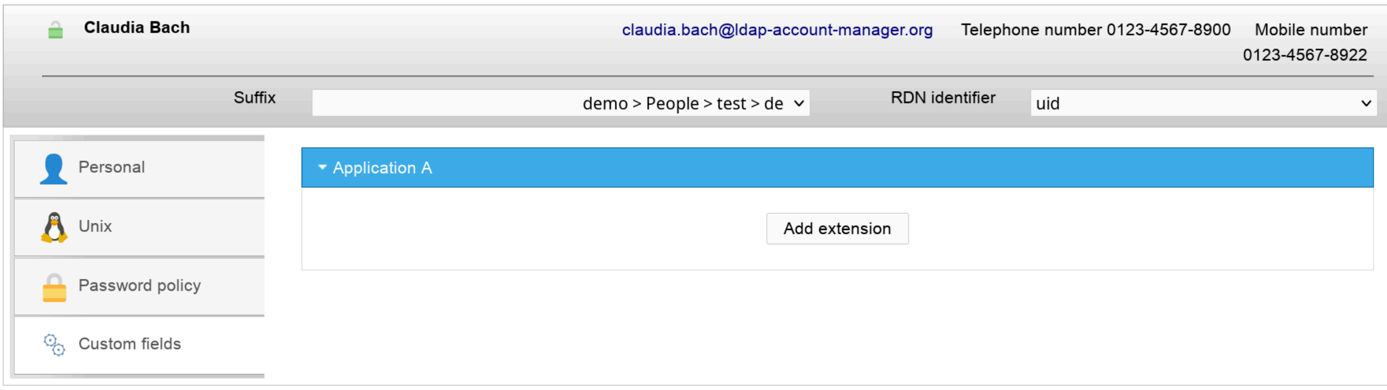
Object classes

Add new field

Move ↓

Delete group

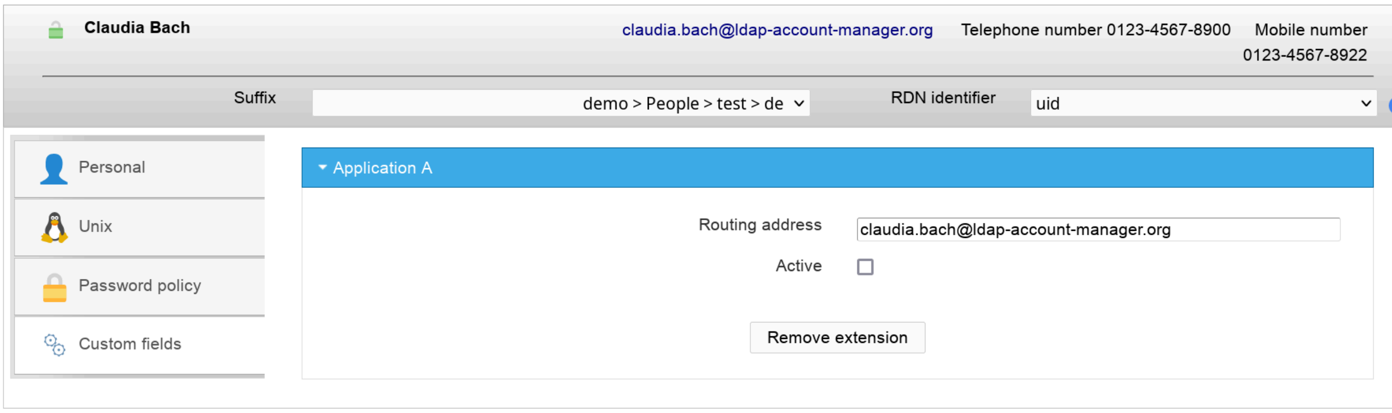
The group may look like when you edit a user.



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

Suffix: demo > People > test > de

RDN identifier: uid



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

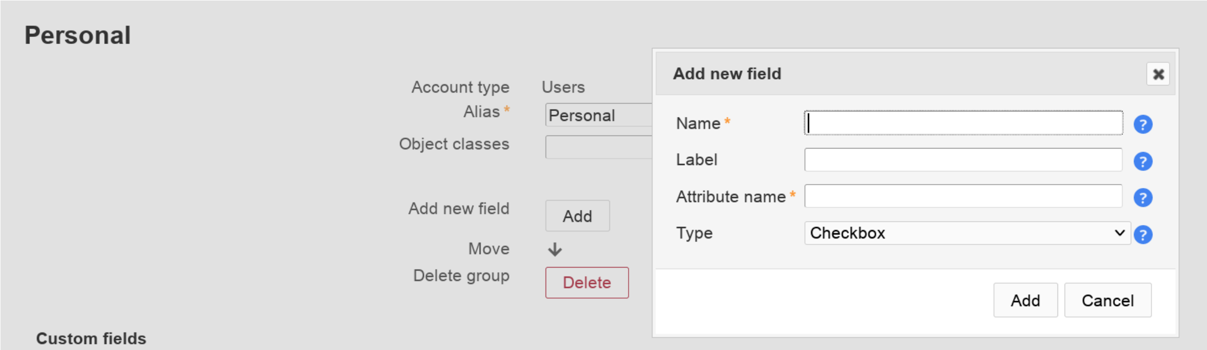
Routing address: claudia.bach@ldap-account-manager.org

Active □

Adding fields:

Now you can add a new field that manages an LDAP attribute. Simply fill the fields and press on "Add".

Please note that the field name cannot be changed later. It is the unique ID for this field.



Personal

Account type	Users
Alias *	Personal
Object classes	
Add new field	Add
Move	↓
Delete group	Delete

Custom fields

Add new field

Name *	
Label	
Attribute name *	
Type	Checkbox

Examples for fields and their representation:

Text field:

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

You can also enable auto-completion. In this case LAM will search all accounts for the given attribute and provide auto-completion hints when the user edits this field. This should only be used if there is a limited number of different values for this attribute.

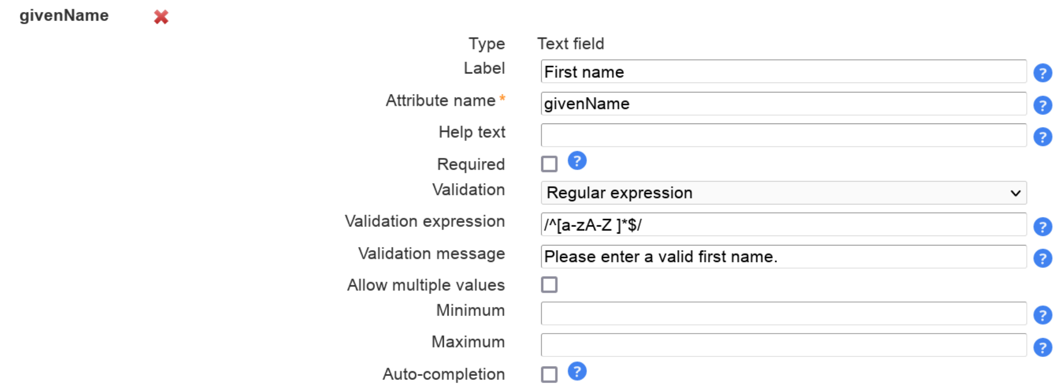
In case your field is a date value you can show a calendar for easy editing.

Example calendar formats:

- d.m.Y: 31.12.2025
- Y-m-d: 2025-12-31
- d M, y: 31 Dec, 25
- d MM, Y: 31 December, 2025

You can escape wildcards with "\". E.g. "d.m.Y \d" will result in "31.12.2025 d".

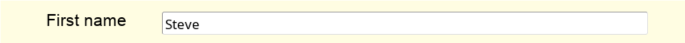
Profile editor: For multi-value fields you can separate multiple values by semicolon in profile editor (e.g. "value1; value2"). LAM will split the text when loading the profile.



givenName

Type	Text field
Label	First name
Attribute name *	givenName
Help text	
Required	□
Validation	Regular expression
Validation expression	/^[a-zA-Z]*$/
Validation message	Please enter a valid first name.
Allow multiple values	□
Minimum	
Maximum	
Auto-completion	□

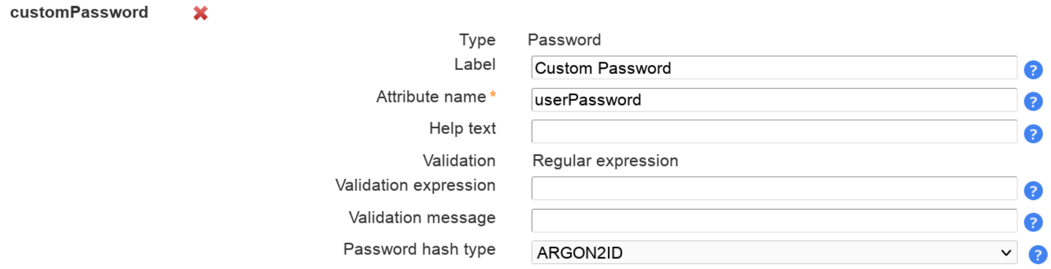
Presentation:



First name	Steve

Password field:

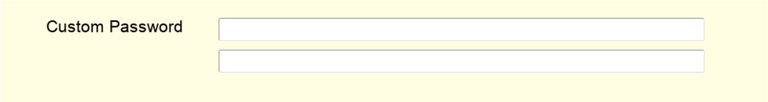
You can also manage custom password fields. LAM Pro will display two fields where the user must enter the same password. You can hash the password if needed.



customPassword ✖

Type	Password
Label	Custom Password
Attribute name *	userPassword
Help text	
Validation	Regular expression
Validation expression	
Validation message	
Password hash type	ARGON2ID

Presentation:

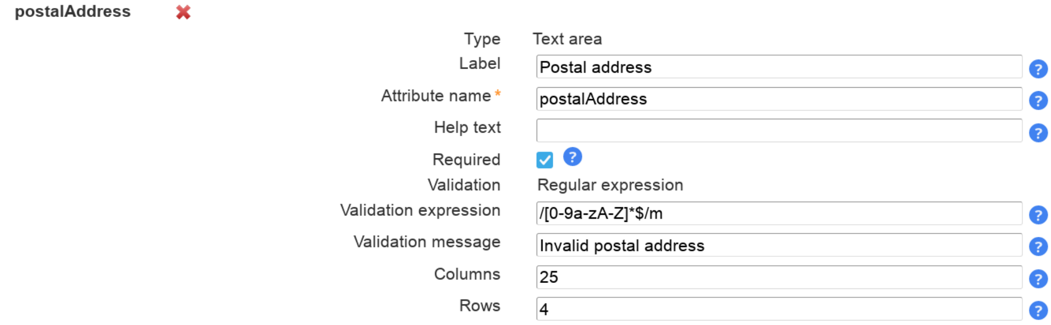


Custom Password	

Text area:

This adds a multi-line field. The options are similar to text fields. Additionally, you can set the size with the number of columns and rows.

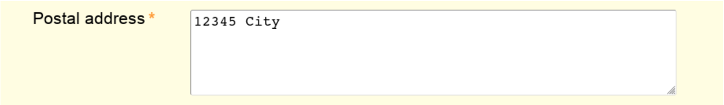
Please note that the validation expression should be set to multi-line. This is done by adding "m" at the end.



postalAddress ✖

Type	Text area
Label	Postal address
Attribute name *	postalAddress
Help text	
Required	☑
Validation	Regular expression
Validation expression	/[0-9a-zA-Z]*$/m
Validation message	Invalid postal address
Columns	25
Rows	4

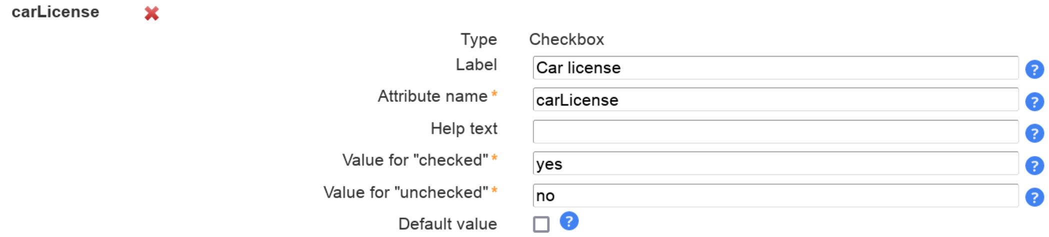
Presentation:



Postal address *	12345 City

Checkbox:

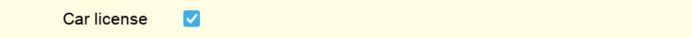
Sometimes you may want to allow only yes/no values for your LDAP attributes. This can be represented by a checkbox. You can specify the values for checked and unchecked. The default value is set if the LDAP attribute has no value.



carLicense ✖

Type	Checkbox
Label	Car license
Attribute name *	carLicense
Help text	
Value for "checked" *	yes
Value for "unchecked" *	no
Default value	□

Presentation:

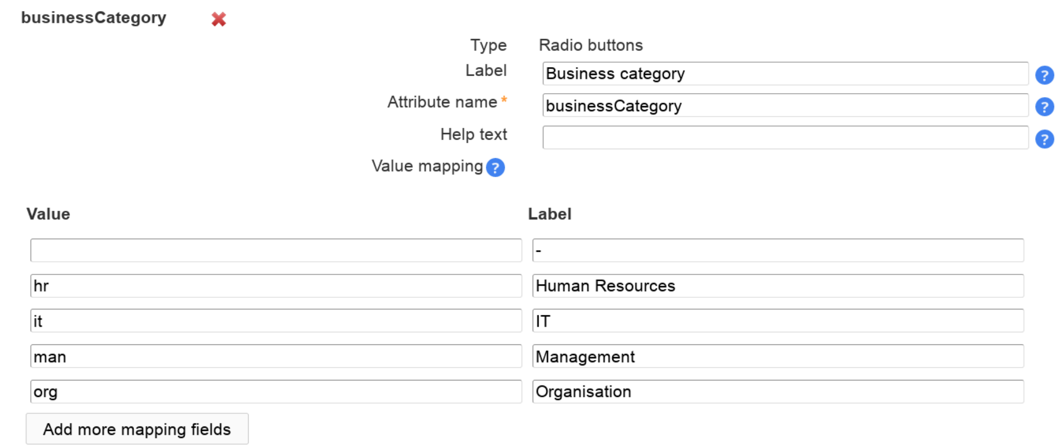


Car license ☑

Radio buttons:

This displays a list of radio buttons where the user can select one value.

You can specify a mapping of LDAP attribute values and their display (label) on the Self Service page. To add more mapping fields please press "Add more mapping fields".

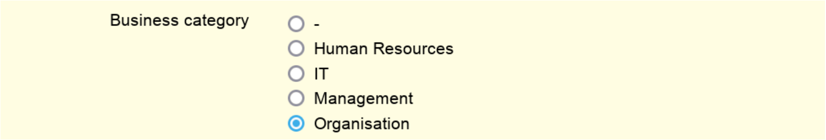


businessCategory ✖

Type	Radio buttons
Label	Business category
Attribute name *	businessCategory
Help text	
Value mapping	

Value	Label
	-
hr	Human Resources
it	IT
man	Management
org	Organisation

Presentation:

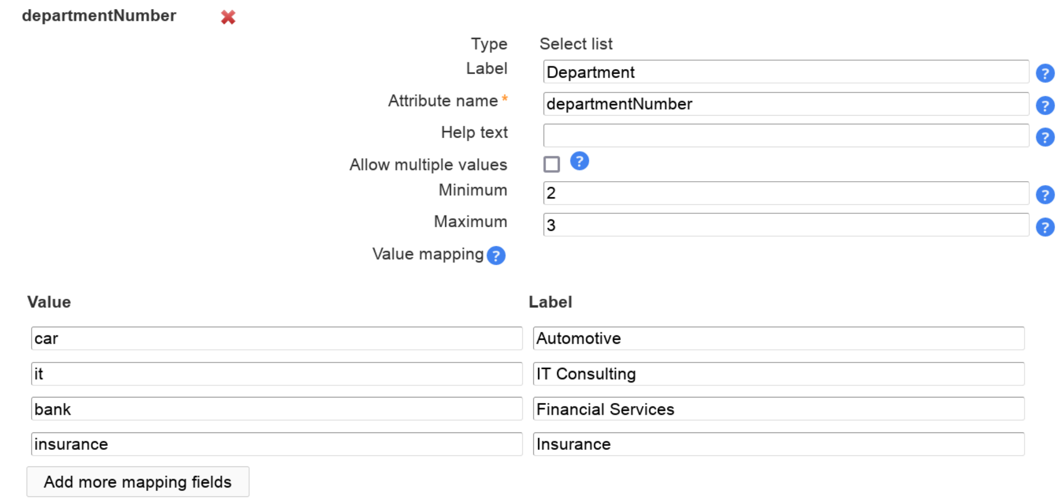


Business category
○ -
○ Human Resources
○ IT
○ Management
● Organisation

Select list:

Select lists allow the user to select a value in a large list of options. The definition of the possible values and their display is similar to radio buttons.

You can also allow multiple values.

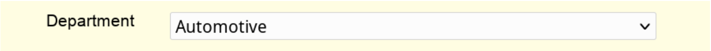


departmentNumber ✖

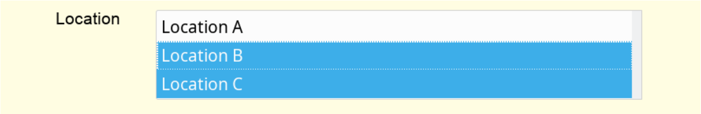
Type	Select list
Label	Department
Attribute name *	departmentNumber
Help text	
Allow multiple values	□
Minimum	2
Maximum	3
Value mapping	

Value	Label
car	Automotive
it	IT Consulting
bank	Financial Services
insurance	Insurance

Presentation:



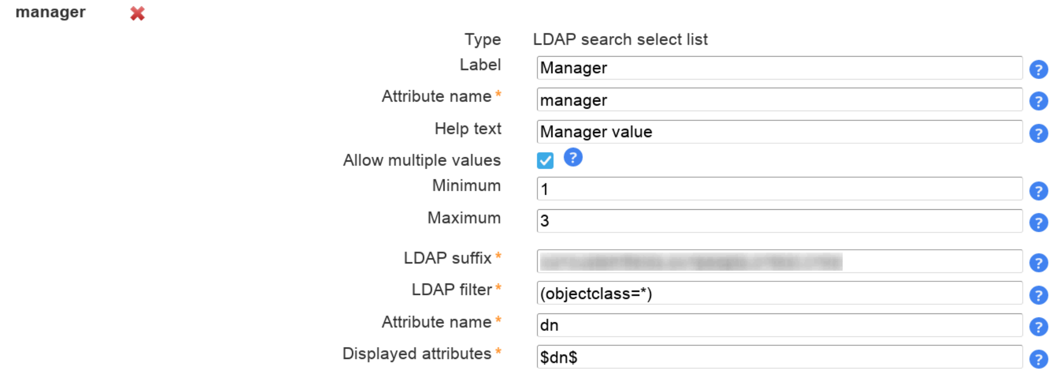
Department: Automotive



Location	Location A Location B Location C

LDAP search select list

This is similar to "Select list" but the option are read from LDAP. You can use this to define e.g. a DN selection list. Multiple values are supported.



manager ✖

Type	LDAP search select list
Label	Manager
Attribute name *	manager
Help text	Manager value
Allow multiple values	☑
Minimum	1
Maximum	3
LDAP suffix *	[redacted]
LDAP filter *	(objectclass=*)
Attribute name *	dn
Displayed attributes *	dn

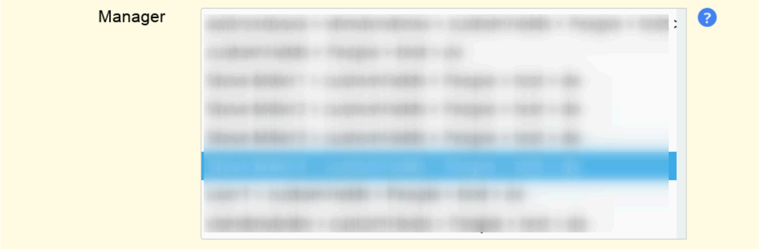
LDAP suffix: The LDAP DN that is used as starting point to search for LDAP entries.

LDAP filter: Only LDAP entries that match this filter will be used. If all entries should be used then use "(objectclass=*)".

Attribute name: The values of this attribute will be used to build the selection list.

Display attributes: List of attributes to show as label for the options in select box. Attribute wildcards are surrounded by "$", e.g. "$cn$" will be replaced by "cn" attribute. Default is "dn".

Presentation:

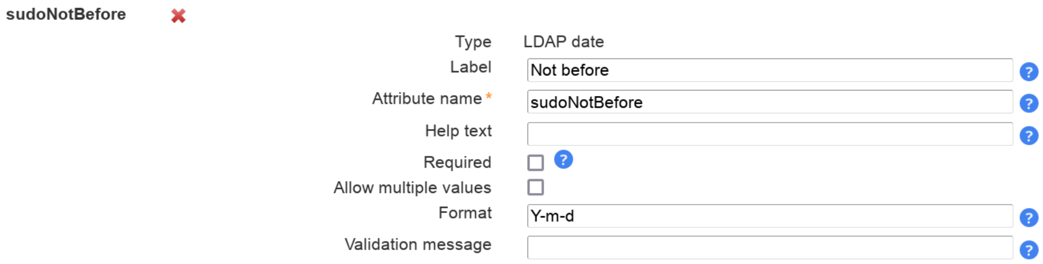


Manager	[redacted]

LDAP date

Use this for LDAP attributes with syntax "Generalized Time" (1.3.6.1.4.1.1466.115.121.1.24).

LAM will automatically set hour/minute/second to "0". If this is not intended please use type "LDAP date and time".

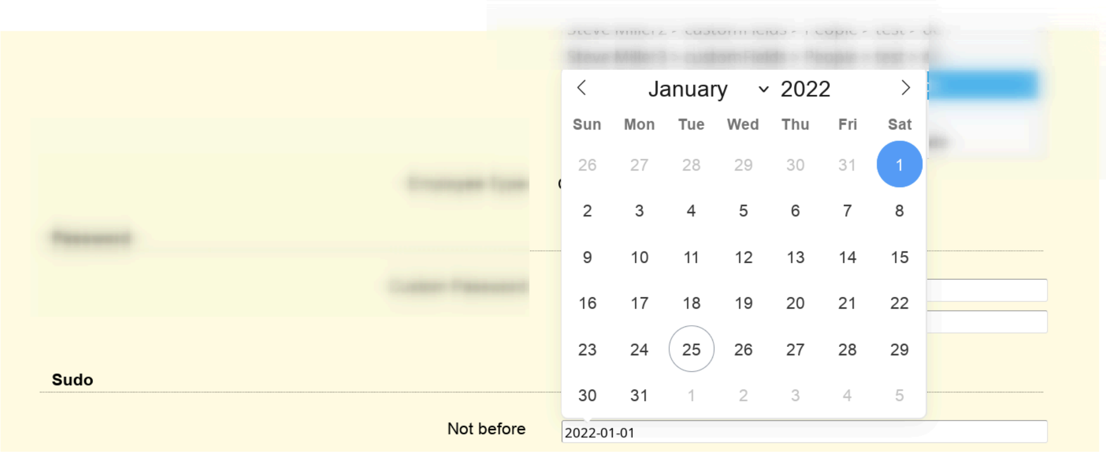


sudoNotBefore ✖

Type	LDAP date
Label	Not before
Attribute name *	sudoNotBefore
Help text	
Required	☐
Allow multiple values	☐
Format	Y-m-d
Validation message	

Presentation:

LAM will display a calendar to select the date.



January 2022

Sun	Mon	Tue	Wed	Thu	Fri	Sat
26	27	28	29	30	31	1
2	3	4	5	6	7	8
9	10	11	12	13	14	15
16	17	18	19	20	21	22
23	24	25	26	27	28	29
30	31	1	2	3	4	5

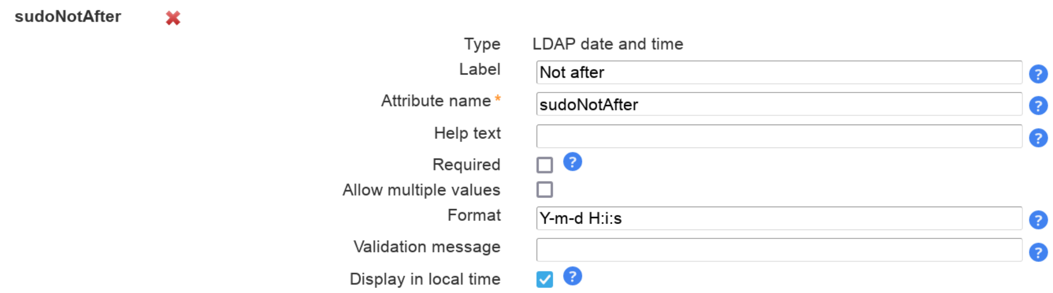
Sudo

Not before 2022-01-01

LDAP date and time

Use this for LDAP attributes with syntax "Generalized Time" (1.3.6.1.4.1.1466.115.121.1.24).

LAM can convert the displayed value to the configured time zone of your server/self service profile. In this case, please activate "Display in local time".

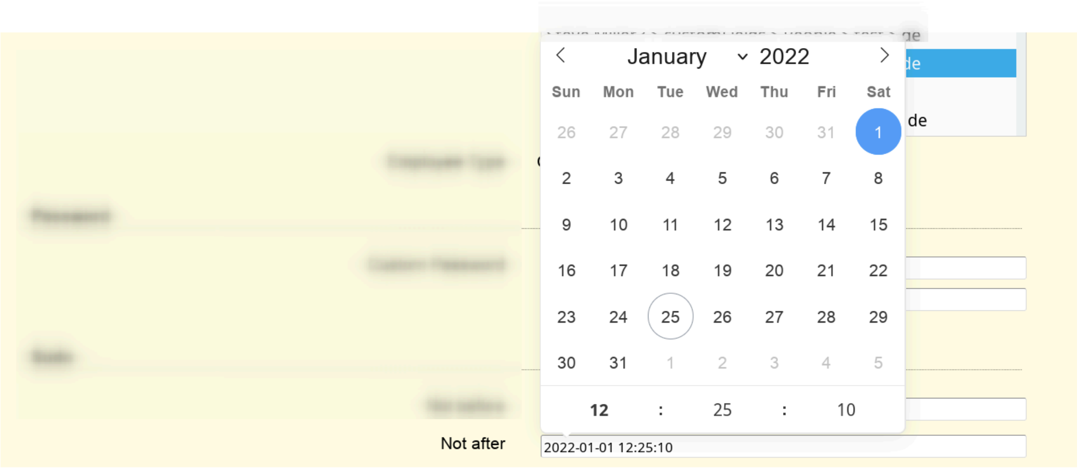


sudoNotAfter ✖

Type	LDAP date and time
Label	Not after
Attribute name *	sudoNotAfter
Help text	
Required	□
Allow multiple values	□
Format	Y-m-d H:i:s
Validation message	
Display in local time	☑

Presentation:

LAM will display a calendar to select the date and time.



January 2022

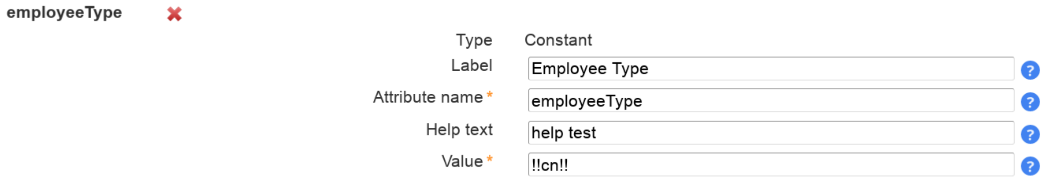
Sun	Mon	Tue	Wed	Thu	Fri	Sat
26	27	28	29	30	31	1
2	3	4	5	6	7	8
9	10	11	12	13	14	15
16	17	18	19	20	21	22
23	24	25	26	27	28	29
30	31	1	2	3	4	5

12 : 25 : 10

Not after 2022-01-01 12:25:10

Constant value

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



employeeType ✖

Type	Constant
Label	Employee Type
Attribute name *	employeeType
Help text	help test
Value *	!!cn!!

Wildcards:

- %attribute%: attribute value
- @attribute@: first character of attribute
- ?attribute?: first character of attribute in lower case
- !attribute!: first character of attribute in upper case
- ??attribute??: attribute in lower case
- !!attribute!!: attribute in upper case
- ((attribute)): space if attribute is set
- §attribute|;§; attribute values separated by ";" (you can set other separators if you want)

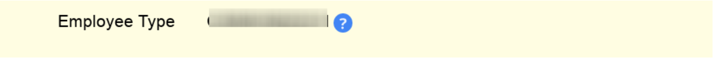
Examples for attributes gn="Steve", sn="Miller" and memberUid=("user1", "user2") (specified value -> resulting LDAP value):

Table 4.3.

Constant value	Resulting LDAP value
my constant	my constant
%gn%	Steve
%gn%((gn))%sn%	Steve Miller (would be "Miller" if gn is empty)
§memberUid|, §	user1, user2

Presentation:

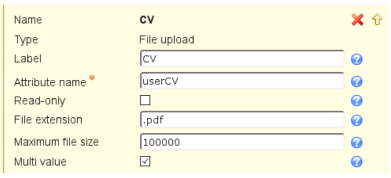
The LDAP value will be shown as text.



Employee Type

File upload:

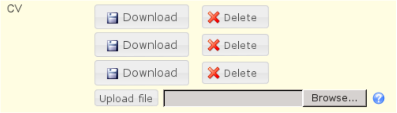
This is used for binary data. You can restrict uploaded data to a given file extension and set the maximum file size.



Name	**CV**
Type	File upload
Label	CV
Attribute name *	userCV
Read-only	□
File extension	.pdf
Maximum file size	100000
Multi value	☑

Presentation:

The uploaded data may also be downloaded via LAM.



Validation expressions:

The validation expressions follow the standard of Perl regular expressions [http://perldoc.perl.org/perlre.html]. They start and end with a "/". The beginning of a line is specified by "^" and the end by "$".

Examples:

/^[a-z0-9]+$/ allows small letters and numbers. The value must not be empty ("+").

/^[a-z0-9]+$/i allows small and capital letters ("i" at the end means ignore case) and numbers. The value must not be empty ("+").

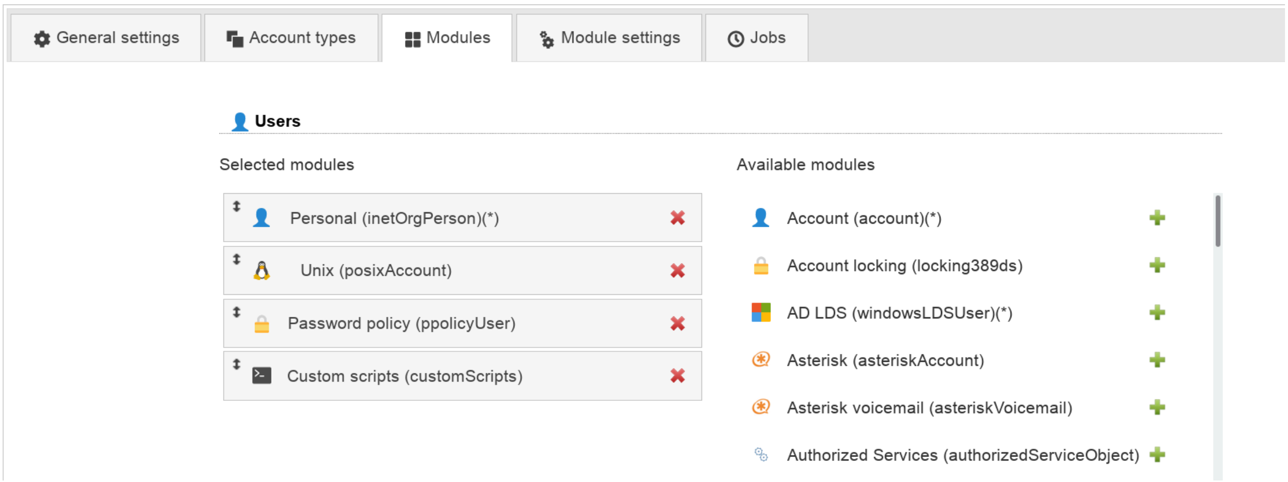
Special characters that must be escaped with "\": "\", ".", "(", ")"

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

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.



Users

Selected modules

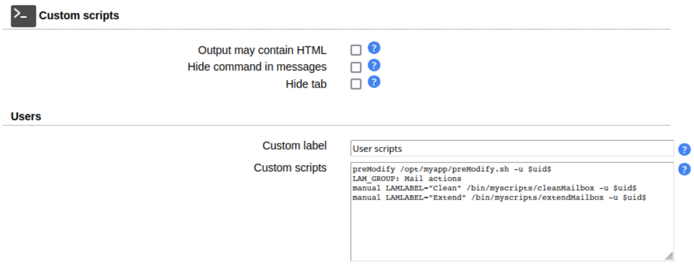
- Personal (inetOrgPerson)(*)
- Unix (posixAccount)
- Password policy (ppolicyUser)
- Custom scripts (customScripts)

Available modules

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

In "Module settings" you can specify multiple scripts for each action type (e.g. preModify) 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. Please note that the syntax changed with version 9.2 (see below).



Custom scripts

Output may contain HTML □

Hide command in messages □

Hide tab □

Users

Custom label: User scripts

Custom scripts:

```
preModify /opt/myapp/preModify.sh -u $uid$
LAM_GROUP: Mail actions
manual LAMLABEL="Clean" /bin/myscripts/cleanMailbox -u $uid$
manual LAMLABEL="Extend" /bin/myscripts/extendMailbox -u $uid$
```

Label:

Here you can enter a descriptive label for the module tab inside LAM.

Syntax:

Please enter one script per line. Each line has the following format: <action> <script>

E.g.: preModify /usr/bin/myCustomScript -u uid

Syntax (pre 9.2):

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 LAMLABEL="text" before the command then LAM will use the text as label for the button in account edit screen.

Script:

You can execute any script which is located on the filesystem of your webserver. The path may be absolute or relative to the PATH-variable of the environment of your webserver process. It is also possible to add commandline arguments to your scripts. Additionally, LAM will resolve wildcards to LDAP attributes. If your script includes an wildcard in the format $ATTRIBUTE$ then LAM will replace it with the attribute value of the current LDAP entry. The values of multi-value attributes are separated by commas. E.g. if you create an account with the attribute "uid" and value "steve" then LAM will resolve "uid" to "steve".

Please note that manual scripts can only use the current LDAP attribute values of the account. Any modifications done that are not saved will not be available. Manual scripts are also not available for new accounts that are not yet saved to LDAP.

You can switch LAM's logging to debug mode if you are unsure which attributes with which values are available.

The following special wildcards are available for automatic scripts:

- **$INFO.lamLoginDn$:** the DN of the user that is logged in to LAM.
- **$INFO.lamProfileName$:** the current server or self service profile name
- **$INFO.debug$:** list of all possible wildcards and their values (e.g. "$objectClass$:posixAccount,inetOrgPerson; $loginShell$:/bin/bash; $gidNumber$:12345; uid:userid...")
- **$INFO.userPasswordClearText$:** cleartext password when Unix/Windows password is changed (e.g. useful for external password synchronisation) for new/modified accounts
- **$INFO.userPasswordStatusChange$:** provides additional information if the Personal/Unix password locking status was changed, possible values: locked, unlocked, unchanged
- **$INFO.passwordSelfResetAnswerClearText$**: cleartext answer to security question
- **$INFO.389lockingStatusChange$:** for 389ds account locking, provides information if account was unlocked. Possible values: unchanged, unlocked
- **$INFO.389deactivationStatusChange$:** for 389ds account locking, provides information if account was deactivated. Possible values: unchanged, activated, deactivated
- **$INFO.isNewAccount$:** specifies if the account already exists or is newly created (yes|no)
- **$INFO.passwordUpdated$:** specifies if the user password was changed (yes|no)
- **$INFO.passwordChangeType$:** password type (manual|random|none) where "none" means no password change
- **$INFO.passwordChangeModules$:** module names of password change operation (e.g. "posixAccount")
- **$INFO.forcePasswordChange$:** a password change was forced (yes|no)
- **$INFO.sendPasswordViaEmail$:** send password via email (yes|no)
- **$INFO.sendPasswordAlternateAddress$:** alternate email address for password email if set (e.g. "test@example.com")
- **$NEW.<attribute>$:** the value of a new attribute (e.g. $NEW.telephoneNumber$) for modified accounts
- **$DEL.<attribute>$:** the value of a deleted attribute (e.g. $DEL.telephoneNumber$) for modified accounts
- **$MOD.<attribute>$:** the new value of a modified attribute (e.g. $MOD.telephoneNumber$) for modified accounts
- **$ORIG.<attribute>$:** the original value of an attribute (e.g. $ORIG.telephoneNumber$) for modified accounts

Grouping of manual scripts:

If you have a larger number of manual scripts then you can divide them into groups. Add a line "LAM_GROUP: My group description" when you want to start a new group.

Example:

```
preModify /opt/myapp/preModify.sh -u $uid$
LAM_GROUP: Mail actions
manual LAMLABEL="Clean" /bin/myscripts/cleanMailbox -u $uid$
manual LAMLABEL="Extend" /bin/myscripts/extendMailbox -u $uid$
```

Interactive parameters for manual scripts

You can define parameters that are specified by the user on the script execution page. E.g., this can be used to specify a target environment (dev/qa/prod).

Interactive parameters allow the user to select the right value instead of having the need to duplicate script entries.

Format: LAM_{TYPE}_{NAME}: {label}={value(s)}

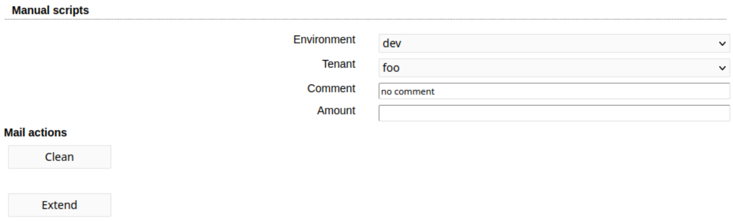
Possible input types:

- Selection
  - Parameter name needs to start with "LAM_SELECTION_", e.g. "LAM_SELECTION_ENV".
  - Values must be separated by semicolons (e.g. "dev;qa;prod")
- Text input
  - Parameter name needs to start with "LAM_TEXT_", e.g. "LAM_TEXT_COMMENT".
  - Value is optional, will be used as default if present.

The parameters can then be used as wildcards in the commands similar to attribute values.

Example:

```
LAM_SELECTION_ENV: Environment=dev;qa;prod
LAM_SELECTION_TENANT: Tenant=foo;bar
LAM_TEXT_COMMENT: Comment=no comment
LAM_TEXT_AMOUNT: Amount
manual LAMLABEL="Clean" /bin/myscripts/cleanMailbox -u $uid$ -e $LAM_SELECTION_ENV$
manual LAMLABEL="Extend" /bin/myscripts/extendMailbox -u $uid$ -e $LAM_SELECTION_TENANT$
manual /bin/myscripts/syncWithCRM -u $uid$ -c $LAM_TEXT_COMMENT$
manual LAMLABEL="Some app" /bin/myscripts/syncWithSomeApp -u $uid$ -a $LAM_TEXT_AMOUNT$
```



Manual scripts

Environment: dev

Tenant: foo

Comment: no comment

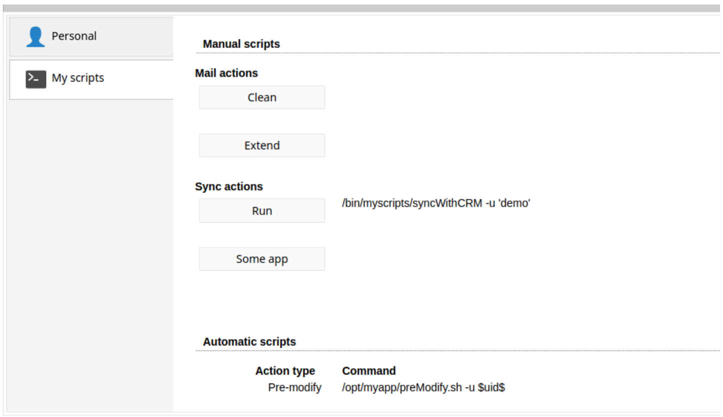
Amount:

Mail actions

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.



Manual scripts

Mail actions

Clean

Extend

Sync actions

Run /bin/myscripts/syncWithCRM -u 'demo'

Some app

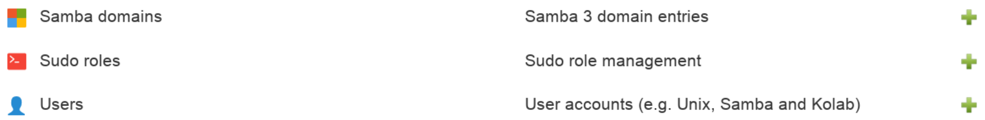
Automatic scripts

Action type	Command
Pre-modify	/opt/myapp/preModify.sh -u uid

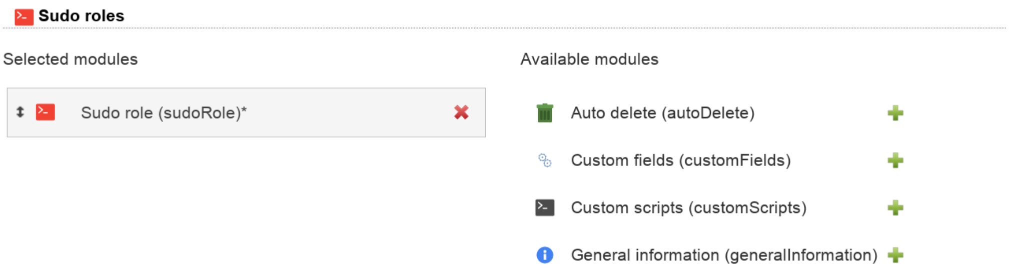
Sudo roles (LAM Pro)

You can manage your sudo roles in LDAP if you have installed the sudo-ldap package or compiled sudo with LDAP support [http://www.sudo.ws/sudo/readme_ldap.html].

To activate sudo management in LAM Pro edit your server profile and add the type "Sudo roles".



Samba domains	Samba 3 domain entries	+
Sudo roles	Sudo role management	+
Users	User accounts (e.g. Unix, Samba and Kolab)	+



Sudo roles

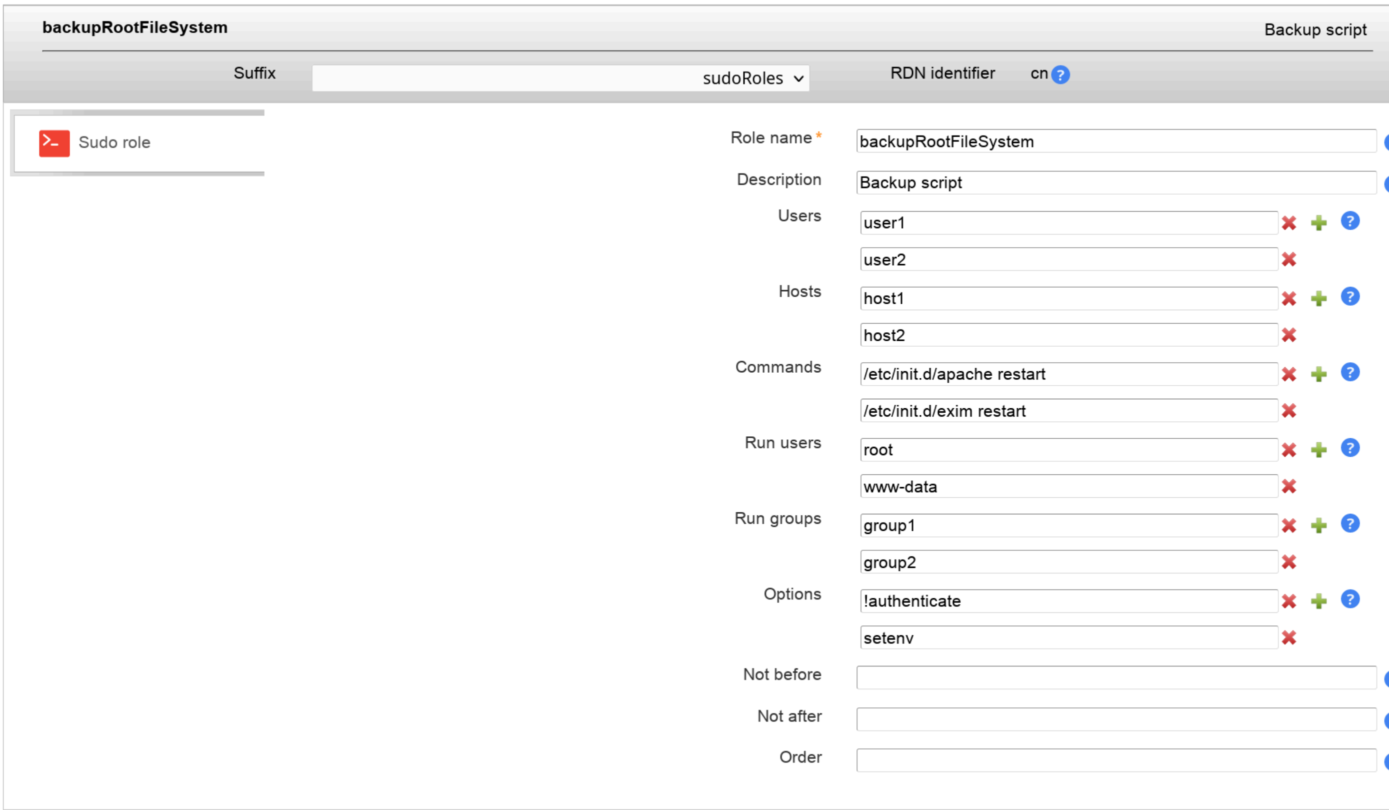
Selected modules

- Sudo role (sudoRole)* ✖

Available modules

- Auto delete (autoDelete) +
- Custom fields (customFields) +
- Custom scripts (customScripts) +
- General information (generalInformation) +

Now you can create sudo commands.



backupRootFileSystem Backup script

Suffix: sudoRoles RDN identifier: cn

Sudo role

Role name*	backupRootFileSystem
Description	Backup script
Users	user1 user2
Hosts	host1 host2
Commands	/etc/init.d/apache restart /etc/init.d/exim restart
Run users	root www-data
Run groups	group1 group2
Options	!authenticate setenv
Not before	
Not after	
Order	

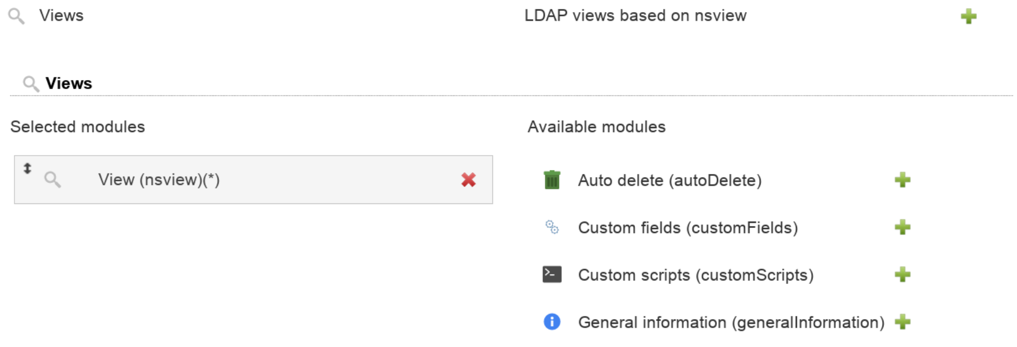
The sudo roles in LDAP work similar to those in /etc/sudoers. You can specify who may run which commands as which user. It is also possible to specify options like NOPASSWD.

LDAP views based on nsview (LAM Pro)

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

Configuration:

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



Views LDAP views based on nsview

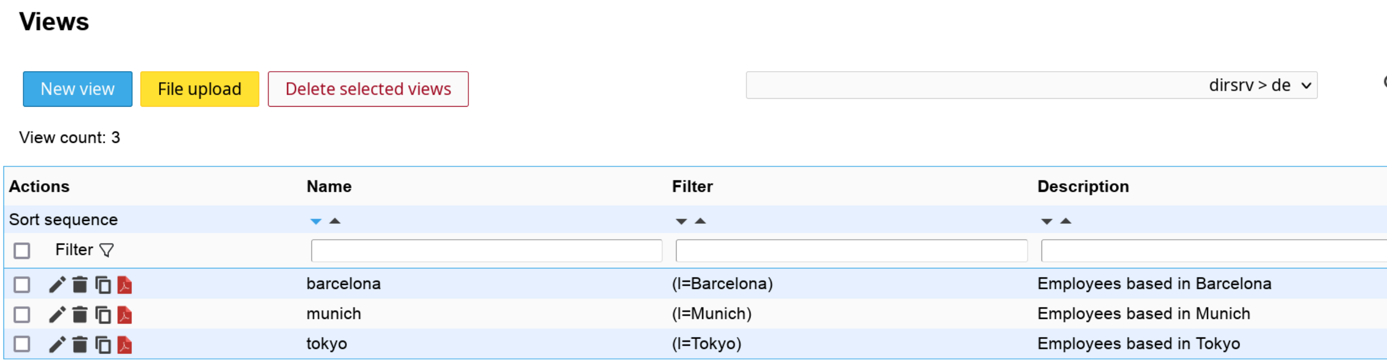
Views

Selected modules: View (nsview)(*)

Available modules:

- Auto delete (autoDelete)
- Custom fields (customFields)
- Custom scripts (customScripts)
- General information (generalInformation)

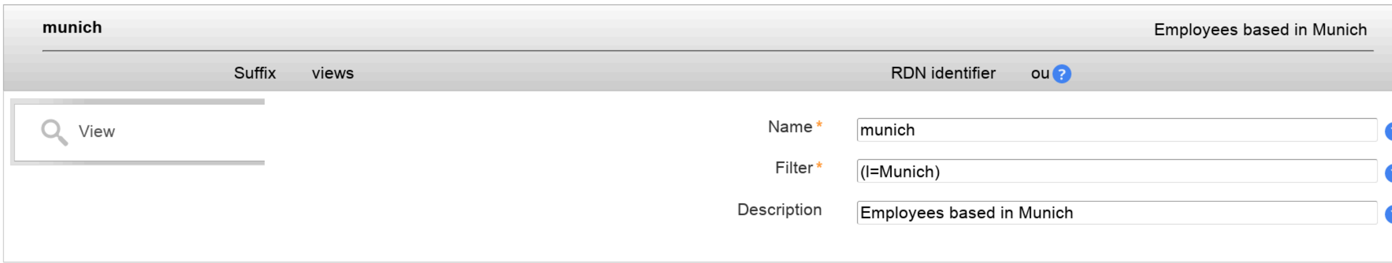
Now you are ready to create your views. Each view has a name, LDAP filter and an optional description.



Views

View count: 3

Actions	Name	Filter	Description
Sort sequence			
□ Filter			
□	barcelona	(l=Barcelona)	Employees based in Barcelona
□	munich	(l=Munich)	Employees based in Munich
□	tokyo	(l=Tokyo)	Employees based in Tokyo



munich — Employees based in Munich

Suffix: views — RDN identifier: ou

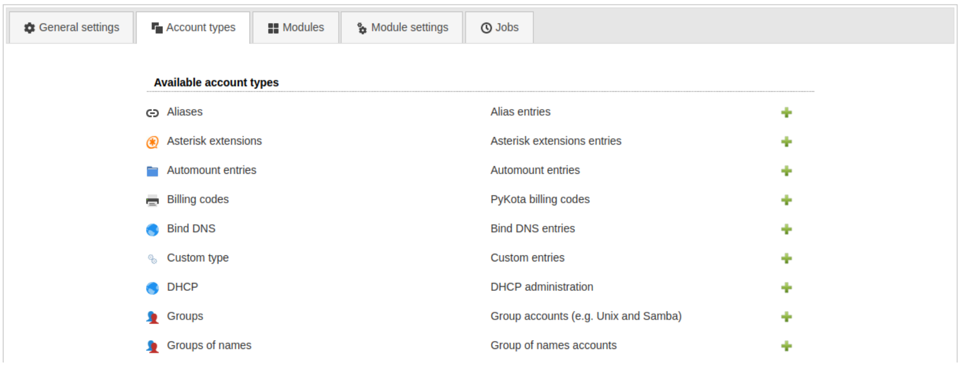
Name *	munich
Filter *	(l=Munich)
Description	Employees based in Munich

Apache Guacamole (LAM Pro)

Apache Guacamole offers remote desktop connections based on RDP/VNC.

Configuration

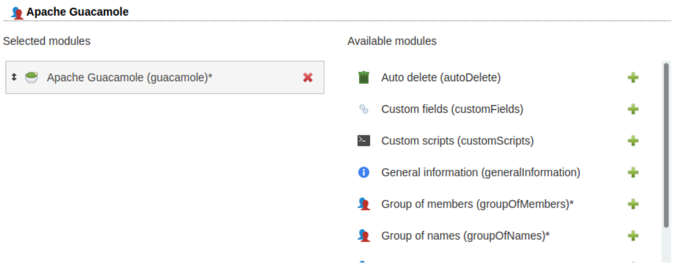
Please create a new group or group of names type on tab "Account types".



Available account types

Aliases	Alias entries
Asterisk extensions	Asterisk extensions entries
Automount entries	Automount entries
Billing codes	PyKota billing codes
Bind DNS	Bind DNS entries
Custom type	Custom entries
DHCP	DHCP administration
Groups	Group accounts (e.g. Unix and Samba)
Groups of names	Group of names accounts

Then add the Guacamole module on tab "Modules".

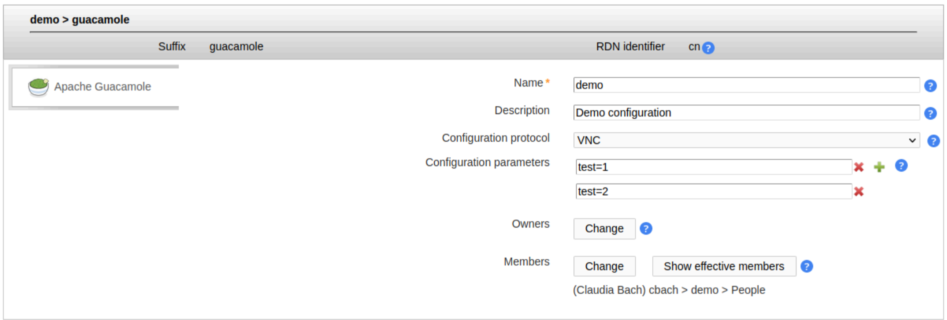


Apache Guacamole

Selected modules:
- Apache Guacamole (guacamole)*

Available modules:
- Auto delete (autoDelete)
- Custom fields (customFields)
- Custom scripts (customScripts)
- General information (generalInformation)
- Group of members (groupOfMembers)*
- Group of names (groupOfNames)*

Now you can manage the Guacamole entries with protocol and parameters.


demo > guacamole

Suffix guacamole RDN identifier cn

Name* demo

Description Demo configuration

Configuration protocol VNC

Configuration parameters test=1
test=2

Owners Change

Members Change Show effective members
(Claudia Bach) cbach > demo > People

Auto delete (LAM Pro)

This module allows to mark any new entry to be marked for auto deletion. The cleanup is done by the LDAP server itself. Please note that this will not delete any relations etc. in other entries (e.g. group memberships).

Requirements

- LDAP server with DDS (Dynamic Directory Services) support: your LDAP server needs to be configured to allow auto deletion of entries. See e.g. OpenLDAP configuration [http://www.openldap.org/doc/admin24/overlays.html].
- Your user has the right to set a deletion date. This is configured on your LDAP server via ACLs. E.g. OpenLDAP requires manage rights to attribute "entryTtl".

Restrictions

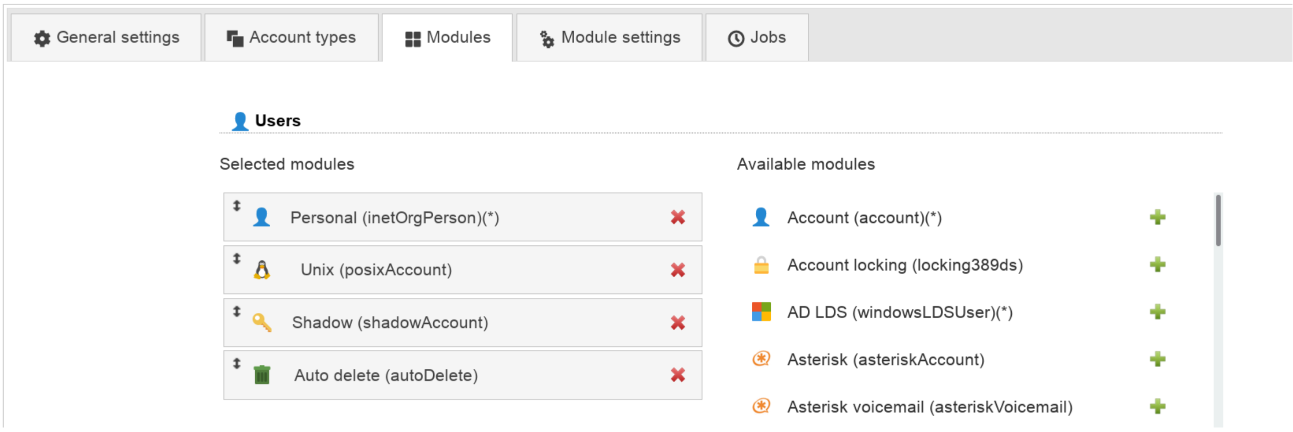
The maximum time for auto deletion is one year and six days. This is a restriction by the DDS standard itself. The deletion date can be extended for existing accounts but always by a maximum of one year and six days.

You should configure the maximum TTL value on your LDAP server as default is often much less than a year.

A deletion date on an existing entry cannot be removed but only be extended.

Configuration

You can add the auto delete module to any account type.



Users

Selected modules

- Personal (inetOrgPerson)(*)
- Unix (posixAccount)
- Shadow (shadowAccount)
- Auto delete (autoDelete)

Available modules

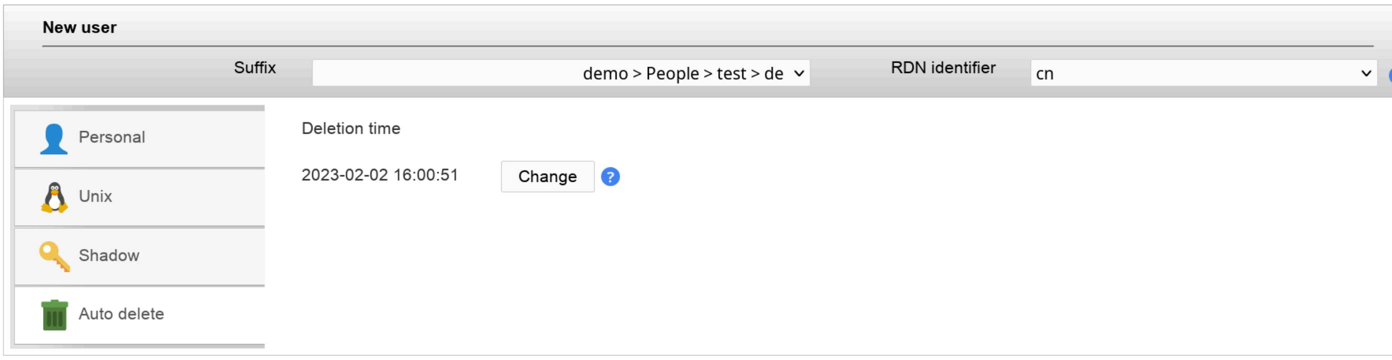
- Account (account)(*)
- Account locking (locking389ds)
- AD LDS (windowsLDSUser)(*)
- Asterisk (asteriskAccount)
- Asterisk voicemail (asteriskVoicemail)

Usage

You can set a deletion time for any new account. Please note the restrictions above. If you get an error about invalid TTL then you might have exceeded the maximum TTL.

Existing accounts cannot be marked for deletion. But you may update the deletion date on existing accounts that are already marked for deletion.

Profile editor can be used to setup a default deletion time.



New user

Suffix: demo > People > test > de

RDN identifier: cn

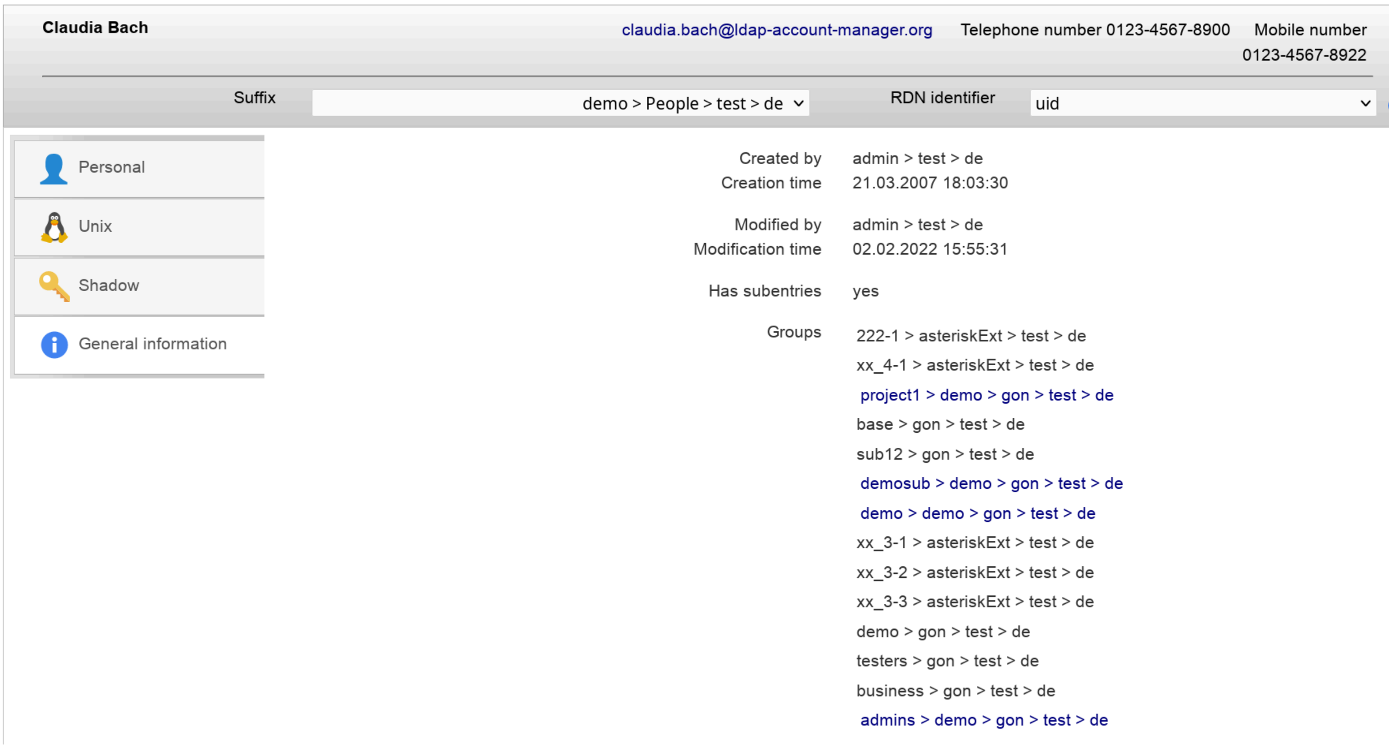
Deletion time

2023-02-02 16:00:51

General information

This module is available for all account types. It shows some internal information about the LDAP entries like the creation time and who modified the entry.

If you use the "memberOf" overlay in OpenLDAP then this will also show group memberships done by the overlay.



Claudia Bach

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

Suffix: demo > People > test > de

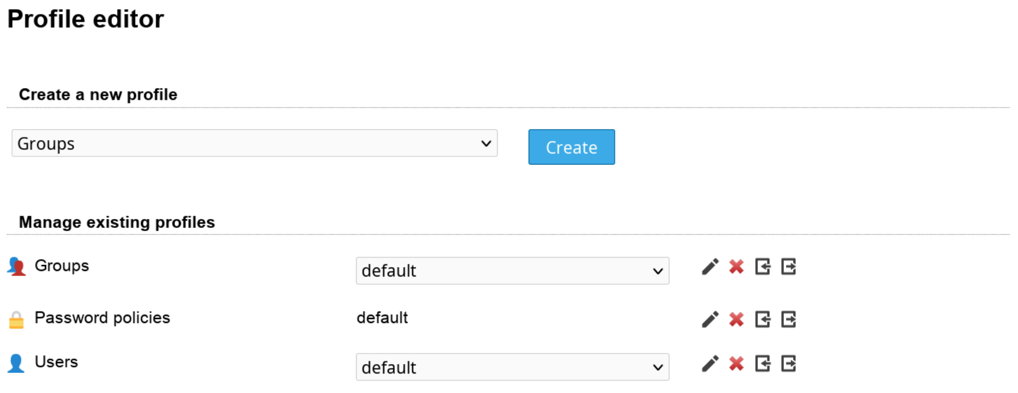
RDN identifier: uid

Created by	admin > test > de
Creation time	21.03.2007 18:03:30
Modified by	admin > test > de
Modification time	02.02.2022 15:55:31
Has subentries	yes
Groups	222-1 > asteriskExt > test > de xx_4-1 > asteriskExt > test > de project1 > demo > gon > test > de base > gon > test > de sub12 > gon > test > de demosub > demo > gon > test > de demo > demo > gon > test > de xx_3-1 > asteriskExt > test > de xx_3-2 > asteriskExt > test > de xx_3-3 > asteriskExt > test > de demo > gon > test > de testers > gon > test > de business > gon > test > de admins > demo > gon > test > de

Chapter 5. Tools

Profile editor

The account profiles are templates for your accounts. Here you can specify default values which can then be loaded when you create accounts. You may also load a template for an existing account to reset it to default values. When you create a new account then LAM will always load the profile named **"default"**. This account profile can include default values for all your accounts.



Profile editor

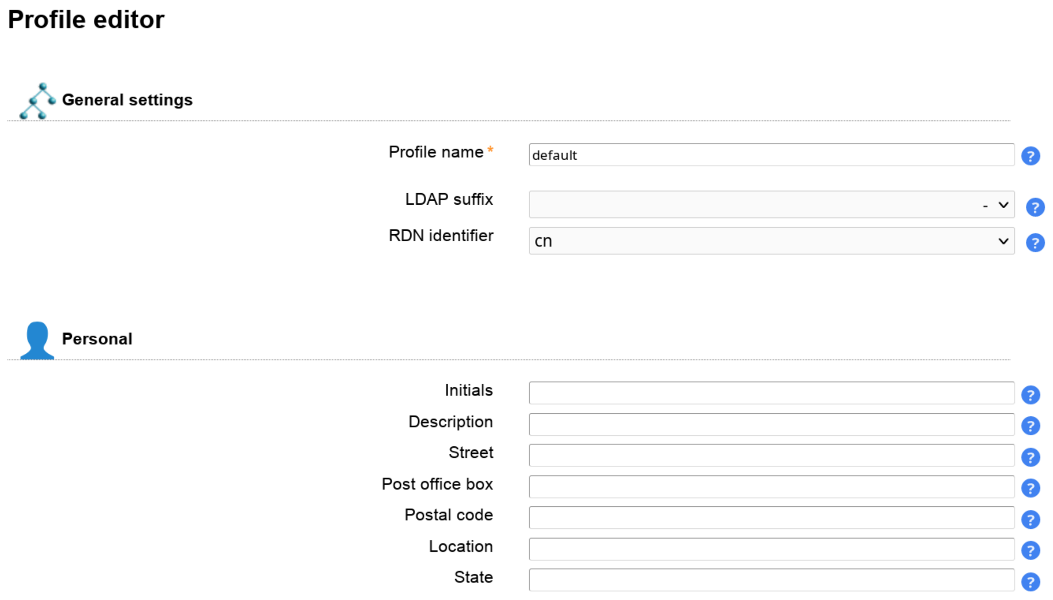
Create a new profile

Groups

Manage existing profiles

Groups	default	
Password policies	default	
Users	default	

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



Profile editor

General settings

Profile name * default

LDAP suffix -

RDN identifier cn

Personal

Initials

Description

Street

Post office box

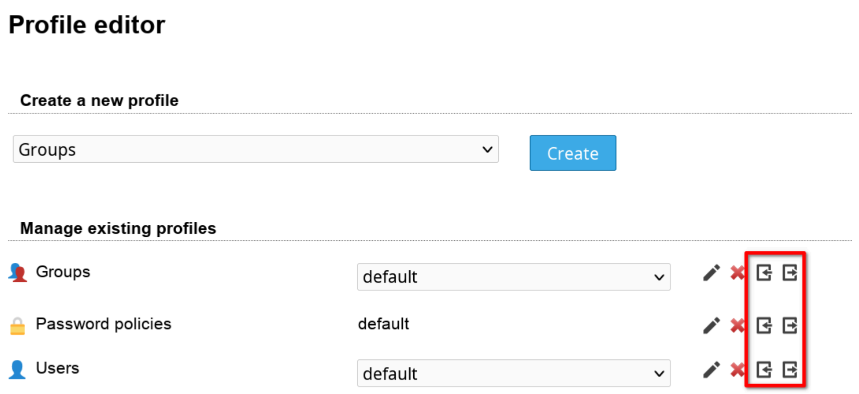
Postal code

Location

State

Import/export:

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



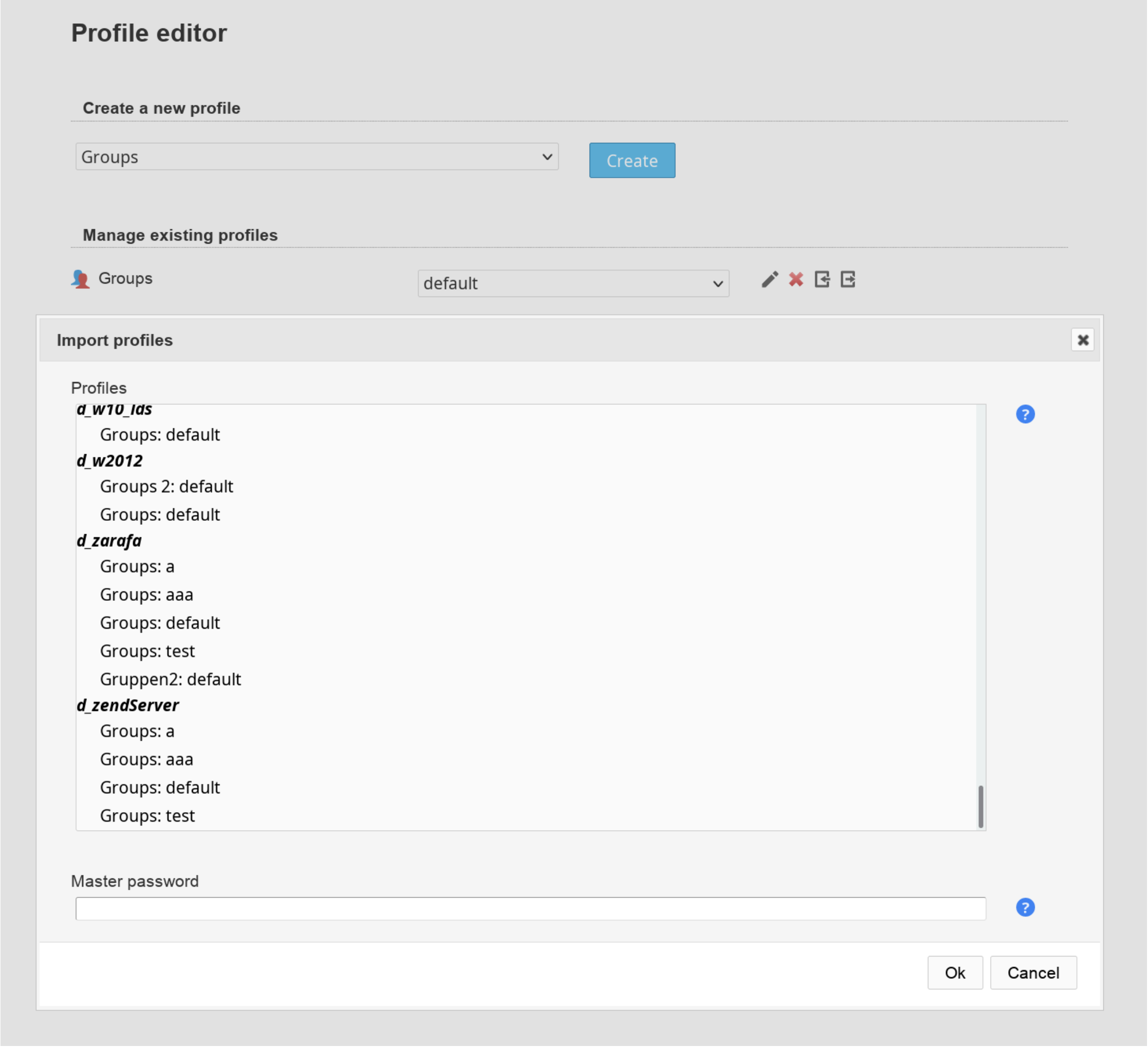
Profile editor

Create a new profile

Groups

Manage existing profiles

Groups	default	
Password policies	default	
Users	default	



Profile editor

Create a new profile

Groups

Manage existing profiles

Groups default

Import profiles

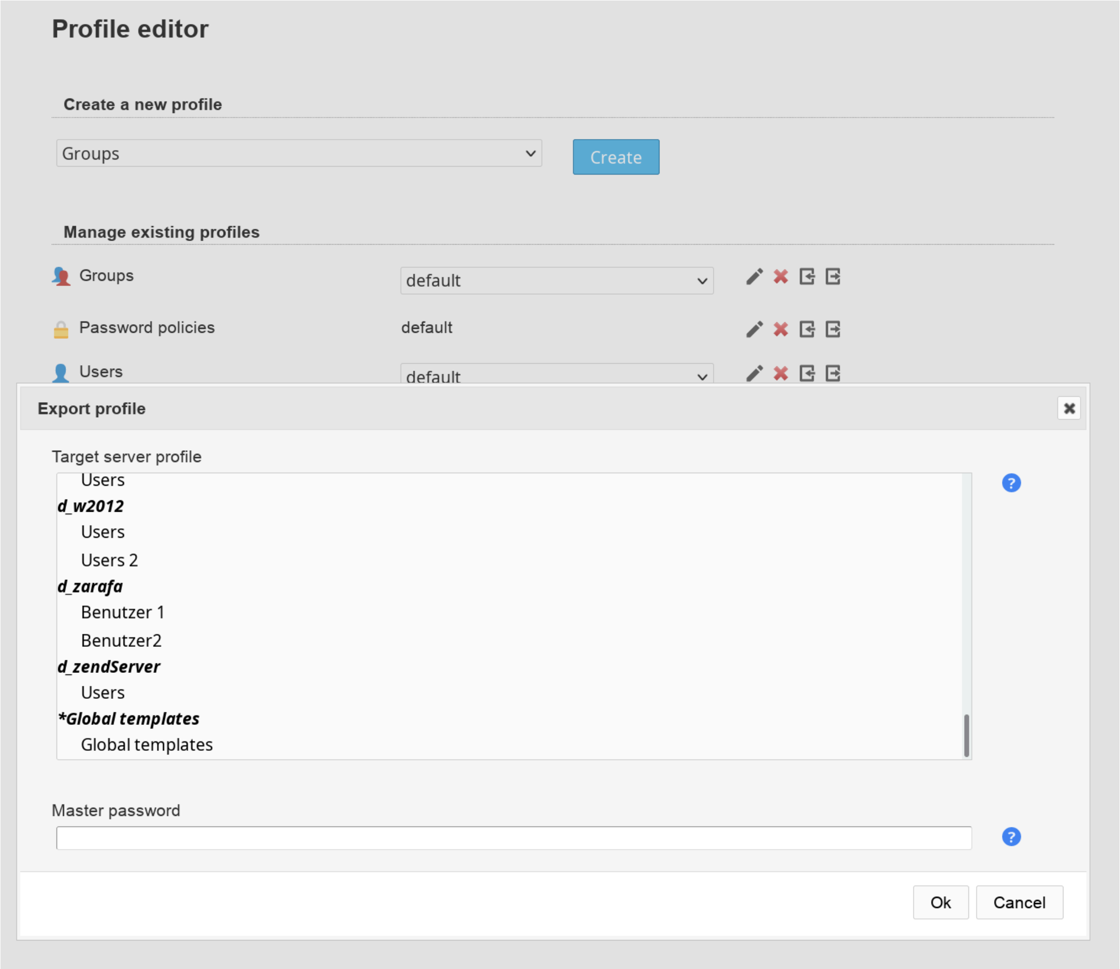
Profiles

d_w10_ids
Groups: default
d_w2012
Groups 2: default
Groups: default
d_zarafa
Groups: a
Groups: aaa
Groups: default
Groups: test
Gruppen2: default
d_zendServer
Groups: a
Groups: aaa
Groups: default
Groups: test

Master password

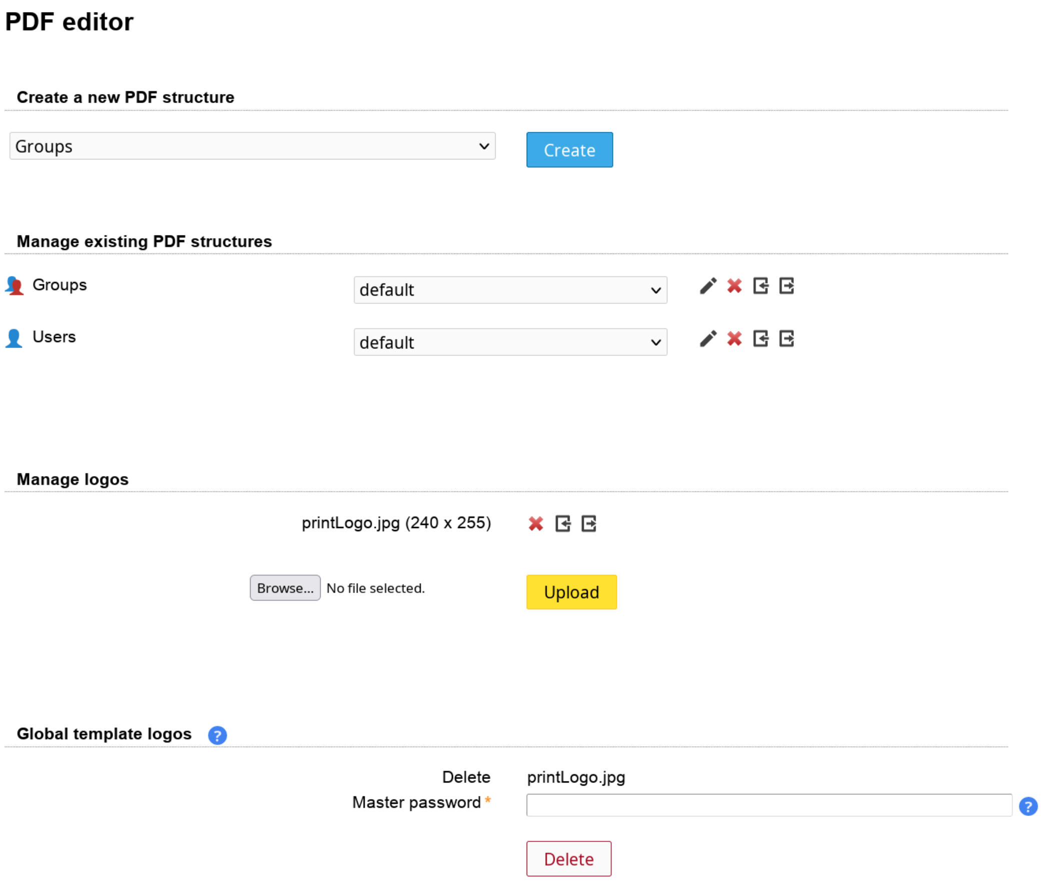
There is a special export target called "*Global templates". All profiles exported here will be copied to all other server profiles (incl. new ones). But existing profiles with the same name are not overwritten. So a profile in global templates is treated as default profile for all server profiles.

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



PDF editor

All accounts in LAM may be exported as PDF files. You can specify the page structure and displayed information by editing the PDF profiles.



PDF editor

Create a new PDF structure

Groups

Manage existing PDF structures

Groups	default
Users	default

Manage logos

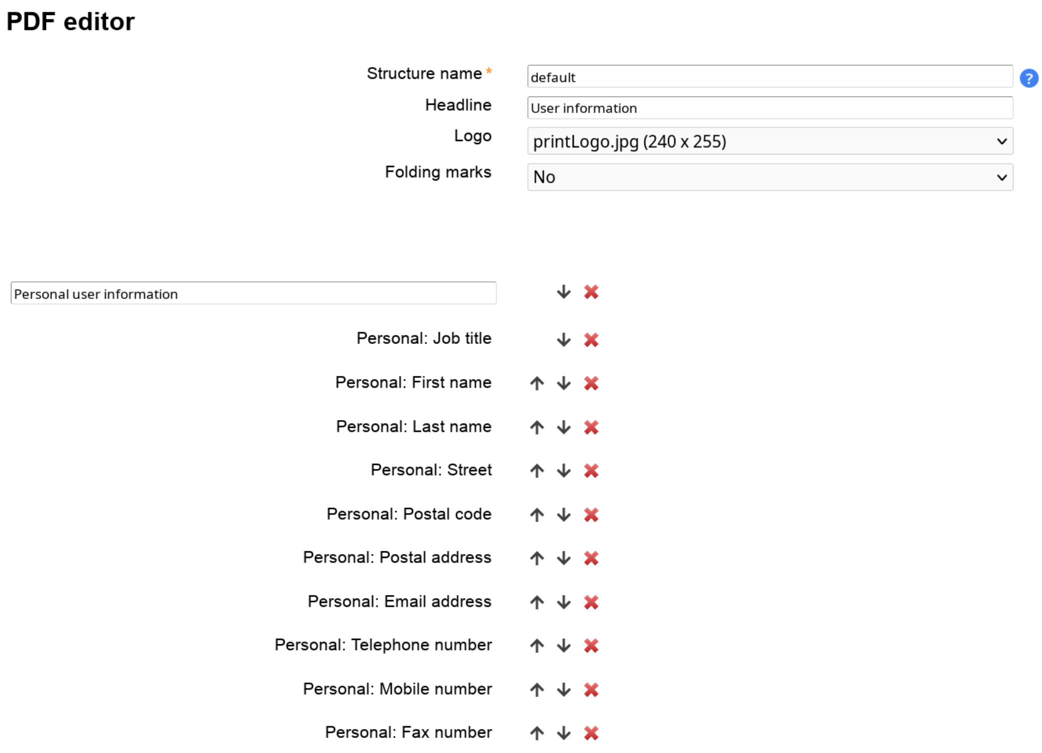
printLogo.jpg (240 x 255)

Global template logos

Delete: printLogo.jpg

Master password *

When you export accounts to PDF then each account will get its own page inside the PDF. There is a headline on each page where you can show a page title. You may also add a logo to each page. To add more logos please use the logo management on the PDF editor main page.



PDF editor

Structure name *	default
Headline	User information
Logo	printLogo.jpg (240 x 255)
Folding marks	No

Personal user information

Personal: Job title

Personal: First name

Personal: Last name

Personal: Street

Personal: Postal code

Personal: Postal address

Personal: Email address

Personal: Telephone number

Personal: Mobile number

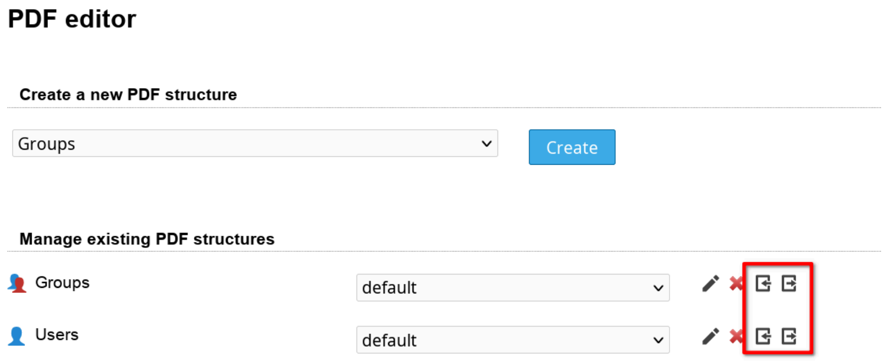
Personal: Fax number

The main part is structured into sections of information. Each section has a title. This can either be static text or the value of an attribute. You may also insert a static text block as section. Sections can be moved by using the arrows next to the section title.

Each section can contain multiple fields which usually represent LDAP attributes. You can simply add new fields by selecting the field name and its position. Then use the arrows to move the field inside the section.

Import/export:

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



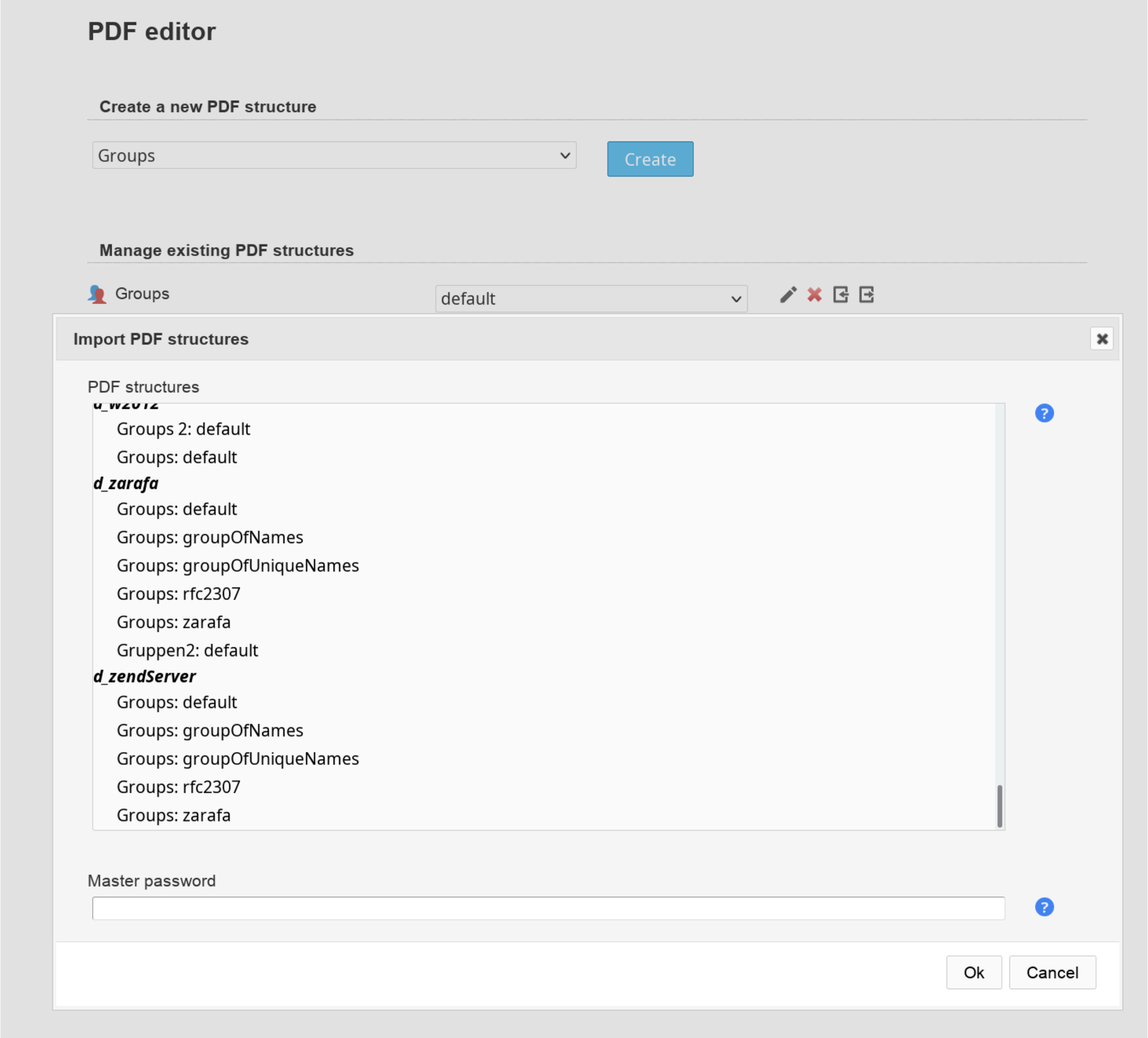
PDF editor

Create a new PDF structure

Groups

Manage existing PDF structures

Groups	default
Users	default



PDF editor

Create a new PDF structure

Groups

Manage existing PDF structures

Groups: default

Import PDF structures

PDF structures

d_w2012
- Groups 2: default
- Groups: default

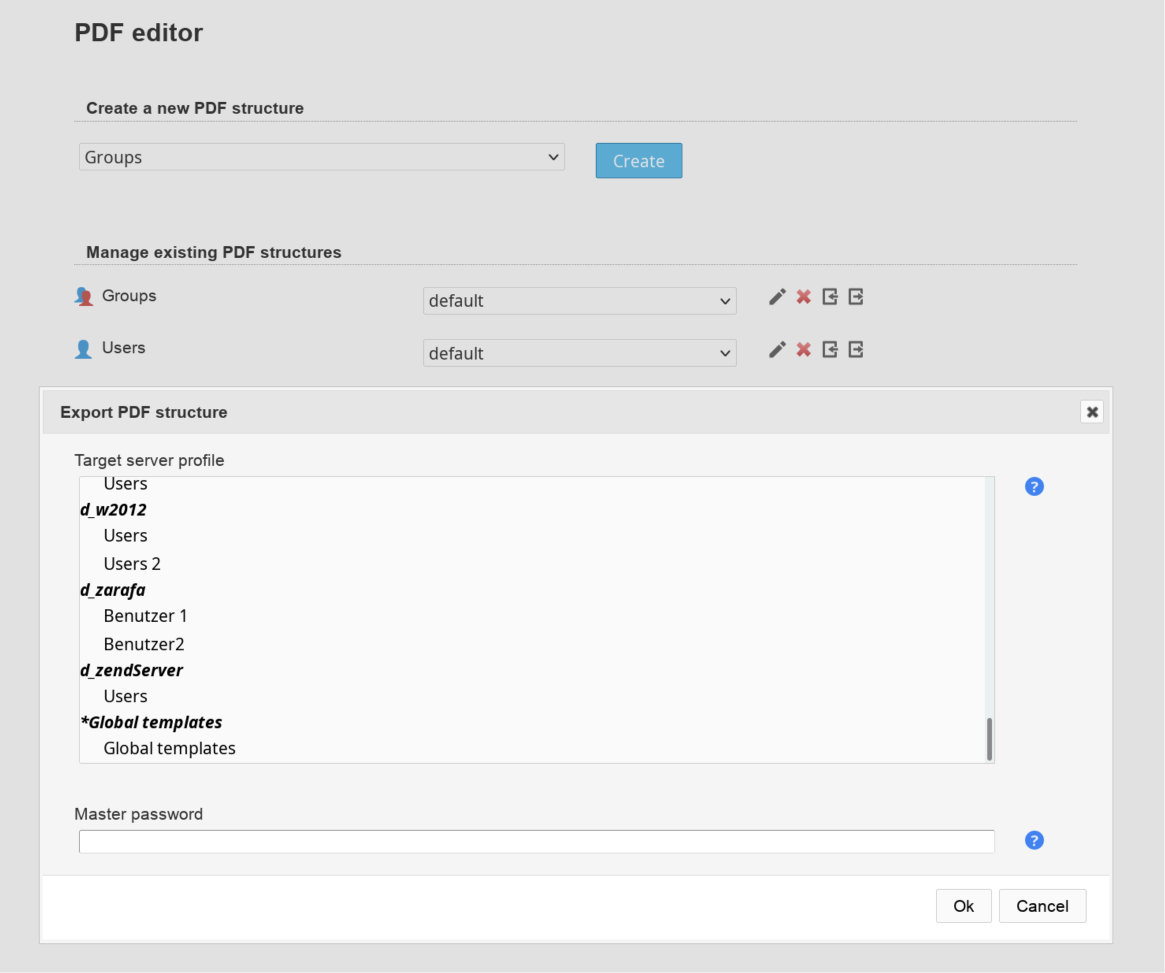
d_zarafa
- Groups: default
- Groups: groupOfNames
- Groups: groupOfUniqueNames
- Groups: rfc2307
- Groups: zarafa
- Gruppen2: default

d_zendServer
- Groups: default
- Groups: groupOfNames
- Groups: groupOfUniqueNames
- Groups: rfc2307
- Groups: zarafa

Master password

There is a special export target called "*Global templates". All PDF structures exported here will be copied to all other server profiles (incl. new ones). But existing PDF structures with the same name are not overwritten. So a PDF structure in global templates is treated as default structure for all server profiles.

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



PDF editor

Create a new PDF structure

Groups

Manage existing PDF structures

Groups: default

Users: default

Export PDF structure

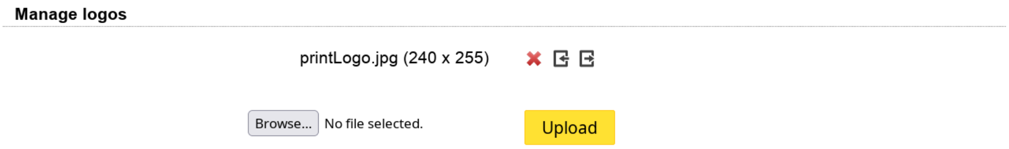
Target server profile

Users
d_w2012
Users
Users 2
d_zarafa
Benutzer 1
Benutzer2
d_zendServer
Users
Global templates
Global templates

Master password

Logo management:

You can upload image files to put a custom logo on the PDF files. The image file name must end with .png or .jpg.



Manage logos

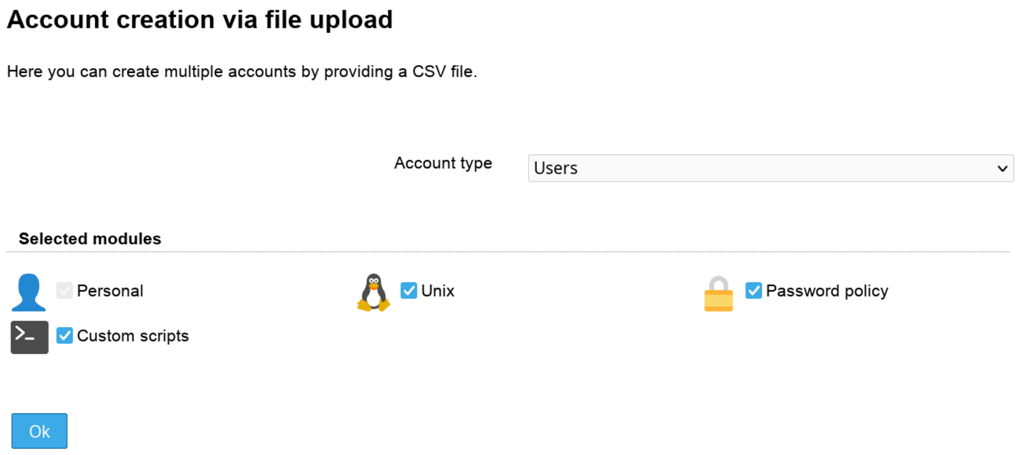
printLogo.jpg (240 x 255)

File upload

When you need to create lots of accounts then you can use LAM's file upload to create them. In contrast to LDAP import/export this operates on account type level.

LAM will read a CSV formatted file and create the related LDAP entries. Please check the data in you CSV file carefully. LAM will do less checks for the file upload than for single account creation.

At the first page please select the account type and what extensions should be activated.



Account creation via file upload

Here you can create multiple accounts by providing a CSV file.

Account type: Users

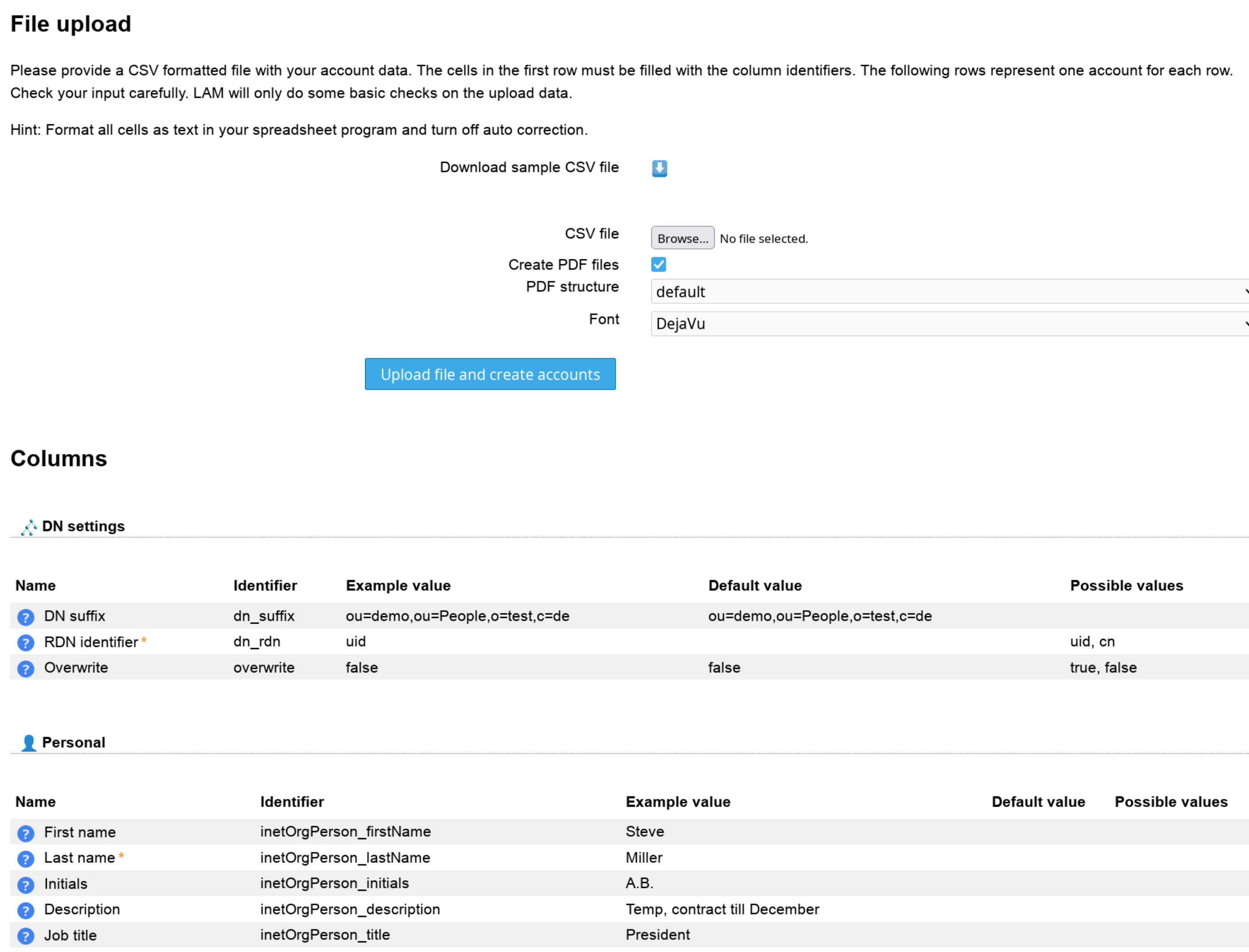
Selected modules

☑ Personal ☑ Unix ☑ Password policy
☑ Custom scripts

The next page shows all available options for the file upload. You will also find a sample CSV file which can be used as template for your CSV file. All red options are required columns in the file. You need to specify a value for each account.

When you upload the CSV file then LAM first does some checks on this file. This includes syntax checks and if all required data was entered. No changes in the LDAP directory are done at this time.

If the checks were successful then LAM will ask again if you want to create the accounts. You will also have the chance to check the upload by viewing the changes in LDIF format.



File upload

Please provide a CSV formatted file with your account data. The cells in the first row must be filled with the column identifiers. The following rows represent one account for each row. Check your input carefully. LAM will only do some basic checks on the upload data.

Hint: Format all cells as text in your spreadsheet program and turn off auto correction.

Download sample CSV file

CSV file: Browse... No file selected.

Create PDF files: ☑

PDF structure: default

Font: DejaVu

Upload file and create accounts

Columns

DN settings

Name	Identifier	Example value	Default value	Possible values
DN suffix	dn_suffix	ou=demo,ou=People,o=test,c=de	ou=demo,ou=People,o=test,c=de	
RDN identifier*	dn_rdn	uid		uid, cn
Overwrite	overwrite	false	false	true, false

Personal

Name	Identifier	Example value	Default value	Possible values
First name	inetOrgPerson_firstName	Steve		
Last name*	inetOrgPerson_lastName	Miller		
Initials	inetOrgPerson_initials	A.B.		
Description	inetOrgPerson_description	Temp, contract till December		
Job title	inetOrgPerson_title	President		

Multi edit

This tool allows you to modify a large list of LDAP entries in batch mode. You can add new attributes/object classes, remove attributes and set attributes to a specific value.

At the beginning, you need to specify where the entries are stored that should be changed. You can select an account suffix, the tree suffix or enter your own DN by selecting "Other".

Next, enter an additional LDAP filter to limit the entries that should be changed. E.g. use "(objectclass=inetOrgPerson)" to filter for users. You may also enter e.g. "(!(objectClass=passwordSelfReset))" to match all accounts that do not yet have the password self reset feature.

Now, it is time to define the changes that should be done. The following operations are possible:

- Add: Adds an attribute value if not yet existing. Please do not use for single-value attributes that already have a value.
- Modify: Sets an attribute to the given value. If the attribute does not yet exist then it is added. If the attribute has multiple values then all other values are removed.
- Delete: Deletes the specified value from this attribute. If you leave the value field blank then all attribute values are removed.

Please note that all actions are run as separate LDAP commands. You cannot add an object class and a required attribute at the same time.

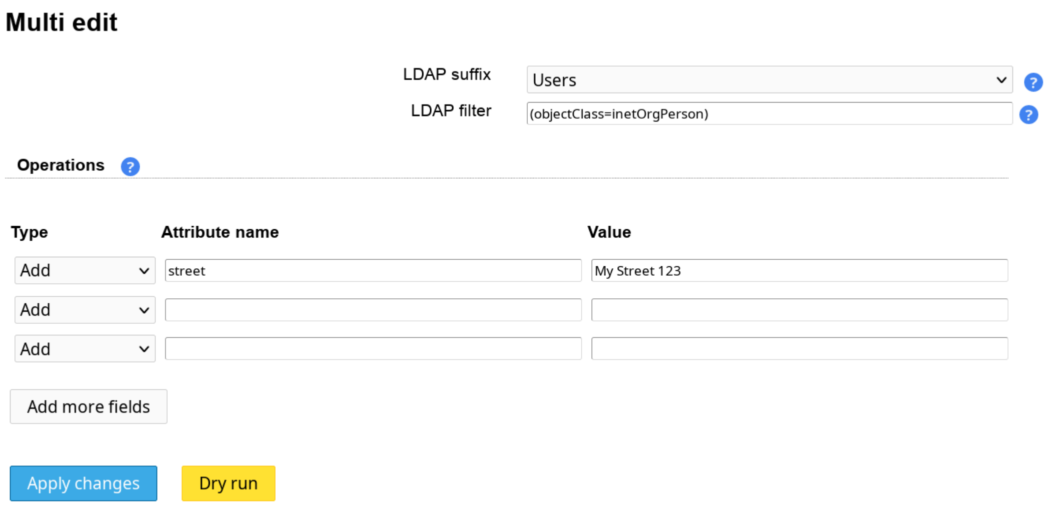
You can use the following wildcards to use existing attribute data of the entries:

- %attribute%: attribute value
- @attribute@: first character of attribute
- ?attribute?: first character of attribute in lower case
- !attribute!: first character of attribute in upper case
- ??attribute??: attribute in lower case
- !!attribute!!: attribute in upper case
- ((attribute)): space if attribute is set
- §attribute|;§; attribute values separated by ";" (you can set other separators if you want)

Examples for attributes gn="Steve", sn="Miller" and memberUid=("user1", "user2") (specified value -> resulting LDAP value):

Table 5.1.

Value	Resulting LDAP value
my value	my value
%gn%	Steve
%gn%((gn))%sn%	Steve Miller (would be "Miller" if gn is empty)
§memberUid|, §	user1, user2



Multi edit

LDAP suffix: Users

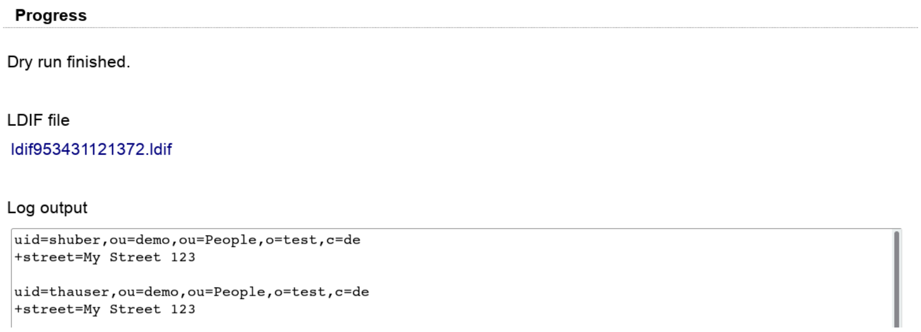
LDAP filter: (objectClass=inetOrgPerson)

Operations

Type	Attribute name	Value
Add	street	My Street 123
Add		
Add		

Dry run

You should always start with a dry run. It will not do any changes to your LDAP directory but print out all modifications that will be done. You will also be able to download the changes in LDIF format to use with ldapmodify. This is useful if you want to adjust some actions manually.



Progress

Dry run finished.

LDIF file

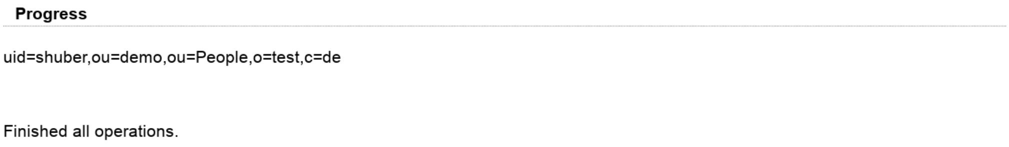
ldif953431121372.ldif

Log output

```
uid=shuber,ou=demo,ou=People,o=test,c=de
+street=My Street 123

uid=thauser,ou=demo,ou=People,o=test,c=de
+street=My Street 123
```

Apply changes

This will run the actions against your LDAP directory. You will see which accounts are edited in the progress area and also if any errors occurred.



Progress

uid=shuber,ou=demo,ou=People,o=test,c=de

Finished all operations.

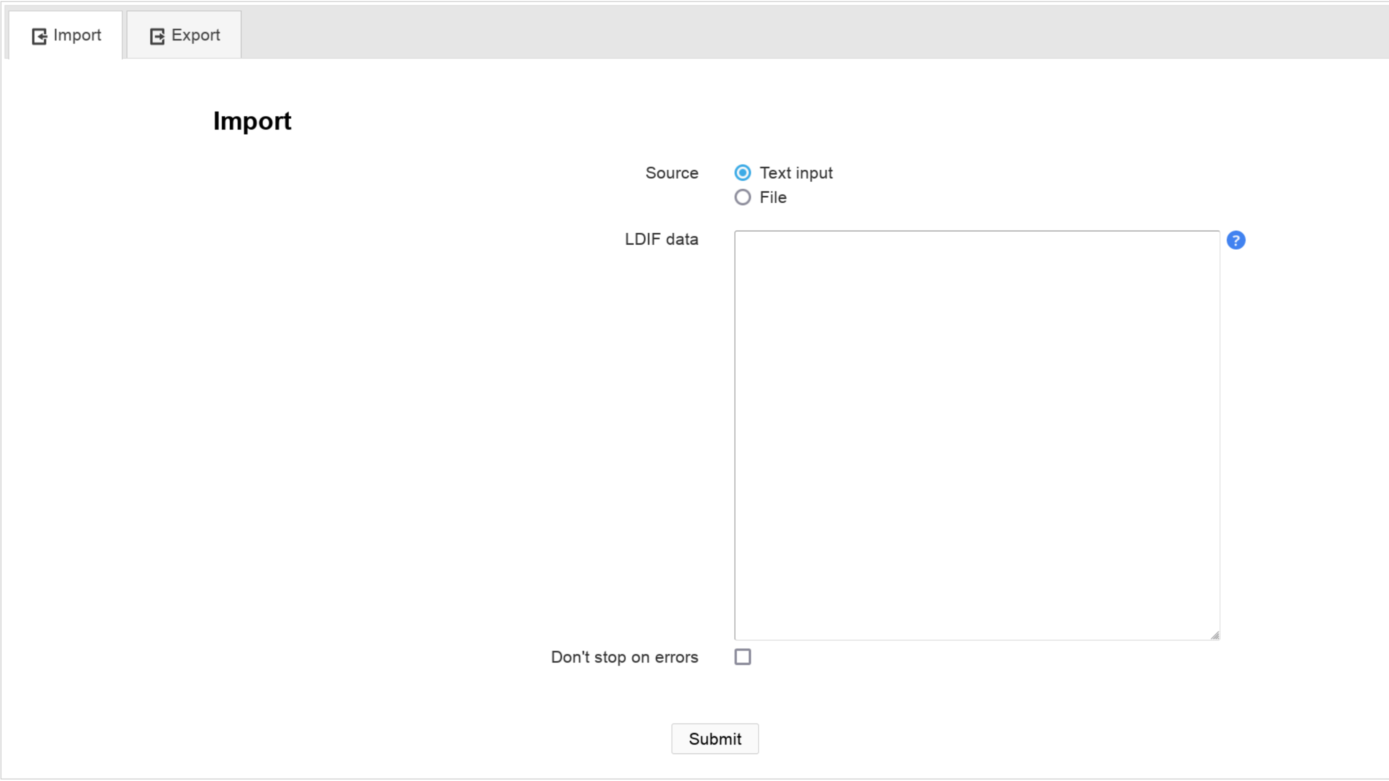
LDAP import/export

Here you can import and export plain LDAP data. In contrast to file upload this operates on plain LDAP attribute level.

Import

The LDAP import supports input data in LDIF [https://en.wikipedia.org/wiki/LDAP_Data_Interchange_Format] format. You can provide plain text or upload an LDIF file.

The "Don't stop on errors" option will cause the import to continue even if entries could not be created.



Import

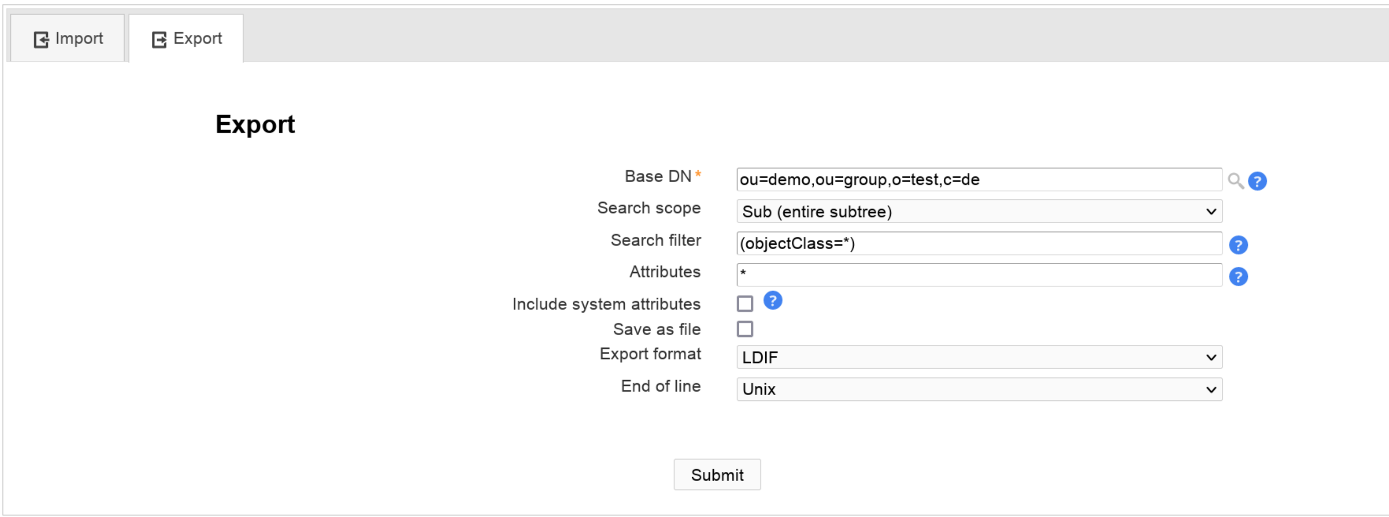
Source: ● Text input ○ File

LDIF data:

Don't stop on errors: □

Export

Here you can export your plain LDAP data as LDIF or CSV file.



Export

Base DN*: ou=demo,ou=group,o=test,c=de

Search scope: Sub (entire subtree)

Search filter: (objectClass=*)

Attributes: *

Include system attributes: □

Save as file: □

Export format: LDIF

End of line: Unix

Base DN: this is the starting point of the export. Enter a DN or press the magnifying glass icon to open the DN selection dialog.

Search scope: You can export just the base DN, base DN + its direct children or the whole subtree.

Search filter: this can be used to filter the entries by specifying a standard LDAP filter. The preselected filter "(objectclass=*)" matches all entries.

Attributes: the list of attributes that should be part of export. "*" matches all standard attributes (excluding system attributes).

Include system attributes: this will also include system attributes like the entry creation time and creator's DN.

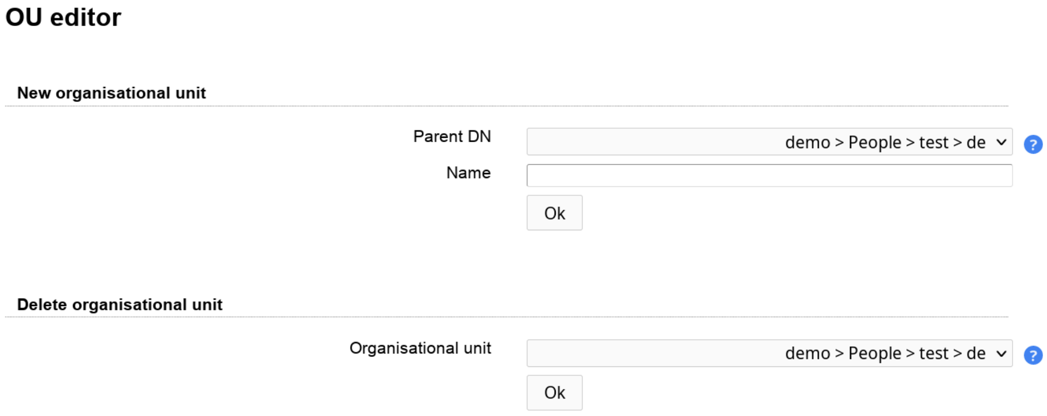
Save as file: will save to file instead of printing the data on the web page.

Export format: you can select LDIF or CSV (e.g. for usage in spreadsheet applications).

End of line: use the one appropriate for your operating system.

OU editor

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



OU editor

New organisational unit

Parent DN: demo > People > test > de

Name:

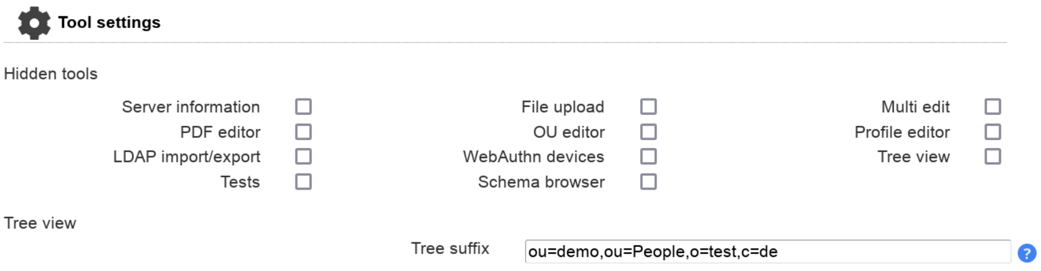
Delete organisational unit

Organisational unit: demo > People > test > de

Tree view

The tree view provides a raw view on your LDAP directory. This feature is for people who are experienced with LDAP and need special functionality which the LAM account modules not provide. E.g. if you want to add a special object class to an account or edit attributes ignoring LAM's syntax checks.

To use this tool you will need to configure its suffix in your LAM server profile on first tab. You can also specify multiple suffixes separated by semicolon.



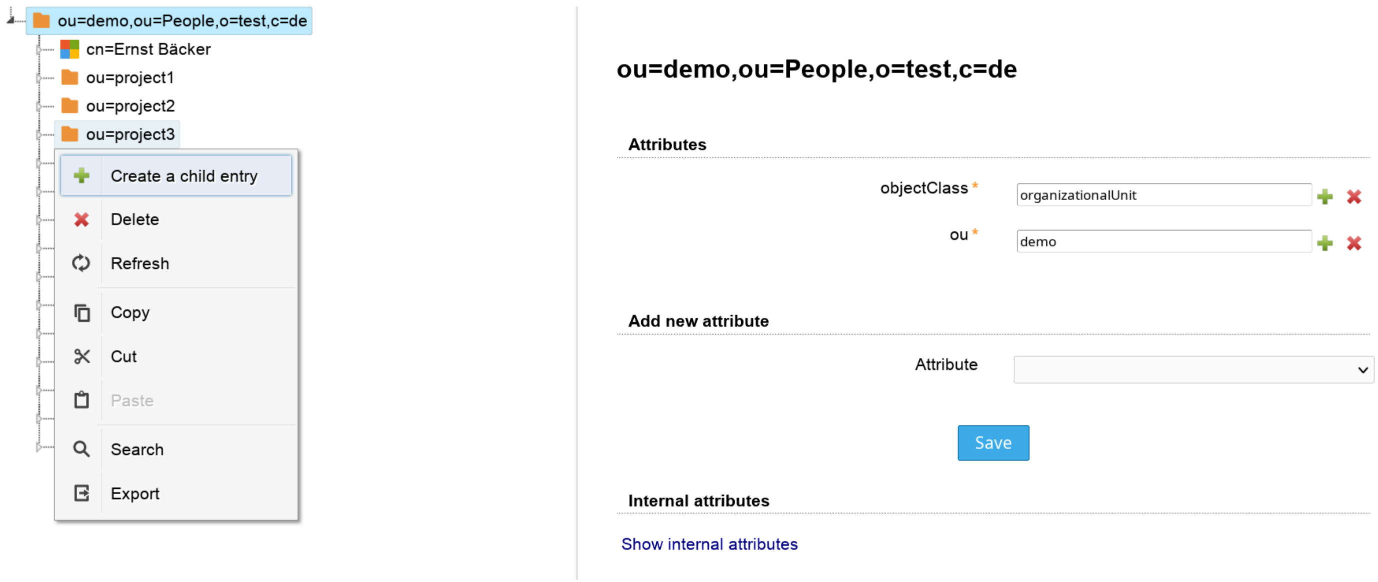
Tool settings

Hidden tools

Server information ☐
PDF editor ☐
LDAP import/export ☐
Tests ☐
File upload ☐
OU editor ☐
WebAuthn devices ☐
Schema browser ☐
Multi edit ☐
Profile editor ☐
Tree view ☐

Tree view

Tree suffix: ou=demo,ou=People,o=test,c=de



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

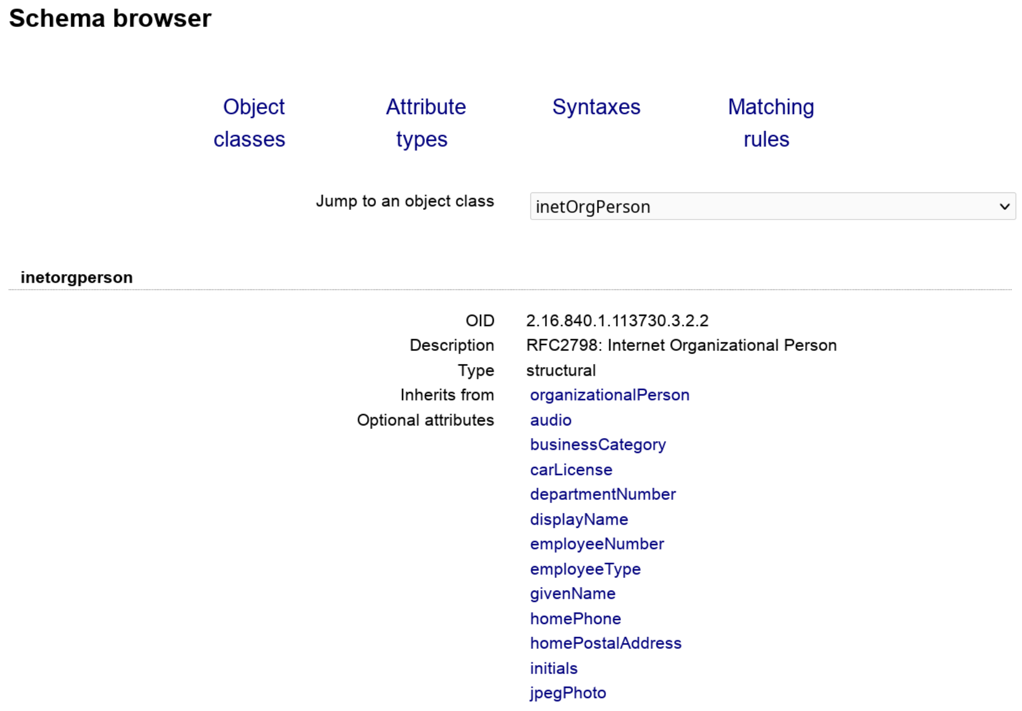
objectClass * organizationalUnit

ou * demo

Attribute

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.



Jump to an object class: inetOrgPerson

inetorgperson

OID: 2.16.840.1.113730.3.2.2
Description: RFC2798: Internet Organizational Person
Type: structural
Inherits from: organizationalPerson
Optional attributes: audio
businessCategory
carLicense
departmentNumber
displayName
employeeNumber
employeeType
givenName
homePhone
homePostalAddress
initials
jpegPhoto

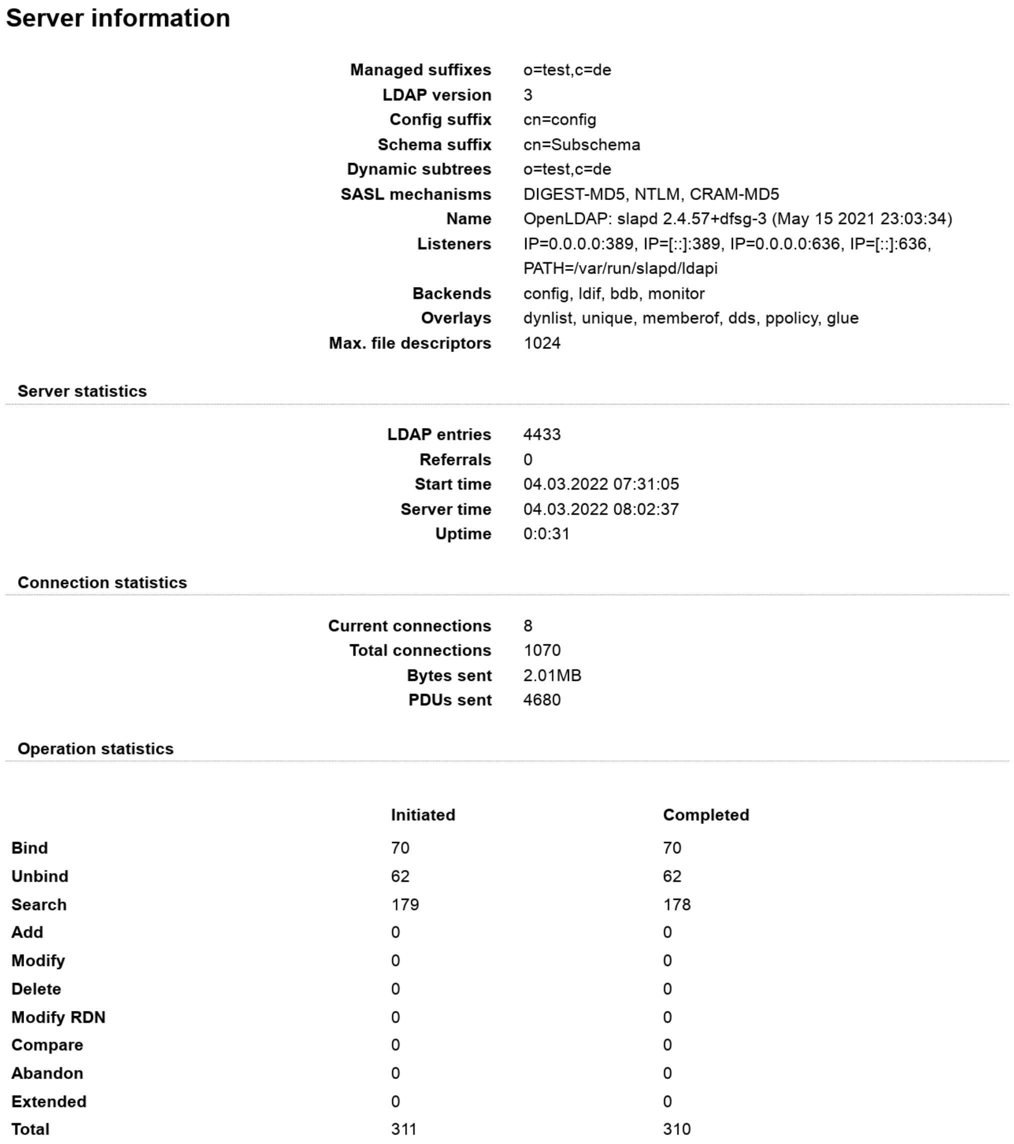
Server information

This shows information and statistics about your LDAP server. This includes the suffixes, used overlays, connection data and operation statistics. You will need "cn=monitor" setup to see all details. Some data may not be available depending on your LDAP server software.

Please see the following links how to setup "cn=monitor":

- OpenLDAP [http://www.openldap.org/doc/admin24/monitoringslapd.html]

- 389 server [http://directory.fedoraproject.org/wiki/Howto:CN%3DMonitor_LDAP_Monitoring]



Server information

Managed suffixes	o=test,c=de
LDAP version	3
Config suffix	cn=config
Schema suffix	cn=Subschema
Dynamic subtrees	o=test,c=de
SASL mechanisms	DIGEST-MD5, NTLM, CRAM-MD5
Name	OpenLDAP: slapd 2.4.57+dfsg-3 (May 15 2021 23:03:34)
Listeners	IP=0.0.0.0:389, IP=[::]:389, IP=0.0.0.0:636, IP=[::]:636, PATH=/var/run/slapd/ldapi
Backends	config, ldif, bdb, monitor
Overlays	dynlist, unique, memberof, dds, ppolicy, glue
Max. file descriptors	1024

Server statistics

LDAP entries	4433
Referrals	0
Start time	04.03.2022 07:31:05
Server time	04.03.2022 08:02:37
Uptime	0:0:31

Connection statistics

Current connections	8
Total connections	1070
Bytes sent	2.01MB
PDUs sent	4680

Operation statistics

	Initiated	**Completed**
Bind	70	70
Unbind	62	62
Search	179	178
Add	0	0
Modify	0	0
Delete	0	0
Modify RDN	0	0
Compare	0	0
Abandon	0	0
Extended	0	0
Total	311	310

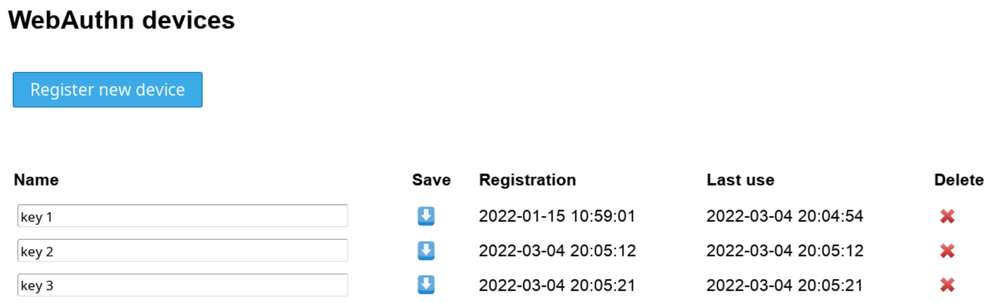
WebAuthn devices

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

Here you can manage your webauthn/FIDO2 devices.

You can register additional security devices and remove old ones. In addition, you can set a name for your devices. This helps if you need to remove a device at a later point.

If no more device is registered then LAM will ask you for registration on next login.



WebAuthn devices

Name	Save	Registration	Last use	Delete
key 1	⬇	2022-01-15 10:59:01	2022-03-04 20:04:54	✖
key 2	⬇	2022-03-04 20:05:12	2022-03-04 20:05:12	✖
key 3	⬇	2022-03-04 20:05:21	2022-03-04 20:05:21	✖

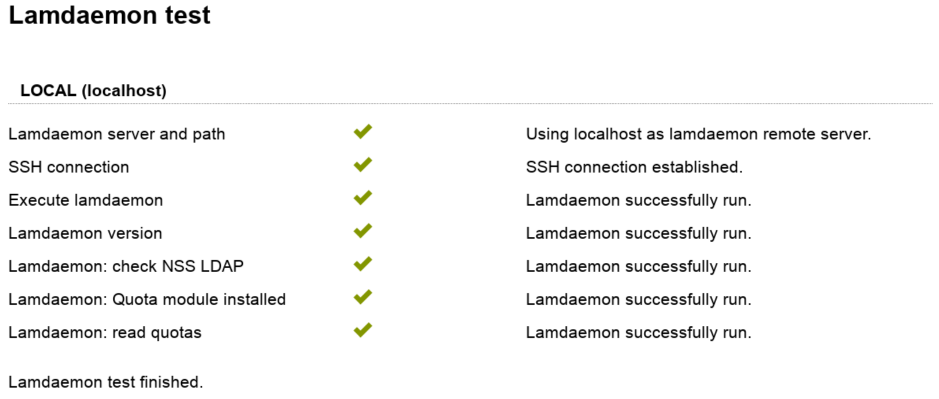
Tests

This allows you to check if your LDAP schema is compatible with LAM and to find possible problems.

Lamdaemon test

LAM provides an external script to manage home directories and quotas. You can test here if everything is setup correctly.

If you get an error like "no tty present and no askpass program specified" then the path to the lamdaemon.pl may be wrong. Please see the lamdaemon installation instructions for setup details.



Lamdaemon test

LOCAL (localhost)

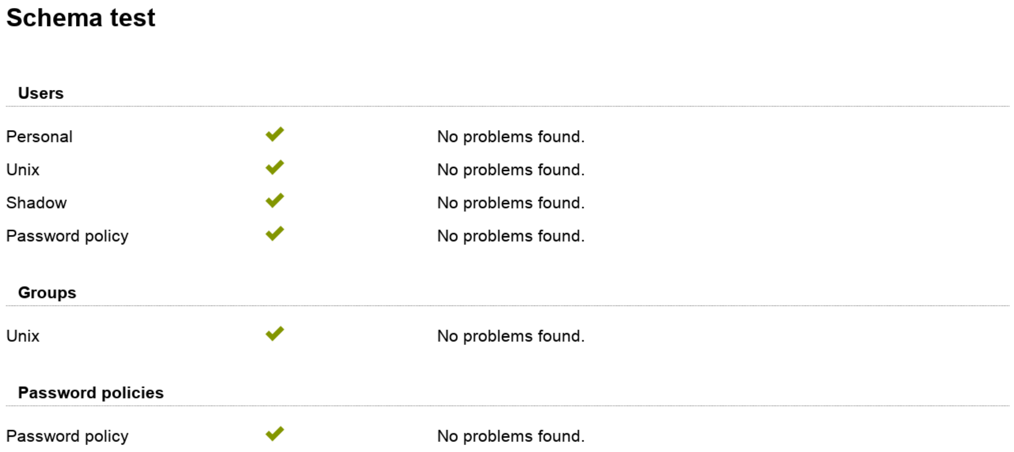
Lamdaemon server and path	✓	Using localhost as lamdaemon remote server.
SSH connection	✓	SSH connection established.
Execute lamdaemon	✓	Lamdaemon successfully run.
Lamdaemon version	✓	Lamdaemon successfully run.
Lamdaemon: check NSS LDAP	✓	Lamdaemon successfully run.
Lamdaemon: Quota module installed	✓	Lamdaemon successfully run.
Lamdaemon: read quotas	✓	Lamdaemon successfully run.

Lamdaemon test finished.

Schema test

This will test if your LDAP schema supports all object classes and attributes of the active LAM modules. If you get a message that something is missing please check that you installed all required schemas.

If you get error messages about object class violations then this test can tell you what is missing.



Schema test

Users

Personal	✓	No problems found.
Unix	✓	No problems found.
Shadow	✓	No problems found.
Password policy	✓	No problems found.

Groups

Unix	✓	No problems found.

Password policies

Password policy	✓	No problems found.

Chapter 6. Access levels and password reset page (LAM Pro)

You can define different access levels for each profile to allow or disallow write access. The password reset page helps your deskside 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**

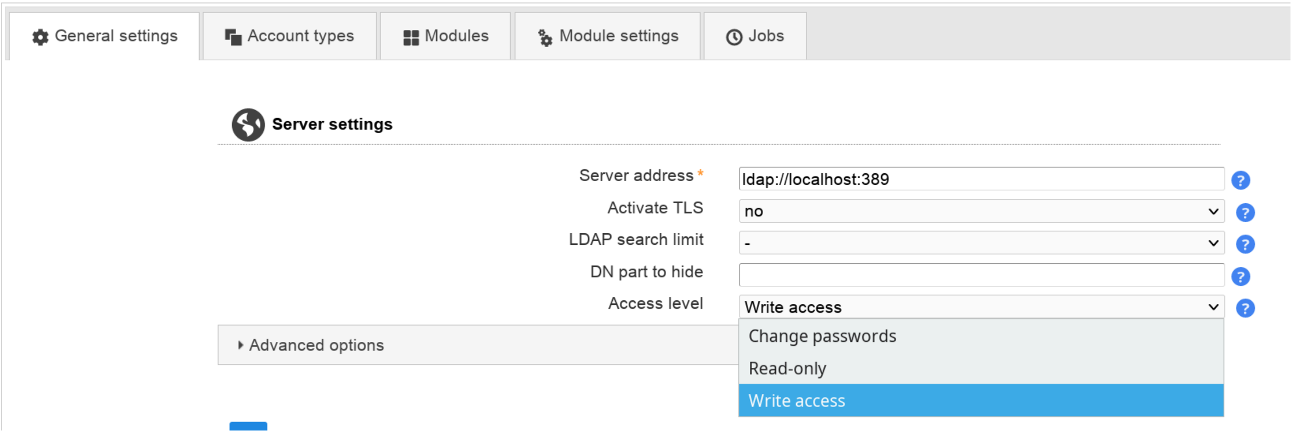
  Similar to "Read only" except that the password reset page is available.

- **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:



Server settings

Server address * ldap://localhost:389

Activate TLS no

LDAP search limit -

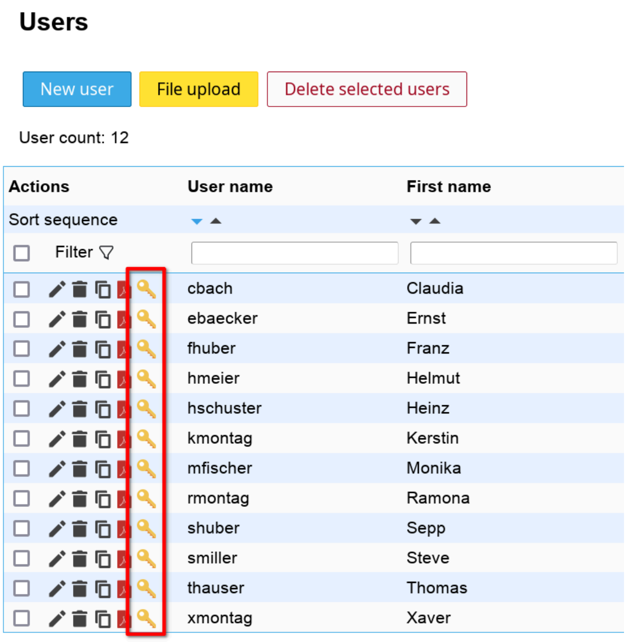
DN part to hide

Access level Write access

Password reset page

This special page allows your deskside support staff to reset the Unix and Samba passwords of your users. Account may also be (un)locked If you set the access level to "Change passwords" then LAM will not allow any changes to the LDAP database except password changes via this page. The account pages will be still available in read-only mode.

You can open the password reset page by clicking on the key symbol on each user account:



Users

User count: 12

Actions	User name	First name
Sort sequence	▼ ▲	▼ ▲
□ Filter ▽		
□	cbach	Claudia
□	ebaecker	Ernst
□	fhuber	Franz
□	hmeier	Helmut
□	hschuster	Heinz
□	kmontag	Kerstin
□	mfischer	Monika
□	rmontag	Ramona
□	shuber	Sepp
□	smiller	Steve
□	thauser	Thomas
□	xmontag	Xaver

There are three different options to set a new password. You can further restrict these options in server profile settings.

- **set random password and display it on screen**

  This will set the user's password to a random value. The password will be 11 characters long with a random combination of letters, digits and ".-_".

  You may want to use this method to tell users their new passwords via phone.

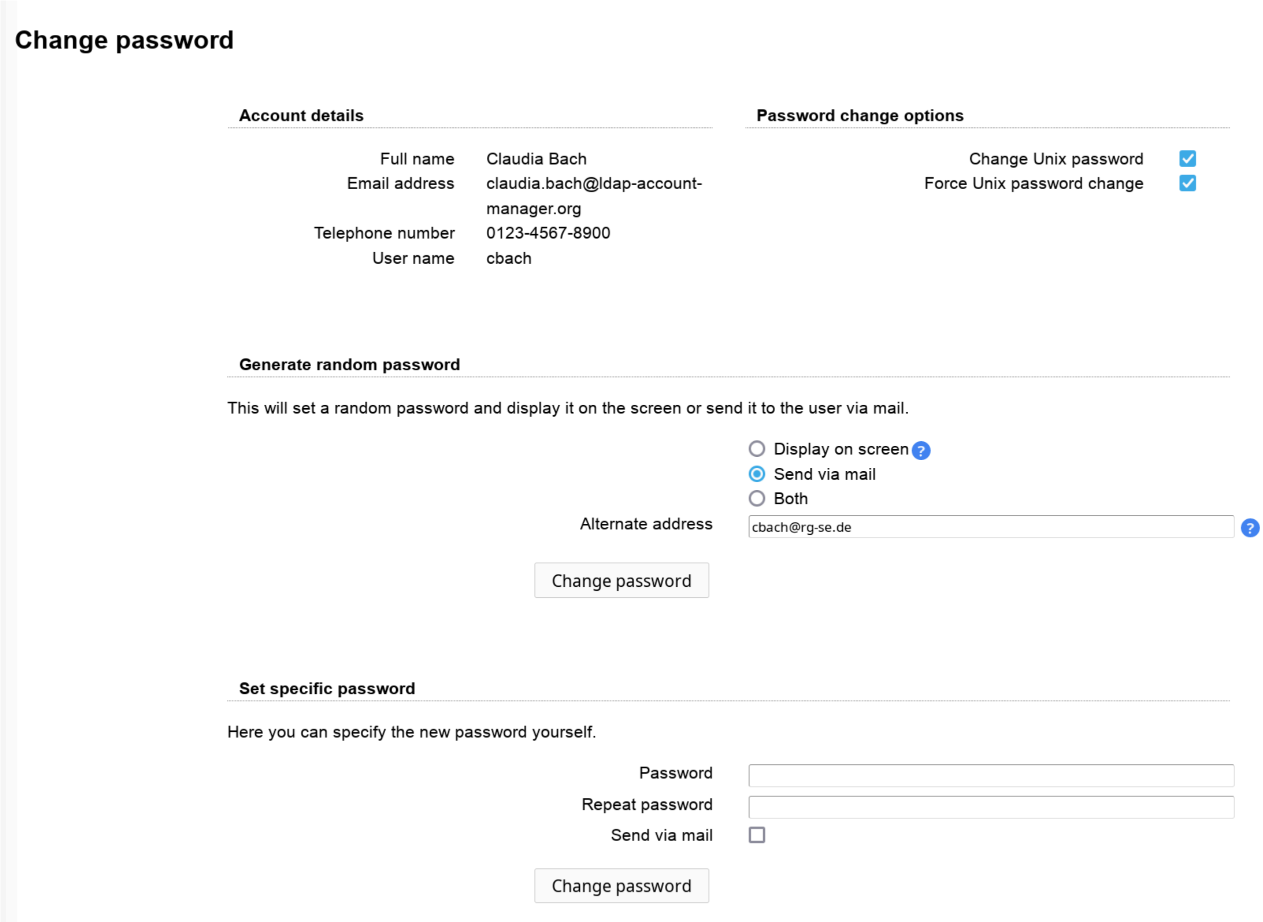
- **set random password and mail it to user**

  If the user account has set the mail attribute then LAM can send your user a mail with the new password. You can change the mail template to fit your needs. Please configure your LAM server profile to setup the sender address, subject and mail body. See here for setting up your SMTP server.

  Using this method will prevent that your support staff knows the new password.

- **set specific password**

  Here you can specify your own password.



Change password

Account details

Full name	Claudia Bach
Email address	claudia.bach@ldap-account-manager.org
Telephone number	0123-4567-8900
User name	cbach

Password change options

Change Unix password ☑
Force Unix password change ☑

Generate random password

This will set a random password and display it on the screen or send it to the user via mail.

○ Display on screen
● Send via mail
○ Both

Alternate address: cbach@rg-se.de

Change password

Set specific password

Here you can specify the new password yourself.

Password:
Repeat password:
Send via mail □

Change password

LAM will display contact information about the user like the user's name, email address and telephone number. This will help your deskside support to easily contact your users.

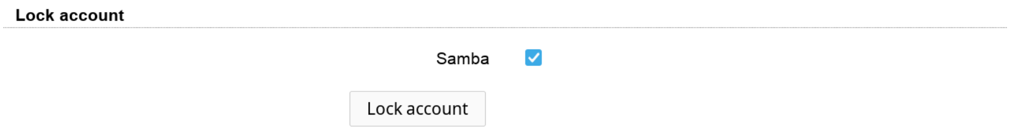
Options:

Depending on the account there may be additional options available.

- **Sync Samba NT/LM password with Unix password:** If a user account has Samba passwords set then LAM will offer to synchronize the passwords.
- **Unlock Samba account:** Locked Samba accounts can be unlocked with the password change.
- **Update Samba password timestamps:** This will set the timestamps when the password was changed (sambaPwdLastSet). Only existing attributes are updated. No new attributes are added.
- **Sync Kerberos password with Unix password:** This will also update the Heimdal Kerberos password.
- **Sync Asterisk (voicemail) password with Unix password:** Changes also the Asterisk passwords.
- **Force password change:** This will force the user to change his password at next login. This option supports Shadow, Samba 3 and PPolicy (automatically detected).

Account (un)locking:

Depending if the account includes a Unix/Samba extension and PPolicy is activated the page will show options to (un)lock the account. E.g. if the account is fully unlocked then there will be no unlocking options printed.



Lock account

Samba ☑

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.

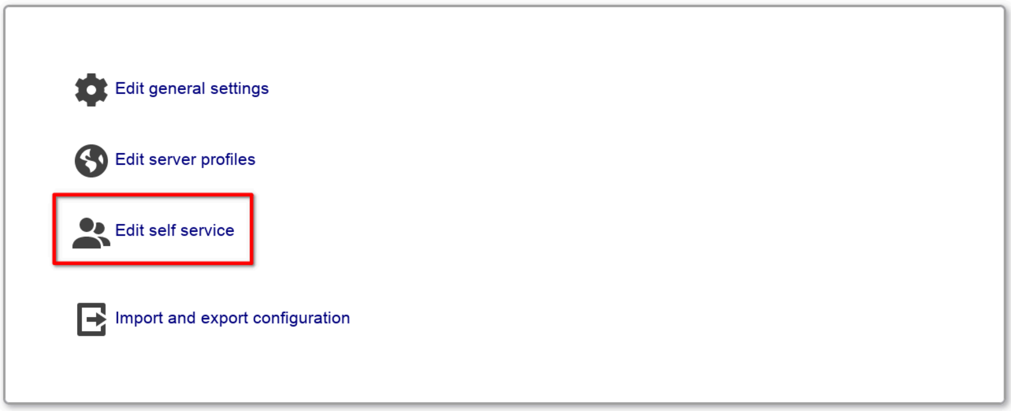
Other LDAP servers

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.

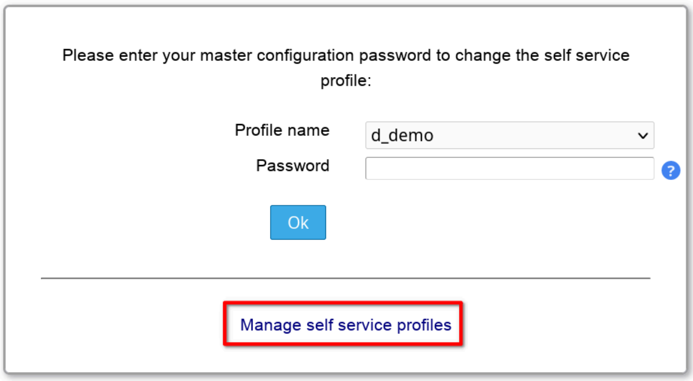
Creating a self service profile

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



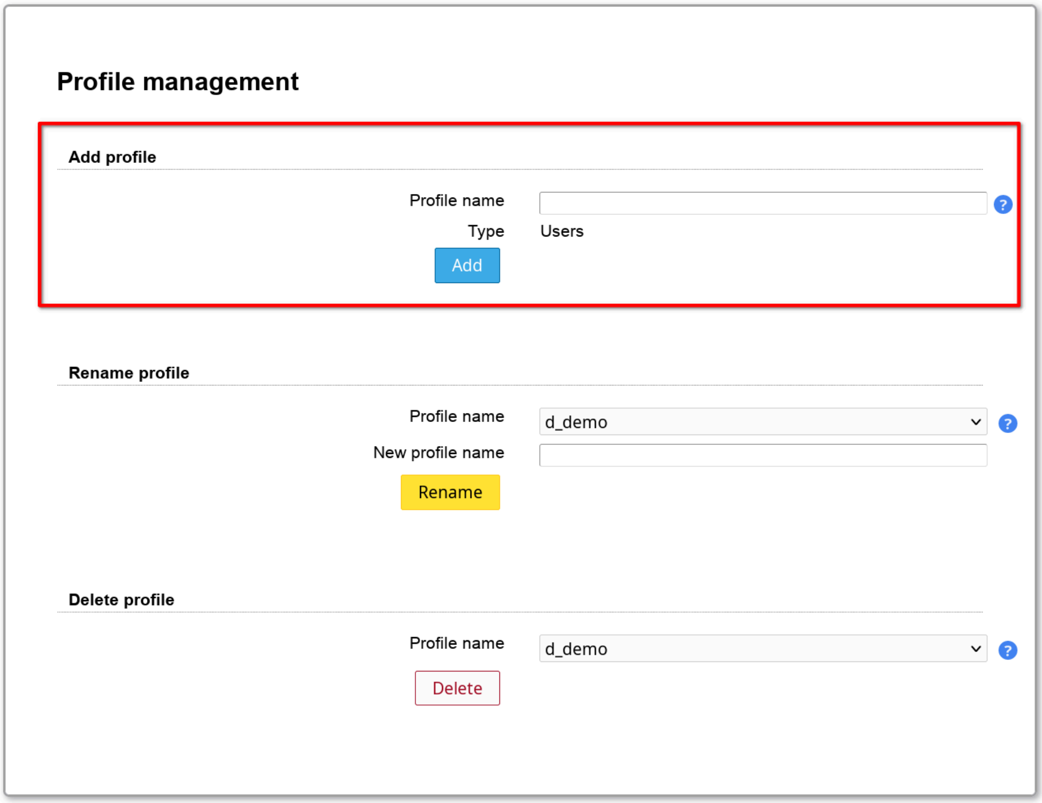
Now we need to create a new self service profile. Click on the link to manage the self service profiles.


Please enter your master configuration password to change the self service profile:

Profile name d_demo

Password

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



Profile management

Add profile

Profile name

Type Users

Rename profile

Profile name d_demo

New profile name

Delete profile

Profile name d_demo

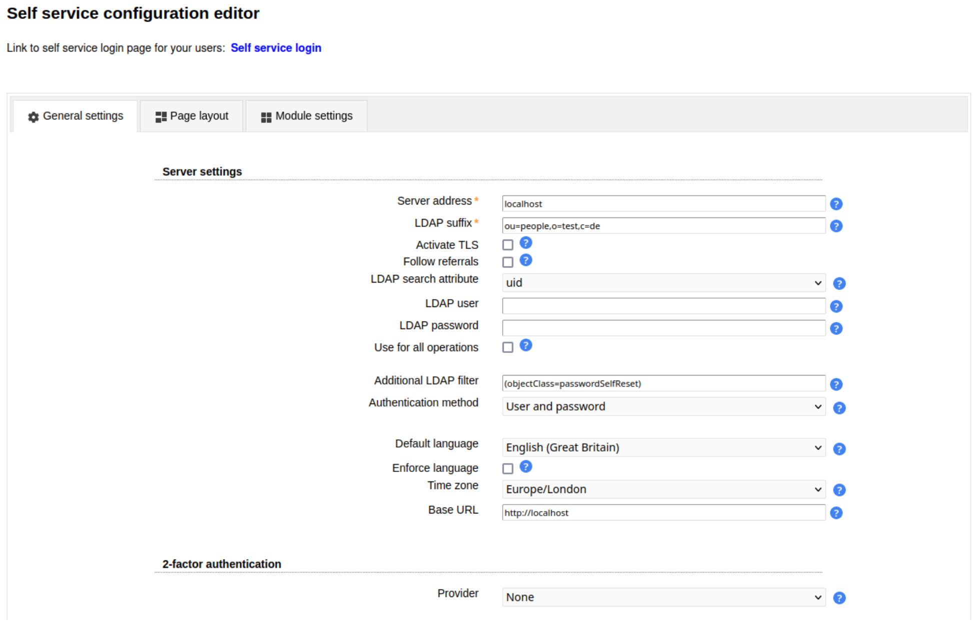
Now go back to the profile login and enter your master configuration password to edit your new profile.

Edit your new profile

General settings

On top of the page you see the link to the user login page. Copy this link address and give it to your users.

Below the link you can specify several options.



Self service configuration editor

Link to self service login page for your users: Self service login

Server settings

Server address * localhost

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

Activate TLS □

Follow referrals □

LDAP search attribute uid

LDAP user

LDAP password

Use for all operations □

Additional LDAP filter (objectClass=passwordSelfReset)

Authentication method User and password

Default language English (Great Britain)

Enforce language □

Time zone Europe/London

Base URL http://localhost

2-factor authentication

Provider None

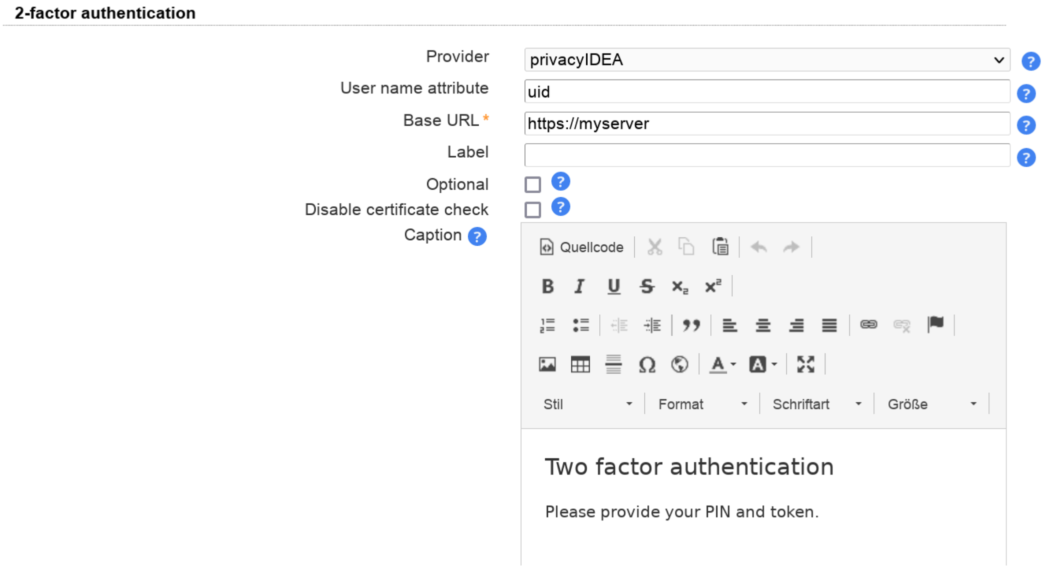
Table 7.1. General options

Server address	The address of your LDAP server. For LDAP+SSL use "ldaps://myserver"
Activate TLS	Activates TLS encryption. Please note that this cannot be combined with LDAP+SSL ("ldaps://").
LDAP suffix	The part of the LDAP tree where LAM should search for users
LDAP search attribute	Here you can specify if your users can login with user name + password, email + password or other attributes.
Follow referrals	By default LAM will not follow LDAP referrals. This is ok for most installations. If you use LDAP referrals please activate the referral option in advanced settings.
LDAP user + password	The DN and password which is used to search for users in the LDAP database. It is sufficient if this DN has only read rights. If you leave these fields empty LAM will try to connect anonymously.
Use for all operations	By default LAM will use the credentials of the user that logged in to self service for read/modify operations. If you select this box then the connection user specified before will be used instead. Please note that this can be a security risk because the user requires write access to all users. You need to make sure that your LAM server is well protected.
Additional LDAP filter	Use this to enter an additional LDAP filter (e.g. "(objectClass=passwordSelfReset)") to reduce the number of accounts who may use self service.
Authentication method	The default method is user and password login. You can also enable HTTP authentication for your users. This way the web server is responsible to authenticate your users. LAM will use the given user name + password for the LDAP login. To setup HTTP authentication in Apache please see this link [http://httpd.apache.org/docs/2.2/howto/auth.html]. If you use Okta or OpenID for 2FA then you can also select to trust the 2FA provider. In this case the user does not need to enter any password in LAM itself (SSO).
Default language	This language is preselected on login.
Enforce language	Disables language selection and uses default language.
Time zone	Please provide your time zone.
Base URL	Please enter the base URL of your webserver (e.g. https://www.example.com). This is used to generate links in emails for password self reset and user self registration.
Login attribute label	This is the description for the LDAP search attribute. Set it to something which your users are familiar with.
Password field label	This text is placed as label for the password field on the login page. LAM will use "Password" if you do not enter any text.
Login caption	This text is displayed on the login page inside the login mask.

Login footer	This text is displayed on the login page below the login mask.
Main page caption	This text is displayed on the self service main page where your users change their data.
Main page footer	This text is displayed as footer on the self service main page where your users change their data.
Page header	This HTML code will be placed on top of all self service pages. E.g. you can use this to place your custom logo. Any HTML code is permitted.
Base color	Here you can change the background color for the user pages.
Additional CSS links	Here you can specify additional CSS links to change the layout of the self service pages. This is useful to adapt them to your corporate design. Please enter one link per line.

2-factor authentication

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



2-factor authentication

Provider: privacyIDEA

User name attribute: uid

Base URL *: https://myserver

Label:

Optional: □

Disable certificate check: □

Caption:

Two factor authentication

Please provide your PIN and token.

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

- privacyIdea [https://www.privacyidea.org/]
- YubiKey [https://www.yubico.com/]
- Duo [https://duo.com/]
- WebAuthn/FIDO2 [https://en.wikipedia.org/wiki/WebAuthn]
- Okta [https://www.okta.com/]
- OpenID [https://openid.net/]

privacyIDEA

- Base URL: please enter the URL of your privacyIDEA instance
- User name attribute: please enter the LDAP attribute name that contains the user ID (e.g. "uid")
- Optional: By default LAM will enforce to use a token and reject users that did not setup one. You can set this check to optional. But if a user has setup a token then this will always be required.
- Disable certificate check: This should be used on development instances only. It skips the certificate check when connecting to verification server.

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

YubiKey

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

Duo

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

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

WebAuthn/FIDO2

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

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

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

Okta

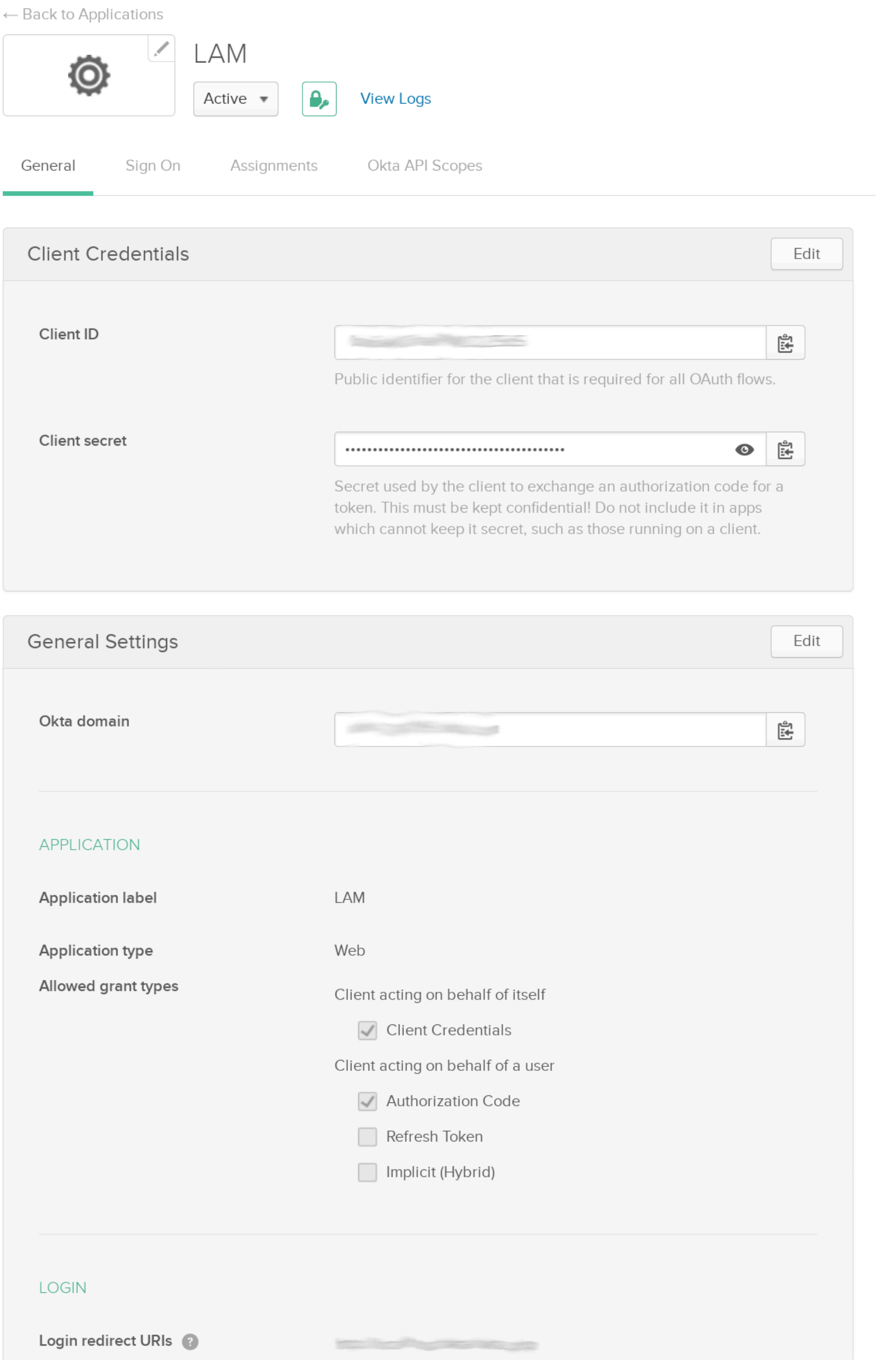
This requires to register a new application of type "Web".

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

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

LAM options:

- User name attribute: please enter the LDAP attribute name that contains the user ID (e.g. "mail").
- Base URL: please enter the URL of your Okta domain (e.g. https://mydomain.okta.com)
- Client id: please enter your application client id.
- Secret key: please enter your application secret key.



Client Credentials

Client ID: [redacted]

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

Client secret: ••

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

General Settings

Okta domain: [redacted]

APPLICATION

Application label: LAM

Application type: Web

Allowed grant types:

Client acting on behalf of itself

☑ Client Credentials

Client acting on behalf of a user

☑ Authorization Code

□ Refresh Token

□ Implicit (Hybrid)

LOGIN

Login redirect URIs: [redacted]

OpenID

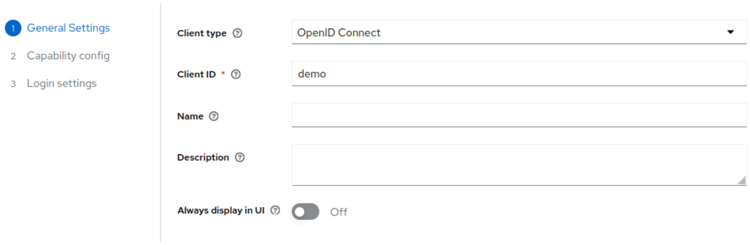
This will use an OpenID server as 2nd factor for authentication.

LAM options:

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

KeyCloack example configuration:

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



Client type: OpenID Connect

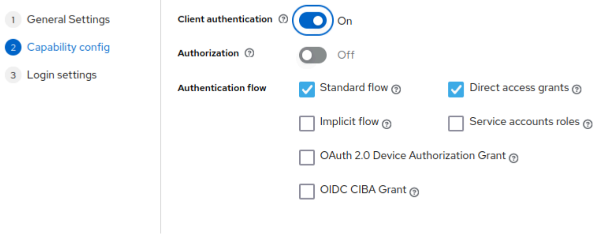
Client ID *: demo

Name:

Description:

Always display in UI: Off

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

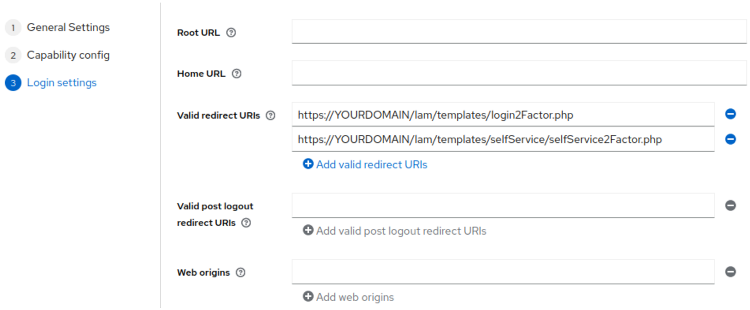


Client authentication: On

Authorization: Off

Authentication flow: ☑ Standard flow ☑ Direct access grants ☐ Implicit flow ☐ Service accounts roles ☐ OAuth 2.0 Device Authorization Grant ☐ OIDC CIBA Grant

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



Root URL:

Home URL:

Valid redirect URIs: https://YOURDOMAIN/lam/templates/login2Factor.php
https://YOURDOMAIN/lam/templates/selfService/selfService2Factor.php

Valid post logout redirect URIs:

Web origins:

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

Example configuration values:

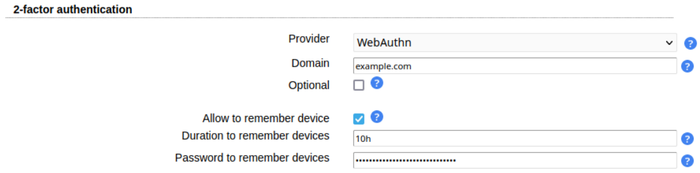
- User name: uid
- Base URL: http://openidserver/auth/realms/master

- Client id: demo
- Secret key: 59bdf504-b76e-4138-8421-ef662b2c6c83

Remember device

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

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



2-factor authentication

Provider: WebAuthn

Domain: example.com

Optional: ☐

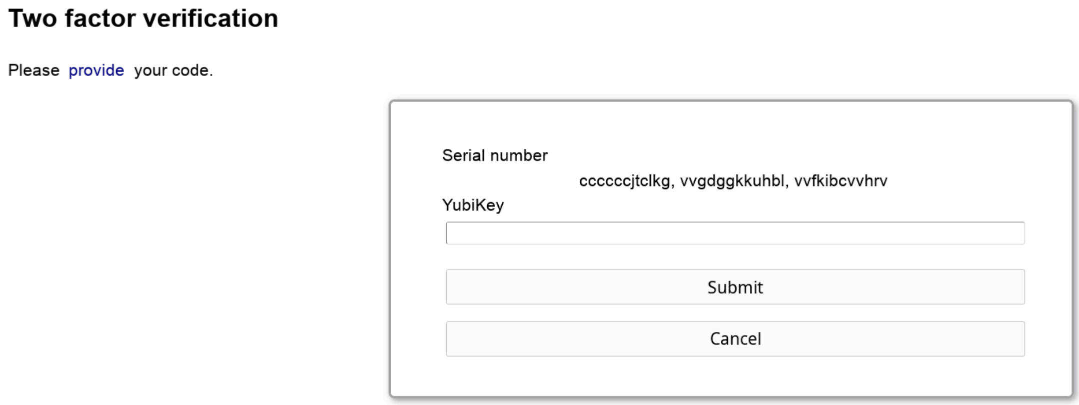
Allow to remember device: ☑

Duration to remember devices: 10h

Password to remember devices: ••••••••••••••••••••••••••••••

Login

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



Two factor verification

Please provide your code.

Serial number

cccccjtclkg, vvgdggkkuhbl, vvfkibcvvhrv

YubiKey

Captcha

LAM Pro can optionally display a captcha to verify that logins are not from robots. Captchas will be displayed when you tick the checkbox to secure login with a captcha. The supported captcha providers are:

Google reCAPTCHA

You will need the site and secret key for your domain. They can be retrieved from here: https://www.google.com/recaptcha

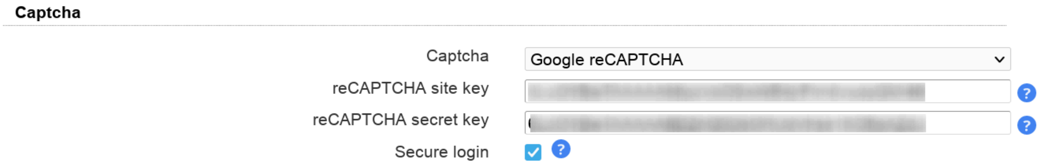
Please note that your web server must be able to access "https://www.google.com/recaptcha/api/siteverify" to verify the captchas.

Friendly Captcha

Please enter your site (see applications) and API key. The web server must be able to contact "https://api.friendlycaptcha.com" for verification.

hCaptcha

Please enter your site and secret key (not API key). The web server must be able to contact "https://hcaptcha.com" for verification.



Captcha

Captcha	Google reCAPTCHA
reCAPTCHA site key	[redacted]
reCAPTCHA secret key	[redacted]
Secure login	☑

Lamdaemon

This section is only required if you want to display file system quotas or create home directories via lamdaemon.

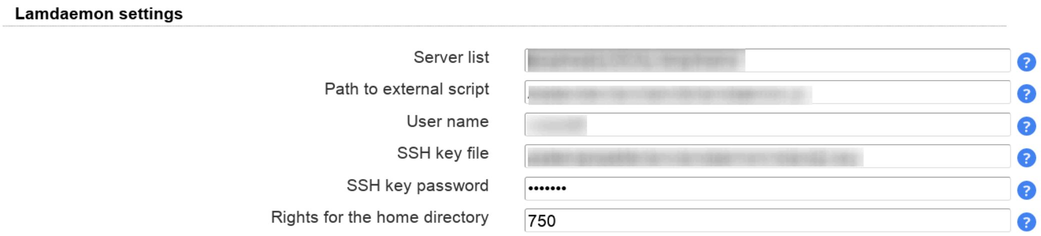
Server list format options:

- "server": "server" is the DNS name of your script server
- "server:NAME": NAME is the display name of this server
- "server:NAME:/prefix": /prefix is the directory prefix for all operations. E.g. creating a home directory "/home/user" would create "/prefix/home/user" then.

You need to provide a fixed user name.

Self service requires a SSH connection with SSH key. Please generate a SSH key pair and provide the location to the **private** key file. If the key is protected by a password you can also specify it here.

In case you want to create home directories during user self registration please provide the rights for it (e.g. 750).



Lamdaemon settings

Server list	[redacted]
Path to external script	[redacted]
User name	[redacted]
SSH key file	[redacted]
SSH key password	•••••••
Rights for the home directory	750

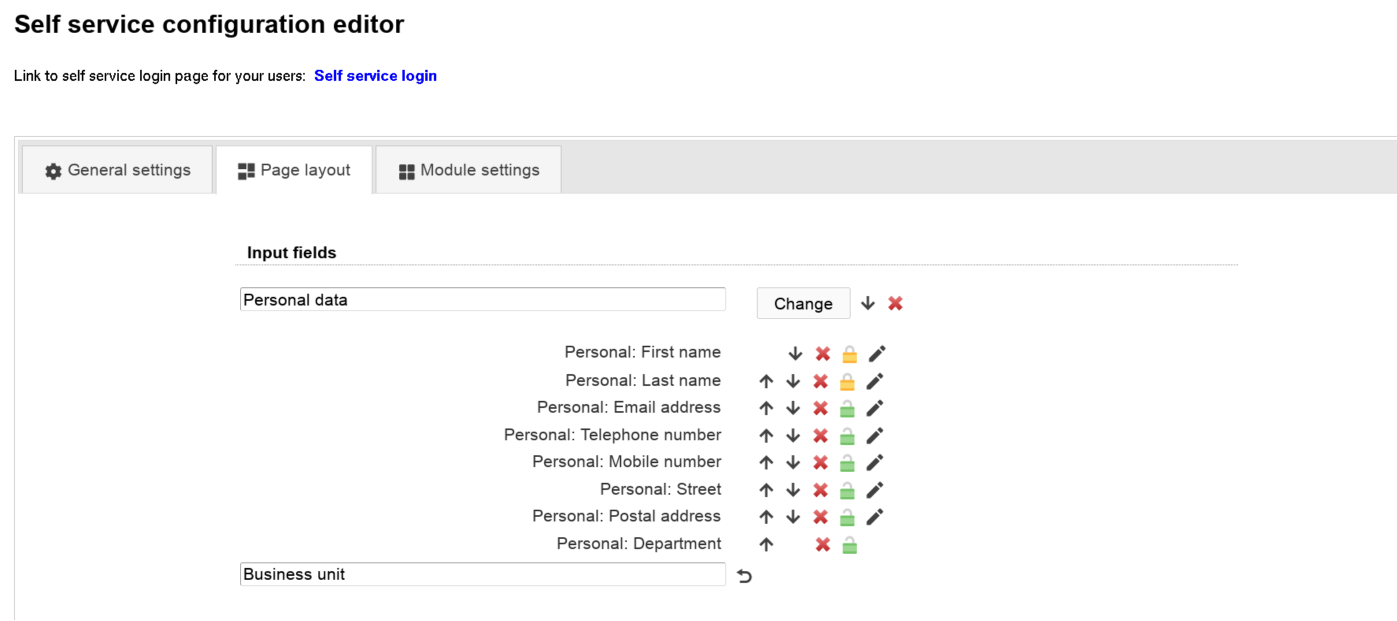
Page layout

Here you can specify what input fields your users can see. It is also possible to group several input fields.

Please use the arrow signs to change the order of the fields/groups.

You may also set some fields as read-only for your users. This can be done by clicking on the lock symbol. Read-only fields can be used to show your users additional data on the self service page that must not be changed by themselves (e.g. first/last name).

Sometimes, you may want to set a custom label for an input field. Click on the edit icon to set your own label text (Personal: Department is relabeled as "Business unit" here).



Self service configuration editor

Link to self service login page for your users: Self service login

Input fields

Personal data

Personal: First name
Personal: Last name
Personal: Email address
Personal: Telephone number
Personal: Mobile number
Personal: Street
Personal: Postal address
Personal: Department

Business unit

Possible input fields

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

Table 7.2. Self service fields

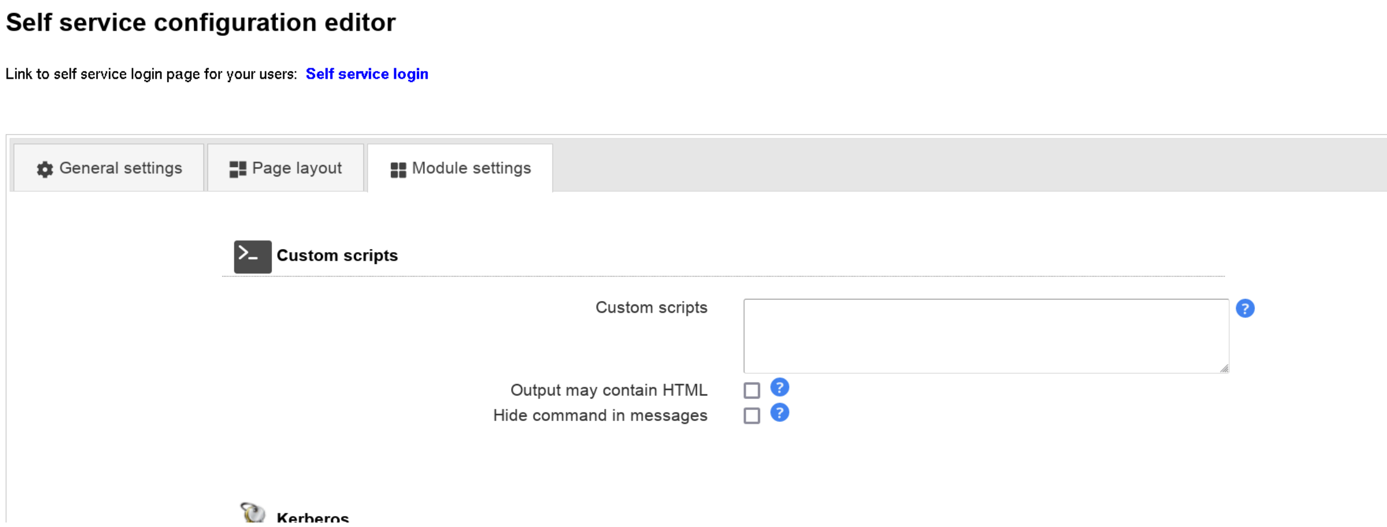
Account type	Option	Description
Account locking	Password expiration	Read only value of password expiration date
Asterisk (voicemail)	Sync Asterisk password with Unix password	This is a hidden field. It will update the Asterisk password each time the Unix password is changed.
Group of names	Group memberships (read-only)	
Kerberos	Sync Kerberos password with Unix password	This is a hidden field. It will update the Kerberos password each time the Unix password is changed.
Kolab	Delegates	Allows to manage delegate permissions
	Invitation policy	Invitation policy management
Password policy	Last password change	read-only
Password self reset	Question	Security question selection
	Answer	Security answer
	Backup email	(External) backup email address that has no relation to user password.
Personal	Business category	
	Car license	
	Department	
	Description	
	Email address	
	Fax number	

	First name	
	Home telephone number	
	Initials	
	Job title	
	Last name	
	Location	
	Mobile number	
	Office name	
	Organisation	
	Organisational unit	
	Photo	Shows the user photo if set. The user may also remove the photo or upload a new one.
	Postal address	
	Postal code	
	Post office box	
	Registered address	
	Room number	
	State	
	Street	
	Telephone number	
	User certificates	Upload of user certificates in PEM or DER format
	User name	
	Web site	
Mail routing	Local address (read-only)	
	Mail routing address (read-only)	
OpenLDAP TOTP	OpenLDAP TOTP token + serial number	See OpenLDAP TOTP
Quota	Quota (read-only)	Displays the user's system quote. Requires lamdaemon configuration.
Samba 3	Password	Input field to set a new NT/LM password. The attribute "sambaPwdLastSet" 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 "sambaPwdLastSet" on password change	Updates the password timestamp when password is synchronized with Unix.
	Last password change (read-only)	Displays the date and time of the user's last password change.

Shadow	Account expiration date (read-only)	
	Last password change (read-only)	Displays the date and time of the user's last password change (Unix).
Windows (AD, AD LDS, Samba 4)	Password	Change the user's password
	Location	
	Mail alias (read-only)	
	Office name	
	Postal code	
	Post office box	
	Proxy-Addresses (read-only)	
	State	
	Street	
	Telephone number	
	Web site	
Unix	Common name	
	Group memberships (read-only)	
	Login shell	
	Password	This is also the source for several password synchronization options.
	Sync Unix password with Windows password	This is a hidden field. It will update the Unix password each time the Windows password is changed.
WebAuthn	WebAuthn devices	Allows the user to manage his webauthn/FIDO2 security keys.
Kopano	"Send as" privileges	Define user who may send mails as this user
	Email aliases	Email aliases
PyKota	Balance (read-only)	Current balance for printing
	Total paid (read-only)	Total money paid
	Payment history	History of user payments
	Job history	History of printed jobs

Module settings

This allows to configure some module specific options (e.g. custom scripts or password hash type).



Self service configuration editor

Link to self service login page for your users: Self service login

Custom scripts

Custom scripts

Output may contain HTML □

Hide command in messages □

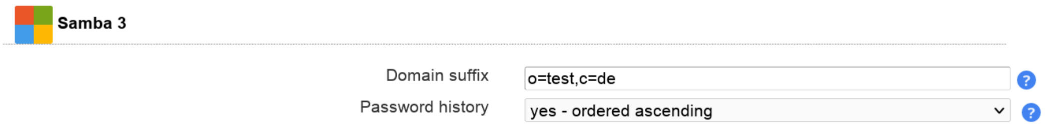
Kerberos

Samba 3

LAM Pro can check the password history and minimum age for Samba 3 password changes. In this case please provide the LDAP suffix where your Samba 3 domain(s) are stored.

If you leave the field empty then no history and age checks will be done.

Password history: depending on your LDAP server you might need ascending or descending order. Just switch the setting if the password history is not correctly updated.



Samba 3

Domain suffix: o=test,c=de

Password history: yes - ordered ascending

Password self reset

Schema installation

Please install the LDAP schema as described here.

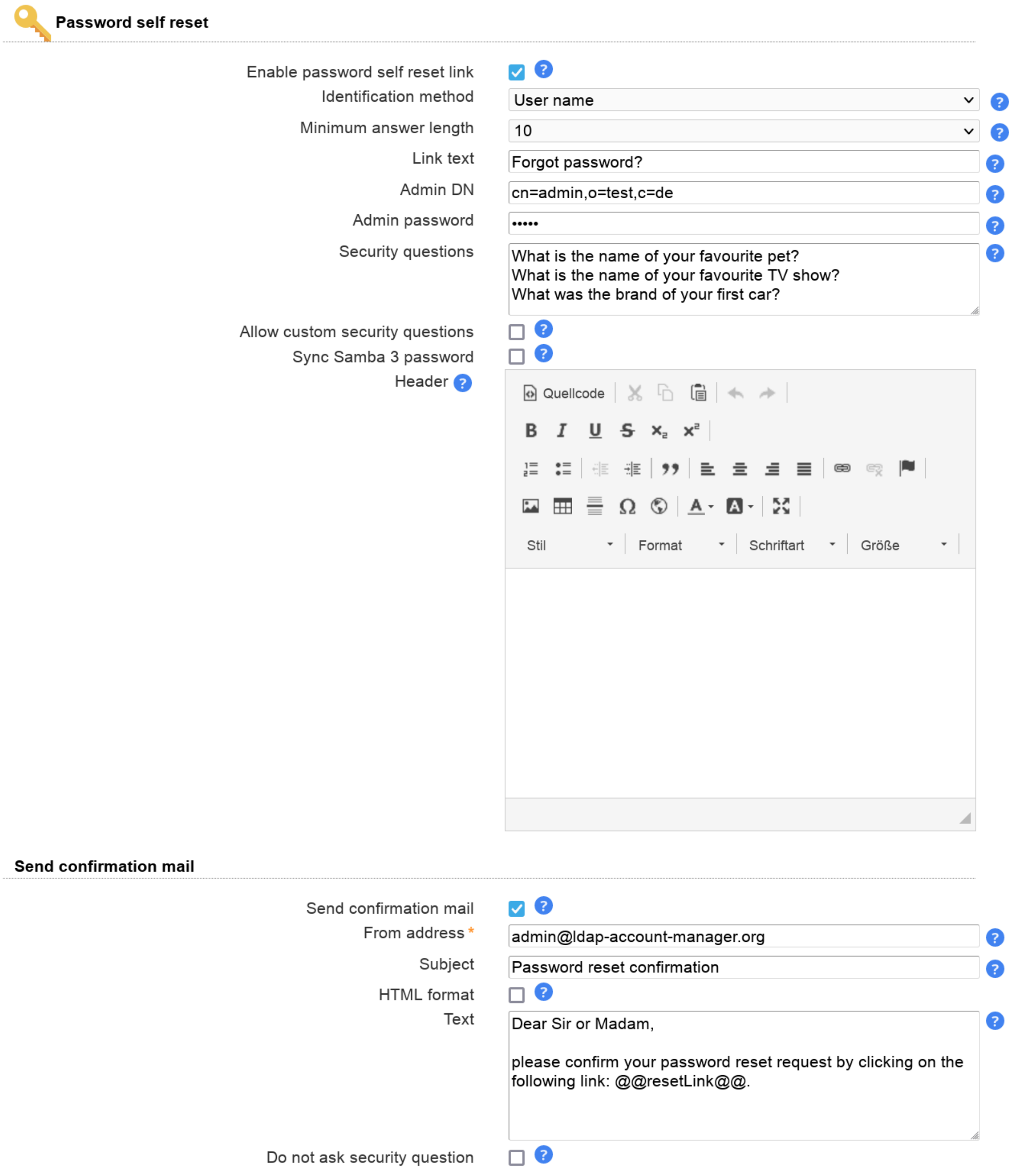
Settings

You can allow your users to reset their passwords themselves. This will reduce your administrative costs for cases where users forget their passwords.

To enable this feature please activate the checkbox "Enable password self reset link".

Hint: Please note that LAM Pro uses security questions by default. Activate confirmation mails and then deactivate security questions if you want to use only email validation.

The password reset must be finished by the user within 24h or the process must be restarted.



Password self reset

Enable password self reset link	☑
Identification method	User name
Minimum answer length	10
Link text	Forgot password?
Admin DN	cn=admin,o=test,c=de
Admin password	•••••
Security questions	What is the name of your favourite pet? What is the name of your favourite TV show? What was the brand of your first car?
Allow custom security questions	□
Sync Samba 3 password	□
Header	

Send confirmation mail

Send confirmation mail	☑
From address *	admin@ldap-account-manager.org
Subject	Password reset confirmation
HTML format	□
Text	Dear Sir or Madam, please confirm your password reset request by clicking on the following link: @@resetLink@@.
Do not ask security question	□

Identification method, used LDAP attributes:

- Email: mail
- Employee number: employeeNumber
- Self service login attribute: same as configured on first tab of self service profile
- User name: uid
- User name and email address: uid and mail
- User name or email address: uid and mail

You can now configure the minimum answer length for password reset answers. This is checked when you allow you users to specify their answers via the self service. Additionally, you can specify the text of the password reset link (default: "Forgot password?"). The link is displayed below the password field on the self service login page.

Next, please enter the DN and password of an LDAP entry that is allowed to reset the passwords. This entry needs write access to the attributes shadowLastChange, pwdAccountLockedTime and userPassword. It also needs read access to uid, mail, passwordSelfResetQuestion and passwordSelfResetAnswer. Please note that LAM Pro saves the password on your server file system. Therefore, it is required to protect your server against unauthorised access.

Please also specify the list of password reset questions that the user can choose.

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

You can inform your users via mail about their password change. The mail can include the new password by using the special wildcard "@@newPassword@@". Additionally, you may want to insert other wildcards that are replaced by the corresponding LDAP attributes. E.g. "@@uid@@" will be replaced by the user name. See here for setting up your SMTP server.

LAM Pro can send your users an email with a confirmation link to validate their email address. Of course, this should only be used if the email account is independent from the user password (e.g. at external provider) or you use the backup email address feature. The mail body must include the confirmation link by using the special wildcard "@@resetLink@@". Additionally, you may want to insert other wildcards that are replaced by the corresponding LDAP attributes. E.g. "@@uid@@" will be replaced by the user name.

There is also an option to skip the security question at all if email verification is enabled. In this case the password can be reset directly after clicking on the confirmation link. Please handle with care since anybody with access to the user's mail account can reset the password.

Captcha support

LAM Pro can optionally display a captcha to verify that password resets are not from robots. The captcha provider is configured on "General settings" tab.

Captchas will be displayed when you tick the checkbox to use a captcha.

Captcha

Use captcha ☑ ?

Troubleshooting:

1. You get messages like "Unable to find user account."

This can have multiple reasons:

- security questions enabled but no security question and/or answer set for this user
- user name + email combination does not exist
- no connection to LDAP server

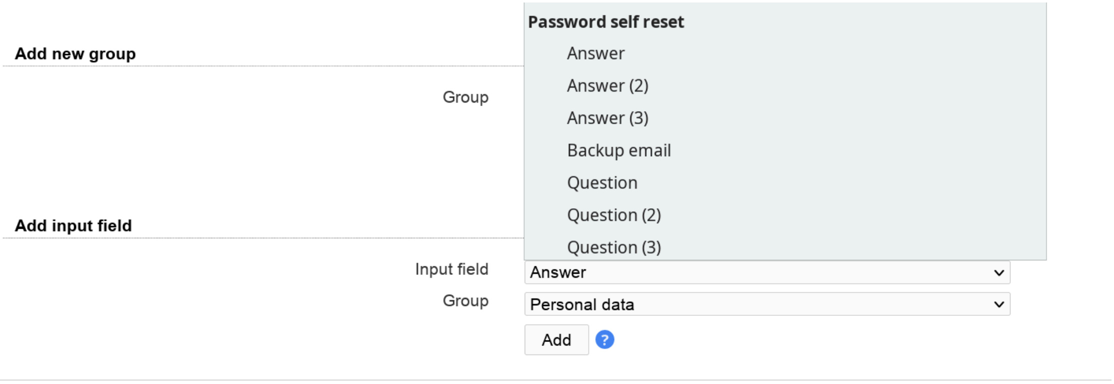
Turn on logging in LAM's main configuration settings. The exact reason is logged on notice level.

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

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

New fields for self service page

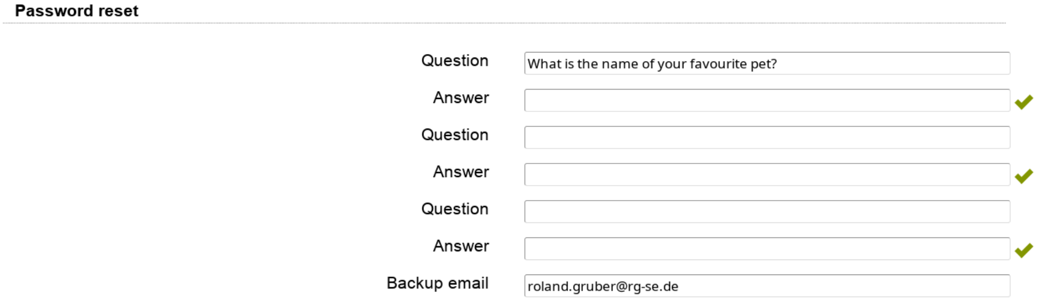
There are special fields that you may put on the self service page for your users. These fields allow them to change the reset questions and its answers. It is also possible to set a backup email address to reset passwords with an external email address.



Input field: Answer

Group: Personal data

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



Question: What is the name of your favourite pet?

Answer: ✓

Question:

Answer: ✓

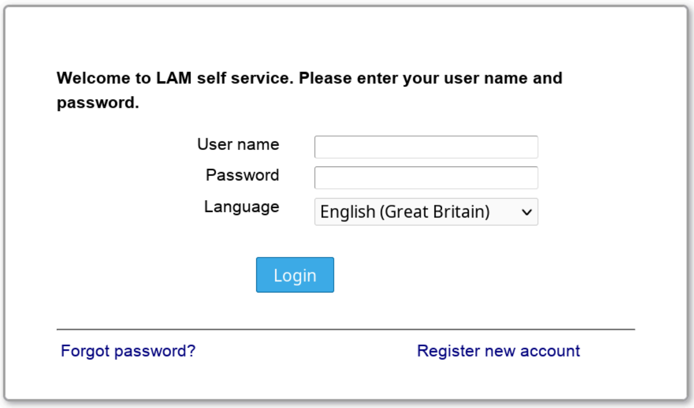
Question:

Answer: ✓

Backup email: roland.gruber@rg-se.de

Password reset link

After activating the password self reset feature there will be a new link on the self service login page. The text can be configured as described above (default: "Forgot password?").

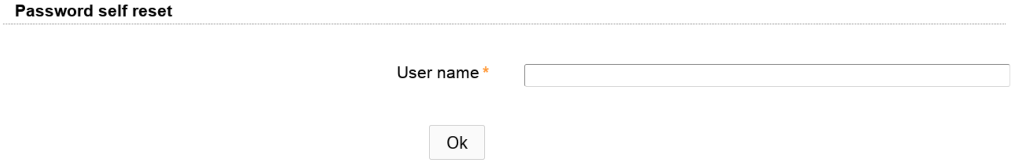

Welcome to LAM self service. Please enter your user name and password.

User name:

Password:

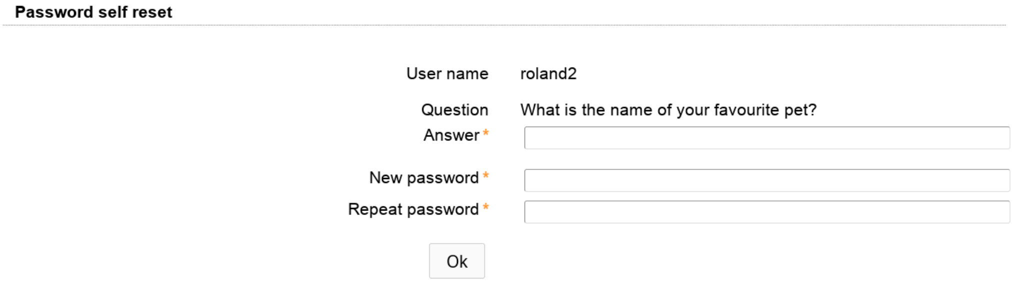
Language: English (Great Britain)

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



User name *:

LAM Pro will use this information to find the correct LDAP entry of this user. It then displays the user's security questions and input fields for his new password. If the answer is correct then the new password will be set. Additionally, pwdAccountLockedTime will be removed and shadowLastChange updated to the current time if existing.



Password self reset

User name: roland2

Question: What is the name of your favourite pet?

Answer *

New password *

Repeat password *

Prefilling the input fields

You might want to provide personalized URLs to your users that already prefill the fields in first step of password self reset. This can be done by adding an additional URL parameter with the attribute name in lower case.

LAM will not generate these URLs for you. This needs to be done by the system that provides the URL to your user.

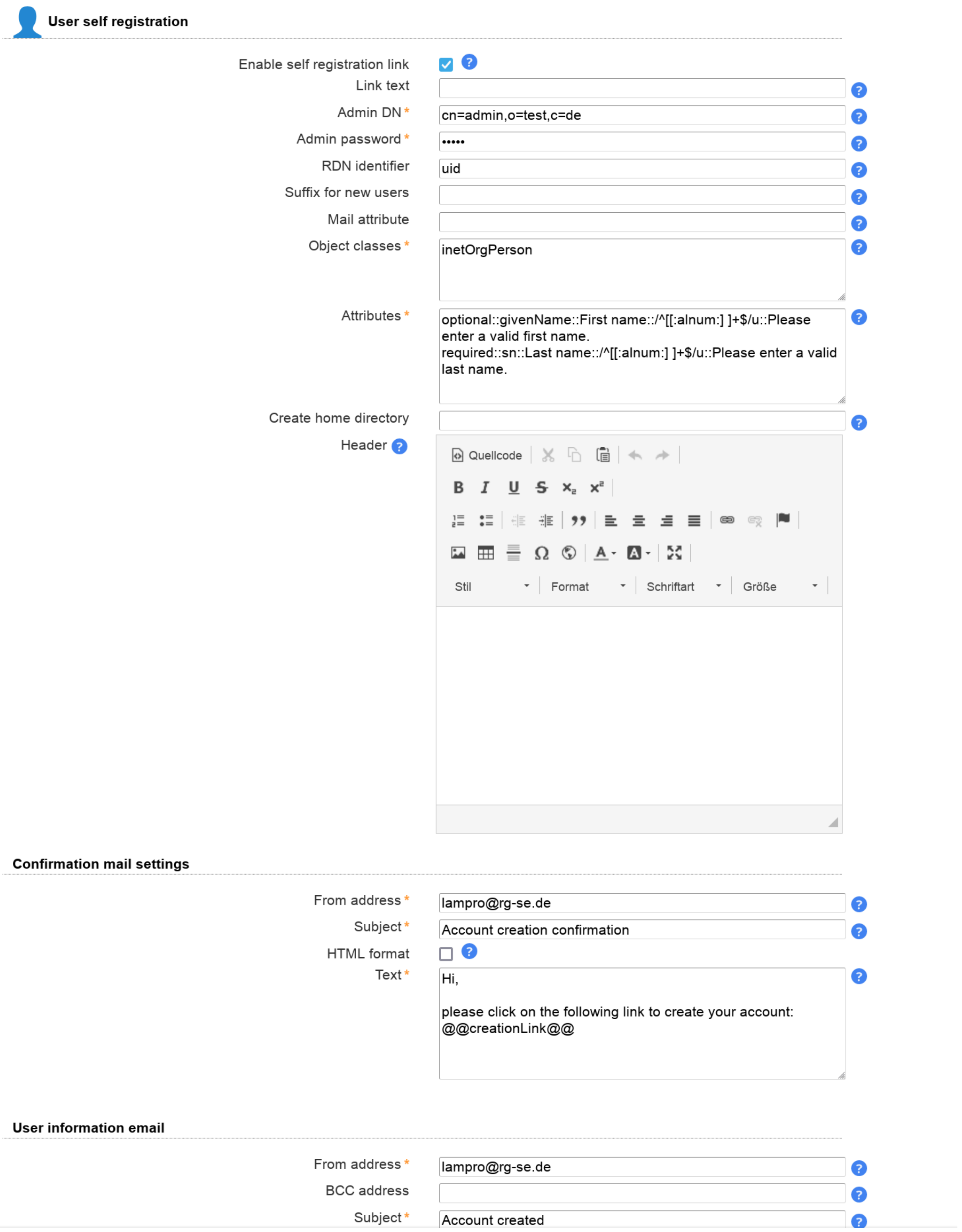
Examples:

- /lam/templates/selfService/selfServiceSP.php?scope=user&name=myProfile&page=passwordSelfReset&language=en_GB.utf8**&uid=yourUserId**
- /lam/templates/selfService/selfServiceSP.php?scope=user&name=myProfile&page=passwordSelfReset&language=en_GB.utf8**&mail=yourUserId@company.com**
- /lam/templates/selfService/selfServiceSP.php?scope=user&name=myProfile&page=passwordSelfReset&language=en_GB.utf8**&uidmail=yourUserId** (for "user or email" method)
- /lam/templates/selfService/selfServiceSP.php?scope=user&name=myProfile&page=passwordSelfReset&language=en_GB.utf8**&customattribute=yourUserId**

User self registration

With LAM Pro your users can create their own accounts if you like. LAM Pro will display an additional link on the self service login page that allows you users to create a new account including email validation (see here for setting up your SMTP server).

You enable this feature in your self service profile. Just activate the checkbox "Enable self registration link".



User self registration

Enable self registration link ☑

Link text

Admin DN * cn=admin,o=test,c=de

Admin password * •••••

RDN identifier uid

Suffix for new users

Mail attribute

Object classes * inetOrgPerson

Attributes * optional::givenName::First name::/^[[:alnum:]]+$/u::Please enter a valid first name.
required::sn::Last name::/^[[:alnum:]]+$/u::Please enter a valid last name.

Create home directory

Header

Confirmation mail settings

From address * lampro@rg-se.de

Subject * Account creation confirmation

HTML format □

Text * Hi,

please click on the following link to create your account:
@@creationLink@@

User information email

From address * lampro@rg-se.de

BCC address

Subject * Account created

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 (attribute "mail") are mandatory anyway and need not be specified. Just in case you use the legacy attribute "email" for account it needs to be specified (attribute "mail" will then not be shown).

Each line represents one LDAP attribute. The settings are separated by "::". The first setting specifies the field type. The second setting is the LDAP attribute name (add ";binary" to attribute names for file upload). Depending on the field type you can enter additional options:

Table 7.3.

Description	Type	Attribute name	First option	Second option	Third option
An optional input field that is displayed on the registration page.	optional	e.g. "givenName" or "jpegPhoto;binary"	Label that is displayed on page	Optional regular expression for validation (e.g. "/^[0-9a-zA-Z]+$/"). For binary fields the file name will be checked.	Validation message if value does not match validation expression.
A required input field that is displayed on the registration page. Self registration cannot be done if such a field is left empty by the user.	required	e.g. "sn" or "jpegPhoto;binary"	Label that is displayed on page	Optional regular expression for validation (e.g. "/^[0-9a-zA-Z]+$/"). For binary fields the file name will be checked.	Validation message if value does not match validation expression.
Constant attribute value, not visible for the user. Can be used to set some initial values or data that must not be edited by the user.	constant	e.g. "homeDirectory"	attribute value, supports wirldcards to insert other attribute values (e.g. "@@uid@@")		
Auto-numbering for attributes such as uidNumber. Will do a search for attribute values in the given range and use highest value + 1.	autorange	e.g. uidNumber	LDAP search base, e.g. ou=people,dc=company,dc=com	Minimum value, e.g. 1000	Maximum value, e.g. 2000

For a syntax description of validation expressions see here [http://perldoc.perl.org/perlre.html]. Validation is optional, you can leave these options blank.

Examples:

Unix account:

optional::givenName::First name::/^[[:alnum:]]+$/u::Please enter a valid first name.

required::sn::Last name::/^[[:alnum:]]+$/u::Please enter a valid last name.

constant::homeDirectory::/home/@@uid@@

autorange::uidNumber::ou=people,dc=company,dc=com::10000::20000

If you use the object class "inetOrgPerson" and do not provide the "cn" attribute then LAM will set it to the user name value.

Active Directory/Samba4:

required::cn::Common Name::/^[[:alnum:]]+$/u::Enter common name.

constant::userPrincipalName::@@uid@@@samba4.test

constant::sAMAccountName::@@uid@@

constant::userAccountControl::512

Binary file:

required::jpegPhoto;binary::Photo::/.jp(e)?g$/i::Please select a JPG file

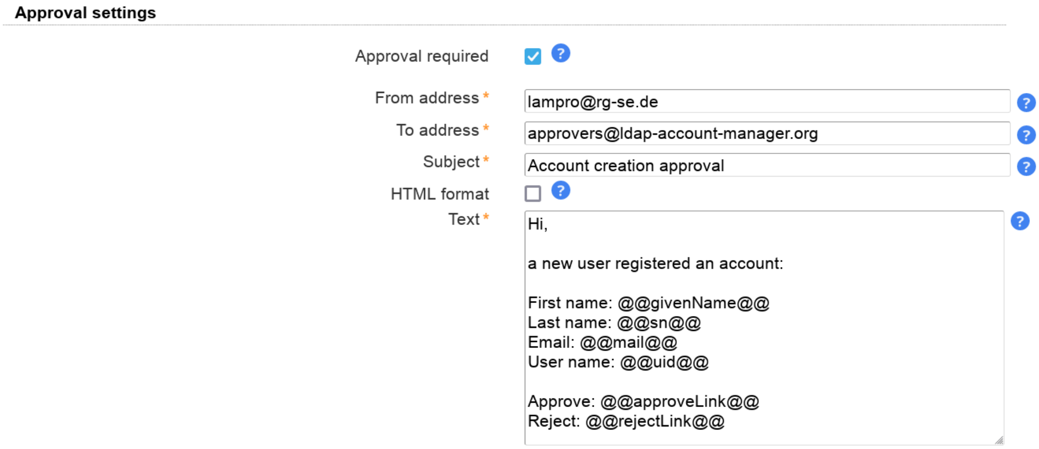
Please note that only simple input boxes are supported for account registration. The user may log in to self service when his account was created to manage all his attributes.

Create home directory: This will create the home directory via lamdaemon. The user must have the following attributes: uid, uidNumber, gidNumber, homeDirectory

Approval

You can send the account request to an administrator for approval. The email will include links for approval/reject. Please use the wildcards @@approveLink@@ and @@rejectLink@@ for this.

If the request was rejected then no email will be sent to the user.



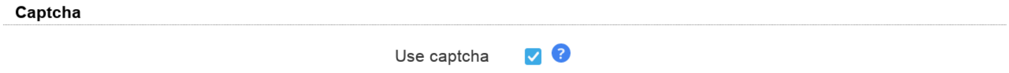
Approval settings

Approval required	☑
From address*	lampro@rg-se.de
To address*	approvers@ldap-account-manager.org
Subject*	Account creation approval
HTML format	□
Text*	Hi, a new user registered an account: First name: @@givenName@@ Last name: @@sn@@ Email: @@mail@@ User name: @@uid@@ Approve: @@approveLink@@ Reject: @@rejectLink@@

Captcha support

LAM Pro can optionally display a captcha to verify that registrations are not from robots. The captcha provider is configured on "General settings" tab.

Captchas will be displayed when you tick the checkbox to use a captcha.

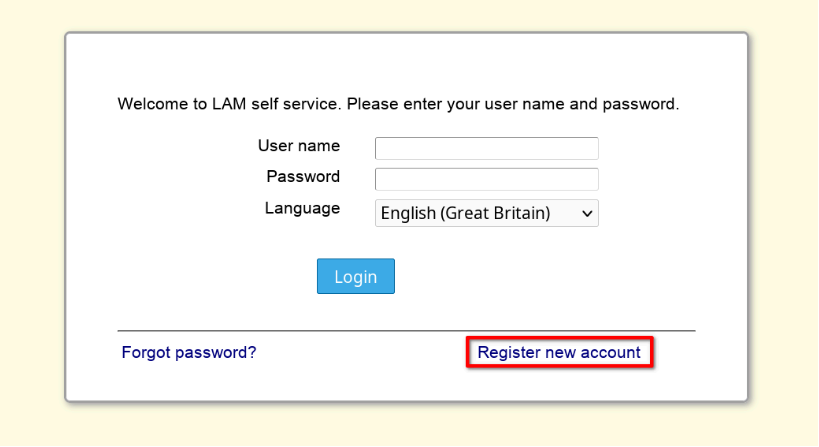


Captcha

Use captcha ☑

User view:

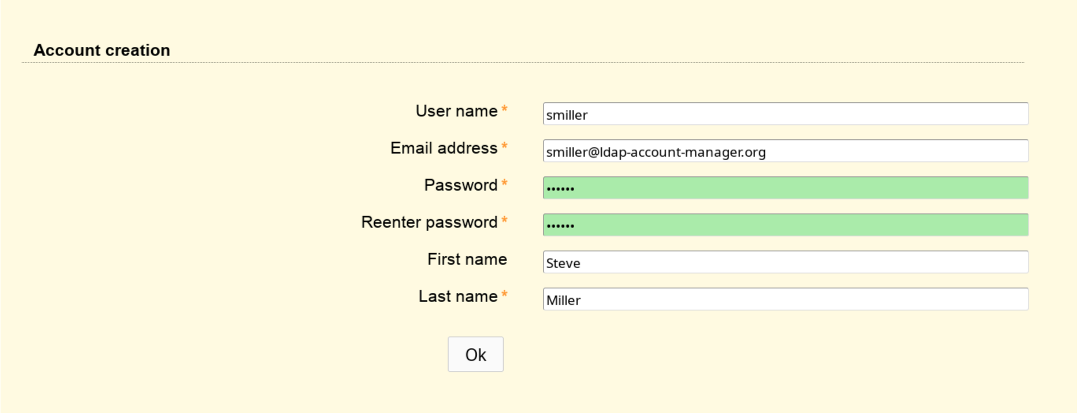
The user can register by clicking on a link on the self service login page:



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

User name	
Password	
Language	English (Great Britain)

Here he can insert the data that you specified in the self service profile:



Account creation

User name *	smiller
Email address *	smiller@ldap-account-manager.org
Password *	••••••
Reenter password *	••••••
First name	Steve
Last name *	Miller

LAM will then send him an email with a validation link that is valid for 24 hours. When he clicks on this link then the account will be created in the self service user suffix. The DN will look like this: *uid=<user name>,...*

Request Access

Use this feature to allow your users to request access for group memberships/ownerships. Requests will require the approval by the group owners/managers and optionally a special approver group (leave empty for owner/manager approval only).

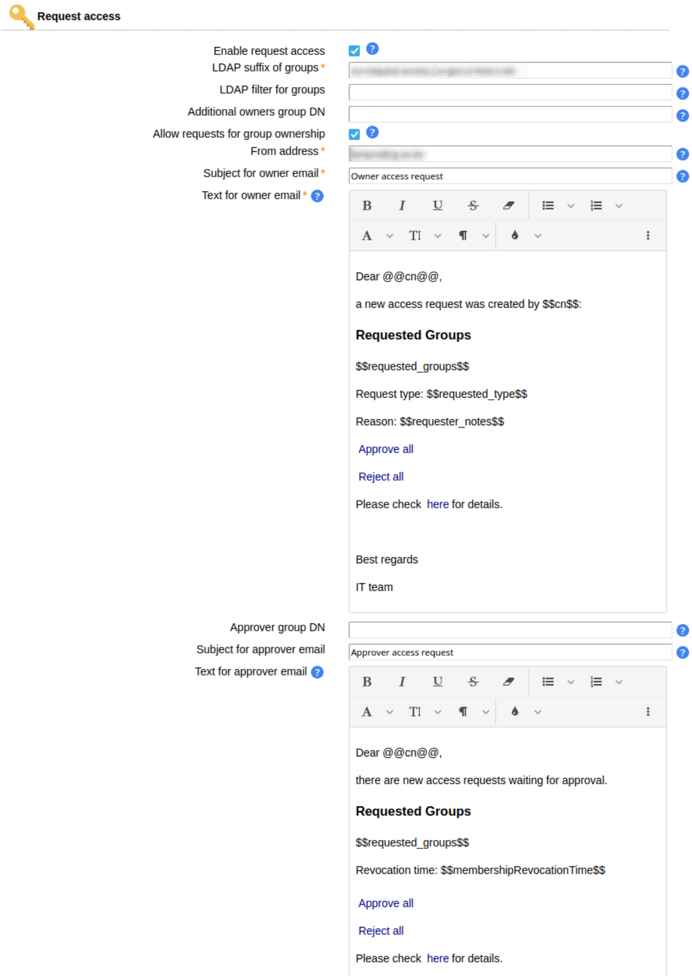
Setup cleanup

Please use the global cron job to clean any outdated requests or history entries. Here you can configure how long requests should be kept open and when to clean the history.

Module Configuration

First, the request access module needs to be activated and configured on tab "Module settings". Here tick "Enable request access" and provide the information where your groups are located.

Group of names, group of unique names and Windows groups are supported. The LDAP filter is optional, LAM will offer the user only groups of (unique) names or Windows groups that have defined owners/managers unless an additional owner group is defined.



Request access

Enable request access	☑
LDAP suffix of groups *	[redacted]
LDAP filter for groups	
Additional owners group DN	
Allow requests for group ownership	☑
From address *	[redacted]
Subject for owner email *	Owner access request
Text for owner email *	

Dear @@cn@@,

a new access request was created by $$cn$$:

Requested Groups

$$requested_groups$$

Request type: $$requested_type$$

Reason: $$requester_notes$$

Approve all

Reject all

Please check here for details.

Best regards

IT team

Approver group DN	
Subject for approver email	Approver access request
Text for approver email	

Dear @@cn@@,

there are new access requests waiting for approval.

Requested Groups

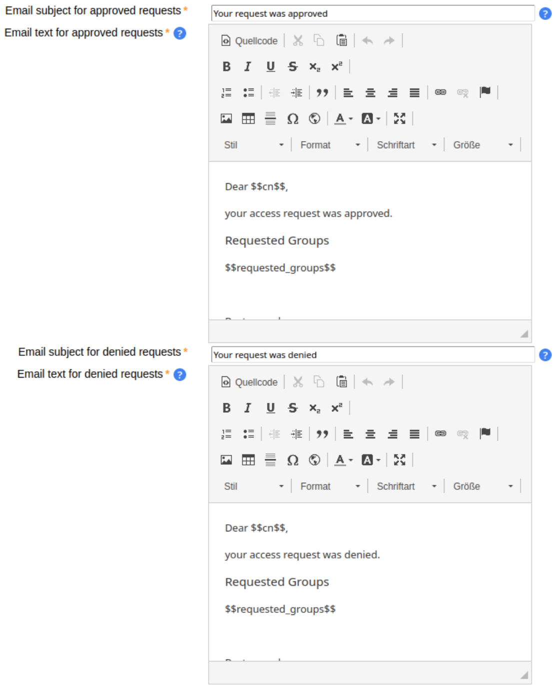
$$requested_groups$$

Revocation time: $$membershipRevocationTime$$

Approve all

Reject all

Please check here for details.



Email subject for approved requests *: Your request was approved

Email text for approved requests *:

Dear $$cn$$,

your access request was approved.

Requested Groups

$$requested_groups$$

Email subject for denied requests *: Your request was denied

Email text for denied requests *:

Dear $$cn$$,

your access request was denied.

Requested Groups

$$requested_groups$$

The email body texts support wildcards. You can use group owner/approver LDAP attributes in the form @@attribute@@ (e.g. @@uid@@ for the user name).

The requester's LDAP attributes can be used in the form $$attribute$$ (e.g. $$uid$$ for the user name). This is supported for mails to the group owners/managers and the approval/deny mails to the requester.

The wildcard $$requested_groups$$ will resolve to the requested groups. This is available for all mails.

In addition, $$requested_groups_member$$ and $$requested_groups_owner$$ can be used to inject the groups for member or owner requests (only emails for approved/denied requests).

Use the wildcard $$requested_type$$ in owner emails to get the request type (Member/Owner). The request type label is replaced in the language of the requester's self service session.

The wildcard $$requester_notes$$ resolves to the requester's optional notes. This is available for the mails to the group owners/managers.

Use $$request_comment$$ to inject the owner's or approver's comment. This can be used in mails to approvers and requesters.

The wildcards $$approveLink$$ and $$rejectLink$$ resolve to an URL that allows to approve/deny all requests listed in $$requested_groups$$. This is available for the mails to the group owners/managers and approvers. Use it as target URL for a link inside the email body.

The wildcard $$membershipRevocationTime$$ resolves to the revocation date of the membership if set. It is available for the mails to the approvers.

Example for owner email:

Dear @@cn@@,

a new access request was created by $$cn$$:

Requested groups: $$requested_groups$$

Reason: $$requester_notes$$

```
Approve all: $$approveLink$$
Deny all: $$rejectLink$$

Please check here (link to self service) for details.

Best regards,
IT team
```

Example for approver email:

```
Dear @@cn@@,

there are new access requests waiting for approval:

$$requested_groups$$

Comment: $$request_comment$$

Approve all: $$approveLink$$
Deny all: $$rejectLink$$

Please check here (link to self service) for details.

Best regards,
IT team
```

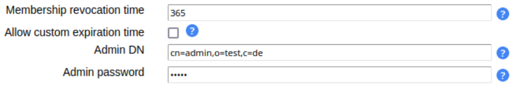
Example for approved/denied request email:

```
Dear $$cn$$,

your access request was approved/denied.
Requested groups: $$requested_groups$$
Comment: $$request_comment$$

Best regards,
IT team
```

Membership Revocation

You can select to revoke memberships after a given time. LAM will then remove them using global cron job once the time is reached. Please configure the following settings. If you use multiple self-service profiles for requester/owner/approver views then you need to configure this in the one that group owners use.

If you do not specify a revocation time then memberships/ownerships will not expire unless a custom revocation time is used. Allowing custom revocation times enables group owners to enter a custom date of revocation or no revocation time. The admin DN and password are used to perform the LDAP operation to remove the memberships.



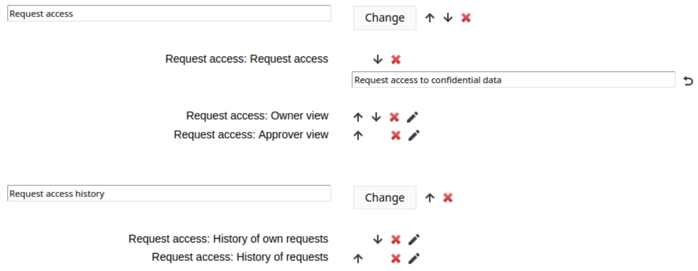
Membership revocation time: 365
Allow custom expiration time: □
Admin DN: cn=admin,o=test,c=de
Admin password: •••••

Field Configuration

Next, the fields need to be added to the "Page layout" tab. There are three fields:

- Request Access: Request access - User view that allows to initiate the process.
- Request Access: Owner view - Owner view for group owners.
- Request Access: Approver view - Approver view for approver group
- Request Access: History of own requests - History of the current user's requests
- Request Access: History of requests - History of all requests
  - Users that have no approver role see only requests for their managed groups
  - Users that are neither approver nor managing groups will not see anything
- Request access: Revocation information - Displays when roles will be revoked by the system
  - Users that have no approver role see only their managed groups
  - Users that are neither approver nor managing groups will not see anything

You can set custom labels using the pencil icon.



Request access — Change

Request access: Request access — Request access to confidential data

Request access: Owner view

Request access: Approver view

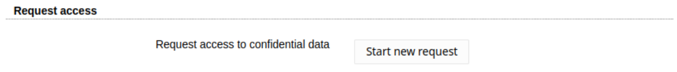
Request access history — Change

Request access: History of own requests

Request access: History of requests

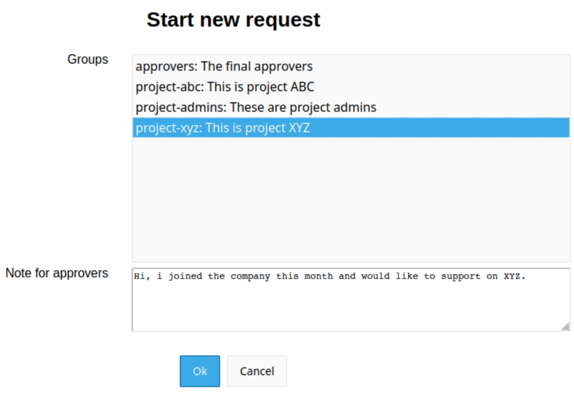
Request view

The user sees a button to open the new request dialog. Here the groups can be selected and an optional note can be provided.



Request access

Request access to confidential data — Start new request



Start new request

Groups:
- approvers: The final approvers
- project-abc: This is project ABC
- project-admins: These are project admins
- project-xyz: This is project XYZ

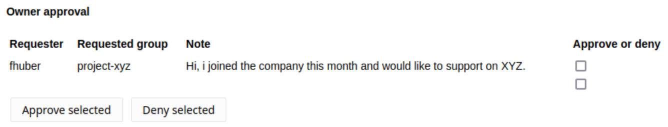
Note for approvers: Hi, i joined the company this month and would like to support on XYZ.

Ok Cancel

Owner/approver view

Once the request is created, all owners of the respective groups get an email notification. They can then enter self service and view their open requests.

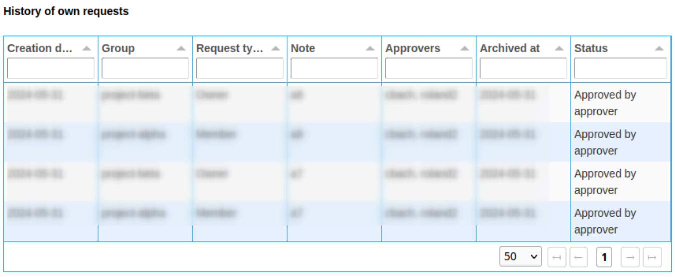
If an approver group is configured then its members will get an email notification after owner approval. In case no approver group is configured, the permissions are directly granted when the owner approves the request.



Owner approval

Requester	Requested group	Note	Approve or deny
fhuber	project-xyz	Hi, i joined the company this month and would like to support on XYZ.	□ □

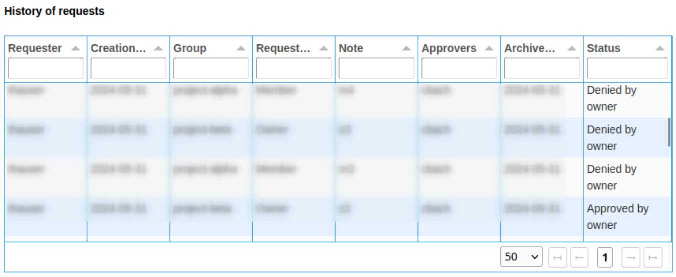
Own request history



History of own requests

Creation d...	Group	Request ty...	Note	Approvers	Archived at	Status
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	Approved by approver
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	Approved by approver
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	Approved by approver
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	Approved by approver

Request history



History of requests

Requester	Creation...	Group	Request...	Note	Approvers	Archive...	Status
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	Denied by owner
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	Denied by owner
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	Denied by owner
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	Approved by owner

Custom fields

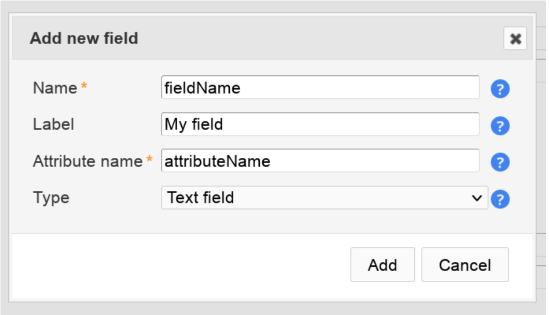
This module allows you to manage LDAP attributes that are not covered by the other LAM modules (e.g. if you use custom LDAP schemas). You can fully define how your input fields look like:

- Label
- LDAP attribute name
- Unique name for field
- Help text
- Read-only display
- Field type: text, password, text area, checkbox, radio buttons, select list, file upload, LDAP date (and time), constant
- Validation via regular expression
- Error message if validation fails

To create custom fields for the Self Service please edit your Self Service profile and switch to tab "Module settings". Here you can add a new field. Simply fill the fields and press on "Add".

Please note that the field name cannot be changed later. It is the unique ID for this field.

After you created your fields please press on "Sync fields with page layout". Now you can switch to tab "Page layout" and add your new fields like any other standard field.



Add new field

Name *	fieldName
Label	My field
Attribute name *	attributeName
Type	Text field

Examples for fields and their representation in Self Service:

Text field:

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

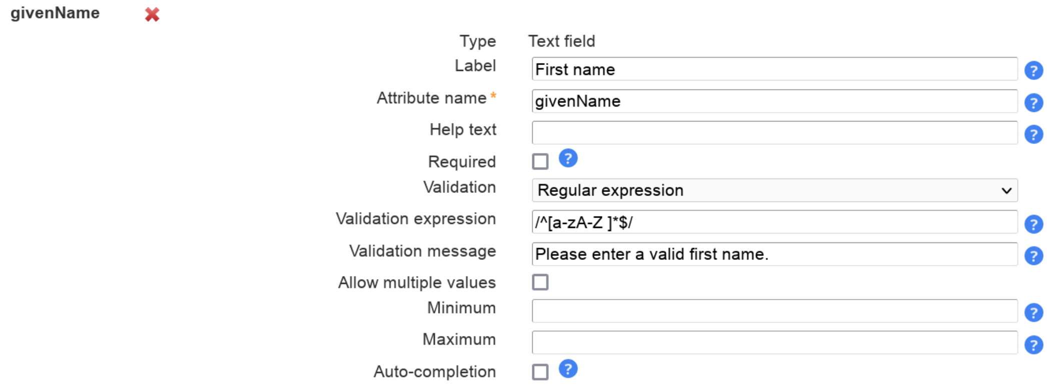
You can also enable auto-completion. In this case LAM will search all accounts for the given attribute and provide auto-completion hints when the user edits this field. This should only be used if there is a limited number of different values for this attribute.

In case your field is a date value you can show a calendar for easy editing.

Example calendar formats:

- d.m.Y: 31.12.2025
- Y-m-d: 2025-12-31
- d M, y: 31 Dec, 25
- d MM, Y: 31 December, 2025

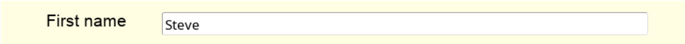
You can escape wildcards with "\". E.g. "d.m.Y \d" will result in "31.12.2025 d".



givenName

Type	Text field
Label	First name
Attribute name *	givenName
Help text	
Required	□
Validation	Regular expression
Validation expression	/^[a-zA-Z]*$/
Validation message	Please enter a valid first name.
Allow multiple values	□
Minimum	
Maximum	
Auto-completion	□

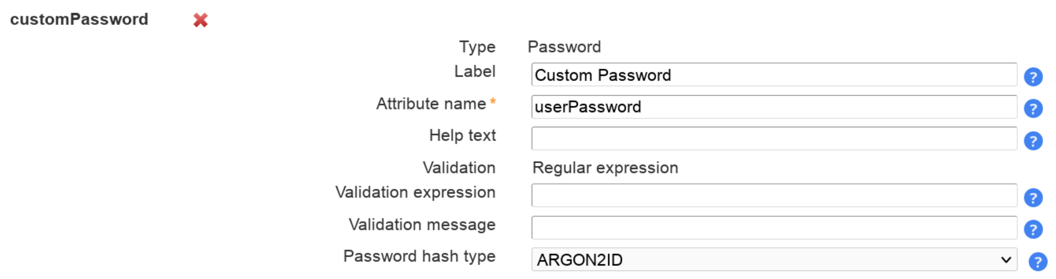
Presentation in Self Service:



First name	Steve

Password field:

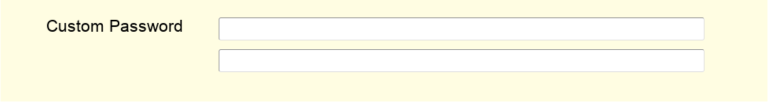
You can also manage custom password fields. LAM Pro will display two fields where the user must enter the same password. You can hash the password if needed.



customPassword ✖

Type	Password
Label	Custom Password
Attribute name *	userPassword
Help text	
Validation	Regular expression
Validation expression	
Validation message	
Password hash type	ARGON2ID

Presentation in Self Service:

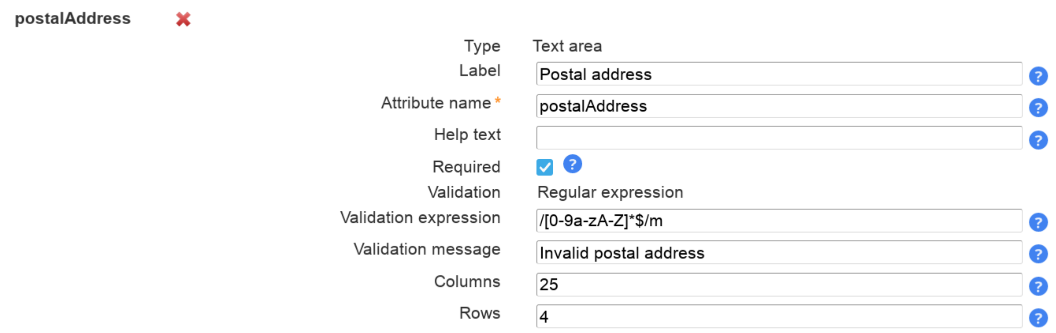


Custom Password

Text area:

This adds a multi-line field. The options are similar to text fields. Additionally, you can set the size with the number of columns and rows.

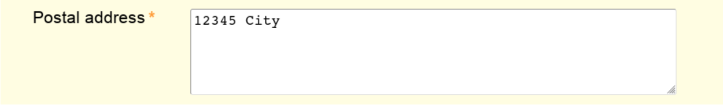
Please note that the validation expression should be set to multi-line. This is done by adding "m" at the end.



postalAddress ✖

Type	Text area
Label	Postal address
Attribute name *	postalAddress
Help text	
Required	☑
Validation	Regular expression
Validation expression	/[0-9a-zA-Z]*$/m
Validation message	Invalid postal address
Columns	25
Rows	4

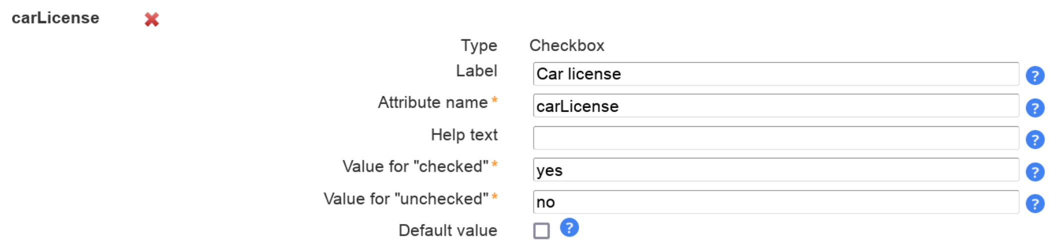
Presentation in Self Service:



Postal address *	12345 City

Checkbox:

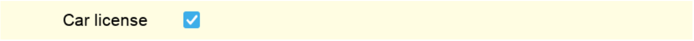
Sometimes you may want to allow only yes/no values for your LDAP attributes. This can be represented by a checkbox. You can specify the values for checked and unchecked. The default value is set if the LDAP attribute has no value.



carLicense ✖

Type	Checkbox
Label	Car license
Attribute name *	carLicense
Help text	
Value for "checked" *	yes
Value for "unchecked" *	no
Default value	□

Presentation in Self Service:

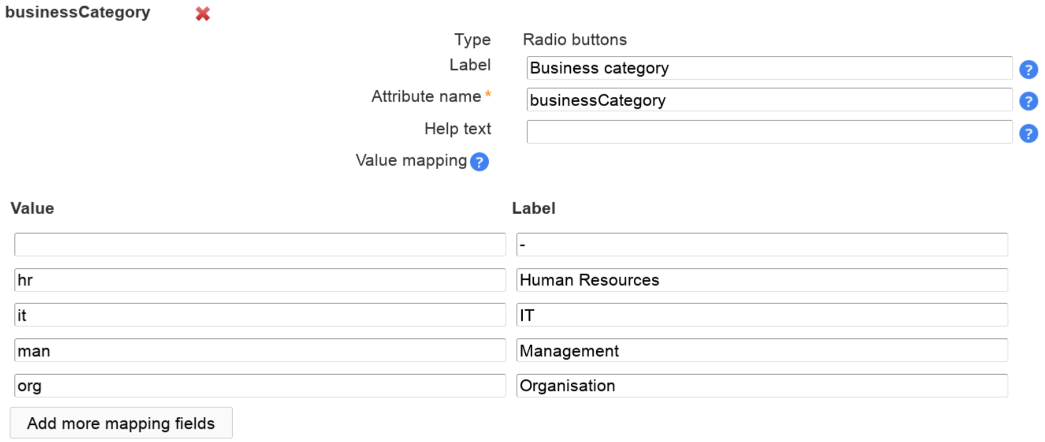


Car license ☑

Radio buttons:

This displays a list of radio buttons where the user can select one value.

You can specify a mapping of LDAP attribute values and their display (label) on the Self Service page. To add more mapping fields please press "Add more mapping fields".

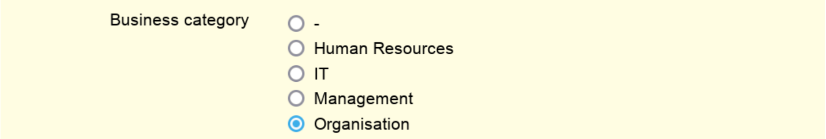


businessCategory ✖

Type	Radio buttons
Label	Business category
Attribute name *	businessCategory
Help text	
Value mapping	

Value	Label
	-
hr	Human Resources
it	IT
man	Management
org	Organisation

Presentation in Self Service:



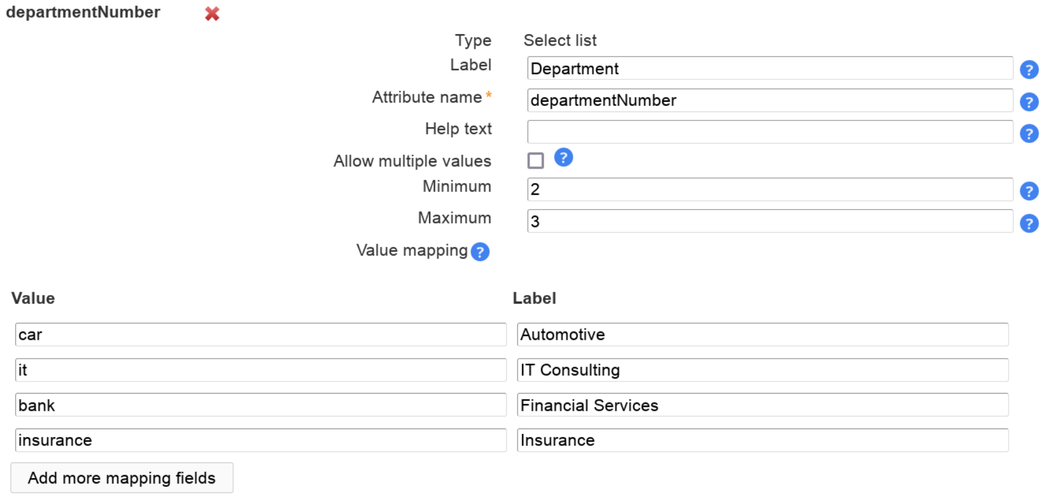
Business category

○ -
○ Human Resources
○ IT
○ Management
● Organisation

Select list:

Select lists allow the user to select a value in a large list of options. The definition of the possible values and their display is similar to radio buttons.

You can also allow multiple values.

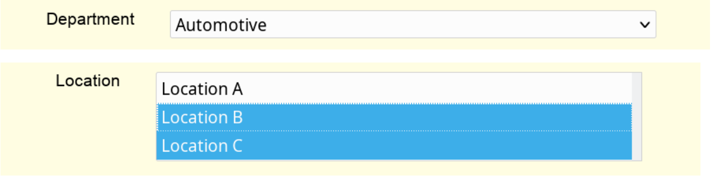


departmentNumber ✖

Type	Select list
Label	Department
Attribute name *	departmentNumber
Help text	
Allow multiple values	□
Minimum	2
Maximum	3
Value mapping	

Value	Label
car	Automotive
it	IT Consulting
bank	Financial Services
insurance	Insurance

Presentation in Self Service:

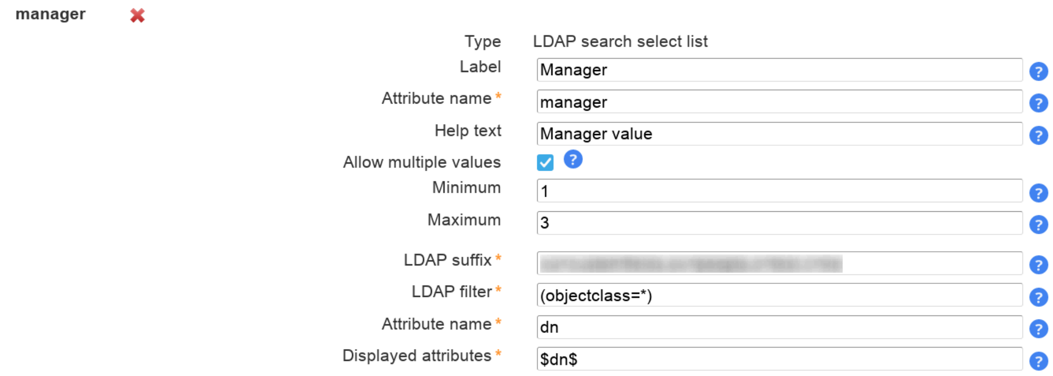


Department: Automotive

Location: Location A, Location B (selected), Location C (selected)

LDAP search select list

This is similar to "Select list" but the option are read from LDAP. You can use this to define e.g. a DN selection list. Multiple values are supported.



manager ✖

Type	LDAP search select list
Label	Manager
Attribute name *	manager
Help text	Manager value
Allow multiple values	☑
Minimum	1
Maximum	3
LDAP suffix *	
LDAP filter *	(objectclass=*)
Attribute name *	dn
Displayed attributes *	dn

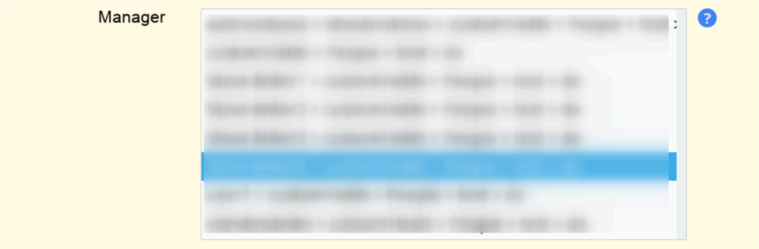
LDAP suffix: The LDAP DN that is used as starting point to search for LDAP entries.

LDAP filter: Only LDAP entries that match this filter will be used. If all entries should be used then use "(objectclass=*)".

Attribute name: The values of this attribute will be used to build the selection list.

Display attributes: List of attributes to show as label for the options in select box. Attribute wildcards are surrounded by "$", e.g. "$cn$" will be replaced by "cn" attribute. Default is "dn".

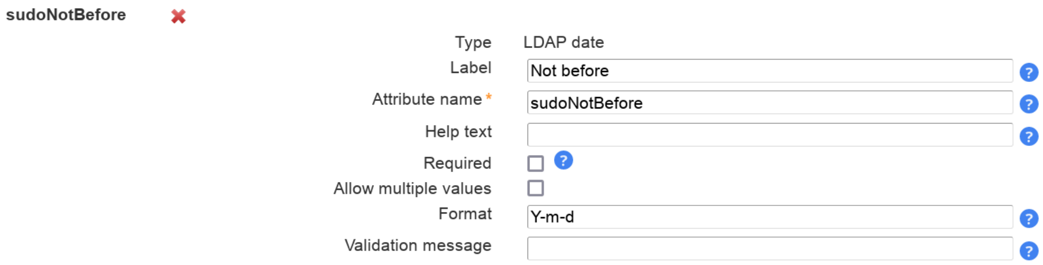
Presentation:



LDAP date

Use this for LDAP attributes with syntax "Generalized Time" (1.3.6.1.4.1.1466.115.121.1.24).

LAM will automatically set hour/minute/second to "0". If this is not intended please use type "LDAP date and time".

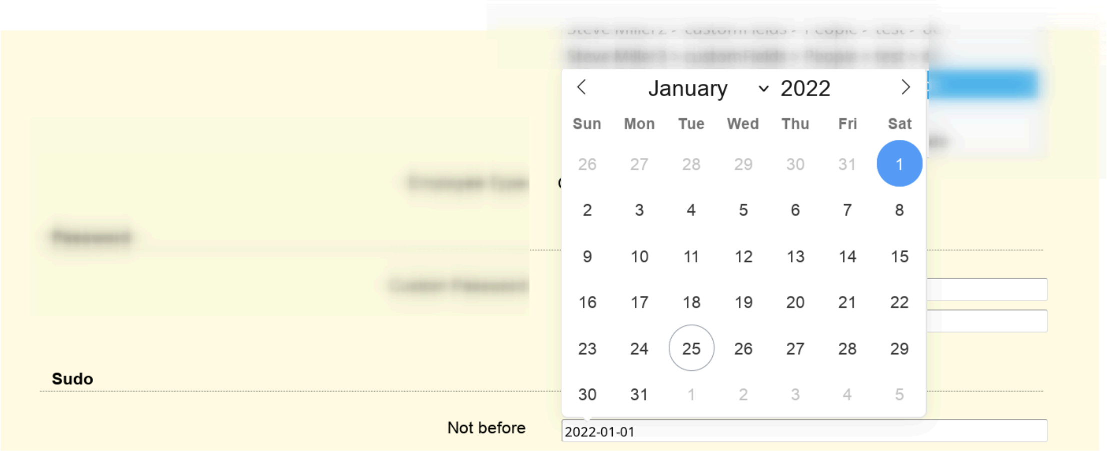


sudoNotBefore ✖

Type	LDAP date
Label	Not before
Attribute name *	sudoNotBefore
Help text	
Required	☐
Allow multiple values	☐
Format	Y-m-d
Validation message	

Presentation:

LAM will display a calendar to select the date.

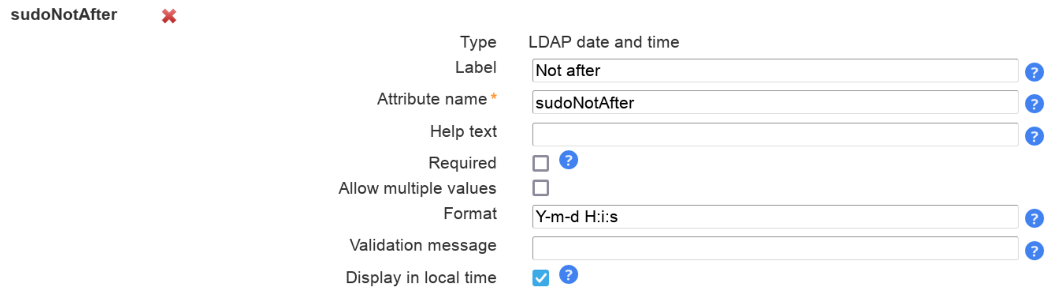


Not before 2022-01-01

LDAP date and time

Use this for LDAP attributes with syntax "Generalized Time" (1.3.6.1.4.1.1466.115.121.1.24).

LAM can convert the displayed value to the configured time zone of your server/self service profile. In this case, please activate "Display in local time".

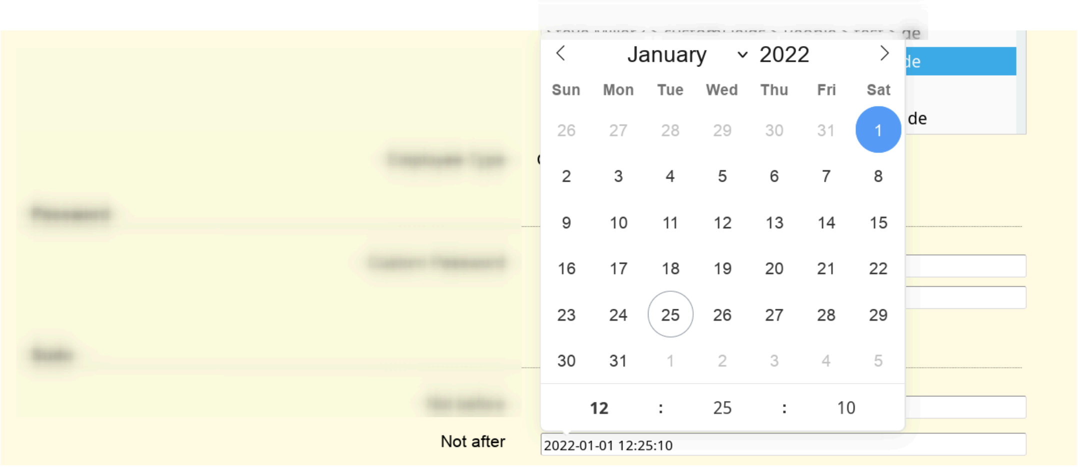


sudoNotAfter ✖

Type	LDAP date and time
Label	Not after
Attribute name*	sudoNotAfter
Help text	
Required	□
Allow multiple values	□
Format	Y-m-d H:i:s
Validation message	
Display in local time	☑

Presentation:

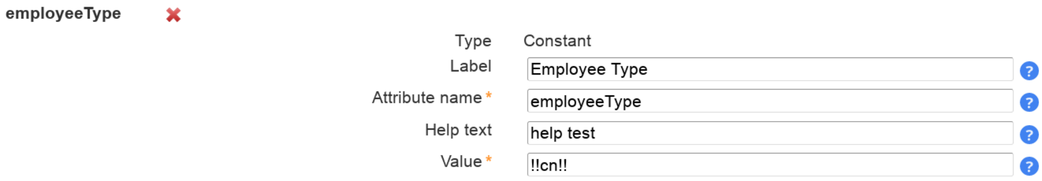
LAM will display a calendar to select the date and time.



Not after 2022-01-01 12:25:10

Constant value

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



employeeType ✖

Type	Constant
Label	Employee Type
Attribute name *	employeeType
Help text	help test
Value *	!!cn!!

Wildcards:

- %attribute%: attribute value
- @attribute@: first character of attribute
- ?attribute?: first character of attribute in lower case
- !attribute!: first character of attribute in upper case
- ??attribute??: attribute in lower case
- !!attribute!!: attribute in upper case
- ((attribute)): space if attribute is set
- §attribute|;§; attribute values separated by ";" (you can set other separators if you want)

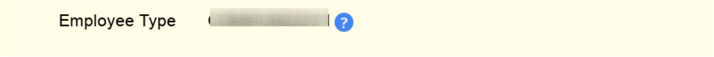
Examples for attributes gn="Steve", sn="Miller" and memberUid=("user1", "user2") (specified value -> resulting LDAP value):

Table 7.4.

Constant value	Resulting LDAP value
my constant	my constant
%gn%	Steve
%gn%((gn))%sn%	Steve Miller (would be "Miller" if gn is empty)
§memberUid|, §	user1, user2

Presentation:

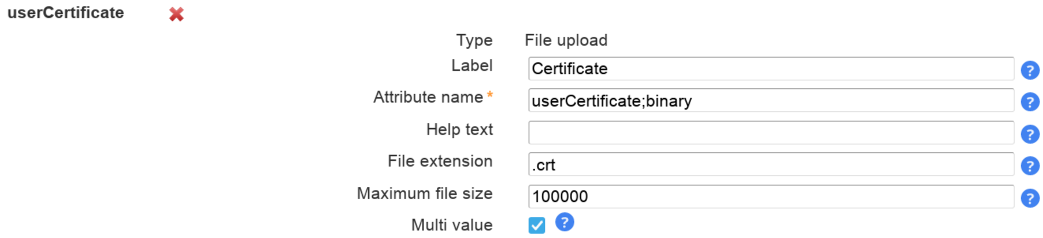
The LDAP value will be shown as text.



Employee Type [redacted]

File upload:

This is used for binary data. You can restrict uploaded data to a given file extension and set the maximum file size.

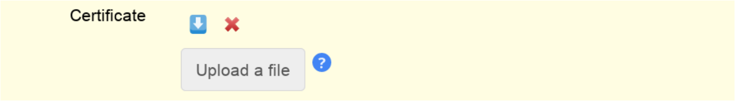


userCertificate ✖

Type	File upload
Label	Certificate
Attribute name *	userCertificate;binary
Help text	
File extension	.crt
Maximum file size	100000
Multi value	☑

Presentation:

The uploaded data may also be downloaded via LAM.



Certificate

Validation expressions:

The validation expressions follow the standard of Perl regular expressions [http://perldoc.perl.org/perlre.html]. They start and end with a "/". The beginning of a line is specified by "^" and the end by "$".

Examples:

/^[a-z0-9]+$/ allows small letters and numbers. The value must not be empty ("+").

/^[a-z0-9]+$/i allows small and capital letters ("i" at the end means ignore case) and numbers. The value must not be empty ("+").

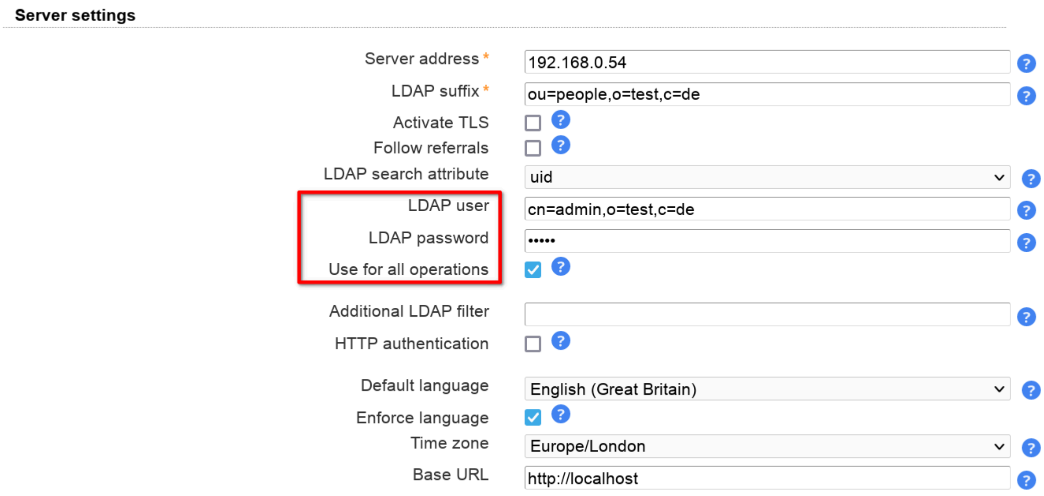
Special characters that must be escaped with "\": "\", ".", "(", ")"

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

OpenLDAP TOTP

This allows your users to setup OpenLDAP TOTP tokens.

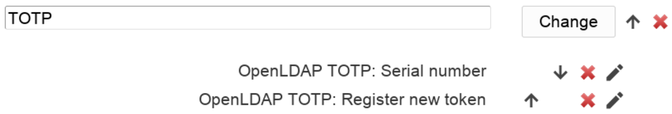
Please note that this requires to use a bind user that is also used for all operations. This user needs to be able to add/remove the TOTP object classes and attributes.



Server settings

Server address *	192.168.0.54
LDAP suffix *	ou=people,o=test,c=de
Activate TLS	□
Follow referrals	□
LDAP search attribute	uid
LDAP user	cn=admin,o=test,c=de
LDAP password	•••••
Use for all operations	☑
Additional LDAP filter	
HTTP authentication	□
Default language	English (Great Britain)
Enforce language	☑
Time zone	Europe/London
Base URL	http://localhost

On page layout tab you can then add the fields for serial number (optional) and the token. Users will then be able to manage their token via self service.



TOTP

OpenLDAP TOTP: Serial number

OpenLDAP TOTP: Register new token

On module settings tab please provide the DN of your TOTP settings entry (object class "oathTOTPParams").

OpenLDAP TOTP

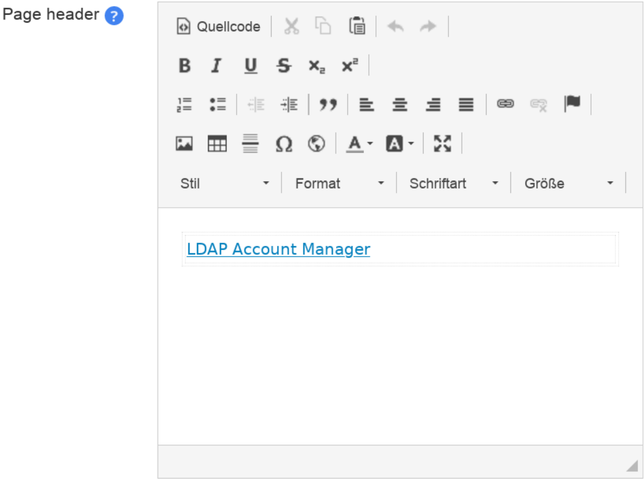
OTP parameters: ou=People,[redacted]

Adapt the self service to your corporate design

LAM Pro allows you to integrate customs CSS style definitions and design the header of all self service pages. This way you can integrate you own logo and use your company's colors.

Custom header

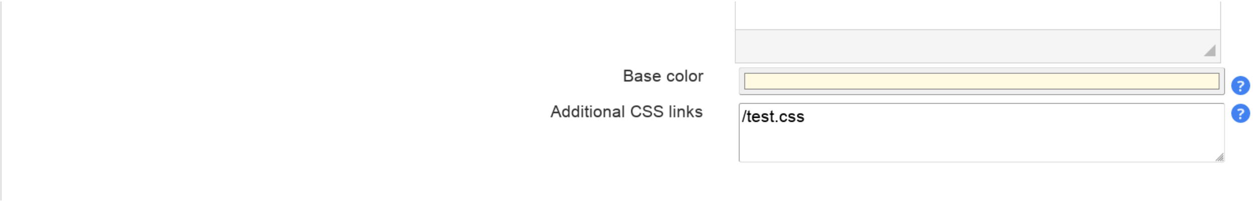
The default LAM Pro header includes a logo and a horizontal line. You can enter any HTML code here. It will be included in the self services pages after the body tag.



Page header: LDAP Account Manager

CSS files

Usually, companies have regulations about their corporate design and use common CSS files. This assures a common appearance of all intranet pages (e.g. colors and fonts). To include additional CSS files just use the following setting for this task. The additional CSS links will be added after LAM Pro's default CSS link. This way you can overwrite LAM Pro's style.



Base color

Additional CSS links: /test.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	
	AD LDS	user, group		AD LDS built-in	
	Kolab 2/3 users	kolabUser	kolab2/3.schema, rfc2739.schema	Part of Kolab 2/3 installation	
	Asterisk (extension)	AsteriskSIPUser, AsteriskExtension	asterisk.schema	Part of Asterisk installation	
	PyKota users, groups, printers and billing codes	pykotaObject, pykotaAccount, pykotaAccountBalance, pykotaGroup, pykotaPrinter, pykotaBilling	pykota.schema	Part of PyKota installation	
	Mail routing	inetLocalMailRecipient	misc.schema	Part of OpenLDAP installation	
	Hosts	hostObject, device	ldapns.schema	Part of libpam-ldap installation	The device object class is only available in LAM Pro.
	Authorized services	authorizedServiceObject	ldapns.schema	Part of libpam-ldap installation	
	Mail aliases	nisMailAlias	misc.schema	Part of OpenLDAP installation	
	Qmail user	qmailUser	qmail.schema	Part of qmail_ldap [http://	LAM Pro only

	Account type	Object class(es)	Schema name	Source	Notes
				www.nrg4u.com/]	
	MAC addresses	ieee802device	nis.schema	Part of OpenLDAP installation	
	IP addresses	ipHost	nis.schema	Part of OpenLDAP installation	LAM Pro only
	Puppet	puppetClient	puppet.schema	Puppet on GitHub [https://github.com/puppetlabs/puppet/blob/master/ext/ldap/puppet.schema]	
	EDU person	eduPerson	eduperson.schema	http://middleware.internet2.edu [http://middleware.internet2.edu/eduperson/]	
	Simple Accounts	account	cosine.schema	Part of OpenLDAP installation	
	SSH public keys	ldapPublicKey	openssh-lpk.schema	Included in patch from http://code.google.com/p/openssh-lpk/	
	SSH public keys (AD)	-	built-in	AD/Samba 4 built-in	
	Filesystem quotas	systemQuotas	quota.schema	Linux DiskQuota [http://sourceforge.net/projects/linuxquota/]	
	Group of (unique) names	groupOfNames, groupOfUniqueNames, groupOfMembers	core.schema	Part of OpenLDAP installation	LAM Pro only
	Groups	organizationalRole	core.schema	Part of OpenLDAP installation	LAM Pro only
	DHCP	dhcpOptions, dhcpSubnet, dhcpServer	dhcp.schema	Part of LAM installation: docs/schema/dhcp.schema	The LDAP suffix should be set to your dhcpServer entry.
	Bind dyndb-ldap	idnsZone, idnsRecord	schema.ldif	Part of bind-dyndb-ldap	LAM Pro only
	Bind DLZ DNS	dlzZone, dlzHost, dlzSOARecord, dlzNSRecord, dlzARecord, dlzMXRecord, dlzCNameRe-	dlz.schema	Part of Bind DLZ patch [http://bind-dlz.sourceforge.net/]	LAM Pro only

	Account type	Object class(es)	Schema name	Source	Notes
		cord, dlzPTRRecord			
	Aliases	alias, uidObject	core.schema	Part of OpenLDAP installation	LAM Pro only
	NIS netgroups	nisNetgroup	nis.schema	Part of OpenLDAP installation	
	NIS objects	nisObject	nis.schema	Part of OpenLDAP installation	LAM Pro only
	Automount objects	automount	autofs.schema, rfc2307bis.schema	Autofs LDAP	LAM Pro only
	Oracle databases	orclNetService	oidbase.schema, oidnet.schema, 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
	PowerDNS	dNSDomain2, domainRelatedObject	dnsdomain2.schema	Part of OpenLDAP installation	LAM Pro only
	FreeRadius users	radiusprofile	openldap.schema	Part of FreeRadius installation	
	Heimdal Kerberos	krb5KDCEntry	hdb.schema	Part of Heimdal Kerberos installation	LAM Pro only
	MIT Kerberos	krbPrincipal, krbPrincipalAux, krbTicketPolicyAux	kerberos.schema	Part of MIT Kerberos installation	LAM Pro only
	Simple Security Object	simpleSecurityObject	core.schema	Part of OpenLDAP installation	LAM Pro only
	Sudo roles	sudoRole	sudo.schema	Part of sudo-ldap installation	LAM Pro only
	Kopano	kopano-user, kopano-contact, kopano-group, kopano-dynamicgroup, kopano-addresslist, kopano-server	kopano.ldif	Part of Kopano installation	LAM Pro only
	IMAP mailboxes	-	-	-	Does not require any schema.

	Account type	Object class(es)	Schema name	Source	Notes
🔍	LDAP views	nsview, organizationalunit	built-in	Part of LDAP server installation (e.g. 389 server)	LAM Pro only
🥣	Apache Guacamole	guacConfigGroup	guacConfigGroup.ldif	Part of Guacamole Auth LDAP installation	LAM Pro only
🗑	All	dynamicObject	built-in with DDS module	Part of LDAP server installation	LAM Pro only, requires DDS extension on LDAP server side
TAK	TAK	takUser	tak-*.ldif	Part of LAM installation: docs/schema/tak-*.ldif	

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 labe
#!!!! $ semanage fcontext -a -t httpd_var_lib_t /var/lib/ldap-account-manager/config/lam
#!!!! $ 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 attaker needs read access to the session file (e.g. by another Apache instance) to exploit this.

Protection of your LDAP password and directory contents

You have to install the OpenSSL extension for PHP to enable encryption.

Your LDAP password is stored encrypted in the session file. The key and IV to decrypt it are stored in two cookies. We use OpenSSL/AES to encrypt the password. All data that was read from LDAP and needs to be stored in the session file is also encrypted.

Apache configuration

Security headers

LAM already sets several security headers by default. For production machines it is recommended to run LAM with "https://" enabled. In this case the HSTS header should be set, e.g. like this:

```
Header always set Strict-Transport-Security "max-age=31536000"
```

This will enforce browsers to connect via "https://". Please note that you need to make sure that your installation has a valid certificate now and in the future. The configuration requires mod_headers to be active.

Sensitive directories

LAM includes several .htaccess files to protect your configuration files and temporary data. Apache is often configured to not use .htaccess files by default. Therefore, please check your Apache configuration and change the override setting to:

AllowOverride All

If you are experienced in configuring Apache then you can also copy the security settings from the .htaccess files to your main Apache configuration.

If possible, you should not rely on .htaccess files but also move the config and sess directory to a place outside of your WWW root. You can put a symbolic link in the LAM directory so that LAM finds the configuration/session files.

Security sensitive directories:

config: Contains your LAM configuration and account profiles

- LAM configuration passwords (SSHA hashed)
- default values for new accounts
- directory must be accessibly 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 browsable

Use LDAP HTTP authentication for LAM

With HTTP authentication Apache will be responsible to ask for the user name and password. Both will then be forwarded to LAM which will use it to access LDAP. This approach gives you more flexibility to restrict the number of users that may access LAM (e.g. by requiring group memberships).

First of all you need to load additional Apache modules. These are "mod_ldap [http://httpd.apache.org/docs/2.2/mod/mod_ldap.html]" and "mod_authnz_ldap [http://httpd.apache.org/docs/2.2/mod/mod_authnz_ldap.html]".

Next you can add a file called "lam_auth_ldap" to /etc/apache/conf.d. This simple example restricts access to all URLs beginning with "lam" to LDAP authentication.

```
<location /lam>
  AuthType Basic
  AuthBasicProvider ldap
  AuthName "LAM"
  AuthLDAPURL "ldap://localhost:389/ou=People,dc=company,dc=com?uid"
  Require valid-user
</location>
```

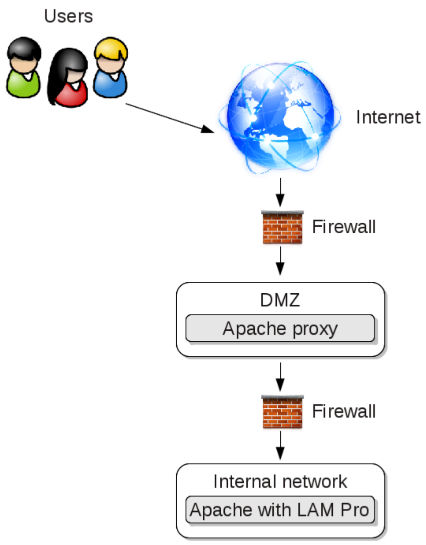
You can also require that your users belong to a certain Unix group in LDAP:

```
<location /lam>
  AuthType Basic
  AuthBasicProvider ldap
  AuthName "LAM"
  AuthLDAPURL "ldap://localhost:389/ou=People,dc=company,dc=com?uid"
  Require valid-user
  # force membership of lam-admins
  AuthLDAPGroupAttribute memberUid
  AuthLDAPGroupAttributeIsDN off
  Require ldap-group cn=lam-admins,ou=group,dc=company,dc=com
</location>
```

Please see the Apache documentation [http://httpd.apache.org/docs/2.2/mod/mod_authnz_ldap.html] for more details.

Self Service behind proxy in DMZ (LAM Pro)

In some cases you might want to make the self service accessible via the internet. Here is an Apache config to forward only the required URLs via a proxy server (lamproxy.company.com) in your DMZ to the internal LAM server (lam.company.com).



This configuration allows your users to open https://lamproxy.company.com which will then proxy the self service on the internal server.

```
<VirtualHost lamproxy.company.com:443>
        ServerName lamproxy.company.com
        ErrorLog /var/log/apache2/lam-proxy-error.log
        CustomLog /var/log/apache2/lam-proxy-access.log combined
        DocumentRoot /var/www/lam-proxy
        <Proxy *>
            Require all granted
        </Proxy>
        SSLProxyEngine on
        SSLEngine on
        SSLCertificateFile /etc/apache2/ssl/apache.pem
        ProxyPreserveHost On
        ProxyRequests off
        loglevel info

        # redirect front page to self service login page
        RewriteEngine on
        RedirectMatch ^/$ /templates/selfService/selfServiceLogin.php?scope=user\&name=

        # proxy required URLs
        ProxyPass /tmp https://lam.company.com/lam/tmp
        ProxyPass /sess https://lam.company.com/lam/sess
        ProxyPass /templates/lib https://lam.company.com/lam/templates/lib
        ProxyPass /templates/selfService https://lam.company.com/lam/templates/selfServ
        ProxyPass /templates/misc https://lam.company.com/lam/templates/misc
        ProxyPass /style https://lam.company.com/lam/style
        ProxyPass /graphics https://lam.company.com/lam/graphics

        ProxyPassReverse /tmp https://lam.company.com/lam/tmp
        ProxyPassReverse /sess https://lam.company.com/lam/sess
        ProxyPassReverse /templates/lib https://lam.company.com/lam/templates/lib
        ProxyPassReverse /templates/selfService https://lam.company.com/lam/templates/s
        ProxyPassReverse /templates/misc https://lam.company.com/lam/templates/misc
        ProxyPassReverse /style https://lam.company.com/lam/style
        ProxyPassReverse /graphics https://lam.company.com/lam/graphics
</VirtualHost>
```

Nginx configuration

There is no fully automatic setup of Nginx but LAM provides a ready-to-use configuration file.

Security headers

LAM already sets several security headers by default. For production machines it is recommended to run LAM with "https://" enabled. In this case the HSTS header should be set.

This will enforce browsers to connect via "https://". Please note that you need to make sure that your installation has a valid certificate now and in the future.

The example configurations below already include a commented example for "Strict-Transport-Security" (HSTS). You can activate it if needed.

RPM based installations

The RPM package has dependencies on Apache. Therefore, Nginx is not officially supported with this installation mode. Use tar.bz2 if you are unsure.

However, the package also includes an Nginx configuration file. Please include it in your server directive like this:

```
server {
        ...

        include /etc/ldap-account-manager/lam.nginx.conf;

        ...
}
```

The included config file uses "127.0.0.1:9000" for PHP. In case you run PHP with a socket please update the parameter "fastcgi_pass" to e.g. "/var/run/php8-fpm.sock".

DEB based installations

The LAM installation package ships with an Nginx configuration file. Please include it in your server directive like this:

```
server {
        ...

        include /etc/ldap-account-manager/nginx.conf;

        ...
}
```

The included config file uses PHP 8.2. In case you run with a different PHP version please update the parameter "fastcgi_pass" to e.g. "/var/run/php/php8.3-fpm.sock".

tar.bz2 based installations

Please add the following configuration snippet to your server directive.

You will need to change the alias location ("/usr/share/ldap-account-manager") and fastcgi_pass (e.g. "/var/run/php/php-fpm.sock" or "/var/run/php8-fpm.sock") to match your installation.

```
location /lam {
  index index.html;
  alias /usr/share/ldap-account-manager;
  autoindex off;
  # HSTS header to enforce https:// connections
  # add_header Strict-Transport-Security "max-age=31536000";

  location ~ \.php$ {
    fastcgi_split_path_info ^(.+\.php)(/.+)$;
    fastcgi_pass unix:/var/run/php8-fpm.sock;
    fastcgi_index index.php;
    fastcgi_param SCRIPT_FILENAME $request_filename;
    include fastcgi_params;
  }

  location ~ /lam/(tmp/internal|sess|config|lib|help|locale) {
    deny all;
    return 403;
  }

}
```

WebAuthn/FIDO2

LAM allows to secure logins via WebAuthn/FIDO2 [https://en.wikipedia.org/wiki/WebAuthn]. This means your users login with their LDAP password and an additional hardware token (e.g. Yubico Security Key, Windows Hello and many more).

WebAuthn/FIDO2 is a very strong 2-factor-authentication method as it also checks the website domain. This prevents attacks via web proxies.

To use this feature you need to activate the 2-factor authentication in LAM.

LAM admin interface

Please activate WebAuthn/FIDO2 in your LAM server profile. Then users will be asked to authenticate via WebAuthn/FIDO2 on each login.

If no device is registered for a user then LAM will ask for this during login. Afterwards, users can manage their devices with the WebAuthn tool.

LAM Self Service

Please activate WebAuthn/FIDO2 in your LAM self service profile. Then users will be asked to authenticate via WebAuthn/FIDO2 on each login.

If no device is registered for a user then LAM will ask for this during login. Afterwards, users can manage their devices with the WebAuthn field.

Global device management

This is for cases where one of your users has no more access to his device and cannot login anymore. In this case you can delete his device(s) in the LAM main configuration.

Note that devices can only be deleted. Registration of devices can only be done by the user during login or on the management pages listed above.

Appendix C. Typical OpenLDAP settings

Some basic hints to configure the OpenLDAP server:

Size limit:

You will get a message like "LDAP sizelimit exceeded, not all entries are shown." when you hit the LDAP search limit.

OpenLDAP allows by default 500 return values per search, if you have more users/groups/hosts please change this:

slapd.conf:

e.g. "sizelimit 10000" or "sizelimit -1" for unlimited return values

slapd.d:

e.g. "olcSizeLimit: 10000" or "olcSizeLimit: -1" for unlimited return values in /etc/ldap/slapd.d/cn=config.ldif

Unique attributes:

There are cases where you do not want that same attribute values exist multiple times in your database. A good example are UID/GID numbers.

OpenLDAP provides the attribute uniqueness overlay [http://www.openldap.org/doc/admin24/overlays.html] for this task.

Example to force unique UID numbers:

In */etc/ldap/slapd.d/cn=config/cn=module{0}.ldif* add "olcModuleLoad: {3}unique" (replace "3" with the highest existing number plus one).

Now in /etc/ldap/slapd.d/cn=config/olcDatabase={1}bdb.ldif add e.g. "olcUniqueURI: ldap:///?uidNumber?sub"

Indices:

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

```
index objectClass eq
index default sub
index uidNumber eq
index gidNumber eq
index memberUid eq
index cn,sn,uid,displayName pres,sub,eq
# Samba 3.x
index sambaSID eq
index sambaPrimaryGroupSID eq
index sambaDomainName eq
```

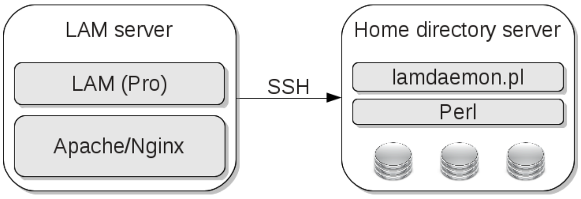
Appendix D. Setup for home directory and quota management

Lamdaemon.pl is used to modify quota and home directories on a remote or local host via SSH (even if homedirs are located on localhost).

If you want wo use it you have to set up the following things to get it to work:

Installation

First of all, you need to install lamdaemon.pl on your remote server where LAM should manage homedirs and/or quota. This is usually a different server than the one where LAM is installed. But there is no problem if it is the same.



Debian based (e.g. also Ubuntu)

Please install the lamdaemon DEB package on your quota/homedir server.

RPM based (Fedora, CentOS, Suse, ...)

Please install the lamdaemon RPM package on your quota/homedir server.

Other

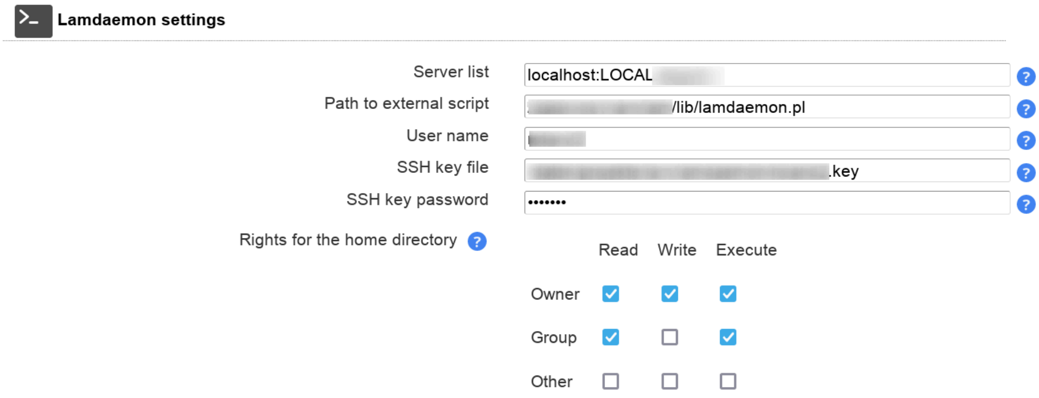
Please copy lib/lamdaemon.pl from the LAM tar.bz2 package to your quota/homedir server. The location may be anywhere (e.g. use /opt/lamdaemon). Please make the lamdaemon.pl script executable.

LDAP Account Manager configuration

- Set the remote or local host in the configuration (e.g. 127.0.0.1)

- Path to lamdaemon.pl, e.g. /srv/www/htdocs/lam/lib/lamdaemon.pl If you installed a DEB or RPM package then the script will be located at /usr/share/ldap-account-manager/lib/lamdaemon.pl.

- Your LAM admin user must be a valid Unix account. It needs to have the object class "posixAccount" and an attribute "uid". This account must be accepted by the SSH daemon of your home directory server. Do not create a second local account but change your system to accept LDAP users. You can use LAM to add the Unix account part to your admin user or create a new account. Please do not forget to setup LDAP write access (ACLs [http://www.openldap.org/doc/admin24/access-control.html]) if you create a new account.



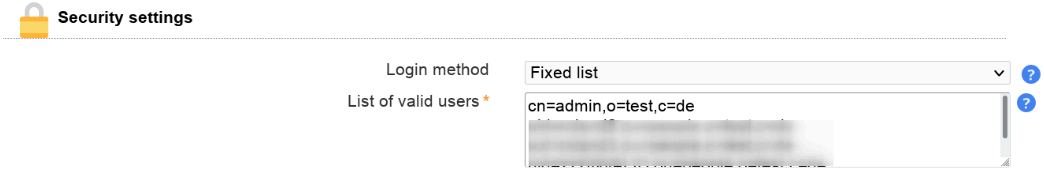
Lamdaemon settings

Server list	localhost:LOCAL [redacted]
Path to external script	[redacted]/lib/lamdaemon.pl
User name	[redacted]
SSH key file	[redacted].key
SSH key password	•••••••

Rights for the home directory

	Read	Write	Execute
Owner	☑	☑	☑
Group	☑	☐	☑
Other	☐	☐	☐

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



Security settings

Login method	Fixed list
List of valid users *	cn=admin,o=test,c=de [redacted]

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 E. Setup password self reset schema (LAM Pro)

New installation

Please see here if you want to upgrade an existing schema version.

Schema installation

Please install the schema that comes with LAM Pro. The schema files are located in:

- tar.bz2: docs/schema
- DEB: /usr/share/doc/ldap-account-manager/docs/schema
- RPM: /usr/share/doc/ldap-account-manager-{VERSION}/schema

OpenLDAP with slapd.conf configuration

For a configuration with slapd.conf-file copy passwordSelfReset.schema to /etc/ldap/schema/ and add this line to slapd.conf:

```
include         /etc/ldap/schema/passwordSelfReset.schema
```

OpenLDAP with slapd.d configuration

For slapd.d configurations you need to upload the schema file passwordSelfReset.ldif via ldapadd command:

ldapadd -x -W -H ldap://*localhost* -D "*cn=admin,o=test,c=de*" -f passwordSelfReset.ldif

Please replace "*localhost*" with your LDAP server and "*cn=admin,o=test,c=de*" with your LDAP admin user (usually starts with cn=admin or cn=manager).

In some cases you might need to import directly on the OpenLDAP server as root:

ldapadd -Y EXTERNAL -H ldapi:/// -f passwordSelfReset.ldif

389 server

Please replace INSTANCE with installation ID, e.g. slapd-389ds.

```
cp passwordSelfReset-389server.ldif /etc/dirsrv/INSTANCE/schema/70pwdreset.ldif
systemctl restart dirsrv.target
```

Samba 4

The schema files are passwordSelfReset-Samba4-attributes.ldif and passwordSelfReset-Samba4-objectClass.ldif.

First, you need to edit them and replace "DOMAIN_TOP_DN" with your LDAP suffix (e.g. dc=samba4,dc=test).

Then install the attribute and afterwards the object class schema file:

```
ldbmodify -H /var/lib/samba/private/sam.ldb passwordSelfReset-Samba4-attributes.ldif --option="dsdb:schema update allowed"=
ldbmodify -H /var/lib/samba/private/sam.ldb passwordSelfReset-Samba4-objectClass.ldif --option="dsdb:schema update allowed
```

Windows

The schema file is passwordSelfReset-Windows.ldif.

First, you need to edit it and replace "DOMAIN_TOP_DN" with your LDAP suffix (e.g. dc=windows,dc=test).

Then install the schema file as administrator on a command line:

```
ldifde -v -i -f passwordSelfReset-Windows.ldif
```

This allows to set a security question + answer for each account.

Schema update

The schema files are located in:

- tar.bz2: docs/schema/updates
- DEB: /usr/share/doc/ldap-account-manager/docs/schema/updates
- RPM: /usr/share/doc/ldap-account-manager-{VERSION}/schema/updates

Schema versions:

1. Initial version (LAM Pro 3.6 - 4.4)
2. Added passwordSelfResetBackupMail (LAM Pro 4.5 - 5.5)
3. Multiple security questions (LAM Pro 5.6)

OpenLDAP with slapd.conf configuration

Install the schema file like a new install (skip modification of slapd.conf file).

OpenLDAP with slapd.d configuration

The upgrade requires to stop the LDAP server.

Steps:

1. Stop OpenLDAP with e.g. "/etc/init.d/slapd stop"
2. Delete the old schema file. It is located in e.g. "/etc/ldap/slapd.d/cn=config/cn=schema" and called "cn={XX}passwordselfreset.ldif" (XX can be any number)
3. Start OpenLDAP with e.g. "/etc/init.d/slapd start"
4. Install the schema file like a new install

Samba 4

Install the these update files by following the install instructions in the file. In case you you upgrade with a version difference of 2 or more you will need to apply all intermediate update scripts.

- samba4_version_1_to_2_attributes.ldif (upgrade from version 1 only)
- samba4_version_1_to_2_objectClass.ldif (upgrade from version 1 only)
- samba4_version_2_to_3_attributes.ldif (upgrade from version 2)
- samba4_version_2_to_3_objectClass.ldif (upgrade from version 2)

Please note that attributes file needs to be installed first.

Windows

Install the file(s) by following the install instructions in the file. In case you you upgrade with a version difference of 2 or more you will need to apply all intermediate update scripts.

- windows_version_1_to_2.ldif (upgrade from version 1 only)
- windows_version_2_to_3.ldif (upgrade from version 2)

Appendix F. Adapt LAM to your corporate design

There are cases where you might want to change LAM's default look'n'feel to better integrate it in your company network. Changes can be done like this:

Change colors, fonts and other parts with custom CSS

You can integrate custom CSS files in LAM. It is recommended to write a separate CSS file instead of modifying LAM's default files.

The CSS files are located in

DEB/RPM: /usr/share/ldap-account-manager/style
tar.bz2: style

LAM will automatically integrate all CSS files in alphabetical order. E.g. you can create a file called "900_myCompany.css" which will be added as last file.

In many cases it can be sufficient to overwrite some CSS variables. See top of 500_layout.css [https://github.com/LDAPAccountManager/lam/blob/develop/lam/style/500_layout.css] for defined variables.

Example:

This will change the background color of all pages to grey.

```
:root {
    --lam-background-color-default: #E7E7E7;
}
```

Change LAM logo:

```
div.lam-header-left img {
    background: url("../graphics/key.svg") center no-repeat;
    box-sizing: border-box;
    width: 32px;
    height: 32px;
    padding-left: 32px;
}
```

You can use the same way to change font/button colors and more.

Change header bar to mark different environments

```
.lam-header {
    box-shadow: 0px 3px 2px -2px red;
}
```

Other images

All images are located in

DEB/RPM: /usr/share/ldap-account-manager/graphics
tar.bz2: graphics

Please note that if you replace images then you need to reapply your changes every time you upgrade LAM.

Special changes with custom JavaScript

In rare cases it might not be sufficient to write custom CSS or replace some image files. E.g. you might want to add custom content to all pages.

For these cases you can add a custom JavaScript file that contains your code.

The JavaScript files are located in

```
 DEB/RPM: /usr/share/ldap-account-manager/templates/lib
 tar.bz2: templates/lib
```

LAM will automatically integrate all .js files in alphabetical order. E.g. you can create a file called "900_myCompany.js" which will be added as last file.

Self service

See here for self service customisations.

Appendix G. Clustering LAM

LAM is a web application based on PHP. Therefore, clustering is not directly a part of the application.

But here are some hints to run LAM in a clustered environment.

Application parts:

LAM can be divided into three parts

- Software
- Configuration files
- Session files and temporary data

Software:

This is the simplest part. Just install LAM on each cluster node. Please note that if you run LAM Pro you will need either one license for each active cluster node or a company license.

Configuration files:

These files include the LAM server profiles, account profiles, PDF structures, ... Usually, they do not change frequently and can be put on a shared file system (e.g. NFS, AFS, ...).

Please link "config" or "/var/lib/ldap-account-manager/config" to a directory on your shared file system.

Session data and temporary files:

These are critical because the files may change on every page load. There are basically two options:

- load balancer with session stickiness: In this case your load balancer will forward all requests of a user to the same cluster node. In this case you can keep the files locally on your cluster nodes. If you already have a load balancer then this is the simplest solution and performs best. The disadvantage is that if a node fails then all users connected to this node will loose their session and need to relogin.
- shared file system: This should only be used if your load balancer does not support session stickiness or you use a different system to distribute request across the cluster. A shared file system will decrease performance for all page loads.

Session data and temporary files are located in "tmp" + "sess" or "/var/lib/ldap-account-manager/tmp" + "/var/lib/ldap-account-manager/sess".

Appendix H. Troubleshooting

Reset configuration password

Server profiles

The password for the server profiles can be reset using the master configuration password. Open LAM configuration -> Edit server profiles ->Manage server profiles for this.

Main configuration

File system storage

In case you lost your master configuration password you need to manually edit the main configuration file (config.cfg) on the file system.

1. Locate config.cfg: On DEB/RPM installations it is in **/usr/share/ldap-account-manager/config** and for tar.bz2 in **config** folder.

2. Locate the "password" line in the file

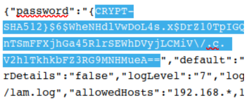
3. Remove the password line in the configuration file

When you open LAM's start page you will now be asked to set a new password.

Database storage

Use a database admin tool (e.g. MySQL Workbench/phpMyAdmin) and connect to your database. Locate the table "main_configuration" and the row with value "config" in column "name". You will now need to edit this value which is in JSON format.

There is an entry "password" followed by a colon. Edit now the value in quotes that comes directly after. Enter your new password in clear text there. Do not remove the quotes.



```
{"password":"{CRYPT-
SHA512}$6$WheNHdlVwDoL4s.x$DrZ10TpIGQ
nTSmFFXjhGa45RlrSEWhDVyjLCMiV\/.c.
V2hlTkhkbFZ3RG9MNHMueA==","default":"
rDetails":"false","logLevel":"7","log
/lam.log","allowedHosts":"192.168.*,1
```

You can now login using your new password. Set the password once again via GUI in main configuration settings. This will then put again a hash value in the config.cfg file.

Reset IP restriction

If you entered a wrong value into the allowed IP list then LAM might lock you out of the system. You can reset the IP list like this.

File system storage

You need to manually edit the main configuration file (config.cfg) on the file system.

1. Locate config.cfg: On DEB/RPM installations it is in /usr/share/ldap-account-manager/config and for tar.bz2 in config folder.

2. Locate the "allowedHosts" entry in the file

3. Remove the line starting with "allowedHosts: "

Now you can edit the IP list again via LAM GUI.

Database storage

Use a database admin tool (e.g. MySQL Workbench/phpMyAdmin) and connect to your database. Locate the table "main_configuration" and the row with value "config" in column "name". You will now need to edit this value which is in JSON format.

There is an entry "allowedHosts" followed by a colon. Now, remove anything of the value in quotes that comes directly after. Do not remove the quotes.

Now you can edit the IP list again via LAM GUI.

Functional issues

Size limit

You will get a message like "LDAP sizelimit exceeded, not all entries are shown." when you hit the LDAP search limit.

- OpenLDAP: See the OpenLDAP settings to fix this.
- 389 server: set nsslapd-sizelimit in cn=config (may also be set per user)
- other LDAP servers: please see your server documentation

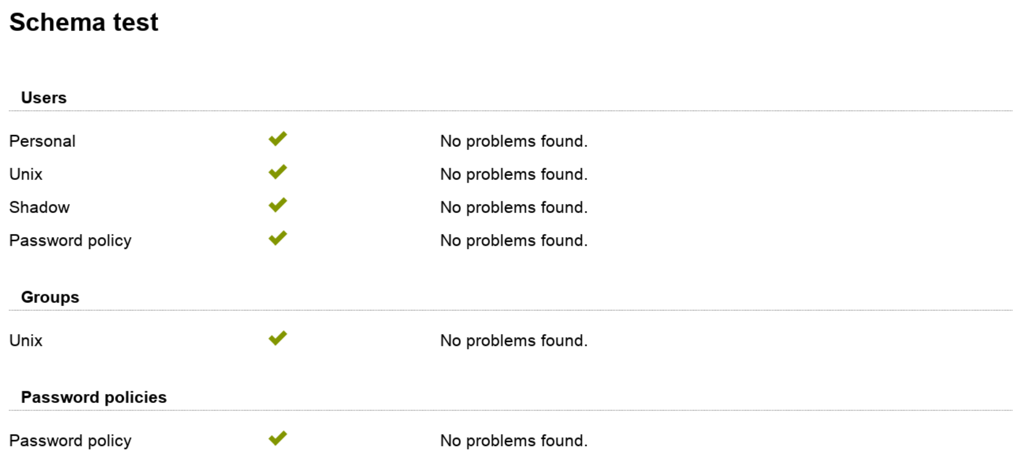
Invalid syntax errors:

If you get any strange errors like "Invalid syntax" or "Invalid DN syntax" please check if your LDAP schema matches LAM's requirements.

Schema test:

This can be done by running "Tools" -> "Tests" -> "Schema test" inside LAM.

If there are any object classes or attributes missing you will get a notice. See LDAP schema files for a list of used schemas. You may also want to deactivate unused modules in your LAM server profile (tab "Modules").



Schema test

Users		
Personal	✓	No problems found.
Unix	✓	No problems found.
Shadow	✓	No problems found.
Password policy	✓	No problems found.
Groups		
Unix	✓	No problems found.
Password policies		
Password policy	✓	No problems found.

LDAP Logging:

If your schema is correct you can turn on LDAP logging to get more detailed error messages from your LDAP server.

OpenLDAP logging:

- slapd.conf: In /etc/ldap/slapd.conf turn logging on with the line "loglevel 256".
- slapd.d: In /etc/ldap/slapd.d/cn=config.ldif please change the attribute "olcLogLevel" to "Stats". Please add a line "olcLogLevel: Stats" if the attribute is missing.

After changing the configuration please restart OpenLDAP. It usually uses /var/log/syslog for log output.

PHP logging

Sometimes it can help to enable PHP logging inside LAM. You can do this in the logging area of LAM's main configuration. Set the logging option to "all" and check if there are any messages printed in your browser window. Please note that not every notice message is an error but it may help to find the problem.

Performance issues

LAM is tested to work with 10000 users with acceptable performance. If you have a larger directory or slow hardware then here are some points to increase performance.

The first step is to check if performance problems are caused by the LAM web server or the LDAP server. Please check which machine suffers from high system load (CPU/memory consumption).

High network latency may also be a problem. For large installations please make sure that LAM web server and LDAP server are located in the same building/server room.

If you run LAM on multiple nodes (DNS load balancing/hardware load balancer) then also check the clustering section.

LDAP server

Use indices

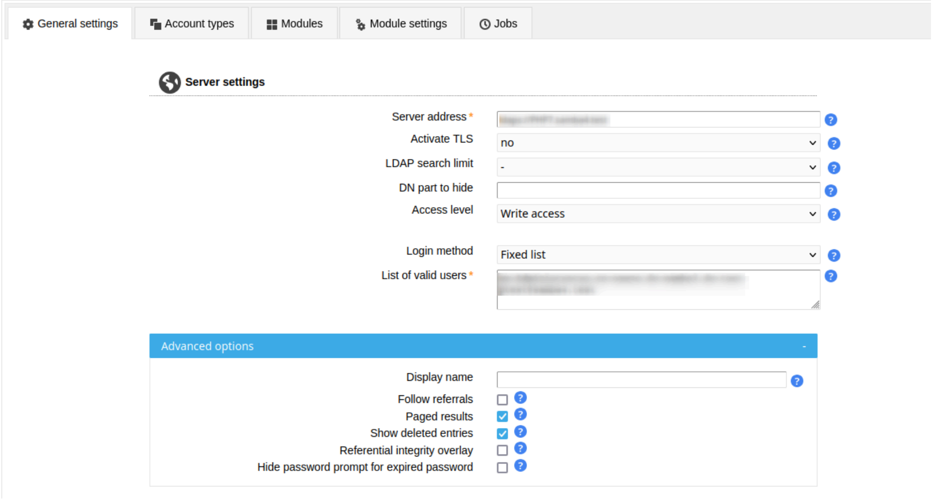
Depending on the queries it may help to add some more indices on the LDAP server. Depending on your LDAP software it may already suggest indices in its log files. See here for typical OpenLDAP indices.

Reduce query results by splitting LDAP management into multiple server profiles

If you manage a very large directory then it might already be separated into multiple subtrees (e.g. by country, subsidiary, ...). Do not use a single LAM server profile to manage your whole directory. Use different server profiles for each separated LDAP subtree where possible (e.g. one for German users and one for French ones).

Limit query results

LAM allows to set an LDAP search limit [general_settings] for each server profile. This will limit the number of entries returned by your LDAP server. Use with caution because it can cause problems (e.g. with automatic UID generation) when LAM is not able to read all entries.



Server settings

Server address * [redacted]
Activate TLS: no
LDAP search limit: -
DN part to hide:
Access level: Write access

Login method: Fixed list
List of valid users * [redacted]

Advanced options

Display name:
Follow referrals ☐
Paged results ☑
Show deleted entries ☑
Referential integrity overlay ☐
Hide password prompt for expired password ☐

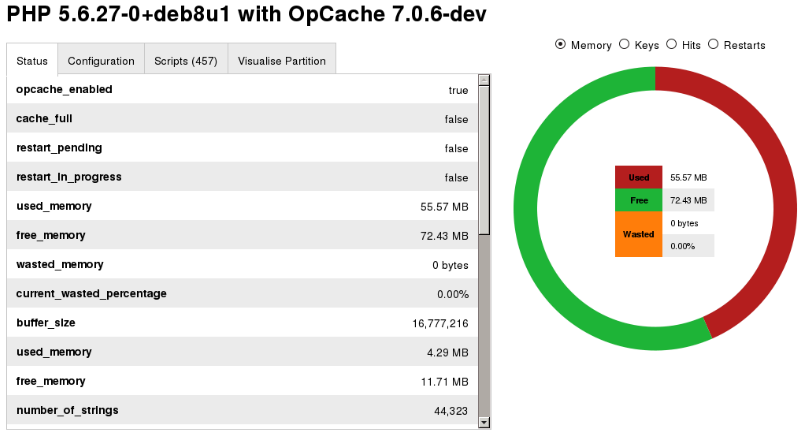
LAM web server

Install a PHP accelerator

There are tools like OpCache [http://php.net/manual/en/book.opcache.php] (free) or Zend Server [http://www.zend.com/en/products/server/] (commercial) that provide caching of PHP pages to improve performance. They will reduce the time for parsing the PHP pages and IO load.

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

OpCache statistics can be shown with opcache-status [https://github.com/rlerdorf/opcache-status].


PHP 5.6.27-0+deb8u1 with OpCache 7.0.6-dev

opcache_enabled	true
cache_full	false
restart_pending	false
restart_in_progress	false
used_memory	55.57 MB
free_memory	72.43 MB
wasted_memory	0 bytes
current_wasted_percentage	0.00%
buffer_size	16,777,216
used_memory	4.29 MB
free_memory	11.71 MB
number_of_strings	44,323

Used	55.57 MB
Free	72.43 MB
Wasted	0 bytes 0.00%