



# Labfolder Server Installation Manual

V2.4.0

Updated April 20, 2021

# Table of Contents

|   |           |
|---|-----------|
| <b>Table of Contents</b>                            | <b>2</b>  |
| <b>New in version 2.4.0</b>                         | <b>4</b>  |
| <b>Requirements for local installation</b>          | <b>5</b>  |
| Hardware and software requirements                  | 5         |
| Labfolder Client Requirements                       | 5         |
| General infrastructure of the Labfolder application | 6         |
| Backup and recovery                                 | 6         |
| Long-term archiving of Labfolder data               | 7         |
| High availability, redundancy and failover          | 8         |
| Update of the operating system and components       | 8         |
| Capacities and Scaling                              | 8         |
| Migrating Labfolder                                 | 9         |
| External connections                                | 9         |
| Log management & rotation                           | 9         |
| <b>Installing and updating Labfolder</b>            | <b>10</b> |
| 1. Install mysql                                    | 10        |
| 2. Install Docker                                   | 11        |
| 3. Install Labfolder                                | 11        |
| <b>Configure Labfolder</b>                          | <b>11</b> |
| Setting the default domain                          | 11        |
| Connecting your MySQL database                      | 12        |
| Set your timezone                                   | 12        |
| Connecting your mail account                        | 12        |
| Customize system mails                              | 13        |
| Configure server event logging                      | 14        |
| Setting the maximum upload file size                | 14        |
| Configure default user and group settings           | 14        |
| Global control of data safeguarding                 | 15        |

|   |           |
|---|-----------|
| Terms of use and privacy statement                  | 16        |
| LDAP Authentication                                 | 17        |
| Activate LDAP                                       | 17        |
| Secure LDAP Connection                              | 18        |
| LDAPS   | 18        |
| LDAP with TLS                                       | 18        |
| Authenticate with DN                                | 19        |
| Authenticate with Attribute                         | 19        |
| Anonymous Search                                    | 20        |
| Search User   | 20        |
| Update existing users after LDAP activation         | 21        |
| Installing certificates for secure LDAP connections | 21        |
| Configuring usage reporting                         | 23        |
| <b>Configure Labregister</b>                        | <b>23</b> |
| Configure maximum number of attributes              | 23        |
| Configure maximum number dropdown options           | 23        |
| <b>Run Labfolder</b>                                | <b>24</b> |
| <b>Update Labfolder</b>                             | <b>24</b> |
| <b>Activating Apps</b>                              | <b>25</b> |
| XHTML   | 25        |
| Dropbox   | 26        |
| <b>Autostart Labfolder</b>                          | <b>27</b> |
| <b>Set up https via nginx reverse proxy</b>         | <b>28</b> |

## New in version 2.4.0

- The database schema has been updated to allow for non-blocking backups. Additional information has been added in the chapter [Backup and recovery](#).
- A bug has been fixed where user passwords were retained in a table when LDAP was activated. Now, passwords are never stored in Labfolder when LDAP is activated, with the consequence that users have to reset the password when LDAP is deactivated. More details can be found in the chapter [LDAP Authentication](#)

# Requirements for local installation

## Hardware and software requirements

For the local installation of Labfolder, the following requirements have to be met:

Hardware:

- Min. 16 GB RAM.



Please note that the Labfolder server will not start when the minimum requirements for RAM availability are not met.

- Hard drive min. 500 GB (higher data volumes require the installation of more hard drive space)
- Min. 2 CPUs 2.6 GHz or faster

Software :



Linux Operating System that is compatible with the latest version of Docker CE (min. 18.09-ce), we recommend a recent version Ubuntu OS.

- Docker CE (min. version 18.09) for running the Labfolder application package on physical or virtual servers
- MySQL database, version 5.7.x latest
- Mysql Tools (mysql, mysqldump)
- Connection to e-mail server with SMTP protocol and an e-mail account for the sending of notifications to users (optional)
- static IP address
- for remote installation, updates and maintenance: remote access (via SSH, root privileges not required)

Updates for the Labfolder software will be distributed for self-installation, with the possibility to request remote assistance for the installation. Software updates of the operating system and external software components are within the responsibility of the customer.

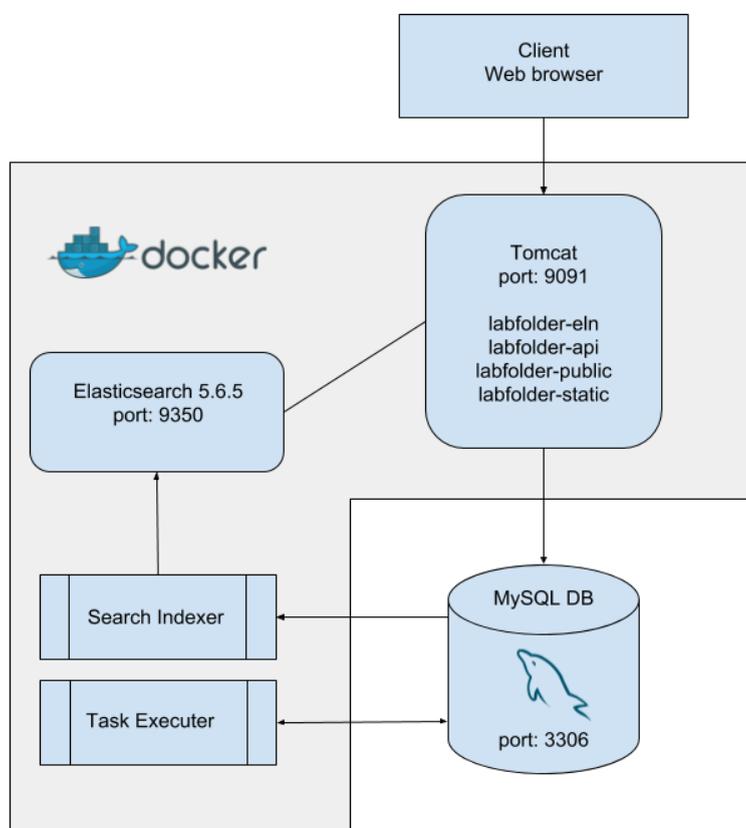
## Labfolder Client Requirements

The Labfolder software and user interface is accessible from any modern web browser (independent of the operating system). The supported browsers are listed on our website: <https://www.labfolder.com/browser-support/>

## General infrastructure of the Labfolder application

Generally, the Labfolder application consists of two parts: A Docker container containing all components of the Labfolder application and a MySQL database. This architecture and the underlying licensing terms make it necessary to pre-install Docker and to either install a MySQL database on the same server or give the Labfolder application access to a database server.

The high-level architecture of Labfolder and its main components is summarized in the graph below:



## Backup and recovery

For the backup and recovery of all data in the Labfolder application, mysqldump can be used. For a detailed overview on how to set-up mysqldump for backup and recovery, please refer to the official documentation at <http://dev.mysql.com/doc/refman/5.7/en/mysqldump.html>. Please note that the contractual liability of Labfolder in case of data loss is limited to the data loss that would have occurred in case of backups being made on a daily basis.

Non-blocking MySQL backups can be initiated with the command

```
$ mysqldump --single-transaction --set-gtid-purged=OFF
```

 When restoring a Labfolder database backup, please note that a database needs to be re-created using the mysql command

```
$ mysql -u root -p -Bse "CREATE SCHEMA labfolder"
```

prior to restoring the database from the database dump. This guarantees that there are no additional or duplicate tables in the schema, which may happen after i.e. in case schema migration could not be completed successfully.

## Long-term archiving of Labfolder data

Generic hard drives, as they are being used in the most common commercial server infrastructures, usually have a life cycle of several years, depending on the manufacturer. In order to prevent data loss in the event of hardware failure, it is thus recommended to create daily backups and consider a regular dump of the Labfolder database to a long-term storage system.

We recommend the installation of a redundant storage hardware (i.e. RAID) and to implement regular backups of the Labfolder database. In such a setup, defective hard drives can be replaced without causing any data loss. Additionally, this set-up allows the secure storage of data beyond the life cycle of a singular hard drive.

The Labfolder installation can also be connected to a database server, through which updates can be managed as well.

While in such a setup, data can be kept in Labfolder for long-term archiving, it is desirable that for long-term storage, specific data can be moved to a long term storage archive in order to provide an economic storage of larger data quantities and to avoid an overflow of the Labfolder database.

For the extraction of Labfolder data from the database and the subsequent long-term archiving, the following procedure can be applied:

1. Scientists or Principal Investigators which are responsible for the management and archiving of scientific data can extract the relevant data via Labfolder's XHTML export. This export allows the extraction of specific data which belong to specific responsible persons or projects.
2. After export, scientists or principal investigators receive a .zip archive which contains all the exported lab notebook entries in html format which provides an offline read-only version of the exported data, together with a folder structure containing all relevant files and thus provides a complete export of all relevant data.
3. The exported .zip archive can be used for long-term archiving on a dedicated long term archiving system.
4. After archiving, scientists or principal investigators can delete the data from the Labfolder database.

Details on the XHTML export can be found in the Labfolder user manual, which is available on our website at <https://www.labfolder.com/manuals-tutorials/>

## High availability, redundancy and failover

High availability and failover of the Labfolder application can be established both on the database level and on the application level.

For high availability and failover on the database level, we recommend using database replication, which also helps to prevent data loss in case of database failure: <https://dev.mysql.com/doc/refman/5.7/en/replication.html>.

Replicated databases can be switched during failover to provide a continuous service of the database functionalities: <https://dev.mysql.com/doc/refman/5.7/en/replication.html>

On the application level, a secondary (virtual) server can be cloned by setting up a copy of the docker container in the same configuration to instantaneously replace the primary application in case of failure.

Note that for the simultaneous running of two Labfolder application servers with a link to the same database (i.e. managed by a load balancer which can, for example, be provided by *nginx*), asynchronous behaviour may be observed at the level of the Search Indexer and the Task Executor, which may result in asynchronous search behaviour and double execution of notifications and tasks.

## Update of the operating system and components

If an update of the operating system or its components like Docker and the MySQL database is required, we recommend stopping the application and proceeding with the update as explained in the [update instructions](#). After the update, the Labfolder installation needs to be restarted.

In case of a database update, we recommend creating a backup of the database before the update.

Without the time required for the database update, an update of Labfolder or external components usually requires only a few minutes of downtime. User sessions are not terminated during restart, as they are stored in the database, but user activities like i.e. saving might be interrupted during restart. We still recommend informing users well in advance and calculate a generous window of service downtime.

## Capacities and Scaling

On a medium size server as described in the specifications above, the Labfolder applications handles several hundred simultaneous users without effort. For a larger number of simultaneous users, we recommend allowing for more extensive hardware requirements.

On average, an active group of 15 scientists generates below 10 GB of Data per year. This number can increase if automated methods or the API are used for

regular bulk upload of data. User quota and maximum upload file size can be controlled by the administrator.

Should the database size become an issue, sharding of the database and setting up parallel installations is possible as well, since the Labfolder license model does not restrict the number of Labfolder server instances you are running.

## Migrating Labfolder

When migrating a Labfolder database from one application or another, always make sure that

- Both Labfolder versions updated to the same version
- Both MySQL 5.7 versions are updated to the same version
- Both Labfolder applications with a connected database have been initialized at least once (with the command  \$ ./labfolder.sh start)

## External connections

If not configured otherwise, the Labfolder application might attempt to make connections to the following external services:

**Google** - if `ACTIVE_USER_REPORT_USE_DEFAULT_MAIL_CLIENT=false`, Labfolder will attempt to connect to gmail in order to send usage reports to Labfolder via port 25. If your contractual agreement requires the sending of regular usage reports, make sure that either port 25 is open for the Labfolder application or you use your own mail account for sending user reports by setting `ACTIVE_USER_REPORT_USE_DEFAULT_MAIL_CLIENT=true`.

**Amazon S3** - if `EXPORT_DOCUMENT_REPOSITORY_TYPE=amazonS3`, Labfolder will attempt to connect to Amazon S3 for the storage of temporary XHTML Export files. In order to store export files locally, set `EXPORT_DOCUMENT_REPOSITORY_TYPE=fileSystem` which will prevent connections to Amazon S3.

**Cloudflare** - Labfolder will attempt a connection to cloudflare for the accelerated pre-loading of web fonts and web scripts. Currently, these resources are not available offline, thus, a connection to cloudflare is necessary to pre-load external resources and allow a flawless display of the user interface. No personal or user data is sent to cloudflare at any time.

## Log management & rotation

The Labfolder application writes log files to the system hard drive to document system behaviour and anomalies. Log management and rotation, however, is not performed by the Labfolder application, which may result in the accumulation of a large number of log records which may ultimately occupy all storage space on the Labfolder server. We thus recommend to install *logrotate* and set it up according to your organisation's requirements for keeping available log records following the [instructions for your individual operating system](#).

# Installing and updating Labfolder

## 1. Install mysql

Download and [install mysql-server](#) v5.7 on the same or on a different server you want Labfolder to run from <https://dev.mysql.com/downloads/mysql/5.7.html> . In case you do not want Labfolder to use the root account, you have to create an account for Labfolder. In case Labfolder will be installed on a different server, you have to make sure to enable remote access to mysql.

If you would like to store all information in the database on a different drive or partition, you need to set the datadir of the mysql-server accordingly during installation following the instructions given in the documentation of mysql here: <https://dev.mysql.com/doc/refman/5.7/en/data-directory-initialization.html>

If you would like to change the data directory (i.e. the location, drive or partition where Labfolder is stored) after the installation, instructions vary depending on the operating system used. For Ubuntu, instructions can be found as follows:



Ubuntu:

<https://www.digitalocean.com/community/tutorials/how-to-move-a-mysql-data-directory-to-a-new-location-on-ubuntu-18-04>

 Please note that Labfolder requires MySQL 5.7 and does not support MS SQL, MySQL 8.x or MariaDB.

 In order to install MySQL 5.7.x instead of MySQL 8.x on Ubuntu 20.04 (Focal Fossa), please follow the instructions [here](#).

After installation of MySQL, a database for Labfolder needs to be created with the following command:

```
$ mysql -u root -p -Bse "CREATE SCHEMA labfolder"
```

Please note that the [max allowed packet](#) size of your MySQL database needs to be increased to allow the upload of large files. The Labfolder application can set additional limits to the maximum file size, we thus recommend setting the variable to a high value, i.e. `max_allowed_packet=500M` (500 MB) when setting up the MySQL server. For more information on how to set the `max_allowed_packet` size, visit <https://stackoverflow.com/questions/8062496/how-to-change-max-allowed-packet-size>

 In MySQL 5.7, it may be necessary to switch the authentication method from `auth_socket` to `mysql_native_password`. Detailed instructions on how to change the authentication method can be found [here](#).

## 2. Install Docker

1. Install Docker CE according to these instructions:



Ubuntu: <https://docs.docker.com/install/linux/docker-ce/ubuntu/>



**On Linux**, follow the [post-installation instructions for docker](#) that allow you to run docker as a non-root user.

2. Reboot your system.

## 3. Install Labfolder

1. Download labfolder.zip from the download link you received together with your license and put it in the directory in which you would like your Labfolder installation files to be in. You can use the command `$ wget "download link"` as well.
2. Extract Labfolder.zip. You might need to install unzip first.
3. You can verify your Labfolder installation by running the command



```
$ ./labfolder.sh verify
```

The script will return OK if the hash sum of your download has been verified.

## Configure Labfolder

Configurations in Labfolder can be made by editing the `server.cnf` file in the Labfolder directory.

### Setting the default domain

The default domain needs to be set for correct link generation in mails (for instance password recovery) in the section `#Network settings`.

1. Set `DEFAULT_DOMAIN` to the DNS or IP address of your server.
2. Set `DEFAULT_HTTP_PROTOCOL=` either to `https://` or to `http://` depending on the protocol you are using.

Please note that this configuration only changes the placeholder in system links and messages Labfolder sends and does not configure the actual protocol of the Labfolder server. If you would like to encrypt the data in transit, follow the instructions for [setting up https via reverse proxy](#).

The correct setting of this parameter is necessary for password recovery and data exports to work properly.

## Connecting your MySQL database

Parameters for connecting your MySQL database are found in the section `#JDBC Properties` in the `server.cnf` file.



**Linux:** If your mysql is not installed on the same server as Labfolder, replace `localhost` in `JDBC_DATABASE_URL` with the IP or DNS of your MySQL server. If you would like to establish a secure connection to your MySQL server, please follow the guidelines listed in the standard documentation of MySQL: <https://dev.mysql.com/doc/refman/5.7/en/group-replication-secure-socket-layer-support-ssl.html>

- Change `JDBC_USERNAME` to the mysql-username you want to use.
- Change `JDBC_PASSWORD` to the password of your username

## Set your timezone

In order for your Labfolder server to display correct server times in the ELN and to allow for the selection of time zones relative to the server time within the application, the timezone of your server needs to be set in the section `#JDBC Properties` in the `server.cnf` file.

Set the variable `JDBC_SERVER_TIMEZONE` to the timezone that you would like to set for your server. The value set for `JDBC_SERVER_TIMEZONE` must follow the nomenclature as listed in the column `TZ` in the list of tz database timezones:

[https://en.wikipedia.org/wiki/List\\_of\\_tz\\_database\\_time\\_zones#List](https://en.wikipedia.org/wiki/List_of_tz_database_time_zones#List)

To see which timezone your MySQL database is currently using, run the command

```
cat /etc/timezone
```

on your server.

## Connecting your mail account

To connect a mail account to the Labfolder application for password retrieval, messaging and usage reporting, change the parameters in the `#Mail client properties` section as described below.



Please note that Labfolder uses default parameters for all variables and will attempt to connect to the Labfolder mail servers and send mails with the address [system@labfolder.com](mailto:system@labfolder.com) if variables are not set in the `#Mail client properties` section. Thus, you need to remove the `#` symbol

from all variables in this section if you want to connect your own account and set the parameters accordingly or leave them blank.

1. Remove the # symbol in front of all lines in the paragraph when connecting a mail account
2. Set the parameter `MAIL_STARTTLS=true` if you are using STARTTLS as authentication encryption, otherwise, comment it out by placing a # symbol in front of the line
3. Set the parameter `MAIL_AUTHENTICATION_ENABLE=true` if your mail server requires authentication, otherwise, comment it out by placing a # symbol in front of the line
4. Enter the URL of your mail server behind the `MAIL_HOST=` parameter
5. Set the `MAIL_PORT=` parameter to the active port of your mail server, default is 25 for *STARTTLS*
6. Set the `MAIL_USERNAME=` parameter to the username required for login, if no login is required, comment it out by placing a # symbol in front of the line
7. Set the `MAIL_PASSWORD=` parameter to the password required for login, if no login is required, comment it out by placing a # symbol in front of the line
8. Set the `MAIL_EMAIL=` to the email address your connected account is using.

Please note that the connected mail account needs to have the permission to pass the firewall if support requests and usage reports shall be sent to the Labfolder team. Usage reports can be disabled separately.

## Customize system mails

The Labfolder system uses a repository of mail templates for sending mails after registration, after being invited to a group, for password retrieval and more. These mail templates are located in the folder *Labfolder/files/mail*.

For each mail template, there are up to three files:

1. A `.html` file containing the HTML version of a mail
2. A `.txt` file containing the text version of the mail, which is used as fallback if HTML is disabled
3. A `.subject` file containing the email subject in text format.

Please note that for editing of an email template, edits have to be made to all files to be reflected in both subject and HTML (if available) and text versions of a file.

Placeholders in curly brackets (i.e. `{0}`, `{1}` etc.) are template-specific placeholders for variables like mail address, name, url etc. We recommend that you leave these placeholders unchanged when editing email templates.

- ⚠ Please note that when updating an existing installation, you will need to copy the files in the Labfolder/files/mail folder from the update package to the same folder in your Labfolder directory.

## Configure server event logging

In the section `#Server Event logging section`, set `LOG_TO_FILE=true` to enable logging of server events to the `labfolder/Files/*` folder. We recommend enabling event logging for a more detailed error reporting.

## Setting the maximum upload file size

To configure the maximum size users can upload to the Labfolder database, in the section `#Maximum upload file size`, set the `FILEUPLOAD_MAXUPLOADSIZE=` to the according size in bytes (default is 25000000).

- ⚠ Please note that when configuring a proxy via *nginx*, the maximum file size for upload defaults to 2 MB. It might be necessary to adjust the maximum file size in *nginx* following the instructions on this website: <http://stackoverflow.com/questions/26717013/how-to-edit-nginx-conf-to-increase-file-size-upload>

- ⚠ Please note that the [max allowed packet](https://stackoverflow.com/questions/8062496/how-to-change-max-allowed-packet-size) size of your MySQL database might further limit the maximum upload file size. You can adjust the `max_allowed_packet` size via editing the `my.cnf` file: <https://stackoverflow.com/questions/8062496/how-to-change-max-allowed-packet-size>

## Configure default user and group settings

To control user and group settings, edit the `#User and group control` section as follows:

1. Set `DEFAULT_GROUP_SIZE` to the maximal number of seats a group should have when it is created. The fallback in case of a missing configuration variable is 3.
2. Set `DEFAULT_GROUP_TYPE_MAXI=true` if a new group should be created as maxi group. MAXI groups have advanced sharing and admin options.
3. Set `DEFAULT_USER_STORAGE` to the number of bytes that a newly created user should have to store his data. The default is 3 GB. Users will be unable to upload files when the quota set in this variable has been reached and will get an error warning. Users will still be able to add text and other content.

- ⚠ Please note that the `DEFAULT_GROUP_SIZE` needs to be increased and the `DEFAULT_GROUP_TYPE_MAXI` needs to be set to `true` if large groups with advanced sharing and admin options should be available.

If `DEFAULT_GROUP_SIZE` is set to a value  $< 1$ , the creation of new groups is not possible. This can be used to prevent the creation of groups by anyone on the server and i.e. only allow Principal Investigators the creation of groups during server set-up and in controlled intervals. As an IT administrator, you can also create groups yourself and ‘transfer’ them to Principal investigators later. For details, refer to the Labfolder admin manual.

The default user and group settings can be used to control the size and mode of newly created groups on a running system, the settings of existing groups remain unchanged.

To change the group size and group type of all groups which are already existing, follow these steps:

1. Log on to the MySQL database via `mysql -u<user> -p<password>`, followed by `use labfolder`
2. Execute the SQL statement `UPDATE 'group' SET 'type' = '2'` to set the group type of the existing group to MAXI.
3. Execute the SQL statement `UPDATE 'group' SET 'seats' = '<group size>'` to set the seat number of the existing groups to `<group size>`

## Global control of data safeguarding

Content can be hidden from entries, and projects and templates can be either hidden or terminally deleted. The terminal deletion of content in Labfolder groups can be prevented by group admins (see also the section ‘Data safeguarding’ in the [Labfolder admin manual](#)).

Data safeguarding preventing the terminal deletion of data can be globally activated for the entire server by setting the variable in the section `#User` and `group control`:

When `FEATURE_GLOBAL_PREVENT_DELETE_CONTENT=true`, data safeguarding is globally activated and cannot be deactivated by group admins. Additionally, groups and private projects cannot be deleted when global data safeguarding is activated. The default value is false, with global safeguarding being deactivated.

Upon global activation of data safeguarding, user data is not deleted when users close their accounts.

Instead, the account is deactivated and no longer accessible to the user, but the data can be retrieved by the administrator any time with the following steps:

1. Connect to the mysql server and authenticate.

## 2. Run the following command:

```
USE <database-name>;  
UPDATE `user` SET  
`email`='<email-address-you-can-access>', `status`=0  
WHERE `email` LIKE  
'||%||<email-address-of-deleted-account>';
```

Where `<email-address-you-can-access>` is an email address you have access to and `<email-address-of-deleted-account>` is the email address with which the deleted account is registered.

3. Go to the notebook login page and follow the "reset password" link to reset the password for the inserted email address `<email-address-you-can-access>` specified in the previous step.
4. You will get an email providing a link to assign a new password.
5. After logging in to the account with the new credentials, you can change the email address in the settings. Please make sure to store the credentials especially when changing the email to an invalid address.



Please note that restoring user data as described above is only possible when global data safeguarding is activated.

Please keep in mind that when activating global data safeguarding, data cannot be deleted from the database, which will lead to a continuing increase in database size.

## Terms of use and privacy statement

On the registration page of Labfolder, URLs for the terms of use which have to be accepted can be customized in the section `#Terms and Privacy links`:

`TERMS_OF_USE_LINK=` for terms of use and

`PRIVACY_LINK=` for privacy information

The default URLs listed above will be redirecting users to generic pages on the Labfolder website which provide general information on the use of Labfolder.

## LDAP Authentication

-  Please note that once the LDAP authentication feature is turned on, only users which are registered on the LDAP server will be able to create accounts for Labfolder or log on to the system.

### **Activate LDAP**

In order for Labfolder to work with an LDAP server a couple of environment variables have to be specified in the # LDAP Authentication section in the server.cnf file.

1. To turn on LDAP authentication include the flag **FEATURE\_LDAP\_AUTHENTICATION=true**
2. Specify the URL used to connect to your LDAP server. This should include the protocol and the port. Two examples are listed below:

```
LDAP_URL=ldap://255.255.255.255:389
```

OR

```
LDAP_URL=ldap://server.company.com:389
```

3. Specify the root distinguished name (DN) of your directory, e.g. **LDAP\_BASE=dc=company,dc=com**

-  Please note that when you deactivate LDAP on your server, all users must request a password reset in order to be able to log on since the LDAP password is not stored in the Labfolder database when LDAP is activated.

## Secure LDAP Connection

There are two ways to configure a secure SSL/TLS connection to your LDAP server.

### 1. LDAPS

Using the LDAPS protocol does automatically apply a secure connection to the server. It can simply be used by setting it up in the `LDAP_URL` variable with this protocol and the corresponding port:

```
LDAP_URL=ldaps://255.255.255.255:636
```

This set, the basic LDAP TLS feature must be disabled, since otherwise the Labfolder server would cause an error by trying to do two SSL handshakes within one request:

```
LDAP_IS_TLS_ENABLED=false
```

### 2. LDAP with TLS

To use the default LDAP protocol with a secure connection, you can use the LDAP TLS feature. To apply this, you want to use the default LDAP protocol in the `LDAP_URL` and set the TLS feature activated:

```
LDAP_URL=ldap://255.255.255.255:389
```

```
LDAP_IS_TLS_ENABLED=true
```

## Authenticate with DN

The most basic way for authentication against the LDAP server is the bind by DN. After you defined the `LDAP_BASE` with the domain components before, you need to define the allowable pattern(s) of a DN relative to the root DN.

Multiple patterns must be separated by a semicolon. Do not include the root DN. The username will be inserted at the position where `{0}` occurs in the pattern.

Here are two possible examples of use of `LDAP_USER_DN_PATTERNS`

1. Single pattern: all users in Organizational Unit *development* can authenticate

```
LDAP_USER_DN_PATTERNS=cn={0},ou=development
```

2. Multiple pattern: all users in Organizational Units *development* and *marketing* > *sales* can authenticate

```
LDAP_USER_DN_PATTERNS=cn={0},ou=development;cn={0},ou=sales,ou=marketing
```

## Authenticate with Attribute

Often the users are not provided with their CN as principal to authenticate. Instead another attribute attached to the LDAP object might be used, for example `uid`, `mail` or `sAmAccountName`.

To enable authentication by any unique attribute, you can use the Attribute Search feature.

- Enable the attribute search by setting the feature flag to `true`:

```
LDAP_IS_ATTRIBUTE_SEARCH_ENABLED=true
```

- Specify the attribute name that the user is supposed to use, using `sAmAccountName` attribute in the example:

```
LDAP_ATTRIBUTE_SEARCH_NAME=sAmAccountName
```

To enable the search for a user with matching attribute value in the LDAP tree, you can either use anonymous search, [if enabled](#) on the LDAP server, or a specified search user that is authenticated against the LDAP server.

## 1. Anonymous Search

To enable anonymous search for attributes simply set:

```
LDAP_ANONYMOUS_READ_ONLY=true
```



Anonymous search will enable all users in LDAP to authenticate against the server and therefore create and use an account in Labfolder.

The pattern matching that can be defined in `LDAP_USER_DN_PATTERNS`, as shown in the [DN authentication section](#), is ignored when using the Attribute Search feature!

Use the Search User configuration to further restrict the scope of enabled users.

## 2. Search User

To specify the search user DN and its password, the parameters `LDAP_SEARCH_USER_DN` and `LDAP_SEARCH_USER_PASSWORD` are required:

```
LDAP_SEARCH_USER_DN=CN=search-user,CN=Users,DC=ad,DC=Labfolder,DC=com
```

```
LDAP_SEARCH_USER_PASSWORD=hcraes
```



The search user must have read access only to those user objects in LDAP, that should be enabled to authenticate with Labfolder.

The pattern matching that can be defined in `LDAP_USER_DN_PATTERNS`, as shown in the [DN authentication section](#), is ignored when using the Attribute Search feature! Limit the availability by further restricting the search user ACLs in LDAP if you want to limit access to certain LDAP sub-structures.

## Update existing users after LDAP activation

If you would like to activate LDAP and you already have users which have been managed by the Labfolder user management, you need to update each user in the user table in the MySQL database as follows:

```
UPDATE user SET ldapUsername = 'ldap-login-id-goes-here' WHERE
email = 'user@email-goes.here';
```

Once LDAP is activated, the login screen will ask for a “Login” which is equivalent to the user name in the LDAP directory (ldapUsername) and will validate against the LDAP server that the user exists and that the password entered during login matches the password stored on the LDAP server.

If LDAP is not activated, the login screen will ask for the e-mail (user-email) and the password stored in the user management system of Labfolder.

## Installing certificates for secure LDAP connections

When installed, Labfolder uses the [Mozilla CA certificate store](#) for the validation of root certificates. When using self-signed certificates which do not have a root certificate that is contained in the CA store, you might face issues when trying to connect to external services, i.e. your LDAP server or mail server via an encrypted connection.

In case of certificate errors caused by unknown root certificates, the following error message appears in the logs which are stored in `~/labfolder/Files/tomcat_logs/labfolder-eln-webapp.log`:

```
'XX:XX:XX,XXX ERROR http-nio-9091-exec-8
de.labfolder.eln.context.HandlerExceptionResolverImpl:92 - simple bind
failed: ip-10-0-0-74:636; nested exception is
javax.naming.CommunicationException: simple bind failed: ip-10-0-0-74:636
[Root exception is javax.net.ssl.SSLException: Connection has been
shutdown: javax.net.ssl.SSLHandshakeException:
sun.security.validator.ValidatorException: PKIX path building failed:
sun.security.provider.certpath.SunCertPathBuilderException: unable to find
valid certification path to requested target]

XX:XX:XX,XXX ERROR http-nio-9091-exec-8
de.labfolder.eln.context.HandlerExceptionResolverImpl:93 -
org.springframework.ldap.CommunicationException
```

In order to prevent this error from happening when using self-signed certificates for securing the connection to the LDAP server, Labfolder offers the possibility to install certificates that are not validated by the Mozilla CA certificate store.

Follow these steps:

1. Create the folder `/certificates` in the `/labfolder/Files` directory either manually or by starting the Labfolder application at least once.
2. Hard link (copy/move) the required certificate file(s) into the folder `/labfolder/Files/certificates`.

Please note that soft links will not work.



Certificate files need to have the file ending `.crt`

recommended access right setup for the certificates is `chmod 400` (read access to only the owner)

3. [Restart](#) the Labfolder server

The successful installation of your certificate is recorded by the message

**Certificate was added to keystore**

in the logs in `~/labfolder/Files/supervisord_logs/supervisord.log`.

## Configuring usage reporting

Anonymised usage statistics can be sent to Labfolder via mail every month. These usage statistics contain the number of registered users on your server, the number of active users on your servers (who have triggered an action in Labfolder over the past month) and an activity count per anonymised user ID.

1. Set `CUSTOMER_IDENTIFIER` to the name of your institution.
2. Set `ACTIVE_USER_REPORT_USE_DEFAULT_MAIL_CLIENT=true` if you would like to use the email account that has been configured in the `# Mail client properties` section of the `server.cnf` file. If set to false, Labfolder will attempt to connect an external SMTP server via port 25.



If you do not want Labfolder to send anonymised user statistics, simply set the variable `FEATURE_ACTIVE_USER_REPORT=false`.

When sending user reports with your own email address, you need to make sure the mail account used is able to send emails outside your domain and network. If `ACTIVE_USER_REPORT_USE_DEFAULT_MAIL_CLIENT=false`, make sure that port 25 can be used by Labfolder to contact an external SMTP server.

## Configure Labregister

[Labregister](#), Labforward's Laboratory Inventory Management System is bundled with Labfolder and can be configured via variables in the same `server.cnf` file.

### Configure maximum number of attributes

Attributes in Labregister represent properties of items managed in a category which are visually represented by columns in the category tables.

The maximum number of attributes (or columns in each table) can be set by the variable `MDB_CATEGORY_MAX_ATTRIBUTE_LIMIT`.

### Configure maximum number dropdown options

Users can configure attributes as dropdowns, where they can define each dropdown option. The maximum number of dropdown options for each attribute on the server can be set by the variable `MDB_DROPDOWN_ATTRIBUTE_MAX_OPTIONS_LIMIT`.

## Run Labfolder

1. Open a terminal and `cd` into your Labfolder installation directory.
2. Run

```
🐧 $ ./labfolder.sh start
```

3. You have to start Labfolder if you reboot your server. For automatically launching Labfolder on startup, please follow the instructions described in the chapter [Autostart Labfolder](#).

Note: Labfolder runs on port 9091 over http. We recommend to use *nginx* in case you want to use a SSL certificate.

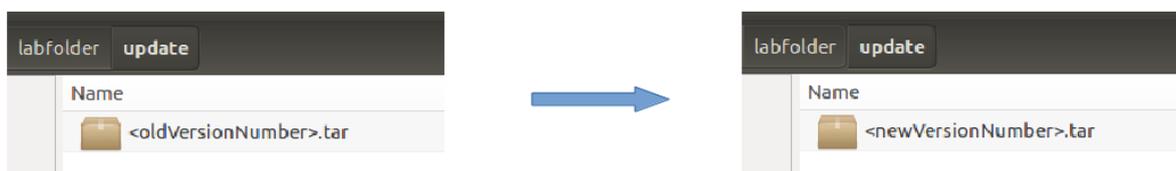
When starting Labfolder, please allow for a few minutes until the Labfolder application can be reached via a web browser.

## Update Labfolder



Please note that it is strongly advised to create a backup of the Labfolder database before every update. If an update has failed and a rollback is required, please make sure to use the backed up version of the database from before the update since schema changes might have occurred during the update. Do not run any previous versions of labfolder against a database that has been going through an update process, whether successful or not.

1. Go to the “update” folder in your Labfolder installation directory and delete all files in there.
2. Download the update from the download link you received together with your license and extract the archive.
3. Replace the „update” folder in your current installation with the one in the downloaded and extracted archive.



4. Go to your Labfolder installation directory and run

```
🐧 $ ./labfolder.sh stop
```

## 5. Replace the

 labfolder.sh

file in your current installation with the one in the downloaded and extracted archive.

6. Replace the `server.cnf` file in your current installation with the one in the downloaded and extracted archive. Variables from the old version of the `server.cnf` file like MySQL credentials can be copied from the old file.
7. Delete all files in the folder `~/labfolder/Files/elasticSearchIndex`
8. If you would like to update the system mails, copy the respective `*.html`, `*.txt` and `*.subject` files from the `/files/mail` directory from the extracted update package into the `/files/mail` directory of Labfolder.
9. For verification of your Labfolder package, copy the file `hash.sha256` from the `/files` directory of the extracted update package into the `/files` directory of Labfolder.
10. Start Labfolder as described in the section “Run Labfolder”.

11. You can verify your Labfolder installation by running the command

 \$ `./labfolder.sh verify`

The script will return OK if the hash sum of your download has been verified.

# Activating Apps

## XHTML

XHTML export provides a quick and easy way for batch export of data in Labfolder. For the default activation of the XHTML App in Labfolder, the values in the `# Xhtml export` section of the `server.cnf` file are set as described below:

```
# Xhtml export
FEATURE_XHTML_EXPORT=true
EXPORT_DOCUMENT_REPOSITORY_TYPE=fileSystem
```

Setting `EXPORT_DOCUMENT_REPOSITORY_TYPE=fileSystem` will result in all files for export being stored in the Labfolder `/files` directory, from which they are automatically deleted after 48 hours.

If you would like to store your XHTML export archives on an Amazon S3 web server, set `EXPORT_DOCUMENT_REPOSITORY_TYPE=amazonS3` and add the following parameters to the `server.cnf` file:

```
AMAZON_S3_EXPORT_DOCUMENT_BUCKET_NAME=<name of AS3 bucket>
AMAZON_S3_EXPORT_DOCUMENT_REGION_NAME=<bucket region on AS3>
AMAZON_ACCESS_KEY=<accesskey>
AMAZON_SECRET_ACCESS=<secret>
```

If you want to deactivate XHTML export, set the value `FEATURE_XHTML_EXPORT=false`.

## Dropbox

Dropbox is a cloud service which allows the storage and syncing of files ([www.dropbox.com](http://www.dropbox.com)). The Labfolder App for Dropbox allows the import of files from Dropbox to Labfolder and the storage of PDF exports from Labfolder in Dropbox. Further information about the Dropbox App can be found in the user manual, which can be downloaded from our website: <https://www.labfolder.com/manuals-tutorials/>.

To activate the Dropbox App, in the #Dropbox section of the `server.cnf` file, set the feature flag

```
FEATURE_DROPBOX=true
```

Once the App is activated, it becomes visible in the Apps section of Labfolder.



For the use of Dropbox by the users, the Labfolder Standalone Server has to be accessible from the internet.

To set up Dropbox you need a Dropbox Developer Access Key to enable API access. You can create it with any Dropbox account. After creating a Dropbox account create and configure the API access by following these steps:

I. Go to <https://www.dropbox.com/developers/apps/create>

1. Choose an API
  - Dropbox API
2. Choose the type of access you need
  - Full Dropbox
3. Name your app

II. After creation of your app in the Dropbox Developers Section, you can access your Dropbox App settings on <https://www.dropbox.com/developers/apps>

Choosing your app there redirects you to the settings page.

Settings to run with Labfolder:

- In the server.cnf file, copy the "App key" as value for the variable `DROPBOX_CONSUMER_KEY=` and the "App secret" for `DROPBOX_CONSUMER_SECRET=` into the server.cnf file

- In the Dropbox Developers Section for your selected App, for the variable "OAuth 2 Redirect URIs", set up the custom URL of your server as follows:

```
http(s)://<your_server_url>/eln/dropbox/oauthCallback
```

## Autostart Labfolder



We recommend installing an autostart routine for Labfolder with [Supervisor](#), a process control system for UNIX-like operating systems. Follow the procedure below to install and configure Supervisor so that Labfolder is automatically started with every restart of the system. This is helpful to prevent outages during system and maintenance restarts.

### 1. Install supervisor

```
$ sudo apt-get install supervisor
```

### 2. Validate supervisor is up and shows status "Active: active (running)"

```
$ sudo service supervisor status
```

### 3. Add Labfolder startup config

a. Open supervisor configuration with editor of your choice, i.e.:

```
$ sudo nano /etc/supervisor/supervisord.conf
```

b. Add the following block, modified to your needs, in the end of the file:

```
[program:labfolder]
directory=/absolute path to your Labfolder directory>*
command=/absolute path to your Labfolder directory>*/Labfolder.sh start
autostart=true
user=user used to run Labfolder - needs to be able to run docker>*
```

\*replace the [variables in braces](#) according to your installation settings

### 4. Restart the machine and validate Labfolder is auto-started by checking the output of `$ docker ps` showing that the Labfolder-standalone container is running.

# Set up https via nginx reverse proxy



We recommend using nginx for setting up https via reverse proxy. Please follow the instructions below to install nginx on Ubuntu:

1. Install [nginx](#):

```
$ sudo apt install nginx
```

Validate nginx is up and running by accessing your localhost on port 80, which should show the nginx welcome page.

2. Edit the default site config of nginx:

```
$ sudo nano /etc/nginx/sites-available/default
```

SSL example configuration:

```
server {  
    listen 80;  
  
    server_name my.server.address;  
    return 302 https://$server_name$request_uri;  
}  
  
server {  
  
    listen 443 ssl;  
  
    # SSL configuration  
    #  
    ssl on;  
    ssl_certificate </etc/ssl/certs/ssl-cert-snakeoil.pem>*;  
    ssl_certificate_key </etc/ssl/private/ssl-cert-snakeoil.key>*;  
    ssl_session_timeout 5m;  
    ssl_protocols TLSv1.1 TLSv1.2;  
    ssl_session_cache shared:SSL:10m;  
  
    server_name <my.server.address>*;  
  
    location / {  
        proxy_set_header X-Forwarded-Ssl on;  
        client_max_body_size 70M;  
        proxy_set_header Upgrade $http_upgrade;
```

```
        proxy_set_header Connection "upgrade";
        proxy_set_header Host $http_host;
        proxy_set_header X-Real-IP $remote_addr;
    proxy_set_header X-Forwarded-For $proxy_add_x_forwarded_for;
        proxy_set_header X-Forwarded-Proto $scheme;
        proxy_set_header X-Frame-Options SAMEORIGIN;
        proxy_pass http://localhost:9091;
    }
}
```

\* Replace the [variables in braces](#) according to the setting your servers IP/hostname/domain name for value [<my.server.address>](#) and by pointing ['ssl\\_certificate'](#) and ['ssl\\_certificate\\_key'](#) to the locations of your valid SSL certificate files.

### 3. Restart the nginx service:

```
$ sudo service nginx restart
```

Now when accessing the host on port 80, an auto redirect to the secure connection via port 443 is done, where your certificates are in place for secure connection.