UNIVERSITÉ DU LUXEMBOURG

LUCET | LUXEMBOURG CENTRE FOR EDUCATIONAL TESTING

OASYS v3.5

OASYS Manual for Administrators

Version: 1.0

September 1, 2025

Contents

1 Introduction **3**

1.1 About OASYS . . . 3

1.2 Purpose of this Manual . . . 3

1.3 Target Audience . . . 3

2 OASYS Installation **5**

2.1 System Requirements . . . 5

2.1.1 Encryption . . . 6

2.2 Baseline Installer . . . 6

2.3 Installation Procedure . . . 7

3 Overview of OASYS Administration **10**

3.1 Admin Roles and Permissions . . . 10

3.1.1 Superadmin . . . 10

3.1.2 Admin . . . 10

3.1.3 Admin with Elevated Rights . . . 11

3.2 Backend Layout and Navigation . . . 12

3.2.1 Admin and Superadmin Apps . . . 12

3.2.2 Standard Backend User Apps (Overview) . . . 13

4 User Management **15**

4.1 User Groups . . . 15

4.1.1 Creating User Groups . . . 15

4.1.2 Assigning Folder Rights . . . 16

4.1.3 Assigning App Access . . . 20

4.2 User Creation and Authentication . . . 21

4.2.1 Creating Users . . . 21

4.2.2 Authentication Methods . . . 22

4.2.3 User Options and Settings . . . 23

4.3 Logs Analyzer . . . 25

4.3.1 Monitoring User Activities . . . 26

5 System Configuration **28**
5.1 Configuring OASYS . . . 28
5.2 System Variables . . . 28
5.3 System and File System Check . . . 32
5.3.1 System Check . . . 32
5.3.2 File System Check . . . 32
5.4 Custom modules . . . 34
5.5 Maintenance Mode . . . 35

6 Localization **36**
6.1 Adding New Languages . . . 36
6.2 Providing Translations . . . 38

7 Backup and Restore **40**
7.1 Database Snapshots . . . 40
7.1.1 Creating a Backup . . . 40
7.1.2 Restoring from Backup . . . 41
7.2 Full System Backups . . . 42
7.2.1 Creating Full Backups . . . 42
7.2.2 Restoring Full Backups . . . 42

8 System Upgrader **44**
8.1 System Information . . . 44
8.2 Update Notifications . . . 45
8.3 Performing Upgrades . . . 45

Chapter 1

Introduction

1.1 About OASYS

OASYS is a multi-platform and multi-device digital testing and assessment system built around **state-of-the-art web-technologies**. OASYS has been carefully **designed around business processes, following a research-based HCI approach**, thus ensuring optimized user experience.

To assure secure data collections and best-possible service, OASYS offers powerful live monitoring for test administrators. Every response is communicated and logged instantaneously on OASYS servers, which minimizes the loss of data even during potential client side computer crashes.

Speaking of security, OASYS developers undergo regular security training, and OASYS underwent state-of-the-art **penetration testing and code review by external security consultants**.

OASYS collects timestamps of every action, thus making the platform an ideal choice for behavioural analysis and data mining.

A load balancing solution allows for around 20K simultaneous client connections in the current server setup.

Although OASYS has been designed primarily as an online assessment system, the client can also run in an app with a server installation on a laptop and a mobile Wi-Fi access point, thus allowing for digital testing in areas with poor or no internet connection.

Since 2010, OASYS has been **used successfully in the Luxembourg school monitoring programme ÉpStan**. Moreover, since 2014, OASYS is also the platform of choice for student course evaluations and various in-house surveys at the University of Luxembourg.

1.2 Purpose of this Manual

This manual provides administrators with the necessary information to install, configure, manage, and maintain an OASYS installation. It covers system setup, system maintenance, user management, content creation, troubleshooting procedures to keep the application up to date and backup procedures.

1.3 Target Audience

This manual is intended for individuals who want to:

- Install OASYS on a web server.
- Perform administrative tasks on an existing OASYS installation.
- Maintain or extend an existing OASYS installation.

Parts of this manual require knowledge of web server systems and access to the system on which OASYS is hosted.

Chapter 2

OASYS Installation

First, download the OASYS installer from http://oasys.lu/download

2.1 System Requirements

- **Apache Web Server** version **2.4.58** or newer
- **PHP** version **8.2.24** or newer
- **MariaDB** version **10.11.9** or newer
- Php **BCMath** Module
- Php **ZIP** Module
- Php **Zlib** Module
- Php **MBSTRING** Module
- php **PDO** Module
- Php **PDO MYSQL** Module
- Php **CURL** Module
- Php **FILEINFO** Module
- Php **post max** size must be greater than **upload max**
- Php **max_execution_time** must be greater than minimum allowed execution time.

Make sure all necessary PHP extensions are enabled on your server for full functionality. The **OASYS installer will also check for the required settings** during the installation process and notify you of any missing components or misconfigurations.

Important Note

To complete the installation, you must have access to your **database root account**. This is required so that the installer can:

- Create a **new database**
- Set up a **dedicated database user** with the necessary permissions

Make sure you have these credentials ready before starting the installation.

2.1.1 Encryption

For security reasons, OASYS encrypts sensitive data before storing it in the database.

While backend user logins will have hashed passwords, for highest security, other sensitive data such as the password to an LDAP server are encrypted using the OpenSSL library.

Also the passwords for test takers are encrypted before being stored in the database. Since these need to be editable in the editor, respectively exportable, they cannot be hashed.

After installation, no encryption key is defined, and OASYS will generate a random key the first time it tries to read the configuration.

For this reason it is imperative, that **the directory <root folder>/conf/ is writable by the webserver user**.

Be aware that you should **backup** the **file <root folder>/conf/crypt.ini** after it has been generated.Without it, parts of your database will be useless and OASYS will not be able to function properly.

Alternatively, you can also define your encryption key in environment variables, by defining thefollowing variables:

- **oasys_aes_key:** The key (32 bit) written in hexadecimal
- **oasys_aes_iv:** The iv (16 bit) written in hexadecimal

As with the database credentials, you can also define custom names for these variables by **editing the file <root folder>/conf/env.ini** and changing the values as you see fit.

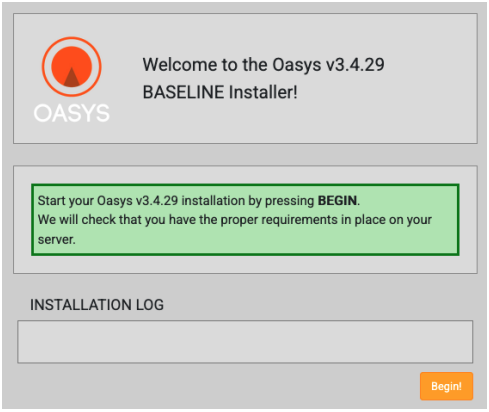
2.2 Baseline Installer

The OASYS installation package comes as a ZIP archive that contains everything needed to get the system up and running on your server.
The Baseline Installer is the installation package for OASYS. After downloading, the installer is uploaded to the web server. The setup is started by accessing the web server directory.
The OASYS installer will guide you step by step through the the setup process, including configuration and database setup.
Keeping the system up to date does not require installing a new version. **A system upgrader is integrated into the backend for performing updates.**

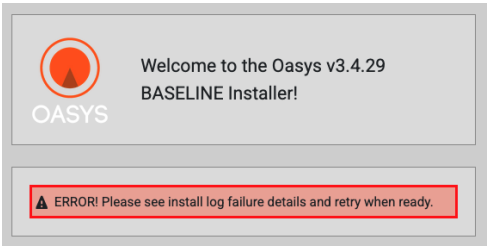
2.3 Installation Procedure

- **Download the ZIP Archive**
  Obtain the OASYS installation ZIP file from the official source or your software provider.
- On your webserver, **create a folder** for the oasys installation.
- **Unpack** the installation archive and **upload** the content to your server folder.
- **Launch the Installer**
  Open your web browser and navigate to the URL where you placed the files. For example: http://yourserver.com/oasys/

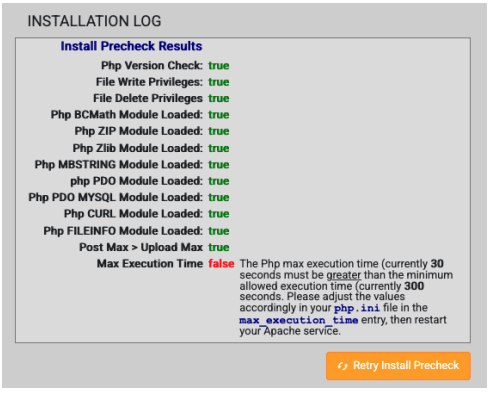
The OASYS installer will guide you through the rest of the setup process, including configuration and database setup.



Click the begin button to start the installation precheck. This will only check the oasys requirements. No changes will be made.

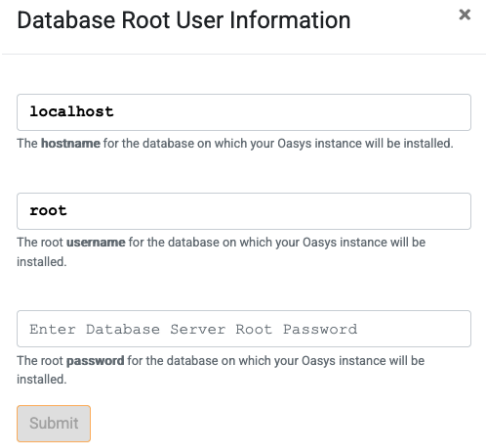


In case, your system does not meet all requirements, you'll see a warning message.



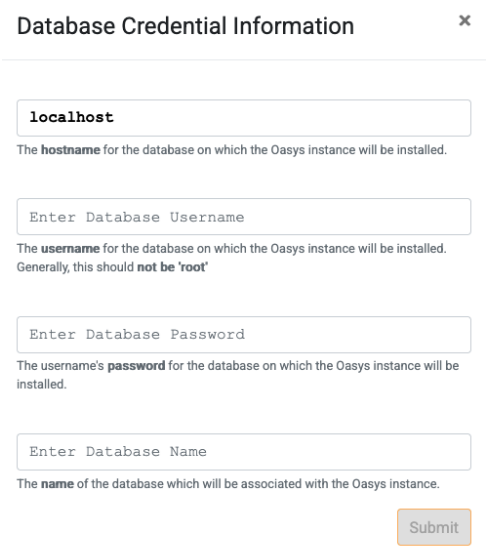
The exact problems are indicated in the log, along with an explanation. Fix them and retry the check. **You will have to restart your webserver to apply the changes made!**

Once the precheck has passed successfully, continue to the **Root Database Credentials**.

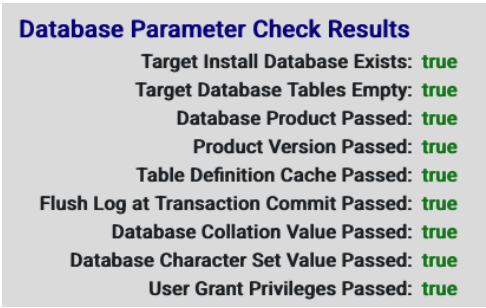


Host and username for the database server are editable.
Be aware, that the user you provide must have the privileges to create a new database and set up a dedicated database user for the OASYS database!

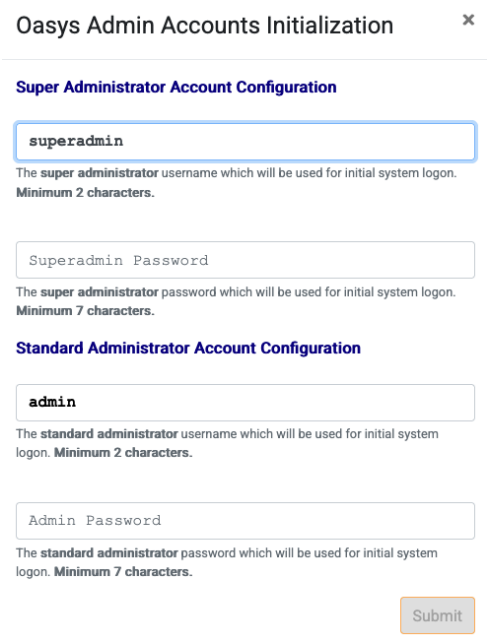
If the user you have provided has the required privileges, click the **User Database Credentials** button.



Enter a username, a password and a database name to be created for your OASYS installation.
If necessary, edit the host.



For the next step, click **Check Database Parameters**.
This will perform a check of the database settings to verify that your database settings meet the requirements for OASYS.
If the settings meet the requirements, click **Start Database Install**.



The next step is setting up initial admin and superadmin accounts.

Super Administrator

- This role is intended to administer the technical part of the OASYS installation.
- Super admins have access to the system variables.
- They can use the upgrader app to update the OASYS version.
- They have the privilege to create admin and super admin users.

Administrator

- This role is intended to administer users and usergroups. This includes setting access permissions for folders.

Submitting this data will create the OASYS database and it's basic content. The next step is **installing the file system**.
As the last step, the installer will **validate the installation.**
You can proceed to the backend login by clicking **Go To Editor**

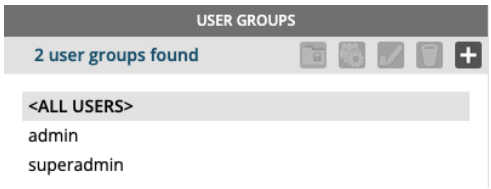
Backend and Frontend

The OASYS frontend URL (login for test takers) is always the URL (and path, if you used a subfolder) you extracted the installer to.
The backend URL is the URL you installed from, followed by **/editor**.

Chapter 3

Overview of OASYS Administration

3.1 Admin Roles and Permissions



There are two predefined user groups in OASYS:

- admin
- superadmin

Users who belong to one of these user groups are granted specific, predefined access permissions.

3.1.1 Superadmin

The superadmin role is primarily intended for maintaining and configuring the OASYS installation. A superadmin has unrestricted access to all functions of OASYS. The privileges of a superadmin include:

- Creating users in the superadmin and admin group.
- Assigning the role of elevated admin to users in the admin group.
- Bulk editing of folder permissions.
- Permission to delete entries from the log analyzer (maintenance).
- Localization (add new test languages to the OASYS installation).
- Manage and change the system settings (OASYS configuration variables).
- Create backups and restore backups.
- Access to the OASYS upgrader in order to keep the installation up to date.

3.1.2 Admin

The default admin role is designed to only manage users. (Except for admin and superadmin users) The privileges of an admin include:

- Create and delete user groups.

- Define menu access for user groups.
- Add and delete users.
- Activate and deactivate users.
- Check folder permissions for user groups.

3.1.3 Admin with Elevated Rights

The elevated admin is an admin with extended privileges.
For making an admin an elevated admin, you have to be logged in with superadmin privileges!

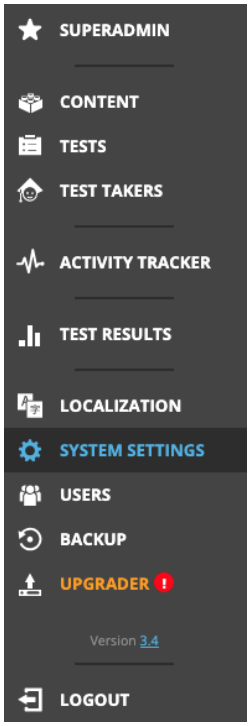
Users Menu in Superadmin View

- Select a user from the admin group.
- In the right column, click on **Elevated Administrator**.
- Toggle the **value** to enable the elevated administrator privileges.

The elevated administrator has the following additional privileges:

- Access to all System Settings
- In the localization app, an elevated administrator can add new languages to OASYS. A normal admin can only edit translations.
- **Users**: Remove or add other users to Admin usergroup
- **Users**: Delete/disable other Administrators
- **Users**: Create Administrators in the Admin usergroup
- **Users**: Modify another Admin level user's account properties
- **Backup**: Download any backup archive file
- **Backup**: Delete any backup archive file
- **Backup**: Restore previous snapshot file

3.2 Backend Layout and Navigation



The main menu is located on the left of the screen. The main menu provides access to the various apps of OASYS.
Depending on the group properties of your user group, the items of the main menu do vary.
This manual covers all the apps that are typically used for OASYS admin tasks.

The toolbar is located on top of the screen. It is context sensitive, meaning its content changes depending on what you are working with. The toolbar provides you with the set of tools that you can currently use.

3.2.1 Admin and Superadmin Apps

For more detailed information, please read the chapters below.

Localization
The purposes of this app are:

- Editing of standard strings displayed in the OASYS frontend, including error messages.
- Adding new test languages to OASYS and provide the translations for the frontend strings.

System Settings
In this app, the variables for configuring OASYS can be used and edited.
You will also find some tools here, such as for system checks.

Users
The OASYS user management.
Here you can edit usergroups, access privileges and users.

Backup
Create and restore full or partial backups of the OASYS installation.

Upgrader
Connect to the upgrade server and keep the OASYS installation up to date.

3.2.2 Standard Backend User Apps (Overview)

More detailed information can be found in the user manual.

Folder Permissions

Setting folder-based access permissions is one of the administrative tasks in OASYS.
Apps with folders are:

- Content
- Tests
- Test Takers

For details, see section **Assigning Folder Rights and App Access**.

The Dashboard
The dashboard is the homepage of the OASYS backend. From here, you have access to your **account settings** (gear icon), a **logout button**, and a **watchlist**.

Locked items

If a backend user sees a padlock icon on one of his bookmarked items, it means he no longer has access to it. This is because the owner has removed or changed the access settings. In order to change the settings, ownership, superadmin or elevated admin privileges are required.

Content
The content manager app is where you can create, edit, and organize the content for tests.

Tests
The Test Manager enables the backend user to create and organize tests or surveys from existing stimuli and / or items.

Test Takers
The test-taker manager enables the backend user of OASYS to create and organize test-takers.

Activity Tracker
In the Activity Tracker, every access by test takers to tests is logged and can be reviewed.
A complete log provides a detailed record of behavior during the test.

Test Results
This app provides access to the test results.
It also is the starting point for manually scoring tests.
The **report builder** is part of the test results menu. The report builder can provide a range of statistics with graphical visualization.

Chapter 4

User Management

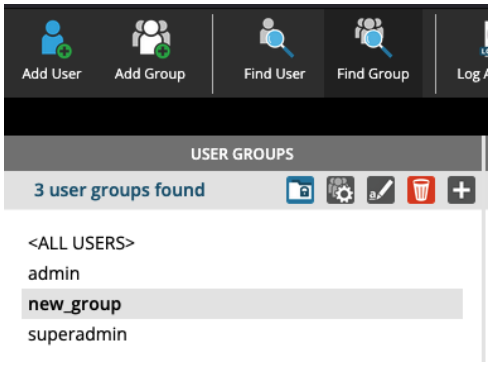
4.1 User Groups

All privileges in OASYS are based on user groups. **There are no individual user privileges, with two exceptions.**

- **Elevated administrator** provides a set of extended privileges.
- **Home folder create** provides the privilege of creating folders on root level. If this is not granted, a user can only create folders within folders his group has write access to.

4.1.1 Creating User Groups

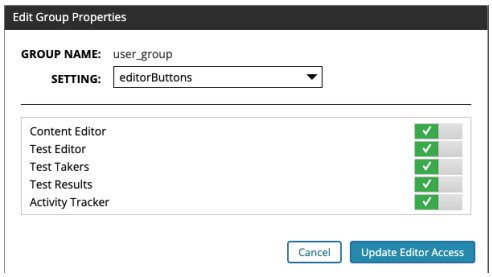
Open the **users app** from the main menu.



Create a user group by:

- Clicking **Add Group** in the top bar.
- Clicking the **plus sign** on top of the user groups column.

You will be prompted for a group name. User group names have to be unique!



After confirming the name, the dialog for the **available apps** will open.
By default, all non-admin apps are activated.
Deactivate app access for the group by unchecking the app(s).

Rename a user group by clicking the **rename button** on top of the user groups column.
Delete a user group by clicking the **delete button** on top of the user groups column.

Predefined User Groups and Filters

OASYS has two predefined usergroups:

- **admin**
- **superadmin**

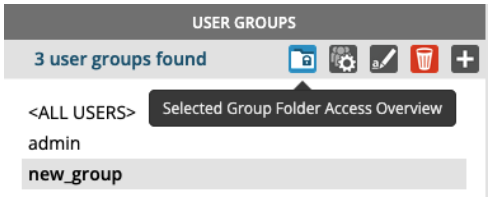
In additioned there are two predefined filters:

- **<ALL USERS>** shows all backend users.
- **<NO GROUP>** shows all users who are not assigned to a group.

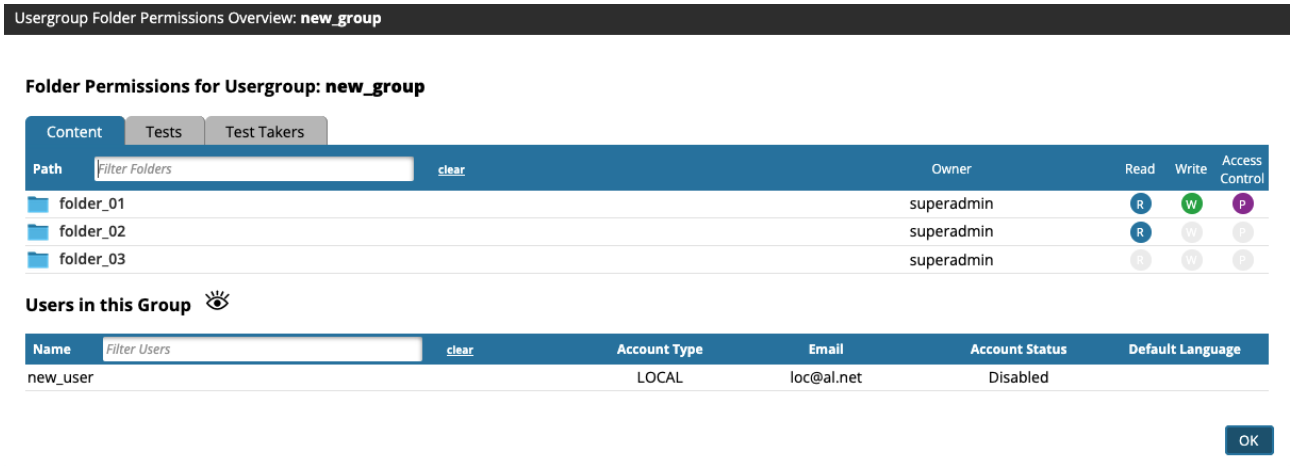
You can't rename or delete the predefined user groups and filters.

4.1.2 Assigning Folder Rights

Folder Permission Overview



Select a user group.
On top of the user groups column, click the access overview button.
The overview is read-only and does not allow editing!



Usergroup Folder Permission Overview

- You can switch between tabs for content, tests and test takers.
- Folders can be filtered by path.
- The second column indicates the owner.
- The last three columns represent the three different permissions in OASYS:
  - Read: Members of the current group can view the content of the folder.

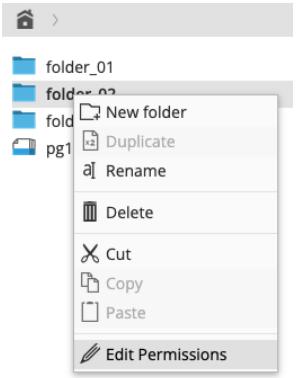
  - Write: Members of the current group can change the content of the folder.
  - Access Control: Members of the current group can change the access settings of the folder.

- **Clicking a folder name brings you directly to the app where you can edit the folder permission.**
- On the bottom, there is an overview of the group's users along with their basic account information.

Assigning Folder Permissions

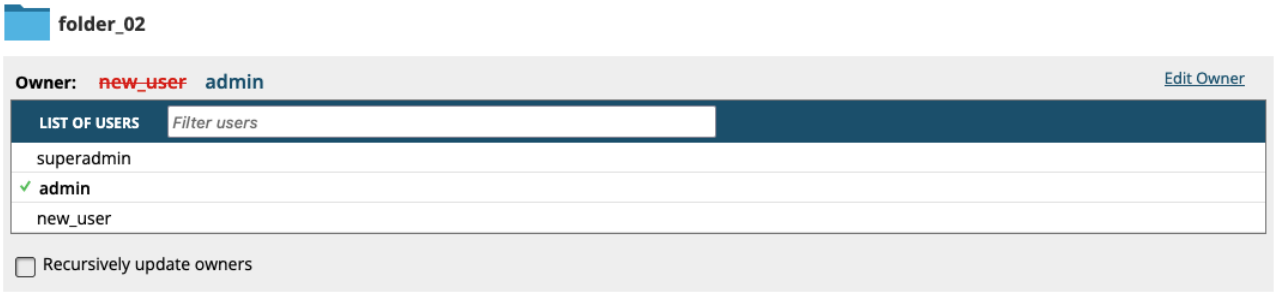
Navigate to the folder you want to assign permissions to. You can do that by:

- Opening the app where the folder is located.
- Clicking the folder in the permission overview.



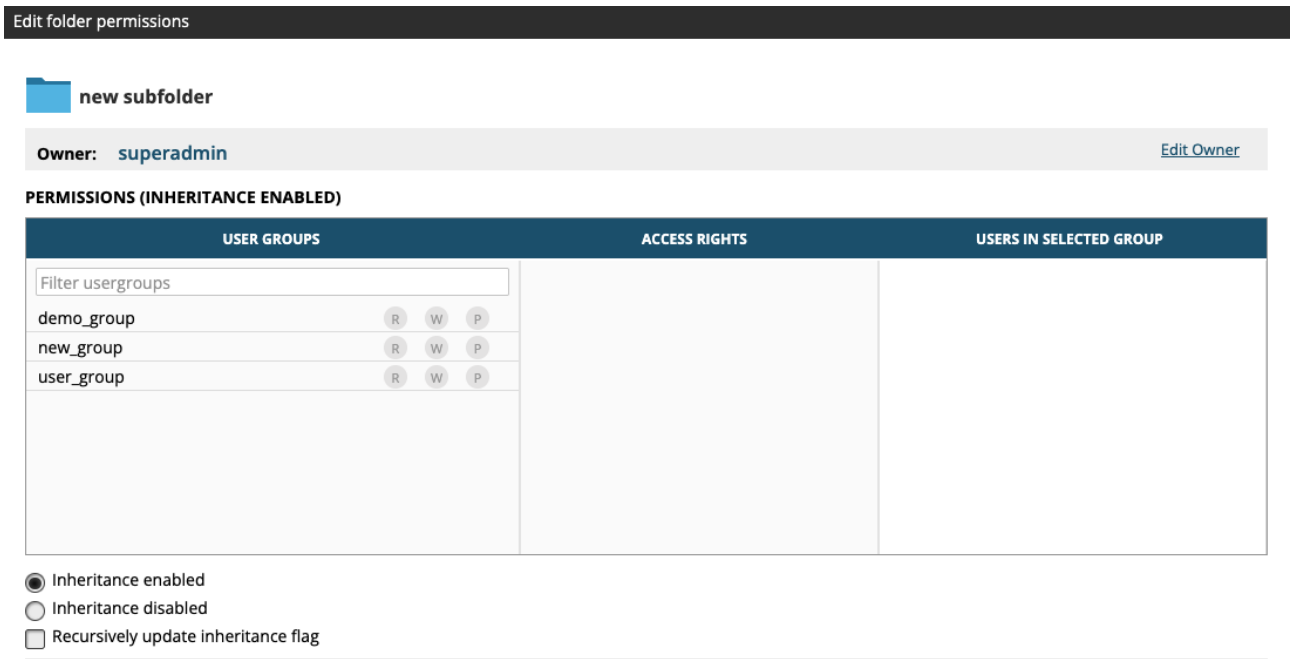
Right-click the folder.
Click **Edit Permissions** in the context menu.
This opens the Folder Permission Dialog, where you can:

  - Change the owner of the folder.
  - Edit read, write and permission editing settings of the folder for the different user groups.



Changing the owner

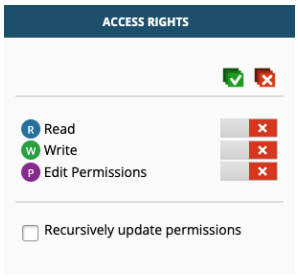
- Click edit owner.
- Select the new owner.
- You can use the search field.
- Check **Recursively update owners** if you want to set the new owner for subfolders, too.



Editing Access Permissions

Select a group to edit its access permissions for the current folder.
Inheritance determines whether you can edit the folder's access permissions directly or if it inherited the permission from the parent folder. If so, you'll have to edit the parent folder's permissions.
You can **disable inheritance** to detach a folder from the inheritance chain.
Recursively update inheritance flag will pass your change of inheritance through the entire tree of subfolders.

Set access permissions by checking/unchecking them.



- Read: Members of the selected group can view the content of the folder.
- Write: Members of the selected group can change the content of the folder.
- Access Control: Members of the selected group can change the access settings of the folder.

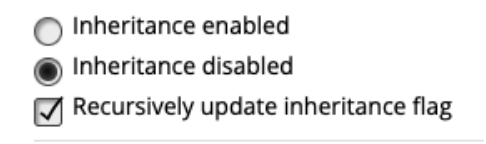
Recursively update permissions will pass your changes of permissions through the entire tree of subfolders.

How Inheritance Works

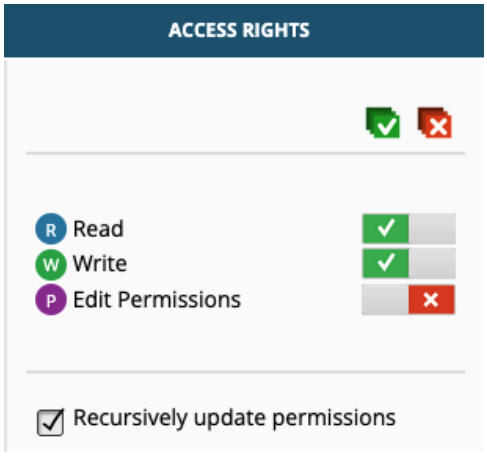
- When you are inside a folder (i.e., not at the root level), the folder can have inheritance enabled. This means it will adopt the permissions of its parent and remain locked to those permissions until inheritance is disabled.
- Non superadmins can only edit one folder at a time.
- The inheritance switch only works **upward** one level: it copies and locks the permissions from the folder's parent. At non-superadmin level, there is no option to enforce inheritance **downward**. Recursive application of permissions is only available to superadmins.

Supercharged Permission Editing and Bulk Permissions Editing

These features are only superadmin accessible!



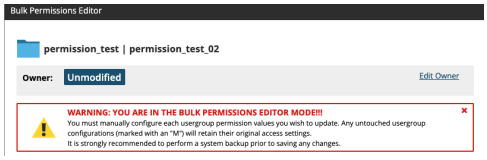
Inheritance flags can be pushed **downward through a tree**, recursively starting anywhere, including the root folder level.
For this, use the settings on the left.



Instead of using **recursive inheritance** to apply and lock permissions across multiple levels, **this option allows you to force a permission set downward through a folder tree** on a one-off basis, without setting any inheritance flags.

- First select a folder.
- Select a group.
- Apply the settings and activate the recursive option.

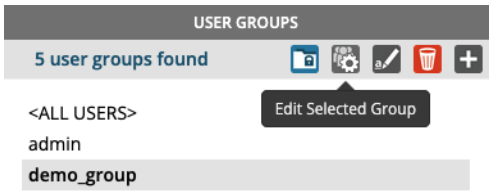
Ownership changes can also be forced down a tree branch recursively, although there is no inheritance option for owners.



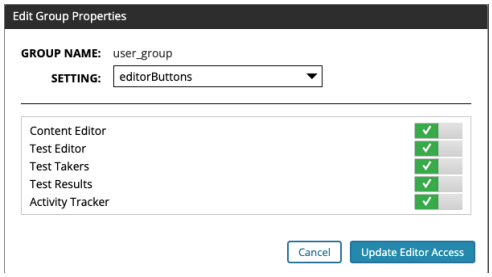
Multiple folders can be selected and modified for mass updates.

- Select multiple folders by holding the shift or command key.
- Right-click and choose **edit permissions**.
- Choose a group, set the changes and apply them to all selected folders.

4.1.3 Assigning App Access



Select a user group.
On top of the user groups column, click the edit selected group button.

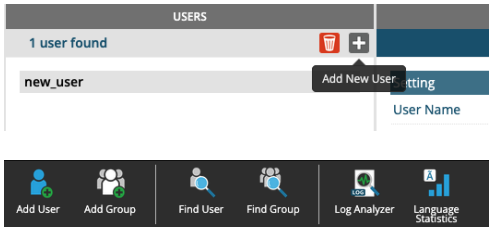


By default, all non-admin apps are activated.
Set the app access for the group by checking/unchecking the app(s).

4.2 User Creation and Authentication

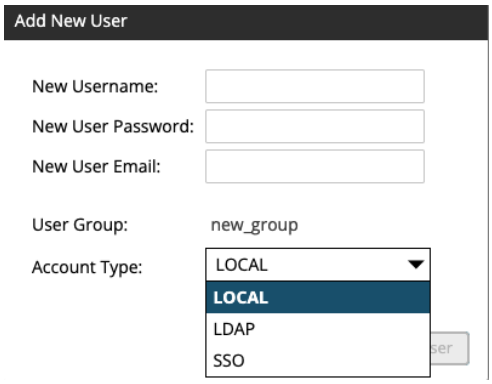
4.2.1 Creating Users

Open the **user app**.
As a first step, you have to **select the group you want the user to be created in.**



Create a new user by:

- Clicking the **plus button** on top of the users column
- or clicking the **Add user button** in the top bar.



- **New Username:** The username must be unique.
- **New User Password:** The password field is only available for local account types!
  Users can change the password in their settings.
- **New User Email:** The forgot my username or password link on the login screen requires a valid email address.(**This feature requires to be set up in the sytem settings!**)

- **Account Type:** The type of authentication used for the login.
  - **LOCAL:** The password is stored in OASYS.
  - **LDAP:** LDAP (Lightweight Directory Access Protocol) is a protocol used to access and manage directory services, such as user and group information, over a network. It is commonly used for authentication and storing organizational data.
  - **SSO:** Single Sign-On (SSO) allows users to log in once and automatically access all connected applications without needing to sign in again.

All account types other than LOCAL require setup in the system settings!

4.2.2 Authentication Methods

Local Authentication

Username and password are stored within the OASYS database. This authentication method doesn't require any additional setup.

LDAP Authentication

This authentication method requires an LDAP server (e.g., Microsoft Active Directory, OpenLDAP)
Navigate to the **system settings**.
Change the following settings according to the parameters of your LDAP server:

- **ldap_appUser:**
  The username used by the application to connect to the LDAP server and perform user searches. This is often a service account with read permissions.
- **ldap_appPass:**
  The (encrypted) password for the ldap_appUser. Needed to authenticate the search account on the LDAP server.
- **ldap_server:**
  The address of the LDAP server. It must start with ldap:// (unencrypted) or ldaps:// (encrypted). Example: ldaps://ldap.example.com.
- **ldap_searchBase:**
  The starting point in the LDAP directory tree for user searches, written as a Distinguished Name (DN). Example: ou=users,dc=example,dc=com.
- **ldap_query:**
  The search pattern used to find users. %1 is a placeholder that will be replaced by the username entered at login. Example: cn=%1 searches by common name.
- **reset_LDAP_Redirect:**
  This is the URL where users will be redirected if they need to reset or retrieve their LDAP password information.
  The URL must start with http:// or https://.
  It usually points to an external password management or support page (since LDAP passwords typically can't be reset directly through the application).

Single Sign-On (SSO)

The SSO integration can't be set up by sytem settings only.
The first step is enabling the **SSOSysActive in the system settings.**
For the configuration, you have to edit the following files:

- inc/php/ssodata.php
- inc/php/ssodata_template.php

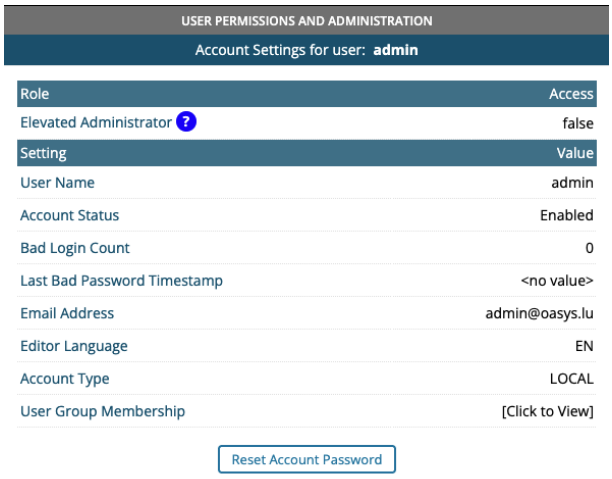
4.2.3 User Options and Settings

User Groups and Privileges

All privileges in OASYS are based on user groups. **There are no individual user privileges, with two exceptions.**

- **Elevated administrator** provides a set of extended privileges.
- **Home folder create** provides the privilege of creating folders on root level. If this is not granted, a user can only create folders within folders his group has write access to.

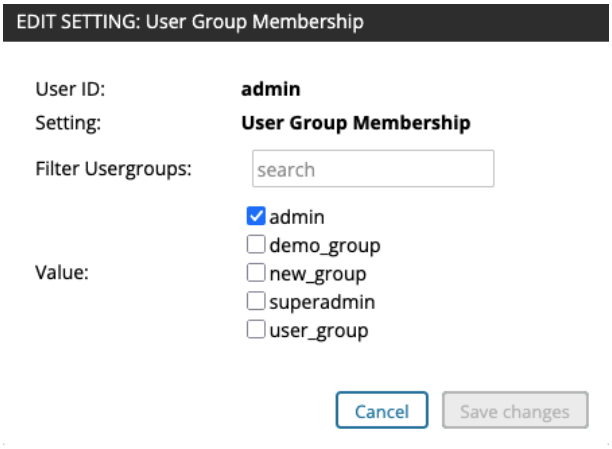
If you want to grant access or administrative privileges to a user, you have to make him member of the corresponding group. **A user can be member of multiple groups!**



Open the **user app**.
Select one of the groups the user you want to edit is in, then select the user. Alternatively, you can use the Find User button in the top menu.
In the right column, you find the settings for the user.
Click an entry in the left column to edit it's value.

- **Elevated Administrator:**
  Only available for users who are members of the admin group.
  The elevated admin is an admin with extended privileges. See chapter Admin Roles and Permissions for details.
- **User Name:**
  The user name can be changed. As the name has to be unique, OASYS won't accept a name, which is already in use.
- **Home Folder Create**
  Privilege to create folders on root level.
  This setting is only available for users who are not members of the admin or superadmin group.
- **Account Status:**
  Accounts can be manually disabled or enabled.
  After 20 failed login attempts, a user will be automatically disabled.
- **Bad Login Count:**
  The count of failed login attempts. This is read only.
- **Last Bad Password Timestamp:**
  Time of the last failed login.

- **Email Address:**
  User email. Users can change their email address in their user profile.
- **Editor Language:**
  Language of the OSYS backend. Users can change this setting in their profile.
- **Account Type:**
  See chapter **Authentication Methods** for details. The type of authentication for the user's backend login.
- **User Group Membership:**



The user will be assigned to all checked groups.

- **Reset Account Password:**
  Users can change their password in their user profile.
  If a user is locked out from his account, the password can be reset with this option.

4.3 Logs Analyzer

The logs analyzer records a specific set of backend user activities, along with the date of the action and the session ID.
The purpose of the Logs Analyzer is to make deletions or renaming of objects by backend users traceable. This is especially important when users report that content they were working on can no longer be found.
The logged modules are:

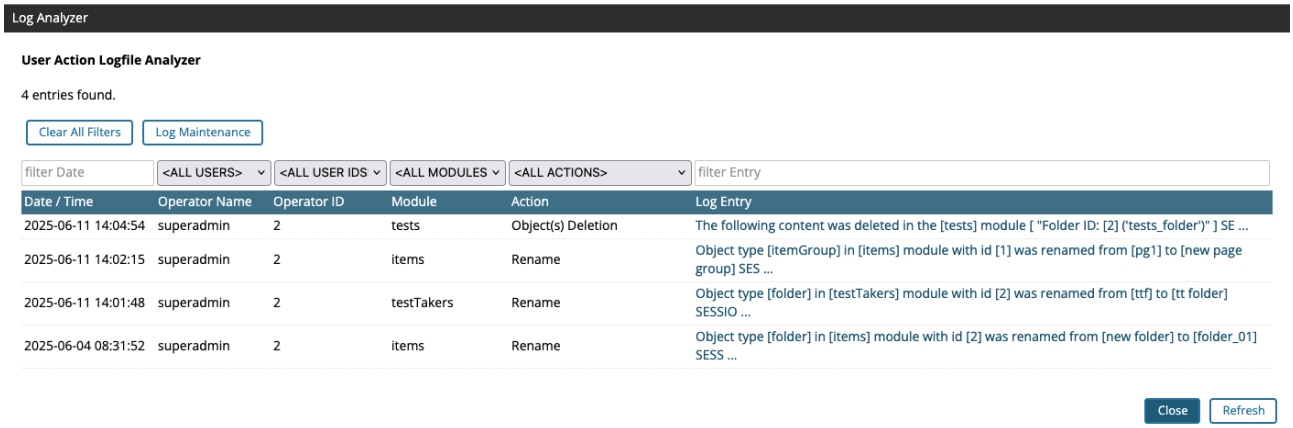
- Contents
- Tests
- Test Takers

The logged actions are:

- Renaming of objects
- Permission update on folders
- Folder owner change
- Object(s) deletion
- Item deletion
- Object move to a different folder
- Test taker results reset
- All password results reset
- Test/password results reset
- Test results reset

If an action is greyed out in the dropdown, it is not present in the current list of entries. (According to the filters applied)

4.3.1 Monitoring User Activities



The Logs Analyzer

Columns

- **Date/Time:**
  The timestamp of the action
- **Operator Name:**
  The backend user's login name.
- **Operator ID:**
  The backend user's database ID
- **Module:**
  The module where the action was taken.
- **Action:**
  The type of the action
- **Log Entry:**
  The corresponding log entry, along with the session ID.
  Click it for the full text version.

Filters

- **Date:**
  Narrows the timeframe of the entries to a specific date.
- **Users:**
  Select a specific user from the dropdown.
  Only users having corresponding log entries are shown.
- **User IDs:**
  Same as users, but listing the users' database IDs.
- **Modules:**
  Narrows the list to a specific module.
- **Actions:**
  Narrows the list to a specific action (see above for the list of logged actions).

- **Filter Entry:**
  Search for entries containing the given search string in the text.

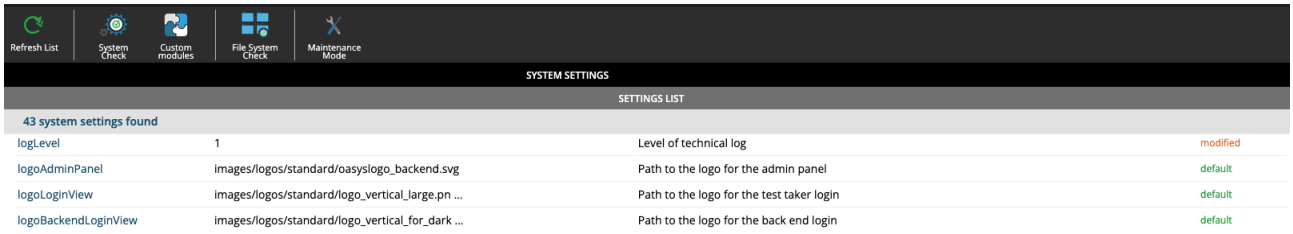
Clear all Filters:
Removes all currently active filters from the list.
Log Maintenance:
Remove older entries from the list according to the time limit chosen from the dropdown.

Chapter 5

System Configuration

5.1 Configuring OASYS

OASYS is configured via the **system settings app (main menu)**. All settings are managed through system variables. An exception is the SSO configuration, which requires editing files. Another tool for configuration is the localization app. It can be used to add additional test languages to an OASYS installation.



System Settings

- 1. Column: Name of the system variable
- 2. Column: Current value
- 3. Column: Description
- 4. Column: Modification info

In order to modify a value, click the first or the last column of the entry.

5.2 System Variables

- **alphaChannel**
  This is an upgrader setting. If it is set to false, the upgrader will only fetch stable releases. If true, the upgrader will fetch prereleases as well. This is only recommended if you need a feature from a prerelease before the next stable release is published.
- **ajaxTimeout**
  Defines the time limit (in milliseconds) for how long the system waits for an AJAX response before considering it failed. Adjust this according to your server's responsiveness and performance.

- **allowContextMenu**
  Enables or disables the browser's context menu (right-click). Activating it may allow unintended features like video controls or Google Translate.

- **customLoginURL**
  By default, a test taker will be redirected to the login screen, after he has finished a test.
  Use this setting to override this behaviour and set a custom URL instead.

- **debugSystem**
  If set to true, detailed error messages for debugging purposes will be displayed in the browser.
  Warning: Should not be enabled in production environments.

- **defaultPassword**
  Allows a default password to be pre-filled on the login page (for test or quick-access setups).
  The frontend login will only ask for the login name.
  Note: The password must be valid and associated to a test!

- **developmentMode**
  When enabled, the system loads CSS and JS files directly (not from blobs).
  Warning: Not for use in production.

- **forceLogoff**
  Automatically logs users off when a test becomes inactive due to time or date restrictions.
  This can be overridden on test level.

- **hideTimeoutMsg**
  Controls whether timeout messages are shown in new tests. If true, the timeout message is hidden.
  This can be overridden on test level.

- **landingPage**
  The default frontend login page can be replaced with this setting.
  This setting requires a custom module!

- **ldap_appUser**
  Username for the LDAP search account.

- **ldap_appPass**
  Encrypted password for the LDAP search account.

- **ldap_server**
  URL of the LDAP server (must start with LDAP:// or LDAPS://).

- **ldap_searchBase**
  Distinguished Name (DN) for the user search base.

- **ldap_query**
  Query string for searching users; %1 is replaced by the username.

- **limitNavigation**
  Default setting for limiting navigation during tests.
  This can be overridden on test level.

- **loginLanguage**
  Default language activated at login.
  Note that all buttons for choosing a language at login will still be available. This setting just controls the preselection.

- **logoAdminPanel**
  The logo used in the admin panel can be replaced.
  The file must be located within the OASYS installation folder. The path must start without a /.

- **logoLoginView**
  The logo used in the frontend login screen can be replaced.
  The file must be located within the OASYS installation folder. The path must start without a /.

- **logoBackendLoginView**
  The logo used in the backend login screen can be replaced.
  The file must be located within the OASYS installation folder. The path must start without a /.

- **logPayload**
  Indicates how much of the frontend network traffic is logged (nothing, just packages or packages with sent data).
  Log entries are stored in the database. Table: logTransfers

- **mediaLocation**
  Location where media is stored (on disk or in the database); **changes require OASYS team support**.

- **menuLanguages**
  List of languages displayed on the frontend login screen.
  If you deactivate all but one language, the language selection buttons will not be displayed.

- **mutationMethod**
  Default mutation method setting for new mutation tests.
  Method can be set to random (a random test will be picked) or to sequential (the next test from the list will be picked).
  This can be overridden on test level.

- **passwordField**
  Defines whether the password field in the frontend login displays the typed text or hides it.

- **retryCount**
  Number of attempts to send test data to the server before OASYS considers the connection as failed.
  In case, the number is exceeded, the test will be blocked. This prevents test takers from continuing with a test which can't send test results to OASYS.

- **saveResults**
  Default setting for whether test results are saved when creating a new test.
  This can be overridden on test level.

- **sendFrequency**
  Frequency (in milliseconds) of sending data packages (test results) from the frontend to the server.

- **sessionTimeout**
  Time (in seconds) to keep a login session active while a backend user doesn't show activity.

- **showScore**
  Default setting for displaying scores in new tests.
  This can be overridden on test level.

- **title**
  The title displayed in the browser tab (for the OASYS frontend). Also used by iOS when creating a homescreen link.

- **useTimer**
  Default setting for enabling the "use timer" option in new tests.
  This can be overridden on test level.

- **waitForMediaCache**
  Default setting for media caching in new tests. If set to true, the test will start when all media is cached.
  This can be overridden on test level. (Name of the property: Wait for media to load)

- **writeLog**
  Determines whether technical log data is written. When enabled, OASYS writes a multitude of logs, for backend as well as for frontend user actions.
  The logs are mostly for the OASYS team. In case support is needed, we might request some specific logfiles from your instance.
  Logs are located in the logs folder on root of your OASYS installation.

- **SSOSysActive**
  Indicates whether Single Sign-On (SSO) integration is active.

- **emailSysActive**
  Indicates whether email functionality is enabled for automated account resets, account validation, etc.

- **SMTP_Host**
  (Encrypted) Outgoing email server address for OASYS Editor.

- **SMTP_Port**
  Email server SMTP port used by OASYS Editor.

- **SMTP_Username**
  (Encrypted) Email server SMTP username for OASYS Editor.

- **SMTP_Password**
  (Encrypted) Email server SMTP password for OASYS Editor.

- **SMTP_From**
  The "FROM" address used for outgoing emails.

- **SMTP_Encryption**
  Defines the encryption type for the SMTP server connection (none, implicit, or TLS upgradable).

- **reset_LDAP_Redirect**
  URL for redirecting LDAP password reset information (must start with "http(s)://").

- **upgraderURL**
  The URL the upgrader app and the upgrader notification use. Don’t change this unless the OASYS team does notify you of a server change!

5.3 System and File System Check

In order to perform a system check or a file system check, navigate to the system settings in the main menu. The buttons for both checks are located in the top bar.

5.3.1 System Check

The system check verifies whether the server environment meets the technical requirements to properly run OASYS.
In summary, this check is a quick way to validate that the hosting environment is correctly configured and compatible with the currently installed OASYS version.
It checks:

- PHP version and required PHP modules
- Database system and version
- Server and database configuration limits (e.g., memory, execution time)
- User privileges
- System time synchronization

The purpose of the system check is:

- To ensure compatibility between OASYS and the server.
- To prevent runtime errors due to missing modules or incorrect configurations.
- To confirm that the database setup and user permissions meet the application's operational needs.

When to perform this check:

- After updates to the server, PHP, database, or the application itself.
- When migrating OASYS to a new server.
- During troubleshooting if OASYS is not working as expected.

5.3.2 File System Check

The file system check verifies the integrity of OASYS' file structure by comparing the current files against a baseline (a known, correct file set).
It looks for:

- Additional files (unexpected files that might indicate tampering or leftover files)
- Missing files (required files that are no longer present)
- Modified files (files that differ from the original version, based on checksum)

The purpose of the file system check is:

- To detect unauthorized changes or file corruption.
- To ensure that no critical files have been accidentally deleted or altered.
- To identify potential security risks from extra or modified files.

When to perform this check:

- Regularly as part of system maintenance.
- After a software update or patch.
- If there is suspicion of a security breach.
- After manual file system changes or migrations.

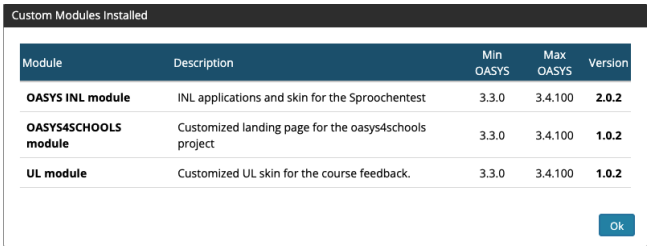
Clean up Files:
If there are leftover files from old versions of OASYS which are not part of the exclusion list, the button will remove those files permanently. This is to keep the system in line with the exact system files that should be there. If a file is found to be "different" by not matching the checksum value, that file is **not** removed with the Clean up Files button.
Only files which are

- not in the checksum list and
- not in the exclusion list

are removed with this cleanup button.

5.4 Custom modules

Custom Modules are modules that can extend, modify, or partially replace functionalities of OASYS. This could include, for example, advanced test management features or custom skins.
If you plan to use OASYS and require extensions, feel free to contact us through the OASYS website.
Custom modules are typically integrated via the main menu or are available as additional options within specific apps.
The **custom modules button** in the top menu of the **system settings** provides an overview of the installed custom modules:



- Min OASYS: Minimum required OASYS version for the installed version of the module.
- Max OASYS: Maximum tested OASYS version for the installed version of the module.
- Version: Currently installed version of the module.

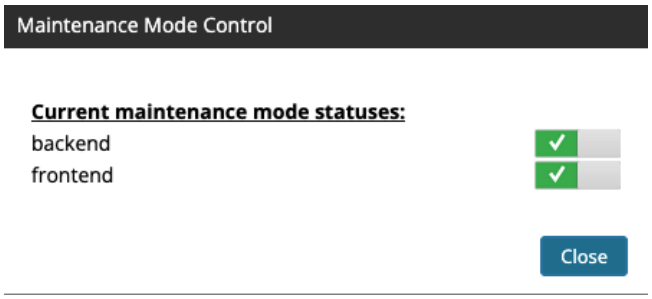
Custom modules are usually delivered with a custom OASYS installer.
The OASYS **upgrader** will recognize the installed module and integrate its newest version in the upgrade process.
In case there is no compatible version of the module, the upgrader will issue a warning and will not perform the upgrade.

5.5 Maintenance Mode

Maintenance mode is a system state that temporarily locks the web application for regular users while allowing administrators to carry out system updates, configurations, or troubleshooting tasks without interference.
Purpose:

- Protects system integrity during updates.
- Prevents user disruptions and potential data inconsistencies.
- Provides a safe environment for backend maintenance.

Maintenance mode is typically used during planned updates, configuration changes, or system checks that could temporarily impact normal operation.
OASYS has two separate maintenance modes:



- **Backend:**
  Only the backend is set to maintenance mode. All backend users are locked out, except super-admins.
- **Frontend:**
  The interface for test takers is locked. The backend is accessible for all backend users.

Chapter 6

Localization

OASYS is natively designed for multilingual tests. The approach is to provide each content element in multiple languages simultaneously during creation.

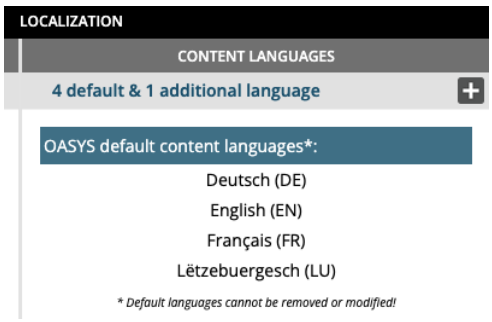
When working on a test page, you can add languages, remove languages or change the current language.

Within the test page, you can switch languages using tabs.

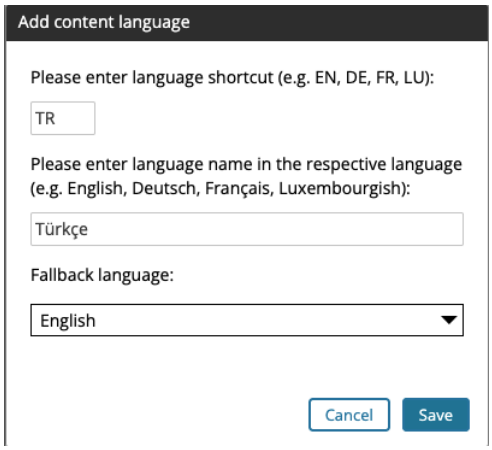
The language of the menu elements in the frontend will change according to the language currently selected by the test taker.
The available languages are defined in the **localization app**.

6.1 Adding New Languages

Languages are added via the **localization app (main menu)**.

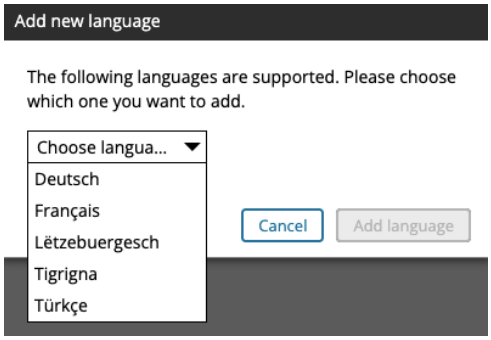


In the right column, there is the list of the default languages.
If there are additional languages, they are listed below.
Click the **plus sign** on top of the column to add a new test language.



Enter

- The **language shortcode** which is used wherever the name is abbreviated.
- The **language name** in the respective language.
- A **fallback language** which will be used where a translation is missing.

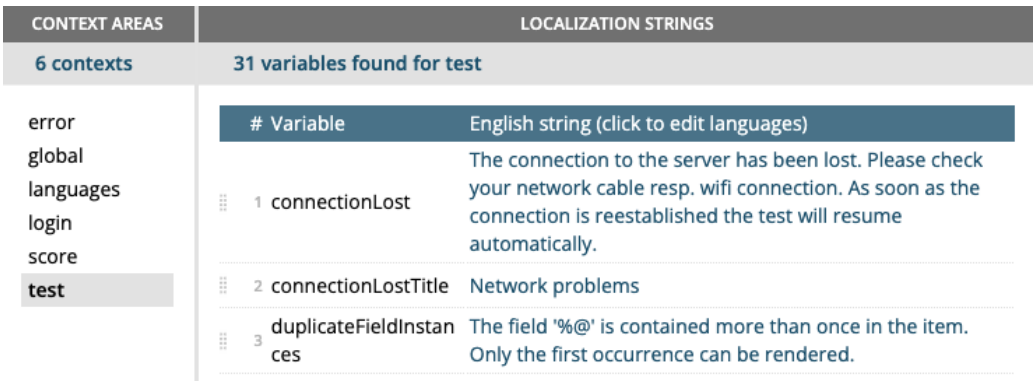


The additional language will be available when **adding a language to a content page.**

And it will be available for **activation for a test.**

6.2 Providing Translations

When adding a new language to OASYS, translations for skin elements (buttons, menu elements) and messages must be provided.
OASYS stores these translations as string values in variables. If a string value is not available in a language, the value of the fallback language will be used.
String translation is done in the **first two columns of the localization app**.

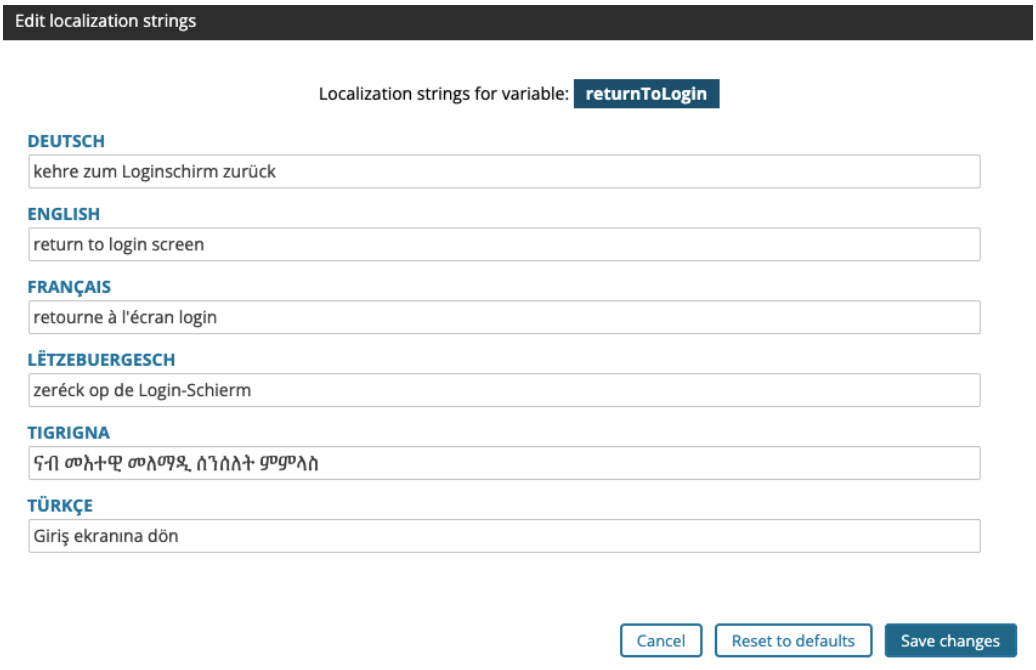


Context Areas

Context areas are groups of variables containing strings related to the same topic.
Select a context area to show its variables in middle column.

Localization Strings

The second column lists all variables of the selected context.
The **variable** column shows the name, the other column shows the current English string value of the variable.
Click the string value to edit the translations.



The translation dialog lists all currently available test languages. You can:

- edit an existing translation.
- add missing translations

Once all variables of all contexts are translated, the localization is complete.

Chapter 7

Backup and Restore

OASYS has two different backup options.
Both are located in the **backup app in the main menu.**
A **snapshot** creates a backup of the *database* and all *uploaded media* at the current point in time.

Use when:

- You want to quickly save the current data state before making minor changes (e.g., content updates, user imports).
- A fast, lightweight backup is sufficient.

A **full backup** includes the entire *OASYS data and file system*, excluding system logs and operational temporary files.

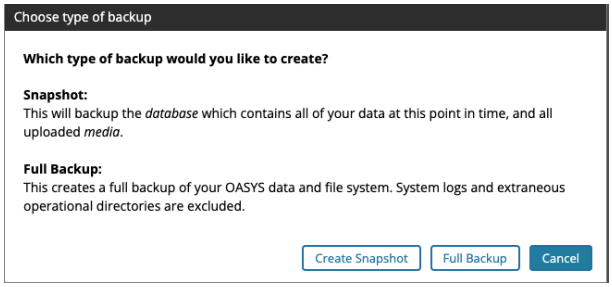
Use when:

- Performing system upgrades or major configuration changes.
- Migrating the application to another server.
- Creating a periodic comprehensive backup for disaster recovery.

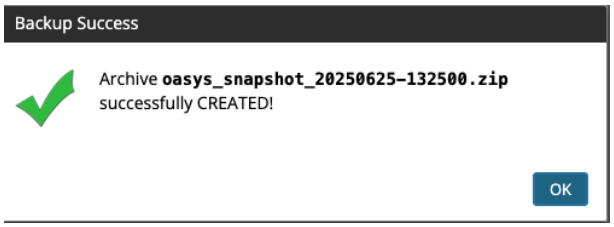
7.1 Database Snapshots

7.1.1 Creating a Backup

Open the **backup** app.
Click the **plus sign** in the upper right of the backup list.



Choose **Create Snapshot**.

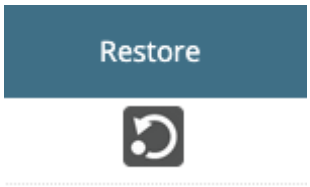


You'll get a success message.

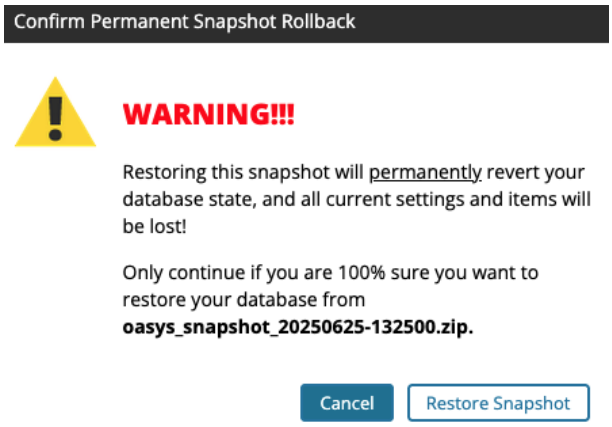
The snapshot will appear in the backup list.

7.1.2 Restoring from Backup

Open the **backup** app.
Locate the snapshot you want to restore in the backup list.



Click the **restore button** next to your snapshot.



Read the warning before you continue.

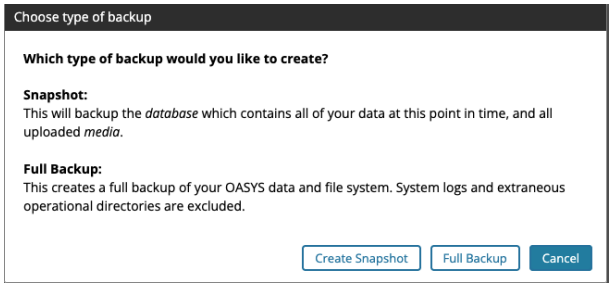
Snapshot Compatibility

An older database snapshot might not be compatible with a newer OASYS version!
OASYS has a built-in comaptibility check for this scenario.
An old snapshot will be blocked from being restored when its database version is not compatible with the current Oasys version.

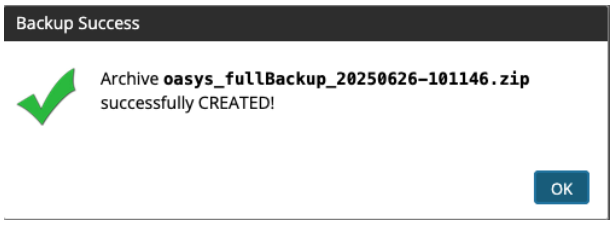
7.2 Full System Backups

7.2.1 Creating Full Backups

Open the **backup** app.
Click the **plus sign** in the upper right of the backup list.



Choose **Full Backup**.



You'll get a success message.

The backup will appear in the backup list.

7.2.2 Restoring Full Backups

Open the **backup** app.
Locate the backup you want to restore in the backup list.

Click the **download button** next to your backup.

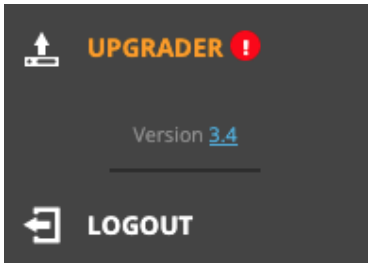
- Connect to your webserver.
- Go to your Oasys root folder, and remove all files (including any hidden files and/or directories).
- Copy your downloaded backup archive ZIP file to your Oasys root.
- Unzip the zip archive.
- In your preferred database management software (or via your organization's DBA), remove the database which was being used for your Oasys instance.

- Re-create the database which was just removed, and leave empty (or request this operation to be done by your DBA).
- There will be a single .sql file in the Oasys root after extracting the archive — restore the contents of this file back into your database using your database software, or command line *(e.g., mariadb -u[user] -p[password] my_oasys_db_name < oasys-backup-oasys-20250101-120000.sql)*, or request this operation to be done by your DBA.
- Remove the .sql file from the root of your Oasys application directory after confirming that the system has been restored successfully **(this part is critical and should not be skipped, otherwise, future snapshot and backup operations can be adversely affected)**.

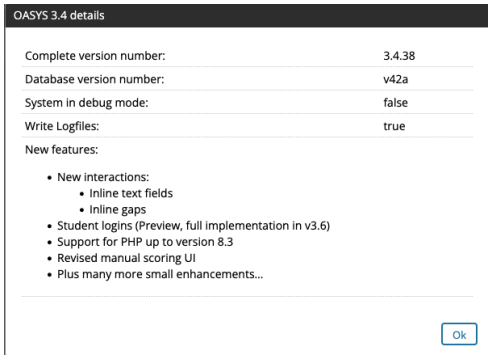
Chapter 8

System Upgrader

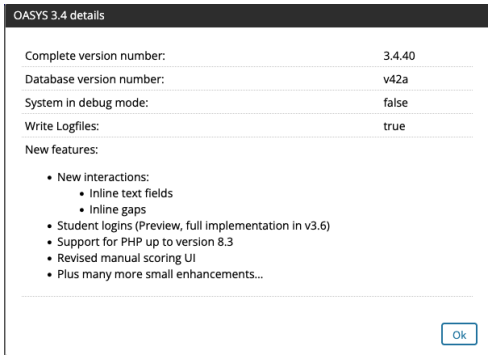
8.1 System Information



The currently installed OASYS version is displayed on the bottom of the main menu, right above the logout button.
Click the version number for detailed version information.



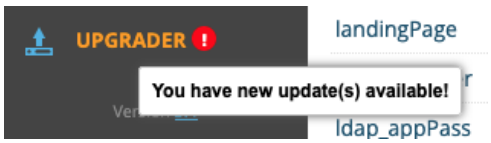
The popup screen shows the **complete version number**. The last two digits indicate subversions and hotfixes.
The OASYS database is versioned. As it doesn't change with every upgrade, the version number is different from the software version number.
System in debug mode and **write logfiles** are system settings. If the values aren't as intended by you, you can change them in the settings manager.
New features shows a list of changes which were introduced with the currently installed OASYS version.



Return to the popup screen after the upgrade.
The complete version number should have changed.
The OASYS database version only changes if the upgrade includes a database change.
System in debug mode and **write logfiles** should be as intended by you. The upgrade shouldn't change these settings.
Check the **new features** to be informed about changes in the software.

8.2 Update Notifications

The upgrader app is the tool to keep an OASYS installation on the newest available version.



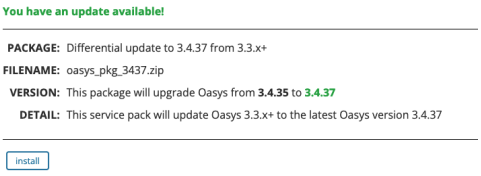
OASYS checks the update server for new versions. If there is an update available, you'll see a red exclamation mark close to the menu entry.

Custom Modules

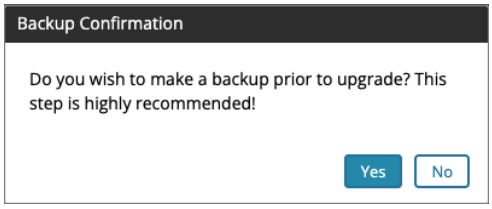
If you have custom modules installed, your OASYS installation is set up with a custom installer.
This does not affect the use of the upgrader!
The upgrader will automatically recognize your custom modules and integrate newer versions of your custom modules in the update.
In case, there are currently no version of your custom modules which are compatible with the new OASYS version, the update will be rejected.

8.3 Performing Upgrades

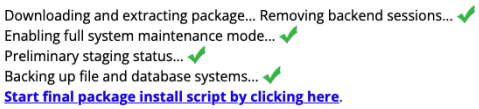
Click the **UPGRADER** button in the main menu.



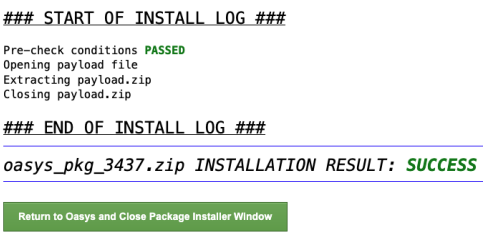
If there is an update, you'll see detailed information. Click **install** to start a precheck.



You will be prompted to perform a backup. When done, the backup will be available in the **backup** app.



If the precheck was passed without any errors, click the link below the check to perform the upgrade.



You will be directed to the installation log screen.
Click the button below to return to OASYS.