



ownCloud Server Administration Manual

Release 10.0.10

The ownCloud developers

November 19, 2018

1	Introduction	1
1.1	ownCloud Videos and Blogs	1
1.2	Target Audience	1
2	Release Notes	3
2.1	Changes in 10.0.10	3
2.2	Changes in 10.0.9	7
2.3	Changes in 10.0.8	12
2.4	Changes in 10.0.7	15
2.5	Changes in 10.0.6	16
2.6	Changes in 10.0.5	16
2.7	Changes in 10.0.4	17
2.8	Changes in 10.0.3	19
2.9	Changes in 10.0.1	20
2.10	Changes in 10.0.0	22
2.11	Changes in 9.1	22
2.12	Changes in 9.0	24
2.13	Changes in 8.2	25
2.14	Changes in 8.1	25
2.15	Changes in 8.0	27
2.16	Changes in 7.0	29
3	What's New in ownCloud 10.0.10	33
4	Installation	35
4.1	System Requirements	35
4.2	Deployment Recommendations	37
4.3	Deployment Considerations	46
4.4	Manual Installation on Linux	48
4.5	Linux Package Manager Installation	57
4.6	The Installation Wizard	59
4.7	Installing with Docker	66
4.8	Command Line Installation	69
4.9	Configuration Notes & Tips	70
4.10	Troubleshooting	73
4.11	Changing Your ownCloud URL	73
4.12	Installing and Managing Apps	74
4.13	Supported Apps in ownCloud	76
4.14	SELinux Configuration	77
4.15	NGINX Configuration	80
4.16	Using Let's Encrypt SSL Certificates	91

5	Upgrading	99
5.1	Upgrade PHP on RedHat 7 and Centos 7	99
5.2	Upgrade Marketplace Applications	100
6	Configuration	103
6.1	Database Configuration	103
6.2	File Sharing and Management	111
6.3	How To Install and Configure an LDAP Proxy-Cache Server	164
6.4	Mimetypes Management	177
6.5	Server Configuration	180
6.6	User Management	304
7	Maintenance	351
7.1	Maintenance Mode Configuration	351
7.2	Backing up ownCloud	351
7.3	How to Upgrade Your ownCloud Server	354
7.4	Upgrade ownCloud From Packages	355
7.5	Upgrading ownCloud with the Updater App	357
7.6	Manual ownCloud Upgrade	360
7.7	Restoring ownCloud	364
7.8	Migrating to a Different Server	365
7.9	How To Manually Move a Data Directory	368
8	Issues and Troubleshooting	371
8.1	General Troubleshooting	371
8.2	Code Signing	377
8.3	Impersonating Users	381
9	Enterprise Features	385
9.1	Installation	385
9.2	Firewall Configuration	391
9.3	Ransomware Protection	396
9.4	File Management	399
9.5	External Storage	402
9.6	User Management	424
9.7	Creating Branded ownCloud Clients	434
9.8	Logging Apps	435
9.9	Server Branding	435
9.10	Document Classification and Policy Enforcement	436
10	The ownCloud X Appliance	447
10.1	What is the Appliance?	447
10.2	How to Install the Appliance	447
10.3	The ownCloud X Appliance Enterprise Trial	453
10.4	ownCloud Appliance Login Information	454
10.5	How to Update ownCloud	454
10.6	Managing UCS	461
10.7	Install Antivirus Software in the ownCloud Appliance	467
10.8	How To Add Certificates	470
10.9	Active Directory Integration	472
10.10	Backup	472
10.11	Working on Documents in the ownCloud Appliance	473
10.12	Firewall protected environment	510
11	FAQ	511

11.1	How do I transfer files from one user to another?	511
11.2	How do I deal with problems caused by using self-signed SSL certificates?	511
11.3	I'm the admin and I lost my password! What do I do now!	511
11.4	What is a Federated System?	511

INTRODUCTION

Welcome to the ownCloud Server Administration Guide. This guide describes [administration tasks for ownCloud](#), the flexible open source file synchronization and sharing solution. ownCloud includes the ownCloud server, which runs on Linux, client applications for Microsoft Windows, Mac OS X and Linux, and mobile clients for the Android and Apple iOS operating systems.

[Current editions of ownCloud manuals are always available online at doc.owncloud.org and doc.owncloud.com.](#)

ownCloud server is available in three editions:

- The free community-supported server. This is the core server for all editions.
- The Standard Subscription for customers who want paid support for the core Server, without Enterprise applications.
- The Enterprise Subscription provides paid support for the Enterprise Edition. This includes the core Server and Enterprise apps.

See *What's New in ownCloud 10.0.10* for more information on the different ownCloud editions.

1.1 ownCloud Videos and Blogs

See the [official ownCloud channel](#) and [ownClouders community channel](#) on YouTube for tutorials, overviews, and conference videos.

Visit [ownCloud Planet](#) for news and developer blogs.

1.2 Target Audience

This guide is for users who want to install, administer, and optimize their ownCloud servers. To learn more about the ownCloud Web user interface, and desktop and mobile clients, please refer to their respective manuals:

- [ownCloud User Manual](#)
- [ownCloud Desktop Client](#)
- [ownCloud Android App](#)
- [ownCloud iOS App](#)

RELEASE NOTES

- *Changes in 10.0.10*
- *Changes in 10.0.9*
- *Changes in 10.0.8*
- *Changes in 10.0.7*
- *Changes in 10.0.6*
- *Changes in 10.0.5*
- *Changes in 10.0.4*
- *Changes in 10.0.3*
- *Changes in 10.0.1*
- *Changes in 10.0.0*
- *Changes in 9.1*
- *Changes in 9.0*
- *Changes in 8.2*
- *Changes in 8.1*
- *Changes in 8.0*
- *Changes in 7.0*

2.1 Changes in 10.0.10

Dear ownCloud administrator, please find below the changes and known issues in ownCloud Server 10.0.10 that need your attention. You can also read [the full ownCloud Server changelog](#) for further details on what has changed.

2.1.1 Official PHP 7.2 Support

After announcing the future deprecation of PHP 5.6 and 7.0 with the [10.0.8 release](#), ownCloud Server now follows up by officially adding PHP 7.2 support. The Server Core and all apps maintained by ownCloud have received a full QA cycle and are proven to work reliably with PHP 7.2.

ownCloud Server is also being prepared for PHP 7.3, which is [scheduled to become available by the end of 2018](#). **If you are still using versions 5.6 or 7.0, please plan an upgrade to 7.2 soon.** See the system requirements in the [ownCloud Documentation](#).

Note: With PHP 7.2 some extensions have changed. If you have not yet upgraded, you need to install `php-openssl`. See #30337 for more information.

2.1.2 New Local User Creation Flow

In previous versions, administrators created local users by entering a username and a password. In many cases this is undesirable, as administrators set the password for new users and need to provide it via a second communication channel. For this reason the local user creation flow has been changed to expect a username and an email address, which will be used to send an activation link to new users.

This way user creation is easier and more secure as new users are informed automatically and can choose a password in self-service. For cases where administrators want to set the initial password, it's possible to deviate from the default by setting the option “*Set a password for new users*” on the bottom left settings cog. The former option “*Send email to new users*” has been removed, as this change made it obsolete.

2.1.3 HTTP API for Search

ownCloud Server 10.0.10 introduces an HTTP API for search functionality. It enables the use of search terms to query the server and the delivery of search results via HTTP (WebDAV). In upcoming releases, ownCloud clients will make use of it to search content on the server, without the need to have them available locally.

In combination with the Full-Text Search integration, which is soon to be released as an ownCloud Server extension (Community Edition), HTTP API for Search will boost usability and productivity for users. For example, they will be able to search through all the content which they store in their account and quickly find files on their smartphones.

2.1.4 Native Brute-Force Protection

Together with the new server version, another security-enhancing extension is available, **Brute Force Protection**. This extension is tasked with preventing attackers from guessing user passwords (brute-force attack) by delaying subsequent failed login attempts for a user account from the same IP address.

While in the past similar functionality was only achievable via third party applications, such as *Fail2Ban*, this extension provides the functionality natively, configurable by ownCloud administrators on the **Security settings** section.

The new extension supersedes the former **Security** extension together with the new **Password Policy** extension, which has been released with ownCloud Server 10.0.9. This community-contributed extension is well-tested, but out of ownCloud's general support scope. However, individual support can be obtained on request.

2.1.5 Improved Reliability for Uploads Via Web Interface on Unreliable Connections

The reliability of the file upload feature in the ownCloud web interface has been improved. When uploading larger amounts of data on unreliable connections (e.g., on the train or with mobile data) you have to deal with interruptions and timeouts, which in the past required users to restart stalled uploads from the beginning in the worst case.

On top of ownCloud's chunking mechanism, which splits large files into pieces and uploads them separately, there's new logic that takes care of retrying stalled chunks. With this, uploads can now continue from the point they froze when a connection becomes available again.

2.1.6 New Option to Prevent Sharing With Specific System Groups

System groups in ownCloud can have many purposes. They can be used for sharing with many users at once, for feature and access restrictions, or for storage mounts to specific users - just to name a few. In some cases, especially in larger deployments, it's undesirable that groups which are used for other purposes are also available for sharing. To prevent users from sharing with such groups, administrators can now blacklist the respective system groups using the option *"Exclude groups from receiving shares"* in the administration settings *"Sharing"* section.

2.1.7 New Options for the occ Command to Reset User Passwords

The occ command `user:resetpassword` allows system administrators to reset or change user passwords. It has been extended to provide the additional options `--send-email` and `--output-link`, which can be used to send a password reset link to the user via mail and output the password reset link to the command line, respectively. This change is in line with the new local user creation flow, which is explained above, and can also be used for further processing with scripts. See the ownCloud Documentation and the `--help` option for more information.

2.1.8 New Default Minimum Supported Desktop Client Version

To ensure clean and reliable operation of the ownCloud platform it is important to stay up-to-date with the latest releases for the server as well as the clients. To take care of compatibility between the server and desktop clients, the minimum version the server will accept connections from has been raised to **version 2.3.3**. While it's recommended to keep up with later versions, this is the new default value. It can be changed by altering the `config.php` parameter `'minimum.supported.desktop.version'` => `'2.3.3'`, if absolutely necessary.

2.1.9 New Option to Configure the Language of Mail Notifications for Public Links

Usually ownCloud renders mail notifications in the language of the recipients, when they are known. For the **recently improved feature** to send public links with a personal note directly from the user interface, the recipients' language can't be determined automatically, it just knows the recipients' mail addresses.

ownCloud therefore uses the language of the user who sent the notification, which can have the drawback that recipients can't understand them. **This is still the default behavior but administrators can now change it via a dropdown menu *"Language used for public mail notifications for shared files"* in the settings *"Sharing"* section.**

2.1.10 Theming Changes

Mail templates for share notifications do not strip line breaks from the personal note anymore. This affects the HTML (`core/templates/mail.php`) and plain text (`core/templates/altmail.php`) mail templates. The default templates shipped with ownCloud Server 10.0.10 have been modified to accommodate these changes. If your custom theme overrides these templates, you have to follow up with the changes:

- Replace the following line of the HTML template

```
p($l->t("Personal note from the sender: %s.", [$_['personal_note']]));
```

with

```
print_unescaped($l->t("Personal note from the sender: <br> %s.",
$_['personal_note']));
```

- Replace the following line of the plain text template

```
print_unescaped($l->t("Personal note from the sender:  %s.",
[$_['personal_note']]));
with
print_unescaped($l->t("Personal note from the sender:  \n %s.",
[$_['personal_note']]));
```

2.1.11 Other Notable Changes

- Allow automated SSL certificate verifications for CAs other than Let's Encrypt. See [#31858](#) for further details.
- “/” and “%” are now valid characters in group names. See [#31109](#) for further details.
- New audit events for login action with token or Apache. See [_#31985](#) for further details.
- Log entries for exceeding user quota: Loglevel changed to “debug” (Insufficient storage exception is now logged with “debug” log level).
- The app for embedding external sites to the app launcher (“*external*”) now supports icons that originate from theme apps.
- The `occ` command to deactivate storage encryption (`occ encryption:decrypt-all`) has received stability improvements and can now read the required recovery key from an environment variable which is very helpful for a scripted per-user decryption process.

2.1.12 Solved Known Issues

ownCloud Server 10.0.10 takes care of [10.0.9 known issues](#) and provides remedies for several others:

- The Password Policy extension now works with two- or multi-factor authentication extensions. See [#32058](#) for further details.
- The `Versions` feature now works also when the `Comments` app is disabled. See [#32208](#) for further details.
- E-mail addresses with subdomains with hyphens are now also accepted for public link emails. See [#32281](#) for further details.
- Allow null in “Origin” header for third party clients that send it with WebDAV. See [#32189](#) for further details.
- Properly log failed message when token based authentication is enforced (`fail2ban`). See [#31948](#) for further details.
- Deleting a user now also properly deletes their external storages and storage assignments. See [#32069](#) for further details.
- Lockout issues with wrong passwords for Windows Network Drives are mitigated: Fixed mount config in front-end to only load once to avoid side effects. See [#32095](#) for further details.
- Fixed update issue related to `oc_jobs` when automatically enabling market app to assist for update in OC 10. See [#32573](#) for further details.
- Fixed missing migrations in `files_sharing` app and add indices to improve performance. See [#32562](#) for further details.
- Fixed issue with spam filters when sending public link emails. See [#32542](#) for further details.

2.1.13 Known Issues

Currently there are no known issues with ownCloud Server 10.0.10. This section will be updated in the case that issues become known.

2.1.14 For Developers

- Search API for files using WebDAV REPORT and an underlying search provider. See [#31946](#) and [#32328](#) for further details.
- Add information whether user can share to capabilities API. See [#31824](#) for further details.
- Hook `loadAdditionalScripts` now also available for public link page. See [#31944](#) for further details.
- Added URL parameter to files app which opens a specific sidebar tab. See [#32202](#) for further details.
- Allow slashes in generated resource routes in app framework. See [#31939](#) for further details.
- The app for embedding external sites to the app launcher (“*external*”) has been moved to a [separate repository](#). It is still bundled with ownCloud Server releases and can be used normally.

2.2 Changes in 10.0.9

Dear ownCloud administrator, please find below the changes and known issues in ownCloud Server 10.0.9 that need your attention. You can also read [the full ownCloud Server changelog](#) for further details on what has changed.

2.2.1 New Features

Pending Shares

ownCloud Server 10.0.9 introduces new features to close usability gaps and to give users more control over incoming shares. Previously, shared contents would appear, unannounced, in the receiving user’s file hierarchy, and clients would start synchronizing.

Incoming shares can now have a pending state, offering the ability to accept or decline (as known from federated sharing). We anticipate that this will provide a better user experience.

In addition, the [recently introduced notifications framework](#) is being used to inform users via mail.

The bell icon in the web interface and the ownCloud Desktop Client can additionally be used to take action. To switch to the new behavior administrators need to disable the configuration option “Automatically accept new incoming local user shares” in the *Sharing* settings section. By default the option will be enabled to preserve the known behavior.

Note: Mail notifications do not, currently, support asynchronous batch processing. For this reason, ownCloud will send notification emails directly when initiating shares between users. Due to this limitation, sharing with large groups (> 50 users) can take some time and might cause load peaks. [When operating installations with large groups, it is, therefore, not yet recommended to enable the feature.](#)

Overview of pending & rejected shares

In addition to the “*Pending Shares*” feature, ownCloud Server now provides the means to view “*accepted*”, “*pending*” and “*rejected*” incoming shares. Leveraging the “*Shared with you*” filter in the left sidebar of the files view users can now list all incoming shares, their respective states and have the ability to switch between the states easily.

This improvement not only empowers users to accept rejected shares subsequently but also to restore shares that have been unshared before without requiring the owner to share it again.

Password history and expiration

To prepare ownCloud Server for new capabilities in the authentication process, we have introduced an authentication middleware, and a new major version of the [Password Policy](#) extension is now available.

The Authentication Middleware

It:

1. Offers a defined way of inserting mandatory functionality between user authentication and user account access. For example, forcing users to accept legal agreements.
2. Affords the ability to interact with the user during the login process, such as retrieving user details like their email address.

Note: The authentication middleware is *currently* focused on offering new features for the Password Policy extension.

The Password Policy Extension

The Password Policy Extension has got a new major release and has been relicensed (OCL => GPLv2) to be available for community and standard subscription users as well. It now **supports password expiration and history policies for user accounts**.

Note: These features don't apply to users imported from LDAP or other backends but only for local users created by administrators or the [Guests](#) extension.

Imposing password expiration and history policies enhances security for a number of reasons. For example, by forcing users to choose a new password, they can be prevented from using one or more of their previous passwords. In doing this, it encourages them to not use a previous password, which may be known to attackers.

Two further examples are manually expiring passwords and configuring the number of days that have to pass since the last change before the password expires. These help ensure that users change their passwords on a semi-regular basis, making them harder to crack.

However, we encourage administrators to always consider the implication of their password policies, so that they strike an appropriate balance between security and usability. For example, a high frequency of password changes, for instance, might increase security but could also decrease user satisfaction.

To help ensure a good user experience it is possible to configure:

- Email notifications.
- Internal notifications (they appear on the web interface and clients).
- The password history count.
- The days before reminder notification are sent.

Users will always be informed when passwords have expired.

Note: Although the above two password practices are discouraged by NIST, ownCloud is now fully compliant with common password guidelines in enterprise scenarios.

Note: When users employ tokens for client authentication, which can be configured on the user settings page (“App passwords”), those are not affected from password policies.

Note: When imposing password expiration policies on an existing installation it is necessary to take some further actions. Please consult the [ownCloud documentation](#) for guidance.

Technology preview for new S3 Objectstore implementation

ownCloud Server 10.0.9 comes with the prerequisites to be ready for the new S3 Objectstore implementation “*files_primary_s3*”, which will massively improve performance, reliability and protocol-related capabilities. The new extension is available as a technology preview via the [ownCloud Marketplace](#) and will supersede the current Objectstore extension.

It has received extensive testing and is in very good shape. However, there is no out-of-the-box migration from the current *Objectstore* to *files_primary_s3* as this will require individual guidance.

Due to changes to the Versioning API, the [ownCloud Ransomware Protection](#) is not yet compatible with *files_primary_s3*. For now the *_Objectstore_* extension will continue to work as usual. Once the new implementation leaves the technology preview state and migrations have been taken care of, the current implementation will be deprecated.

2.2.2 SWIFT Objectstore deprecation

As the markets are moving in the direction of the [S3 protocol](#) to communicate with object storages, ownCloud will follow this path with a clear focus. To do this, it will be a necessity to deprecate object storage via the [OpenStack SWIFT protocol](#).

The extension will still be available as part of ownCloud Server, but it will neither be maintained nor developed any further by ownCloud, and support will be discontinued. Please make sure to move to the S3 protocol to use object storage as primary storage with future ownCloud Server versions.

2.2.3 New options to display Imprint and Privacy Policy

To enable GDPR and legal compliance in various jurisdictions for ownCloud providers, it is now possible to specify links to Imprint and Privacy Policy:

- In the “*General*” Administration settings section
- Via the following OCC commands:
 - `php occ config:app:set core legal.imprint_url <link>`
 - `php occ config:app:set core legal.privacy_policy_url <link>`

These links can be displayed on all pages of the ownCloud web interface and in the footer of mail notifications. When using one of the default themes provided by ownCloud, as well as the default mail templates, configured links will be automatically included.

For customized themes or mail templates, actions are required to include the links. These are:

1. Add the following at the end of each HTML template to add the footer:

```
<?php print_unescaped($this->inc('html.mail.footer', ['app' => 'core'])); ?>
```

1. Add the following at the end of each plain text template to add the footer:

```
<?php print_unescaped($this->inc('plain.mail.footer', ['app' => 'core'])); ?>
```

1. In a custom theme, change `getShortFooter` and `getLongFooter` in `defaults.php` without links to include the links

2.2.4 Changed behavior of “Exclude groups from sharing” option

The option “*Exclude groups from sharing*”, in the administration settings “*Sharing*” section, enables administrators to exclude groups of users from the ability to initiate file shares. In previous versions this restriction only applied to users who were members of exactly these groups (membership of one or more non-excluded groups bypassed the restriction).

This behavior has been changed to be both more restrictive and to better cover the expectations of administrators. With ownCloud Server 10.0.9, it will apply to all users who are members of at least one of the excluded groups.

2.2.5 Changes to the sharing autocomplete mechanism

In ownCloud Server 10.0.8, the value for *minimum characters to trigger the sharing autocomplete mechanism* has been made configurable and set to 4 by default. As this security-enhancing change came at the expense of usability, and might only be required in special scenarios, the default value has been reverted to 2.

For increased security requirements, the `config.php` option `'user.search_min_length' => 2` can be adjusted. To further improve usability, a hint has been added to inform users about the required character count, to get suggestions.

2.2.6 Improvements for `occ user:list`

To improve the usability of the `occ user:list` command, the output has been made configurable by using the `-a` option, for including certain attributes. This change has mainly been introduced to facilitate automation tasks. Check the `--help` option for more information.

2.2.7 Additional events for audit logging

New events are available for audit logging, among others. These include:

- Changes in user specific settings
- Sending public links via mail; and
- Accepting and rejecting shares

When logs are forwarded to external analyzers, like Splunk, administrators can check to add the new events. The latest version of the Auditing extension (`admin_audit`) is required.

2.2.8 Theming improvements and changes

- HTML templates for `lost password` mails have been added. This is important in case a custom theme is used and it needs manual adjustments.
- The mail notifications framework, *introduced with ownCloud Server 10.0.8*, has been extended to provide a basic framework and notification structure, which can be used by ownCloud features and third party extensions. To support this, mail template wording and structure have been updated. Please review the templates in `apps/notifications/templates/mail/` to align them with your needs.

- Mail templates can now include a footer for HTML (`core/templates/html.mail.footer.php`) and plain text mails (`core/templates/plain.mail.footer.php`). The default templates shipped with ownCloud Server 10.0.9 contain the respective references. For customized mail templates, it is necessary to manually add the references. To do so:
 - Add the following at the end of each HTML template:


```
<?php print_unescaped($this->inc('html.mail.footer', ['app' => 'core'])); ?>
```
 - Add the following at the end of each plain text template:


```
<?php print_unescaped($this->inc('plain.mail.footer', ['app' => 'core'])); ?>
```
- The ownCloud example theme (`theme-example`), which can be used as a solid base to create custom themes, is no longer bundled with ownCloud Server. It now lives in it's own [repository on GitHub](#).

2.2.9 Solved known issues

ownCloud Server 10.0.9 takes care of [10.0.8 known issues](#), and provides remedy for several others:

- Issues with multiple theme apps and the Mail Template Editor [#31478](#)
- OCC command to transfer data between users (`occ transfer:ownership`) works as expected again. Previously, public link shares were not transferred. See [#31176](#) for further details.
- OCC commands to encrypt (`occ encryption:encrypt-all`) and decrypt (`occ encryption:decrypt-all`) user data work correctly again. Previously, shares might have been lost during the encryption process. See [#31600](#) and [#31590](#) for further details.
- Files larger than 10 MB can now properly be uploaded by guest users. See [#31596](#) for further details.
- Issues with public link dialog when collaborative tags app is disabled has been resolved. See [#31581](#) for further details.
- Enabling/disabling of users by group administrators in the web UI works again. See [#31489](#) for further details.
- Issues with file upload using Microsoft EDGE are now circumvented (hard memory limit of 5 GB causing uploads to fail randomly as garbage collection for file chunks did not work properly). See [#31884](#) for further details.

2.2.10 Known issues

The new Password Policy feature “[Password Expiration](#)”:

- Does not work together with Multi-Factor Authentication (e.g. `twofactor_totp`, `twofactor_privacyidea`). Please do not deploy expiration policies yet when Two- or Multi-Factor Authentication extensions are in place. This issue will be solved with the next ownCloud Server release. See [#32059](#) for more information.
- The new Password Policy feature “[Password Expiration](#)” includes an `occ` command to manually force password expiration. Please run it directly after imposing expiration policies on an instance with existing users. Currently the command will only work when the policy *X days until user password expires* has been enabled. This might be confusing and will be solved with the next release of the extension. See [#66](#) for more information.

2.2.11 For developers

- The symfony event for logging has been extended to include the original exception when applicable: [#31623](#)

- Added Symfony event for whenever user settings are changed #31266
- Added Symfony event for whenever a public link share is sent by email #31632
- Added Symfony event for whenever local shares are accepted or rejected #31702
- Added public Webdav API for versions using a new “meta” DAV endpoint #31729 #29637
- Added support for retrieving file previews using Webdav endpoint #29319 #30192

2.3 Changes in 10.0.8

Dear ownCloud administrator, please find below the changes and known issues in ownCloud Server 10.0.8 that need your attention. You can also read [the full ownCloud Server changelog](#) for further details on what has changed.

2.3.1 PHP 5.6 deprecation

PHP 5.6/7.0 active support has ended on January 19th 2017 / December 3rd 2017 and security support [will be dropped by the end of 2018](#). Many libraries used by ownCloud (including the QA-Suite *PHPUnit*) will therefore not be maintained actively anymore which forces ownCloud to drop support in one of the next minor server versions as well. Please make sure to upgrade to PHP 7.1 as soon as possible. See the [system requirements in the ownCloud documentation](#).

2.3.2 Personal note for public link mail notification

One of the usability enhancements of ownCloud Server 10.0.8 is the possibility for users to add a personal note when sending public links via mail. When using customized mail templates it is necessary to either adapt the shipped original template to the customizations or to add the [code block](#) for the personal note to customized templates in order to display the personal note in the mail notifications.

2.3.3 New mail notifications feature

ownCloud Server 10.0.8 introduces a new extensible notification framework. Apart from technical changes under the hood the Notifications app can now also send mails for all notifications that previously were only displayed within the web interfaces (notification bell) or on the Desktop client (notifications API) like incoming federated share or Custom Group notifications, for example. In the “*General*” settings section users can configure whether they want to receive mails for all notifications, only for those that require an action or decide not to get notifications via mail (by default users will only receive notifications when an action is required).

2.3.4 LDAP-related improvements

- When disabling or deleting user accounts in LDAP, the administrator can choose to either *delete* or *disable* respective accounts in ownCloud when executing `occ user:sync (-m, --missing-account-action=MISSING-ACCOUNT-ACTION)`. User accounts that are disabled in ownCloud can now be re-enabled automatically when running `occ user:sync` if they are enabled in LDAP. When this behavior is desired administrators just need to add the `-r, --re-enable` option to their cron jobs or when manually executing `occ user:sync`.
- Furthermore it is now possible to execute `occ user:sync` only for *single* (`-u, --uid=UID`) or *seen* (`-s, --seenOnly`) users (users that are present in the database and have logged in at least once). These new options provide more granularity for administrators in terms of managing `occ user:sync` performance.

- Another notable change in behavior of `occ user:sync` is that administrators now have to explicitly specify the option `-c`, `--showCount` to display the number of users to be synchronized.

2.3.5 New events for audit logging

New events have been added to be used for audit logging, among others. These include *configuration changes* by administrators and users, *file comments (add/edit/delete)* and *updating existing public links*. When logs are forwarded to external analyzers like Splunk, administrators can check to add the new events. The latest version of the Auditing extension (*admin_audit*) is required.

2.3.6 New command to verify and repair file checksums

With ownCloud 10 file integrity checking by computing and matching checksums has been introduced to ensure that transferred files arrive at their target in the exact state as their origin. In some rare cases wrong checksums can be written to the database leading to synchronization issues with e.g. the Desktop Client. To mitigate such situations a new command `occ files:checksums:verify` has been introduced. The command recalculates checksums either for all files of a user or for files within a specified path, and compares them with the values in the database. Naturally the command also offers an option to repair incorrect checksum values (`-r`, `--repair`). Please check the available options by executing `occ files:checksums:verify --help`. Note: Executing this command might take some time depending on the file count.

2.3.7 New config setting to specify minimum characters for sharing autocomplete

For security reasons the default value for minimum characters to trigger the sharing autocomplete mechanism has been set to “4” (previously it was set to “2”). This is to prevent people from easily downloading lots of email addresses or user names by requesting their first letters through the API. As it is a trade-off between security and usability for some scenarios this high security level might not be desirable. Therefore the value now is configurable via the *config.php* option `'user.search_min_length' => 4,`. Please check which value fits your needs best.

2.3.8 New option to granularly configure public link password enforcement

With ownCloud 10 the “*File Drop*” feature has been merged with public link permissions. This kind of public link does not give recipients access to any content, but it gives them the possibility to “drop files”. As a result, it might not always be desirable to enforce password protection for such shares. Given that, passwords for public links can now be enforced based on permissions (*read-only*, *read & write*, *upload only/File Drop*). Please check the administration settings “*Sharing*” section and configure as desired.

2.3.9 New option to exclude apps from integrity check

By verifying signature files the *integrity check* ensures that the code running in an ownCloud instance has not been altered by third parties. Naturally this check can only be successful for code that has been obtained from official ownCloud sources. When providing custom apps (like theme apps) that do not have a signature, the integrity check will fail and notify the administrator. These apps can now be excluded from the *integrity check* by using the *config.php* option `'integrity.ignore.missing.app.signature' => ['app_id1', 'app_id2', 'app_id3'],`. See *config.sample.php* for more information.

2.3.10 New `occ` command to modify user details

It is now possible to modify user details like display names or mail addresses via the command `occ user:modify`. Please append `--help` for more information.

2.3.11 `occ files:scan` can now be executed for groups

Apart from using the `occ files:scan` command for *single users* and *whole instances* it can now be executed for *groups* using `-g, --groups=GROUPS`. Please append `--help` for more information.

2.3.12 New configurable default format for syslog

When using syslog as the log type (`'log_type' => 'syslog'`, in `config.php`) the default format has been changed to include *request IDs* for easier debugging. Additionally the log format has been made configurable using `'log.syslog.format'` in `config.php`. If you require a certain log format, please check the new format and `config.sample.php` on how to change it.

2.3.13 New config option to enable fallback to HTTP for federated shares

For security reasons federated sharing (sharing between different ownCloud instances) strictly requires HTTPS (SSL/TLS). When this behavior is undesired the insecure fallback to HTTP needs to be enabled explicitly by setting `'sharing.federation.allowHttpFallback' => false, to true` in `config.php`.

2.3.14 Migration related to `auth_tokens` (app passwords)

Upgrading to 10.0.8 includes migrations related to `auth_tokens` (*app passwords*). When users have created *app passwords* as separate passwords for their clients the upgrade duration will increase depending on user count. Please consider this when planning the upgrade.

2.3.15 Changed behavior of e-mail autocomplete for public link share dialog

When the “Sharing” settings option Allow users to send mail notifications for shared files for public links is enabled, users can send public links via mail from within the web interface. The behavior of the autocomplete when entering mail addresses in the public link share dialog has been changed. Previously the autocomplete queried for local users, users from federated address books and contacts from CardDAV/Contacts App. As public links are not intended for sharing between ownCloud users (local/federated), those have been removed. Contacts synchronized via CardDAV or created in the Contacts app will still appear as suggestions.

2.3.16 Notifications sent by `occ` can now include links

The command `occ notifications:generate` can be used to send notifications to individual users or groups. With 10.0.8 it is also capable of including links to such notifications using the `-l, --link=LINK` option. Please append `--help` for more information. There is also `Announcementcenter` to conduct such tasks from the web interface but it is currently limited to send notifications to all users. For now administrators can use the `occ` command if more granularity is required.

2.3.17 Global option for CORS domains

For security reasons ownCloud has a *Same-Origin-Policy* that prevents requests to ownCloud resources from other domains than the domain the backend server is hosted on. If ownCloud resources should be accessible from other domains, e.g. for a separate web frontend operated on a different domain, administrators can now globally specify policy exceptions via *CORS (Cross-Origin Resource Sharing)* using `'cors.allowed-domains'` in `config.php`. Please check `config.sample.php` for more information.

2.3.18 Mail Template Editor is now unbundled

The Mail Template Editor has been unbundled from the default apps and is not shipped with the Server anymore. When upgrading ownCloud will try to automatically [install the latest version from the ownCloud Marketplace](#) in case the app was installed before. If this is not possible (e.g. no internet connection or clustered setup) you will either need to disable the app (`occ app:disable templateeditor`) or [download and install it manually](#). Solved known issues ~~~~~ - Bogus “Login failed” log entries have been removed (see [10.0.7 known issues](#)) - The *Provisioning API* can now properly set default or zero quota - User quota settings can be queried through *Provisioning API* - A regression preventing a user from setting their e-mail address in the settings page has been fixed - File deletion as a guest user works correctly (trash bin permissions are checked correctly)

2.3.19 Known issues

- Issues with multiple theme apps and Mail Template Editor

As of ownCloud Server 10.0.5 it is only possible to have one theme app enabled simultaneously. When a theme app is enabled and the administrator attempts to enable a second one this will result in an error. However, when also having the Mail Template Editor enabled in this scenario the administrators “*General*” settings section [will be displayed incorrectly](#). As a remedy administrators can either uninstall the second theme app or disable the Mail Template Editor app.

- `occ transfer:ownership` does not transfer public link shares if they were created by the target user (reshare).

2.3.20 For developers

- The global JS variable “`oc_current_user`” was removed. Please use the public method “`OC.getCurrentUser()`” instead.
- Lots of new Symfony events have been added for various user actions, see changelog for details. Documentation ticket: <https://github.com/owncloud/documentation/issues/3738>‘_
- When requesting a private link there is a new HTTP response header “`Webdav-Location`” that contains the Webdav path to the requested file while the “`Location`” still points at the frontend URL for viewing the file.

2.4 Changes in 10.0.7

ownCloud Server 10.0.7 is a hotfix follow-up release that takes care of an [issue regarding OAuth authentication](#).

Please consider the ownCloud Server 10.0.5 release notes.

2.4.1 Known issues

- When using application passwords, log entries related to “Login Failed” will appear and can be ignored. For people using fail2ban or other account locking tools based on log parsing, please apply [this patch](#) with `patch -p1 < 50c78a4bf4c2ab4194f40111b8a34b7e9cc17a14.patch` ([original pull request here](#)).

2.5 Changes in 10.0.6

ownCloud Server 10.0.6 is a hotfix follow-up release that takes care of an issue during the build process (<https://github.com/owncloud/core/pull/30265>). Please consider the ownCloud Server 10.0.5 release notes.

2.6 Changes in 10.0.5

Dear ownCloud administrator, please find below the changes and known issues in ownCloud Server 10.0.5 that need your attention. You can also read [the full ownCloud Server changelog](#) for further details on what has changed.

2.6.1 Technology preview for PHP 7.2 support

ownCloud catches up with new web technologies. This has mainly been introduced for the open-source community to test and give feedback. PHP 7.2 is not yet supported nor recommended for production scenarios. ownCloud is going to fully support PHP 7.2 with the next major release.

2.6.2 php-intl now is a hard requirement

Please make sure to have the PHP extension installed before upgrading.

2.6.3 Changed: Only allow a single active theme app

The theming behavior has been changed so that only a single theme can be active concurrently. This change ensures that themes can not interfere in any way (e.g., override default theming in an arbitrary order). Please make sure to have the desired theme enabled after upgrading.

2.6.4 Removed old Dropbox external storage backend (Dropbox API v1)

Please switch to the new *External Storage: Dropbox* app (https://marketplace.owncloud.com/apps/files_external_dropbox) with Dropbox API v2 support to continue providing Dropbox external storages to your users.

2.6.5 Fixed: Only set CORS headers on WebDAV endpoint when Origin header is specified

ownCloud Server 10.0.4 known issue is resolved.

2.6.6 Fixes and improvements for the Mail Template Editor

- Known issues are resolved: Mail Template Editor works again, got support for app themes and additional templates were added for customization.
- Mail Template Editor is still bundled with ownCloud Server but will soon be released as a separate app to ownCloud Marketplace.
- Changelog: <https://github.com/owncloud/templateeditor/blob/release/0.2.0/CHANGELOG.md>

2.6.7 Known issues

- When using application passwords, [log entries related to “Login Failed”](#) will appear, please upgrade to 10.0.7 and check the fix mentioned in its release notes.

2.7 Changes in 10.0.4

Dear ownCloud administrator, please find below the changes and known issues in ownCloud Server 10.0.4 that need your attention. You can also read [the full ownCloud Server 10.0.4 changelog](#) for further details on what has changed.

2.7.1 More granular sharing restrictions

The “*Restrict users to only share with users in their groups*” option, in the Sharing settings, restricts users to only share with groups which they are a member of, while simultaneously prohibiting sharing with single users that do not belong to any of the users’ groups.

To make this more granular, we split this option into two parts and added “*Restrict users to only share with groups they are member of*”, which differentiates between users and groups. Doing so makes it possible to restrict users from sharing with all users of an installation, limiting them to only being able to share with groups which they are a member of, and vice versa.

2.7.2 Configurable solution for indistinguishable user display names

The ownCloud sharing dialog displays users according to their display name. As users can choose their display name in self-service (which can be disabled in *config.php*) and display names are not unique, it is possible that a user can’t distinguish sharing results. To cover this case the displayed user identifiers are now configurable. In the Sharing settings administrators can now configure the display of either mail addresses or user ids.

2.7.3 Added “occ files:scan” repair mode to repair filecache inconsistencies

We recommend to use this command when directed to do so in the upgrade process. Please refer to [the occ command’s files:scan –repair documentation](#) for more information.

2.7.4 Detailed mode for “occ security:routes”

Administrators can use the output of this command when using a network firewall, to check the appropriateness of configured rules or to get assistance when setting up.

2.7.5 Added mode of operations to differentiate between single-instance or clustered setup

As ownCloud needs to behave differently when operating in a clustered setup versus a single instance setup, the new *config.php* option `operation.mode` has been added. It can take one of two values: `single-instance` and `clustered-instance`. For example: `'operation.mode' => 'clustered-instance',,`

Currently the Market App (ownCloud Marketplace integration) does not support clustered setups and can do harm when used for installing or updating apps. The new config setting prevents this and other actions that are undesired in cluster mode.

When operating in a clustered setup, it is mandatory to set this option. Please check the [config_sample_php_parameters](#) documentation for more information.

2.7.6 Added `occ dav:cleanup-chunks` command to clean up expired uploads

When file uploads are interrupted for any reason, already uploaded file parts (chunks) remain in the underlying storage so that the file upload can resume in a future upload attempt. However, resuming an upload is only possible until the partial upload is expired and deleted, respectively.

To clean up chunks (expire and delete) originating from unfinished uploads, administrators can use this newly introduced command. The default expiry time is two days, but it can be specified as a parameter to the command. **It is recommended to configure CRON to execute this background job regularly.**

It is not included in the regular ownCloud background jobs so that the administrators have more flexibility in scheduling it. Please check [the background jobs configuration documentation](#) for more information.

2.7.7 Administrators can now exclude files from integrity check in `config.php`

When administrators did intentional changes to the ownCloud code they now have the ability to exclude certain files from the integrity checker. Please check “`config.sample.php`” for the usage of `'integrity.excluded.files'`.

2.7.8 Modification time value of files is now 64 bits long

When upgrading to 10.0.4 migrations may increase update duration dependent on number of files.

2.7.9 Updated minimum supported browser versions

Users with outdated browsers might get warnings. See [the list of supported browser versions](#).

2.7.10 Known issues

- When using application passwords, [log entries related to “Login Failed”](#) will appear, please upgrade to 10.0.7 and check the fix mentioned in its release notes.

2.7.11 10.0.3 resolved known issues

- [SFTP external storages with key pair mode](#) work again
- Added support for MariaDB 10.2.7+
- Encryption panel in admin settings fixed to properly detect current mode after upgrade to ownCloud 10

- Removed double quotes from boolean values in status.php output

2.7.12 Known issues

- Impersonate app 0.1.1 does not work with ownCloud Server 10.0.4. Please update to Impersonate 0.1.2 to be able to use the feature with ownCloud 10.0.4.
- Mounting ownCloud storage via davfs does not work

2.8 Changes in 10.0.3

Dear ownCloud administrator, please find below the changes and known issues of ownCloud Server 10.0.3 that need your attention:

The full ownCloud Server 10.0.3 changelog can be found here: <https://github.com/owncloud/core/blob/stable10/CHANGELOG.md>

- It is now possible to directly upgrade from 8.2.11 to 10.0.3 in a single upgrade process.
- Added occ command to list routes which can help administrators setting up network firewall rules.
- ‘occ upgrade’ is now verbose by default. Administrators may need to adjust scripts for automated setup/upgrade procedures that rely on ‘occ upgrade’ outputs.
- **Reenabled medial search by default**
 - Enables partial search in sharing dialog autocompletion (e.g. a user wants to share with the user “Peter”: Entering “pe” will find the user, entering “ter” will only find the user if the option is enabled)
 - New default is set to enabled as there is no performance impact anymore due to the introduction of the user account table in ownCloud Server 10.0.1.
 - Please check the setting. You need to disable it explicitly if the functionality is undesired.
- All database columns that use the fileid have been changed to bigint (64-bits). For large instances it is therefore highly recommended to upgrade in order to avoid reaching limits.
- **Upgrade and Market app information**
 - Removed “appstoreenabled” setting from config.php. If you want to disable the app store / Marketplace integration, please disable the Market app.
 - Added setting ‘upgrade.automatic-app-update’ to config.php to disable automatic app updates with ‘occ upgrade’ when Market app is enabled
 - On upgrade from OC < 10 the Market app won’t be enabled if “appstoreenabled” was false in config.php.
- Clustering: Better support of read only config file and apps folder
- Default minimum desktop client version in config.php is now 2.2.4.

Known issues

- Added quotes in boolean result values of yourdomain/status.php output
- Setting up SFTP external storages with keypairs does not work. <https://github.com/owncloud/core/issues/28669>
- If you have storage encryption enabled, the web UI for encryption will ask again what mode you want to operate with even if you already had a mode selected before. The administrator must select the mode they had selected before. <https://github.com/owncloud/core/issues/28985>

- Uploading a folder in Chrome in a way that would overwrite an existing folder can randomly fail (race conditions). <https://github.com/owncloud/core/issues/28844>
- Federated shares can not be accepted in WebUI for SAML/Shibboleth users
- For **MariaDB users**: Currently, Doctrine has no support for the breaking changes introduced in MariaDB 10.2.7, and above. If you are on MariaDB 10.2.7 or above, and have encountered the message “1067 Invalid default value for ‘lastmodified’”, [please apply this patch](#) to Doctrine. We expect this bug to be fixed in ownCloud 10.0.4. For more information on the bug, [check out the related issue](#).
- When updating from ownCloud < 9.0 the CLI output may hang for some time (potentially up to 20 minutes for big instances) whilst sharing is updated. This can happen in a variety of places during the upgrade and is to be expected. Please be patient as the update is performed and the output will continue as normal.

2.9 Changes in 10.0.1

Hello ownCloud administrator, please read carefully to be prepared for updates and operations of your ownCloud setup.

- **A new update path:** ownCloud 10.0.1 contains migration logic to allow upgrading directly from 9.0 to 10.0.1.
- **Marketplace:** Please create an account for [the new marketplace](#). Access to optional ownCloud extensions and enterprise apps will be provided by the marketplace from now on. Currently some apps are still shipped with the tarballs / packages and will be moved to the marketplace in the near future.
- **Apps:** *LDAP*, *gallery*, *activity*, *PDF viewer*, and *text editor* were moved to the marketplace.
- **Updates with marketplace:** During the upgrade, enabled apps are also updated by fetching new versions directly from the marketplace. If during an update, sources for some apps are missing, and the ownCloud instance has no access to the marketplace, the administrator needs to disable these apps or manually download and provide the apps before updating.
- **App updates:** Third party apps are not disabled anymore when upgrading.
- **Upgrade migration test:** The upgrade migration test has been removed; see *Test the Upgrade*. (Option `--skip-migration-tests` removed from update command).

Note: The template editor app is not included in the 10.0.1 release due to technical reasons, but will be distributed via the marketplace. However, you can still *edit template files manually*.

2.9.1 Settings

- **Settings design:** Admin, personal pages, and app management are now merged together into a single “Settings” entry.
- **Disable users:** The ability to disable users in the user management panel has been added.
- **Password Policy:** Rules now apply not only to link passwords but also to user passwords.

2.9.2 Infrastructure

- **Client:** You need to update to [the latest desktop client version](#).
- **Cron jobs:** The user account table has been reworked. As a result the Cron job for syncing user backends, e.g., LDAP, needs to be configured.

- **Logfiles:** App logs, e.g., auditing and `owncloud.log`, can now be split, see: https://doc.owncloud.org/server/latest/admin_manual/configuration/server/config_sample_php_parameters.html#logging.

2.9.3 Known Issues

Converting the Database Type doesn't work

Converting a Database from e.g. SQLite to MySQL or PostgreSQL with the `occ db:convert-type` currently doesn't work. See <https://github.com/owncloud/core/issues/27075> for more info.

Installing the LDAP user backend will trigger the installation twice

This causes an SQL error such as the following:

```
sudo -u www-data ./occ market:install user_ldap
user_ldap: Installing new app ...
user_ldap: An exception occurred while executing 'CREATE TABLE `ldap_user_mapping` (`ldap_dn` VARCHAR(255)
SQLSTATE[42S01]: Base table or view already exists: 1050 Table 'ldap_user_mapping' already exists
```

This can be safely ignored. And the app can be used after enabling it. Please be aware that when upgrading an existing ownCloud installation that already has `user_ldap` this error will not occur. It was fixed by <https://github.com/owncloud/core/pull/27982>. However, this could happen for other apps as well that use `database.xml`. If it does please use the same workaround.

SAML authentication only works for users synced with `occ user:sync`

We will re-enable SSO for LDAP users with an update of the app in the market after completing internal testing.

The web UI prevents uninstalling apps marked as shipped, e.g., `user_ldap`

To uninstall, disable the app with `occ` and `rm` the app directory.

Moving files around in external storages outside of ownCloud will invalidate the metadata

All shares, comments, and tags on the moved files will be lost.

Existing LDAP users only show up in the user management page and the share dialog after being synced

The account table introduced in ownCloud 10.0.0 significantly reduces LDAP communication overhead. Password checks are yet to be accounted for. LDAP user metadata in the account table will be updated when users log in or when the administrator runs `occ user:sync "OCA\User_LDAP\User_Proxy"`. We recommend *setting up a nightly Cron job* to keep metadata of users not actively logging in up to date.

Error pages will not use the configured theme but will instead fall back to the community default

2.10 Changes in 10.0.0

- PHP 7.1 support added (supported PHP versions are 5.6 and 7.0+)
- The upgrade migration test has been removed; see *Test the Upgrade*. (Option "--skip-migration-tests" removed from update command)
- Requires to use the latest desktop client version 2.3
- Third party apps are not disabled anymore when upgrading
- User account table has been reworked. CRON job for syncing with e.g. LDAP needs to be configured (see https://doc.owncloud.com/server/latest/admin_manual/configuration/server/occ_command.html#syncing-user-accounts)
- LDAP app is not released with ownCloud 10.0.0 and will be released on the marketplace after some more QA
- files_drop app is not shipped anymore as it's integrated with core now. Since migrations are not possible you will have to reconfigure your drop folders (in the 'Public Link' section of the sharing dialog of the respective folders).
- SAML/Shibboleth with device-specific app passwords: No migration possible; Users need to regenerate device-specific app passwords in the WebUI and enter those in their clients.
- For security reasons status.php can now be configured in config.php to not return server version information anymore ('version.hide'; default 'false'). As clients still depend on version information this is not yet recommended. The default will change to 'true' with 10.0.2 once clients are ready.
- Order of owncloud.log entries changed a bit, please review any application (e.g. fail2ban rules) relying on this file
- **External storages**
 - FTP external storage moved to a separate app (https://marketplace.owncloud.com/apps/files_external_ftp)
 - "Local" storage type can now be disabled by sysadmin in config.php (to prevent users mounting the local file system)

Full changelog: <https://github.com/owncloud/core/wiki/ownCloud-10.0-Features>

2.11 Changes in 9.1

General

- Background jobs (cron) can now run in parallel
- Update notifications in client via API - You can now be notified in your desktop client about available updates for core and apps. The notifications are made available via the notifications API.
- Multi-bucket support for primary objectstore integration
- Support for Internet Explorer below version 11 was dropped
- Symlinks pointing outside of the data directory are disallowed. Please use the *Configuring External Storage (GUI)* with the *Local* storage backend instead.
- Removed `dav:migrate-calendars` and `dav:migrate-addressbooks` commands for `occ`. Users planning to upgrade from ownCloud 9.0 or below to ownCloud 9.1 needs to make sure that their calendars and address books are correctly migrated **before** continuing to upgrade to 9.1.

Authentication

- Pluggable authentication: plugin system that supports different authentication schemes
- Token-based authentication
- Ability to invalidate sessions
- List connected browsers/devices in the personal settings page. Allows the user to disconnect browsers/devices.
- Device-specific passwords/tokens, can be generated in the personal page and revoked
- Disable users and automatically revoke their sessions
- Detect disabled LDAP users or password changes and revoke their sessions
- Log in with email address
- Configuration option to enforce token-based login outside the web UI
- Two Factor authentication plug-in system
- OCC command added to (temporarily) disable/enable two-factor authentication for single users

Note: The current desktop and mobile client versions do not support two-factor yet, this will be added later. It is already possible to generate a device specific password and enter that in the current client versions.

Files app

- Ability to toggle displaying hidden files
- Remember sort order
- Permalinks for internal shares
- Visual cue when dragging in files app
- Autoscroll file list when dragging files
- Upload progress estimate

Federated sharing

- Ability to create federated shares with CRUDS permissions
- Resharing a federated share does not create a chain of shares any more but connects the share owner's server to the reshare recipient

External storage

- UTF-8 NFD encoding compatibility support for NFD file names stored directly on external storages (new mount option in external storage admin page)
- Direct links to the configuration pages for setting up a GDrive or Dropbox application for use with ownCloud
- Some performance and memory usage improvements for GDrive, stream download and chunk upload
- Performance and memory usage improvements for Dropbox with stream download
- GDrive library update provides exponential backoff which will reduce rate limit errors

Shibboleth

- The WebDAV endpoint was changed from `/remote.php/webdav` to `/remote.php/dav`. You need to check your Apache configuration if you have exceptions or rules for WebDAV configured.

Minor additions

- Support for print style sheets

- Command line based update will now be suggested if the instance is bigger to avoid potential timeouts
- Web updater will be disabled if LDAP or shibboleth are installed
- DB/application update process now shows better progress information
- Added `occ files:scan --unscanned` to only scan folders that haven't yet been explored on external storages
- Chunk cache TTL can now be configured
- Added warning for wrongly configured database transactions, helps prevent “database is locked” issues
- Use a capped memory cache to reduce memory usage especially in background jobs and the file scanner
- Allow login by email
- Respect CLASS property in calendar events
- Allow addressbook export using VCFExportPlugin
- Birthdays are also generated based on shared addressbooks

For developers

- New DAV endpoint with a new chunking protocol aiming to solve many issues like timeouts (not used by clients yet)
- New webdav property for share permissions
- Background repair steps can be specified in `info.xml`
- Background jobs (cron) can now be declared in `info.xml`
- Apps can now define repair steps to run at install/uninstall time
- Export contact images via Sabre DAV plugin
- Sabre DAV's browser plugin is available in debug mode to allow easier development around webdav

Technical debt

- PSR-4 autoloading forced for `OC\` and `OCP\`, optional for `OCA\` docs at https://doc.owncloud.org/server/latest/developer_manual/app/classloader.html
- More cleanup of the sharing code (ongoing)

2.12 Changes in 9.0

9.0 requires `.ico` files for favicons. This will change in 9.1, which will use `.svg` files. See [Changing favicon](#) in the Developer Manual.

Home folder rule is enforced in the `user_ldap` application in new ownCloud installations; see [User Authentication with LDAP](#). This affects ownCloud 8.0.10, 8.1.5 and 8.2.0 and up.

The Calendar and Contacts apps have been rewritten and the CalDAV and CardDAV backends of these apps were merged into ownCloud core. During the upgrade existing Calendars and Addressbooks are automatically migrated (except when using the IMAP user backend). As a fallback for failed upgrades, when using the IMAP user backend or as an option to test a migration `dav:migrate-calendars` and/or `dav:migrate-addressbooks` scripts are available (**only in ownCloud 9.0**) via the `occ` command. See [Using occ core commands](#).

Warning: After upgrading to ownCloud 9.0 and **before** continuing to upgrade to 9.1 make sure that all of your and your users Calendars and Addressbooks are migrated correctly. Especially when using the IMAP user backend (other user backends might be also affected) you need to manually run the mentioned `occ` migration commands described above.

Updates on systems with large datasets will take longer, due to the addition of checksums to the ownCloud database. See <https://github.com/owncloud/core/issues/22747>.

Linux packages are available from our [official download repository](#). New in 9.0: split packages. `owncloud` installs ownCloud plus dependencies, including Apache and PHP. `owncloud-files` installs only ownCloud. This is useful for custom LAMP stacks, and allows you to install your own LAMP apps and versions without packaging conflicts with ownCloud. See [Linux Package Manager Installation](#).

New option for the ownCloud admin to enable or disable sharing on individual external mountpoints (see [Mount Options](#)). Sharing on such mountpoints is disabled by default.

2.12.1 Enterprise 9.0

`owncloud-enterprise` packages are no longer available for CentOS 6, RHEL6, Debian 7, or any version of Fedora. A new package, `owncloud-enterprise-files`, is available for all supported platforms, including the above. This new package comes without dependencies, and is installable on a larger number of platforms. System administrators must install their own LAMP stacks and databases. See <https://owncloud.org/blog/time-to-upgrade-to-owncloud-9-0/>

2.13 Changes in 8.2

New location for Linux package repositories; ownCloud admins must manually change to the new repos. See [How to Upgrade Your ownCloud Server](#)

PHP 5.6.11+ breaks the LDAP wizard with a 'Could not connect to LDAP' error. See <https://github.com/owncloud/core/issues/20020>.

`filesystem_check_changes` in `config.php` is set to 0 by default. This prevents unnecessary update checks and improves performance. If you are using external storage mounts such as NFS on a remote storage server, set this to 1 so that ownCloud will detect remote file changes.

XSendFile support has been removed, so there is no longer support for [serving static files](#) from your ownCloud server.

LDAP issue: 8.2 uses the `memberof` attribute by default. If this is not activated on your LDAP server your user groups will not be detected, and you will see this message in your ownCloud log: `Error PHP Array to string conversion at /var/www/html/owncloud/lib/private/template/functions.php#36`. Fix this by disabling the `memberof` attribute on your ownCloud server with the `occ` command, like this example on Ubuntu Linux:

```
sudo -u www-data php occ ldap:set-config "s01" useMemberOfToDetectMembership 0
```

Run `sudo -u www-data php occ ldap:show-config` to find the correct `sNN` value; if there is not one then use empty quotes, `" "`. (See [Using occ core commands](#).)

Users of the Linux Package need to update their repository setup as described in this [blogpost](#).

2.14 Changes in 8.1

Use APCu only if available in version 4.0.6 and higher. If you install an older version, you will see a APCu below version 4.0.6 is installed, for stability and performance reasons we recommend

to update to a newer APCu version warning on your ownCloud admin page.

SMB external storage now based on `php5-libsmbclient`, which must be downloaded from the ownCloud software repositories ([installation instructions](#)).

“Download from link” feature has been removed.

The `.htaccess` and `index.html` files in the `data/` directory are now updated after every update. If you make any modifications to these files they will be lost after updates.

The SabreDAV browser at `/remote.php/webdav` has been removed.

Using ownCloud without a `trusted_domain` configuration will not work anymore.

The logging format for failed logins has changed and considers now the proxy configuration in `config.php`.

A default set of security and privacy HTTP headers have been added to the ownCloud `.htaccess` file, and ownCloud administrators may now customize which headers are sent.

More strict SSL certificate checking improves security but can result in “cURL error 60: SSL certificate problem: unable to get local issuer certificate” errors with certain broken PHP versions. Please verify your SSL setup, update your PHP or contact your vendor if you receive these errors.

The persistent file-based cache (e.g. used by LDAP integration) has been dropped and replaced with a memory-only cache, which must be explicitly configured. See [User Authentication with LDAP](#). Memory cache configuration for the ownCloud server is no longer automatic, requiring installation of your desired cache backend and configuration in `config.php` (see [Memory Caching](#).)

The `OC_User_HTTP` backend has been removed. Administrators are encouraged to use the `user_webdavauth` application instead.

ownCloud ships now with its own root certificate bundle derived from Mozilla’s root certificates file. The system root certificate bundle will not be used anymore for most requests.

When you upgrade from ownCloud 8.0, with encryption enabled, to 8.1, you must enable the new encryption backend and migrate your encryption keys. See [Enabling Master Key Based Encryption from the Command-Line](#).

Encryption can no longer be disabled in ownCloud 8.1. It is planned to re-add this feature to the command line client for a future release.

It is not recommended to upgrade encryption-enabled systems from ownCloud Server 8.0 to version 8.1.0 as there is a chance the migration will break. We recommend migrating to the first bugfix release, ownCloud Server 8.1.1.

Due to various technical issues, by default desktop sync clients older than 1.7 are not allowed to connect and sync with the ownCloud server. This is configurable via the `minimum.supported.desktop.version` switch in `config.php`.

Previews are now generated at a maximum size of 2048 x 2048 pixels. This is configurable via the `preview_max_x` and `preview_max_y` switches in `config.php`.

The ownCloud 8 server is not supported on any version of Windows.

The 8.1.0 release has a minor bug which makes application updates fail at first try. Reload the apps page and try again, and the update will succeed.

The `forcessl` option within the `config.php` and the `Enforce SSL` option within the Admin-Backend was removed. This now needs to be configured like described in [Use HTTPS](#).

WebDAV file locking was removed in ownCloud 8.1 which causes Finder on Mac OS X to mount WebDAV read-only.

2.14.1 Enterprise 8.1

The SharePoint Drive application does not verify the SSL certificate of the SharePoint server or the ownCloud server, as it is expected that both devices are in the same trusted environment.

2.15 Changes in 8.0

2.15.1 Manual LDAP Port Configuration

When you are configuring the LDAP user and group backend application, ownCloud may not auto-detect the LDAP server's port number, so you will need to enter it manually.

2.15.2 No Preview Icon on Text Files

There is no preview icon displayed for text files when the file contains fewer than six characters.

2.15.3 Remote Federated Cloud Share Cannot be Reshared With Local Users

When you mount a Federated Cloud share from a remote ownCloud server, you cannot re-share it with your local ownCloud users. (See *Configuring Federation Sharing* to learn more about federated cloud sharing)

2.15.4 Manually Migrate Encryption Keys after Upgrade

If you are using the Encryption application and upgrading from older versions of ownCloud to ownCloud 8.0, you must manually migrate your encryption keys. See *Enabling Master Key Based Encryption from the Command-Line*.

2.15.5 Windows Server Not Supported

Windows Server is not supported in ownCloud 8.

2.15.6 PHP 5.3 Support Dropped

PHP 5.3 is not supported in ownCloud 8, and PHP 5.4 or better is required.

2.15.7 Disable Apache Multiviews

If Multiviews are enabled in your Apache configuration, this may cause problems with content negotiation, so disable Multiviews by removing it from your Apache configuration. Look for lines like this:

```
<Directory /var/www/owncloud>  
Options Indexes FollowSymLinks Multiviews
```

Delete `Multiviews` and restart Apache.

2.15.8 ownCloud Does Not Follow Symlinks

ownCloud's file scanner does not follow symlinks, which could lead to infinite loops. To avoid this do not use soft or hard links in your ownCloud data directory.

2.15.9 No Commas in Group Names

Creating an ownCloud group with a comma in the group name causes ownCloud to treat the group as two groups.

2.15.10 Hebrew File Names Too Large on Windows

On Windows servers Hebrew file names grow to five times their original size after being translated to Unicode.

2.15.11 Google Drive Large Files Fail with 500 Error

Google Drive tries to download the entire file into memory, then write it to a temp file, and then stream it to the client, so very large file downloads from Google Drive may fail with a 500 internal server error.

2.15.12 Encrypting Large Numbers of Files

When you activate the Encryption application on a running server that has large numbers of files, it is possible that you will experience timeouts. It is best to activate encryption at installation, before accumulating large numbers of files on your ownCloud server.

2.15.13 Enterprise 8.0

Sharepoint Drive SSL Not Verified

The SharePoint Drive application does not verify the SSL certificate of the SharePoint server or the ownCloud server, as it is expected that both devices are in the same trusted environment.

No Federated Cloud Sharing with Shibboleth

Federated Cloud Sharing (formerly Server-to-Server file sharing) does not work with Shibboleth .

Direct Uploads to SWIFT do not Appear in ownCloud

When files are uploaded directly to a SWIFT share mounted as external storage in ownCloud, the files do not appear in ownCloud. However, files uploaded to the SWIFT mount through ownCloud are listed correctly in both locations.

SWIFT Objectstore Incompatible with Encryption App

The current SWIFT implementation is incompatible with any application that uses direct file I/O and circumvents the ownCloud virtual filesystem. Using the Encryption application on a SWIFT object store incurs twice as many HTTP requests and increases latency significantly.

application Store is Back

The ownCloud application Store has been re-enabled in ownCloud 8. Note that third-party apps are not supported.

2.16 Changes in 7.0

2.16.1 Manual LDAP Port Configuration

When you are configuring the LDAP user and group backend application, ownCloud may not auto-detect the LDAP server's port number, so you will need to enter it manually.

2.16.2 LDAP Search Performance Improved

Prior to 7.0.4, LDAP searches were substring-based and would match search attributes if the substring occurred anywhere in the attribute value. Rather, searches are performed on beginning attributes. With 7.0.4, searches will match at the beginning of the attribute value only. This provides better performance and a better user experience.

Substring searches can still be performed by prepending the search term with “*”. For example, a search for `te` will find Terri, but not Nate:

```
occ ldap:search "te"
```

If you want to broaden the search to include Nate, then search for `*te`:

```
occ ldap:search "*te"
```

Refine searches by adjusting the `User Search Attributes` field of the `Advanced` tab in your LDAP configuration on the `Admin` page. For example, if your search attributes are `givenName` and `sn` you can find users by first name + last name very quickly. For example, you'll find Terri Hanson by searching for `te ha`. Trailing whitespaces are ignored.

2.16.3 Protecting ownCloud on IIS from Data Loss

Under certain circumstances, running your ownCloud server on IIS could be at risk of data loss. To prevent this, follow these steps.

- In your ownCloud server configuration file, `owncloud\config\config.php`, set `config_is_read_only` to `true`.
- Set the `config.php` file to read-only.
- When you make server updates `config.php` must be made writeable. When your updates are completed re-set it to read-only.

2.16.4 Antivirus Application Modes

The Antivirus application offers three modes for running the ClamAV anti-virus scanner: as a daemon on the ownCloud server, a daemon on a remote server, or an executable mode that calls `clamscan` on the local server. We recommend using one of the daemon modes, as they are the most reliable.

2.16.5 “Enable Only for Specific Groups” Fails

Some ownCloud applications have the option to be enabled only for certain groups. However, when you select specific groups they do not get access to the app.

2.16.6 Changes to File Previews

For security and performance reasons, file previews are available only for image files, covers of MP3 files, and text files, and have been disabled for all other filetypes. Files without previews are represented by generic icons according to their file types.

2.16.7 4GB Limit on SFTP Transfers

Because of limitations in `phpseclib`, you cannot upload files larger than 4GB over SFTP.

2.16.8 “Not Enough Space Available” on File Upload

Setting user quotas to `unlimited` on an ownCloud installation that has unreliable free disk space reporting– for example, on a shared hosting provider– may cause file uploads to fail with a “Not Enough Space Available” error. A workaround is to set file quotas for all users instead of `unlimited`.

2.16.9 No More Expiration Date On Local Shares

In older versions of ownCloud, you could set an expiration date on both local and public shares. Now you can set an expiration date only on public shares, and local shares do not expire when public shares expire.

2.16.10 Zero Quota Not Read-Only

Setting a user’s storage quota should be the equivalent of read-only, however, users can still create empty files.

2.16.11 Enterprise 7.0

No Federated Cloud Sharing with Shibboleth

Federated Cloud Sharing (formerly Server-to-Server file sharing) does not work with Shibboleth .

Windows Network Drive

Windows Network Drive runs only on Linux servers because it requires the Samba client, which is included in all Linux distributions.

`php5-libsmbclient` is also required, and there may be issues with older versions of `libsmbclient`; see Using External Storage > Installing and Configuring the Windows Network Drive application in the Enterprise Admin manual for more information.

By default CentOS has activated SELinux, and the `httpd` process can not make outgoing network connections. This will cause problems with `curl`, LDAP and `samba` libraries. Again, see Using External Storage > Installing and Configuring the Windows Network Drive application in the Enterprise Admin manual for instructions.

Sharepoint Drive SSL

The SharePoint Drive application does not verify the SSL certificate of the SharePoint server or the ownCloud server, as it is expected that both devices are in the same trusted environment.

Shibboleth and WebDAV Incompatible

Shibboleth and standard WebDAV are incompatible, and cannot be used together in ownCloud. If Shibboleth is enabled, the ownCloud client uses an extended WebDAV protocol

No SQLite

SQLite is no longer an installation option for ownCloud Enterprise Edition, as it not suitable for multiple-user installations or managing large numbers of files.

No Application Store

The application Store is disabled for the Enterprise Edition.

LDAP Home Connector Linux Only

The LDAP Home Connector application requires Linux (with MySQL, MariaDB, or PostgreSQL) to operate correctly.

WHAT'S NEW IN OWNCLOUD 10.0.10

See the [ownCloud 10.0 Features page](#) on Github for a comprehensive list of new features and updates.

INSTALLATION

4.1 System Requirements

4.1.1 Officially Recommended & Supported Options

For *best performance, stability, support, and full functionality* we officially recommend and support:

Server

Platform	Options
Operating System	<ul style="list-style-type: none">• Ubuntu 16.04 and 18.04• Debian 7 and 8• Red Hat Enterprise Linux 6 and 7• Centos Linux 6 and 7• Fedora 27 and 28• SUSE Linux Enterprise Server 12 with SP1, SP2 and SP3• openSUSE Tumbleweed and Leap 15.0, 42.3• Ubuntu 16.04 and 18.04
Database	<ul style="list-style-type: none">• MySQL or MariaDB 5.5+• Oracle 11g• PostgreSQL• SQLite
Web server	<ul style="list-style-type: none">• Apache 2.4 with prefork <i>Multi-Processing Module (MPM)</i> and mod_php
PHP Runtime*	<ul style="list-style-type: none">• 5.6, 7.0, 7.1 & 7.2

Note: *We strongly encourage you to migrate to PHP 7.2. *Ubuntu comes with the full set of required packages out of the box. All other distributions may require additional repositories to deliver certain functionality.

Important: For the future release of ownCloud 10.1, a minimum php version of 7.1 is needed. If you use Ubuntu 16.04:

- PHP 7.1 and 7.2 are only available via ppa. To add a ppa to your system, use this command: `sudo add-apt-repository ppa:user/ppa-name`.
-

Note:

- Red Hat Enterprise Linux & Centos 7 are 64-bit only.
 - Oracle 11g is only supported for the Enterprise edition.
 - SQLite is not encouraged for production use.
-

Mobile

- iOS 9.0+
- Android 4.0+

Web Browser

- Edge (current version on Windows 10)
- IE11+ (except Compatibility Mode)
- Firefox 62 or 60.2 ESR
- Google Chrome 68+
- Safari 11

Hypervisors

- Hyper-V
- VMware ESX
- Xen
- KVM

Desktop

- Windows 7, 8+
- Mac OS X 10.12+ (**64-bit only**)
- CentOS 6 & 7 (64-bit only)
- Debian 7 & 8
- Fedora 27 & 28
- Ubuntu 16.04 & 18.04
- openSUSE Leap 15.0, 42.3

Note: For Linux distributions, we support, if technically feasible, the latest 2 versions per platform and the previous [LTS](#).

4.1.2 Alternative (But Unsupported) Options

If you are not able to use one or more of the above tools, the following options are also available.

Web Server

- NGINX with PHP-FPM

4.1.3 Memory Requirements

Memory requirements for running an ownCloud server are greatly variable, depending on the numbers of users and files, and volume of server activity. ownCloud officially requires a minimum of 128MB RAM. But, we recommend a minimum of 512MB.

Note: *Consideration for low memory environments*

Scanning of files is committed internally in 10k files chunks. Based on tests, server memory usage for scanning greater than 10k files uses about 75MB of additional memory.

4.1.4 Database Requirements

The following are currently required if you're running ownCloud together with a MySQL or MariaDB database:

- Disabled or `BINLOG_FORMAT = MIXED` or `BINLOG_FORMAT = ROW` configured Binary Logging (See: *MySQL / MariaDB with Binary Logging Enabled*)
- InnoDB storage engine (The MyISAM storage engine is not supported, see: *MySQL / MariaDB storage engine*)
- “READ COMMITTED” transaction isolation level (See: *MySQL / MariaDB “READ COMMITTED” transaction isolation level*)

4.2 Deployment Recommendations

What is the best way to install and maintain ownCloud? The answer to that is, as always: “*it depends*”.

This is because every ownCloud customer has their own particular needs and IT infrastructure. However, both ownCloud and the LAMP stack are highly-configurable. Given that, in this document we present a set of general recommendations, followed by three typical scenarios, and finish up with making best-practice recommendations for both software and hardware.

Note: The recommendations presented here are based on a standard ownCloud installation, one without any particular *apps*, *themes*, or *code changes*. But, server load is dependent upon the number of *clients*, *files*, and *user activity*, as well as other usage patterns. Given that, these recommendations are only a rule of thumb based on our experience, as well as that of one of our customers.

4.2.1 General Recommendations

- Operating system: Linux.
- Web server: Apache 2.4.

- Database: MySQL/MariaDB with InnoDB storage engine (MyISAM is not supported, see: [MySQL / MariaDB storage engine](#))
- PHP 5.6+.
- Consider setting up a scale-out deployment, or using [Federated Cloud Sharing](#) to keep individual ownCloud instances to a manageable size.

Note: Whatever the size of your organization, always keep one thing in mind: *The amount of data stored in ownCloud will only grow. So plan ahead.*

4.2.2 ownCloud Administrators Must Have Command Line or Cron Access

We only recommend using hosts that provide command-line or Cron access (ideally both) to *ownCloud administrators*, for three key reasons:

1. Without command-line access, *OCC commands*, required for administrative tasks such as repairs and upgrades, are not available.
2. Without crontab access, you cannot run background jobs reliably. *ajax/cron.php* is available, but it is not reliable enough, because it only runs when people are using the web UI. Additionally, ownCloud relies heavily on *background jobs* especially for long-running operations, which will likely cause PHP timeouts.
3. PHP timeout values are often low. Having low timeout settings can break long-running operations, such as moving a huge folder.

4.2.3 Scenario 1: Small Workgroups and Departments

This recommendation applies if you meet the following criteria:

Option	Value
Number of users	Up to 150 users
Storage size	100 GB to 10TB
High availability level	Zero-downtime backups via Btrfs snapshots, component failure leads to interruption of service. Alternate backup scheme on other filesystems: nightly backups — with service interruption.

Recommended System Requirements

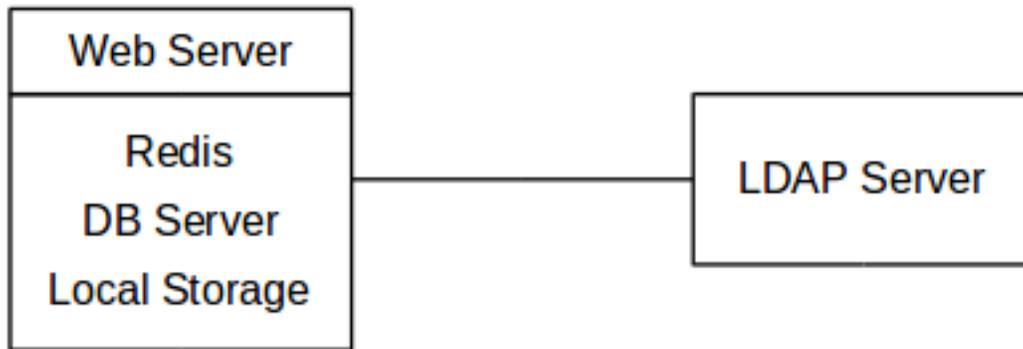
One machine running the application, web, and database server, as well as local storage. Authentication via an existing LDAP or Active Directory server.

Components

One server with at least 2 CPU cores, 16GB RAM, and local storage as needed.

Operating system

Enterprise-grade Linux distribution with full support from an operating system vendor. We recommend both RedHat Enterprise Linux and SUSE Linux Enterprise Server 12.



SSL Configuration

The SSL termination is done in Apache. A standard SSL certificate is required to be installed according to [the official Apache documentation](#).

Load Balancer

None.

Database

MySQL, MariaDB, or PostgreSQL. We currently recommend MySQL / MariaDB, as our customers have had good experiences when moving to a Galera cluster to scale the DB. If using either MySQL or MariaDB, you must use the InnoDB storage engine as MyISAM is not supported, see: [MySQL / MariaDB storage engine](#)

Warning: If you are using MaxScale/Galera, then you need to use at least version 1.3.0. In earlier versions, there is a bug where the value of `last_insert_id` is not routed to the master node. This bug can cause loops within ownCloud and corrupt database rows. You can find out more information [in the issue documentation](#).

Backup

Install ownCloud, the ownCloud data directory, and database on a [Btrfs filesystem](#). Make regular snapshots at desired intervals for zero downtime backups. Mount DB partitions with the “`nodatacow`” option to prevent fragmentation.

Alternatively, you can make nightly backups — with service interruption — as follows:

1. Shut down Apache.
2. Create database dump.
3. Push data directory to backup.
4. Push database dump to backup.
5. Start Apache.

After these steps have been completed, then, optionally, rsync the backup to either an external backup storage or tape backup. See the [Maintenance](#) section of the Administration manual for tips on backups and restores.

Authentication

User authentication via one or several LDAP or Active Directory (AD) servers. See [User Authentication with LDAP](#) for information on configuring ownCloud to use LDAP and AD.

Session Management

Local session management on the application server. PHP sessions are stored in a temporary filesystem, mounted at the operating system-specific session storage location. You can find out where that is by running `grep -R 'session.save_path' /etc/php5` and then add it to the `/etc/fstab` file, for example:

```
echo "tmpfs /var/lib/php5/pool-www tmpfs defaults,noatime,mode=1777 0 0" >> /etc/fstab``
```

Memory Caching

A memory cache speeds up server performance, and ownCloud supports four of them. Refer to [Configuring Memory Caching](#) for information on selecting and configuring a memory cache.

Storage

Local storage.

ownCloud Edition

Standard Edition. See [ownCloud Server](#) or [Enterprise Edition](#) for comparisons of the ownCloud editions.

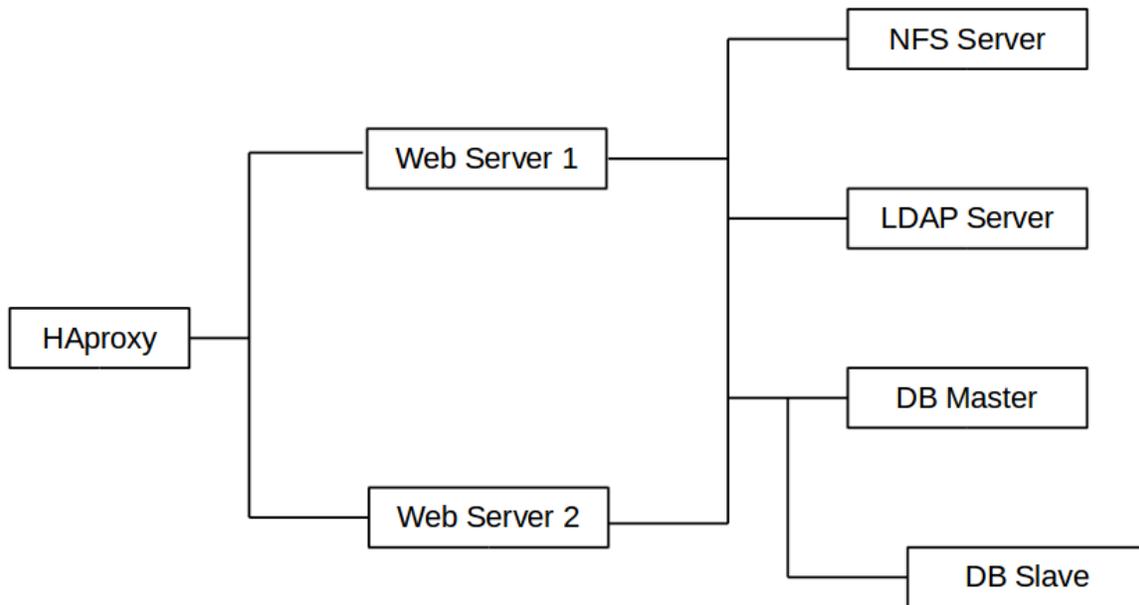
4.2.4 Scenario 2: Mid-Sized Enterprises

These recommendations apply if you meet the following criteria:

Option	Value
Number of users	150 to 1,000 users.
Storage size	Up to 200TB.
High availability level	Every component is fully redundant and can fail without service interruption. Backups without service interruption

Recommended System Requirements

- 2 to 4 application servers.
- A cluster of two database servers.
- Storage on an NFS server.
- Authentication via an existing LDAP or Active Directory server.



Components

- 2 to 4 application servers with four sockets and 32GB RAM.
- 2 DB servers with four sockets and 64GB RAM.
- 1 HAProxy load balancer with two sockets and 16GB RAM.
- NFS storage server as needed.

Operating System

Enterprise grade Linux distribution with full support from an operating system vendor. We recommend both RedHat Enterprise Linux and SUSE Linux Enterprise Server 12.

SSL Configuration

The SSL termination is done in the HAProxy load balancer. A standard SSL certificate is needed, installed according to the HAProxy documentation.

Load Balancer

HAProxy running on a dedicated server in front of the application servers. Sticky session needs to be used because of local session management on the application servers.

Database

MySQL/MariaDB Galera cluster with [master-master replication](#). InnoDB storage engine, MyISAM is not supported, see: [MySQL / MariaDB storage engine](#).

Backup

Minimum daily backup without downtime. All MySQL/MariaDB statements should be replicated to a backup MySQL/MariaDB slave instance.

- Create a snapshot on the NFS storage server.
- At the same time stop the MySQL replication.
- Create a MySQL dump of the backup slave.
- Push the NFS snapshot to the backup.
- Push the MySQL dump to the backup.
- Delete the NFS snapshot.
- Restart MySQL replication.

Authentication

User authentication via one or several LDAP or Active Directory servers. See [User Authentication with LDAP](#) for information on configuring ownCloud to use LDAP and AD.

Session Management

Session management on the application server. PHP sessions are stored in a temporary filesystem, mounted at the operating system-specific session storage location. You can find out where that is by running `grep -R 'session.save_path' /etc/php5` and then add it to the `/etc/fstab` file, for example:

```
echo "tmpfs /var/lib/php5/pool-www tmpfs defaults,noatime,mode=1777 0 0" >> /etc/fstab
```

Memory Caching

A memory cache speeds up server performance, and ownCloud supports four memory cache types. Refer to [Configuring Memory Caching](#) for information on selecting and configuring a memory cache.

Storage

Use an off-the-shelf NFS solution, such as [IBM Elastic Storage](#) or [RedHat Ceph](#).

ownCloud Edition

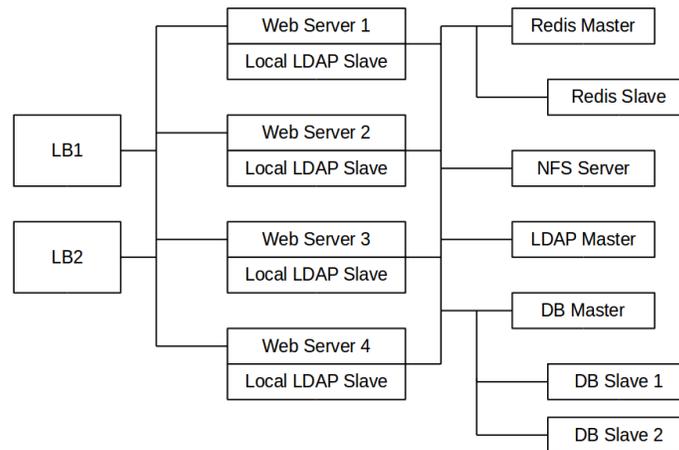
Enterprise Edition. See [ownCloud Server](#) or [Enterprise Edition](#) for comparisons of the ownCloud editions.

4.2.5 Scenario 3: Large Enterprises and Service Providers

Option	Value
Number of users	5,000 to >100,000 users.
Storage size	Up to 1 petabyte.
High availability level	Every component is fully redundant and can fail without service interruption. Backups without service interruption.

Recommended System Requirements

- 4 to 20 application/Web servers.
- A cluster of two or more database servers.
- Storage is an NFS server or an object store that is S3 compatible.
- Cloud federation for a distributed setup over several data centers.
- Authentication via an existing LDAP or Active Directory server, or SAML.



Components

- 4 to 20 application servers with four sockets and 64GB RAM.
- 4 DB servers with four sockets and 128GB RAM.
- 2 Hardware load balancer, for example, [BIG IP from F5](#).
- NFS storage server as needed.

Operating system

RHEL 7 with latest service packs.

SSL Configuration

The SSL termination is done in the load balancer. A standard SSL certificate is needed, installed according to the load balancer documentation.

Load Balancer

A redundant hardware load-balancer with heartbeat, for example, [F5 Big-IP](#). This runs two load balancers in front of the application servers.

Database

MySQL/MariaDB Galera Cluster with 4x master-master replication. InnoDB storage engine, MyISAM is not supported, see: [MySQL / MariaDB storage engine](#).

Backup

Minimum daily backup without downtime. All MySQL/MariaDB statements should be replicated to a backup MySQL/MariaDB slave instance. To do this, follow these steps:

1. Create a snapshot on the NFS storage server.
2. At the same time stop the MySQL replication.
3. Create a MySQL dump of the backup slave.
4. Push the NFS snapshot to the backup.
5. Push the MySQL dump to the backup.
6. Delete the NFS snapshot.
7. Restart MySQL replication.

Authentication

User authentication via one or several LDAP or Active Directory servers, or SAML/Shibboleth. See [User Authentication with LDAP](#) and [Shibboleth Integration](#).

LDAP

Read-only slaves should be deployed on every application server for optimal scalability.

Session Management

Redis should be used for the session management storage.

Caching

Redis for distributed in-memory caching, see [Configuring Memory Caching](#).

Storage

An off-the-shelf NFS solution should be used. Some examples are [IBM Elastic Storage](#) or [RedHat Ceph](#). Optionally, an S3 compatible object store can also be used.

ownCloud Edition

Enterprise Edition. See [ownCloud Server](#) or [Enterprise Edition](#) for comparisons of the ownCloud editions.

Redis Configuration

Redis in a master-slave configuration is a [hot failover setup](#), and is usually sufficient. A slave can be omitted if high availability is provided via other means. And when it is, in the event of a failure, restarting Redis typically occurs quickly enough. Regarding Redis cluster, we don't, usually, recommend it, as it requires a greater level of both maintenance and management in the case of failure. A single Redis server, however, just needs to be rebooted, in the event of failure.

4.2.6 Known Issues

Deadlocks When Using MariaDB Galera Cluster

If you're using [MariaDB Galera Cluster](#) with your ownCloud installation, you may encounter deadlocks when you attempt to sync a large number of files. You may also encounter database errors, such as this one:

```
SQLSTATE[40001]: Serialization failure: 1213 Deadlock found when trying to get lock; try restarting t
```

The issue, [identified by Michael Roth](#), is caused when MariaDB Galera cluster sends write requests to all servers in the cluster; [here is a detailed explanation](#). The solution is to send all write requests to a single server, instead of all of them.

Set `wsrep_sync_wait` to 1 on all Galera Cluster nodes

What the parameter does

When enabled, the node triggers causality checks in response to certain types of queries. During the check, the node blocks new queries while the database server catches up with all updates made in the cluster to the point where the check began. Once it reaches this point, the node executes the original query.

Why enable it

A Galera Cluster write operation is sent to the master while reads are retrieved from the slaves. Since Galera Cluster replication is, by default, not strictly synchronous it could happen that items are requested before the replication has actually taken place.

Note: This setting is disabled by default.

Note: See *the Galera Cluster WSREP documentation* for more details.

4.2.7 References

- Database High Availability
- Performance enhancements for Apache and PHP
- How to Set Up a Redis Server as a Session Handler for PHP on Ubuntu 14.04

4.3 Deployment Considerations

4.3.1 Hardware

- Solid-state drives (SSDs) for I/O.
- Separate hard disks for storage and database, SSDs for databases.
- Multiple network interfaces to distribute server synchronisation and backend traffic across multiple subnets.

Single Machine / Scale-Up Deployment

The single-machine deployment is widely used in the community.

Pros:

- Easy setup: no session storage daemon, use tmpfs and memory caching to enhance performance, local storage.
- No network latency to consider.
- To scale buy a bigger CPU, more memory, larger hard drive, or additional hard drives.

Cons:

- Fewer high availability options.
- The amount of data in ownCloud tends to continually grow. Eventually a single machine will not scale; I/O performance decreases and becomes a bottleneck with multiple up- and downloads, even with solid-state drives.

Scale-Out Deployment

Provider setup:

- DNS round robin to HAProxy servers (2-n, SSL offloading, cache static resources)
- Least load to Apache servers (2-n)
- Memcached/Redis for shared session storage (2-n)
- Database cluster with single Master, multiple slaves and proxy to split requests accordingly (2-n)
- GPFS or Ceph via phprados (2-n, 3 to be safe, Ceph 10+ nodes to see speed benefits under load)
- In case of clustering, your cluster nodes must have the same ownCloud configuration including an identical config.php to avoid any potential issues.

Pros:

- Components can be scaled as needed.
- High availability.
- Test migrations easier.

Cons:

- More complicated to setup.
- Network becomes the bottleneck (10GB Ethernet recommended).
- Currently DB filecache table will grow rapidly, making migrations painful in case the table is altered.

What About NGINX / PHP-FPM?

Could be used instead of HAproxy as the load balancer. But on uploads stores the whole file on disk before handing it over to PHP-FPM.

A Single Master DB is Single Point of Failure, Does Not Scale

When master fails another slave can become master. However, the increased complexity carries some risks: Multi-master has the risk of split brain, and deadlocks. ownCloud tries to solve the problem of deadlocks with high-level file locking.

4.3.2 Software

Operating System

We are dependent on distributions that offer an easy way to install the various components in up-to-date versions. ownCloud has a partnership with RedHat and SUSE for customers who need commercial support. Canonical, the parent company of Ubuntu Linux, also offers enterprise service and support. Debian and Ubuntu are free of cost, and include newer software packages. CentOS is the community-supported free-of-cost Red Hat Enterprise Linux clone. openSUSE is community-supported, and includes many of the same system administration tools as SUSE Linux Enterprise Server.

Web server

Taking Apache and NGINX as the contenders, Apache with mod_php is currently the best option, as NGINX does not support all features necessary for enterprise deployments. Mod_php is recommended instead of PHP_FPM, because in scale-out deployments separate PHP pools are simply not necessary.

Relational Database

More often than not the customer already has an opinion on what database to use. In general, the recommendation is to use what their database administrator is most familiar with. Taking into account what we are seeing at customer deployments, we recommend MySQL/MariaDB in a master-slave deployment with a MySQL proxy in front of them to send updates to master, and selects to the slave(s).

The second best option is PostgreSQL (alter table does not lock table, which makes migration less painful) although we have yet to find a customer who uses a master-slave setup.

What about the other DBMS?

- Sqlite is adequate for simple testing, and for low-load single-user deployments. It is not adequate for production systems.
- Microsoft SQL Server is not a supported option.

- Oracle DB is the de facto standard at large enterprises and is fully supported with ownCloud Enterprise Edition only.

4.3.3 File Storage

While many customers are starting with NFS, sooner or later that requires scale-out storage. Currently the options are GPFS or GlusterFS, or an object store protocol like S3 (supported in Enterprise Edition only) or Swift. S3 also allows access to Ceph Storage.

4.3.4 Session Storage

- Redis is required for *transactional file locking*, provides session persistence, and graphical inspection tools available.
- If you need to scale out Shibboleth you must use Memcached, as Shibboleth does not provide an interface to Redis. Memcached can also be used to scale-out shibd session storage (see [Memcache StorageService](#)).

4.4 Manual Installation on Linux

Installing ownCloud on Linux from our Open Build Service packages is the preferred method (see [Linux Package Manager Installation](#)). These are maintained by ownCloud engineers, and you can use your package manager to keep your ownCloud server up-to-date.

Note: Enterprise customers should refer to [Installing & Upgrading ownCloud Enterprise Edition](#)

If there are no packages for your Linux distribution, or you prefer installing from the source tarball, you can setup ownCloud from scratch using a classic LAMP stack (Linux, Apache, MySQL/MariaDB, PHP). This document provides a complete walk-through for installing ownCloud on Ubuntu 14.04 LTS Server with Apache and MariaDB, using the ownCloud .tar archive.

- [Prerequisites](#)
- [Install the Required Packages](#)
- [Configure Apache Web Server](#)
- [Enable SSL](#)
- [Run the Installation Wizard](#)
- [Set Strong Directory Permissions](#)
- [SELinux](#)
- [php.ini](#)
- [PHP-FPM](#)
- [Other Web Servers](#)

Note: Admins of SELinux-enabled distributions such as CentOS, Fedora, and Red Hat Enterprise Linux may need to set new rules to enable installing ownCloud. See [SELinux](#) for a suggested configuration.

4.4.1 Prerequisites

The ownCloud tar archive contains all of the required third-party PHP libraries. As a result, no extra ones are, strictly, necessary. However, ownCloud does require that PHP has a set of extensions installed, enabled, and configured.

This section lists both the required and optional PHP extensions. If you need further information about a particular extension, please consult the relevant section of [the extensions section of the PHP manual](#).

If you are using a Linux distribution, it should have packages for all the required extensions. You can check the presence of a module by typing `php -m | grep -i <module_name>`. If you get a result, the module is present.

Required

PHP Version

PHP (5.6+, 7.0, 7.1, & 7.2)

Warning: ownCloud recommends the use of PHP 7.2 in new installations. Sites using a version earlier than PHP 7.2 are *strongly encouraged* to migrate to PHP 7.2.

PHP Extensions

Name	Description
Ctype	For character type checking
cURL	Used for aspects of HTTP user authentication
DOM	For operating on XML documents through the DOM API
GD	For creating and manipulating image files in a variety of different image formats, including GIF, PNG, JPEG, WBMP, and XPM.
HASH Message Digest Framework	For working with message digests (hash).
iconv	For working with the iconv character set conversion facility.
intl	Increases language translation performance and fixes sorting of non-ASCII characters
JSON	For working with the JSON data-interchange format.
libxml	This is required for the <code>_DOM_</code> , <code>_libxml_</code> , <code>_SimpleXML_</code> , and <code>_XMLWriter_</code> extensions to work. It requires that libxml2, version 2.7.0 or higher, is installed.
Multibyte String	For working with multibyte character encoding schemes.
OpenSSL	For symmetric and asymmetric encryption and decryption, PBKDF2, PKCS7, PKCS12, X509 and other crypto operations.
PDO	This is required for the <code>pdo_mysql</code> function to work.
Phar	For working with PHP Archives (.phar files).
POSIX	For working with UNIX POSIX functionality.
SimpleXML	For working with XML files as objects.
XMLWriter	For generating streams or files of XML data.
Zip	For reading and writing ZIP compressed archives and the files inside them.
Zlib	For reading and writing gzip (.gz) compressed files.

Tip: The *Phar*, *OpenSSL*, and *cUrl* extensions are mandatory if you want to use [Make to setup your ownCloud environment](#), prior to running either the web installation wizard, or the command line installer.

Database Extensions

Name	Description
pdo_mysql	For working with MySQL & MariaDB.
pgsql	For working with PostgreSQL. It requires PostgreSQL 9.0 or above.
sqlite	For working with SQLite. It requires SQLite 3 or above. This is, usually, not recommended, for performance reasons.

Required For Specific Apps

Name	Description
ftp	For working with FTP storage
sftp	For working with SFTP storage
imap	For IMAP integration
ldap	For LDAP integration
smbclient	For SMB/CIFS integration

Note: SMB/Windows Network Drive mounts require the PHP module smbclient version 0.8.0+; see [SMB/CIFS](#).

Optional

Extension	Reason
Bzip2	Required for extraction of applications
Fileinfo	Highly recommended, as it enhances file analysis performance
Mcrypt	Increases file encryption performance
OpenSSL	Required for accessing HTTPS resources
imagick	Required for creating and modifying images and preview thumbnails

Recommended

For Specific Apps

Extension	Reason
Exif	For image rotation in the pictures app
GMP	For working with arbitrary-length integers

For Server Performance

For enhanced server performance consider installing one of the following cache extensions:

- apcu
- memcached
- redis (>= 2.2.6+, required for transactional file locking)

See [Memory Caching](#) to learn how to select and configure a memcache.

For Preview Generation

- `avconv` or `ffmpeg`
- `OpenOffice` or `LibreOffice`

For Command Line Processing

Extension	Reason
<code>PCNTL</code>	Enables command interruption by pressing <code>ctrl-c</code>

Note: You don't need the WebDAV module for your Web server (i.e. Apache's `mod_webdav`), as ownCloud has a built-in WebDAV server of its own, `SabreDAV`. If `mod_webdav` is enabled you must disable it for ownCloud. (See *Configure Apache Web Server* for an example configuration.)

For MySQL/MariaDB

The InnoDB storage engine is required, and MyISAM is not supported, see: *MySQL / MariaDB storage engine*.

4.4.2 Install the Required Packages

On Ubuntu 16.04 LTS Server

On a machine running a pristine Ubuntu 16.04 LTS server, install the required and recommended modules for a typical ownCloud installation, using Apache and MariaDB, by issuing the following commands in a terminal:

```
# If the add-apt-repository command is not available install software-properties-common
sudo add-apt-repository ppa:ondrej/php
sudo apt-get update

sudo apt-get install -y apache2 mariadb-server libapache2-mod-php7.2 \
    openssl php-imagick php7.2-common php7.2-curl php7.2-gd \
    php7.2-imag php7.2-intl php7.2-json php7.2-ldap php7.2-mbstring \
    php7.2-mysql php7.2-pgsql php-smbclient php-ssh2 \
    php7.2-sqlite3 php7.2-xml php7.2-zip
```

Please note:

- `php7.2-common` provides: `ftp`, `Phar`, `posix`, `iconv`, `ctype`
- The Hash extension is available from PHP 5.1.2 by default
- `php7.2-xml` provides `DOM`, `SimpleXML`, `XML`, & `XMLWriter`
- `php7.2-zip` provides `zlib`

Installing smbclient

To install `smbclient`, you can use the following script. It first installs `PEAR`, which at the time of writing only installs version 1.9.4. However, `smbclient` requires version 1.9.5. So the final two commands upgrade `PEAR` to version 1.9.5 and then install `smbclient` using `Pecl`.

```
#!/usr/bin/expect
spawn wget -O /tmp/go-pear.phar http://pear.php.net/go-pear.phar
expect eof

spawn php /tmp/go-pear.phar

expect "1-11, 'all' or Enter to continue:"
send "\r"
expect eof

spawn rm /tmp/go-pear.phar

pear install PEAR-1.9.5
pecl install smbclient
```

Installing SSH2

To install SSH2, which provides SFTP, you can use the following command:

```
spawn pecl install ssh2
```

Running Additional Apps?

If you are planning on running additional apps, keep in mind that you might require additional packages. See *Prerequisites* for details.

Note: During the installation of the MySQL/MariaDB server, you will be prompted to create a root password. Be sure to remember your password as you will need it during ownCloud database setup.

Additional Extensions

```
apt-get install -y php-apcu php-redis redis-server php7.2-ldap
```

RHEL (RedHat Enterprise Linux) 7.2

Required Extensions

```
# Enable the RHEL Server 7 repository
subscription-manager repos --enable rhel-server-rhsc1-7-eus-rpms
```

```
# Install the required packages
sudo yum install httpd mariadb-server php72 php72-php \
  php72-php-gd php72-php-mbstring php72-php-mysqlnd
```

Optional Extensions

```
sudo yum install -y epel-release http://rpms.remirepo.net/enterprise/remi-release-7.rpm yum-utils \  
  && sudo yum-config-manager --enable remi-php72 \  
  && sudo yum update -y \  
  && sudo yum install -y php72-pecl-apcu \  
    redis php72-php-pecl-redis php72-php-ldap \  
    mariadb-server mariadb
```

Centos 7

```
sudo yum install -y -q epel-release http://rpms.remirepo.net/enterprise/remi-release-7.rpm yum-utils \  
&& sudo yum-config-manager --enable remi-php72 \  
&& sudo yum update -y -q \  
&& sudo yum install -y -q \  
  httpd mariadb-server php72 php72-php php72-php-gd \  
  php72-php-mbstring php72-php-mysqlnd php72-php-cli \  
  php72-pecl-apcu redis php72-php-pecl-redis php72-php-common \  
  php72-php-ldap mariadb-server mariadb \  
&& sudo scl enable php72 bash
```

SLES (SUSE Linux Enterprise Server) 12

Required Extensions

```
zypper install -y apache2 apache2-mod_php7 php7-gd php7-openssl \  
  php7-json php7-curl php7-intl php7-sodium php7-zip php7-zlib
```

Optional Extensions

```
zypper install -y php7-ldap
```

APCu We are not aware of any officially supported APCu package for SLES 12. However, if you want or need to install it, then we suggest the following steps:

```
wget http://download.opensuse.org/repositories/server:/php:/extensions/SLE_12_SP1/ server:php:extensio  
zypper refresh  
zypper install -y php7-APCu
```

Redis The latest versions of Redis servers have shown to be incompatible with SLES 12. Therefore it is currently recommended to download and install version 2.2.7 or a previous release from: <https://pecl.php.net/package/redis>. Keep in mind that version 2.2.5 is the minimum version which ownCloud supports.

If you want or need to install it, we suggest the following steps:

```
zypper refresh  
zypper install -y php7-redis
```

4.4.3 Install ownCloud

Now download the archive of the latest ownCloud version:

- Go to the [ownCloud Download Page](#).
- Go to **Download ownCloud Server > Download > Archive file for server owners** and download either the tar.bz2 or .zip archive.
- This downloads a file named owncloud-x.y.z.tar.bz2 or owncloud-x.y.z.zip (where x.y.z is the version number).
- Download its corresponding checksum file, e.g. owncloud-x.y.z.tar.bz2.md5, or owncloud-x.y.z.tar.bz2.sha256.
- Verify the MD5 or SHA256 sum:

```
md5sum -c owncloud-x.y.z.tar.bz2.md5 < owncloud-x.y.z.tar.bz2
sha256sum -c owncloud-x.y.z.tar.bz2.sha256 < owncloud-x.y.z.tar.bz2
md5sum -c owncloud-x.y.z.zip.md5 < owncloud-x.y.z.zip
sha256sum -c owncloud-x.y.z.zip.sha256 < owncloud-x.y.z.zip
```

- You may also verify the PGP signature:

```
wget https://download.owncloud.org/community/owncloud-x.y.z.tar.bz2.asc
wget https://owncloud.org/owncloud.asc
gpg --import owncloud.asc
gpg --verify owncloud-x.y.z.tar.bz2.asc owncloud-x.y.z.tar.bz2
```

- Now you can extract the archive contents. Run the appropriate unpacking command for your archive type:

```
tar -xjf owncloud-x.y.z.tar.bz2
unzip owncloud-x.y.z.zip
```

- This unpacks to a single owncloud directory. Copy the ownCloud directory to its final destination. When you are running the Apache HTTP server, you may safely install ownCloud in your Apache document root:

```
cp -r owncloud /path/to/webserver/document-root
```

where /path/to/webserver/document-root is replaced by the document root of your Web server:

```
cp -r owncloud /var/www
```

On other HTTP servers, it is recommended to install ownCloud outside of the document root.

4.4.4 Configure Apache Web Server

On Debian, Ubuntu, and their derivatives, Apache installs with a useful configuration, so all you have to do is create a /etc/apache2/sites-available/owncloud.conf file with these lines in it, replacing the **Directory** and other file paths with your own file paths:

```
Alias /owncloud "/var/www/owncloud/"

<Directory /var/www/owncloud/>
    Options +FollowSymlinks
    AllowOverride All

<IfModule mod_dav.c>
    Dav off
</IfModule>

SetEnv HOME /var/www/owncloud
SetEnv HTTP_HOME /var/www/owncloud

</Directory>
```

Then create a symlink to `/etc/apache2/sites-enabled`:

```
ln -s /etc/apache2/sites-available/owncloud.conf /etc/apache2/sites-enabled/owncloud.conf
```

Additional Apache Configurations

- For ownCloud to work correctly, we need the module `mod_rewrite`. Enable it by running:

```
a2enmod rewrite
```

Additional recommended modules are `mod_headers`, `mod_env`, `mod_dir` and `mod_mime`

```
a2enmod headers
a2enmod env
a2enmod dir
a2enmod mime
```

Note: If you want to use the [OAuth2 app](#), then `mod_headers` must be installed and enabled.

- You must disable any server-configured authentication for ownCloud, as it uses Basic authentication internally for DAV services. If you have turned on authentication on a parent folder (via, e.g., an `AuthType Basic` directive), you can disable the authentication specifically for the ownCloud entry. Following the above example configuration file, add the following line in the `<Directory` section

```
Satisfy Any
```

- When using SSL, take special note of the `ServerName`. You should specify one in the server configuration, as well as in the `CommonName` field of the certificate. If you want your ownCloud to be reachable via the internet, then set both of these to the domain you want to reach your ownCloud server.
- Now restart Apache

```
service apache2 restart
```

- If you're running ownCloud in a sub-directory and want to use CalDAV or CardDAV clients make sure you have configured the correct *Service discovery* URLs.

Multi-Processing Module (MPM)

[Apache prefork](#) has to be used. Don't use a threaded MPM like `event` or `worker` with `mod_php`, because PHP is currently *not thread safe*.

4.4.5 Enable SSL

Note: You can use ownCloud over plain HTTP, but we strongly encourage you to use SSL/TLS to encrypt all of your server traffic, and to protect user's logins and data in transit.

Apache installed under Ubuntu comes already set-up with a simple self-signed certificate. All you have to do is to enable the `ssl` module and the default site. Open a terminal and run:

```
a2enmod ssl
a2ensite default-ssl
service apache2 reload
```

Note: Self-signed certificates have their drawbacks - especially when you plan to make your ownCloud server publicly accessible. You might want to consider getting a certificate signed by a commercial signing authority. Check with your domain name registrar or hosting service for good deals on commercial certificates.

4.4.6 Run the Installation Wizard

After restarting Apache, you must complete your installation by running either the Graphical Installation Wizard or on the command line with the `occ` command. To enable this, temporarily change the ownership on your ownCloud directories to your HTTP user (see *Set Strong Directory Permissions* to learn how to find your HTTP user):

```
chown -R www-data:www-data /var/www/owncloud/
```

Note: Admins of SELinux-enabled distributions may need to write new SELinux rules to complete their ownCloud installation; see *SELinux*.

To use `occ` see *Command Line Installation*. To use the graphical Installation Wizard see *The Installation Wizard*.

Warning: Please know that ownCloud's data directory **must be exclusive to ownCloud** and not be modified manually by any other process or user.

4.4.7 Set Strong Directory Permissions

After completing the installation, you must immediately *set the directory permissions* in your ownCloud installation as strictly as possible for stronger security. After you do so, your ownCloud server will be ready to use.

4.4.8 Managing Trusted Domains

All URLs used to access your ownCloud server must be whitelisted in your `config.php` file, under the `trusted_domains` setting. Users are allowed to log into ownCloud only when they point their browsers to a URL that is listed in the `trusted_domains` setting.

Note: This setting is important when changing or moving to a new domain name. You may use IP addresses and domain names.

A typical configuration looks like this:

```
'trusted_domains' => [
    0 => 'localhost',
    1 => 'server1.example.com',
    2 => '192.168.1.50',
],
```

The loopback address, `127.0.0.1`, is automatically whitelisted, so as long as you have access to the physical server you can always log in. In the event that a load-balancer is in place, there will be no issues as long as it sends the correct `X-Forwarded-Host` header.

Note: For further information on improving the quality of your ownCloud installation, please see the *Configuration Notes & Tips* guide.

4.5 Linux Package Manager Installation

Note: Package managers should only be used for single-server setups. For production environments, we recommend installing from [the tar archive](#).

4.5.1 Available Packages

The recommended package to use is `owncloud-files`. It only installs ownCloud, and does not install Apache, a database, or any of the required PHP dependencies.

4.5.2 Installing ownCloud Community Edition

First, install your own LAMP stack, as doing so allows you to create your own custom LAMP stack without dependency conflicts with the ownCloud package. Then, [update package manager's configuration](#).

Configurations are available for the following Linux distributions:

- Ubuntu 14.04 & 16.04
- Debian 7 & 8
- RHEL 6 & 7
- CentOS 7.2 & 7.3
- SLES 11SP4 & 12SP2
- openSUSE Leap 42.2 & 42.3

Note: Repositories for Fedora, openSUSE Tumbleweed, and Ubuntu 15.04 have been dropped. If you use Fedora, use [the tar archive](#) with your own LAMP stack. openSUSE users can rely on LEAP packages for Tumbleweed.

Once your package manager has been updated, follow the rest of the instructions on the download page to install ownCloud. Once ownCloud's installed, run [the Installation Wizard](#) to complete your installation.

Note: See the [System Requirements](#) for the recommended ownCloud setup and supported platforms.

Warning: Do not move the folders provided by these packages after the installation, as this will break updates.

What is the Correct Version?

Package versions are composed of a major, a minor, and a patch number, such as 9.0, 9.1, 10.0, 10.0.1, and 10.0.2. The second number represents a major release, and the third number represents a minor release.

Major Releases

If you want to follow either of the most recent major releases, then substitute `version` with either 9.0 or 10.0.

Minor Releases

If you want to follow any of the four most recent patch releases, then substitute `version` with one of 10.0.1, 10.0.2, 10.0.3, or 10.0.4. Following a minor release avoids you accidentally upgrading to the next major release before you're ready.

The Latest Stable Version

Alternatively you can use `stable` for the latest stable version. If you do, you never have to change it as it always tracks the current stable ownCloud version through all major releases.

4.5.3 Installing ownCloud Enterprise Edition

See *Installing & Upgrading ownCloud Enterprise Edition* for instructions on installing ownCloud Enterprise edition.

4.5.4 Downgrading

Downgrading is not supported and risks corrupting your data! If you want to revert to an older ownCloud version, install it from scratch and then restore your data from backup. Before doing this, file a support ticket (if you have paid support) or ask for help in the ownCloud forums to see if your issue can be resolved without downgrading.

4.5.5 Additional Guides and Notes

See *The Installation Wizard* for important steps, such as choosing the best database and setting correct directory permissions. See *SELinux Configuration* for a suggested configuration for SELinux-enabled distributions such as Fedora and CentOS.

If your distribution is not listed, your Linux distribution may maintain its own ownCloud packages or you may prefer to *install from source*.

Archlinux

The current `stable version` is in the official community repository, and more packages are in the [Arch User Repository](#).

Mageia

The [Mageia Wiki](#) has a good page on installing ownCloud from the Mageia software repository.

Note for MySQL/MariaDB environments

Please refer to *MySQL / MariaDB with Binary Logging Enabled* on how to correctly configure your environment if you have binary logging enabled.

Running ownCloud in a sub-directory

If you're running ownCloud in a sub-directory and want to use CalDAV or CardDAV clients, make sure you have configured the correct *service discovery* URLs.

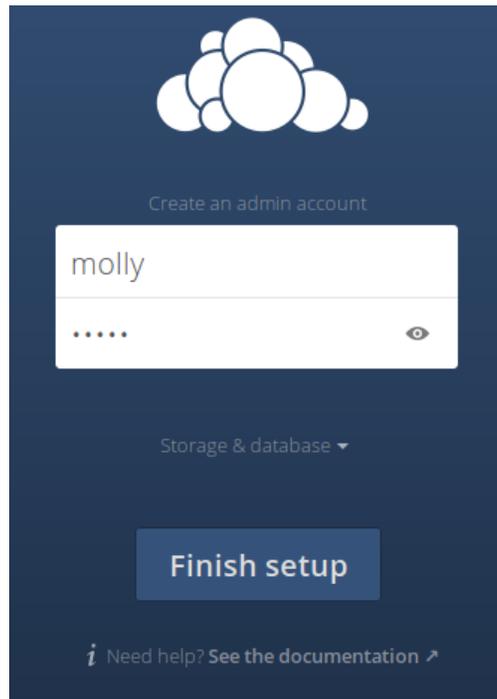
4.6 The Installation Wizard

Warning: If you are planning to use the installation wizard, we **strongly** encourage you to protect it, through some form of [password authentication](#), or [access control](#). If the installer is left unprotected when exposed to the public internet, there is the possibility that a malicious actor could finish the installation and block you out — or worse. So please ensure that only you — or someone from your organization — can access the web installer.

4.6.1 Quick Start

When the ownCloud prerequisites are fulfilled and all ownCloud files are installed, the last step to completing the installation is running the Installation Wizard. This involves just three steps:

1. Point your web browser to `http://localhost/owncloud`
2. Enter your desired administrator's username and password.
3. Click “Finish Setup”.



You're now finished and can start using your new ownCloud server. Of course, there is much more that you *can* do to set up your ownCloud server for best performance and security. In the following sections we will cover important installation and post-installation steps. Note that you must follow the instructions in *Setting Strong Permissions* in order to use the *occ Command*.

4.6.2 In-Depth Guide

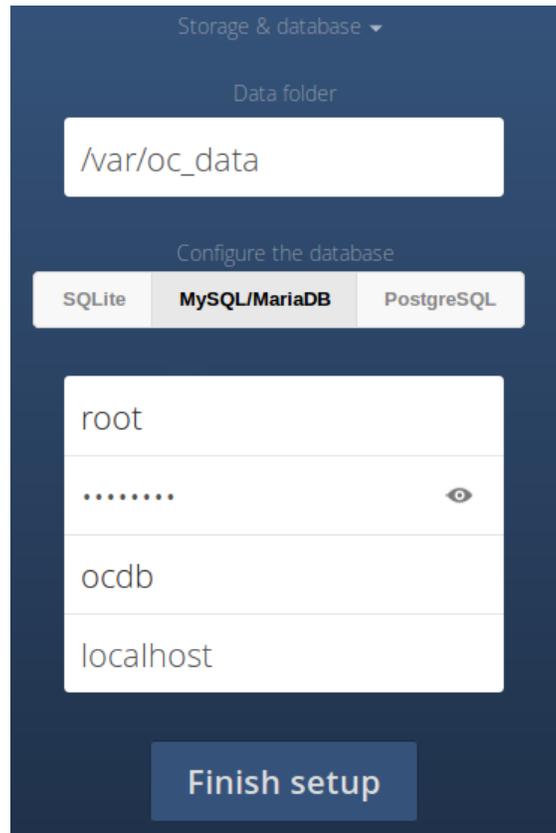
This section provides a more detailed guide to the installation wizard. Specifically, it is broken down into three steps:

1. *Data Directory Location*
2. *Database Choices*

3. Post-Installation Steps

Data Directory Location

Click “Storage and Database” to expose additional installation configuration options for your ownCloud data directory and database.



You should locate your ownCloud data directory outside of your Web root if you are using an HTTP server other than Apache, or you may wish to store your ownCloud data in a different location for other reasons (e.g. on a storage server).

Warning: Please know that ownCloud’s data directory **must be exclusive to ownCloud** and not be modified manually by any other process or user.

It is best to configure your data directory location at installation, as it is difficult to move after installation. You may put it anywhere; in this example is it located in `/var/oc_data`. This directory must already exist, and must be owned by your HTTP user (see *Set Strong Directory Permissions*).

Database Choices

When installing ownCloud Server & ownCloud Enterprise editions the administrator may choose one of 4 supported database products. These are:

- *SQLite*
- *MYSQL/MariaDB*

- *PostgreSQL*
- *Oracle 11g* (Enterprise-edition only)

SQLite

SQLite is the default database for ownCloud Server — but is not supported by the ownCloud Enterprise edition.

Note: SQLite is only good for testing and lightweight single user setups. It has no client synchronization support, so other devices will not be able to synchronize with the data stored in an ownCloud SQLite database.

SQLite will be installed by the ownCloud package and all the necessary dependencies will be satisfied. If you used the package manager to install ownCloud, you may “Finish Setup” with no additional steps to configure ownCloud using the SQLite database for limited use.

MYSQL/MariaDB

MariaDB is the ownCloud recommended database. It may be used with either ownCloud Server or ownCloud Enterprise editions. To install the recommended MySQL/MariaDB database, use the following command:

```
sudo apt-get install mariadb-server
```

If you have an administrator login that has permissions to create and modify databases, you may choose “Storage & Database”. Then, enter your database administrator username and password, and the name you want for your ownCloud database. Alternatively, you can use these steps to create a temporary database administrator account.

```
sudo mysql --user=root mysql
CREATE USER 'dbadmin'@'localhost' IDENTIFIED BY 'Apassword';
GRANT ALL PRIVILEGES ON *.* TO 'dbadmin'@'localhost' WITH GRANT OPTION;
FLUSH PRIVILEGES;
exit
```

For more detailed information, see [MySQL/MariaDB](#).

PostgreSQL

PostgreSQL is also supported by ownCloud. To install it, use the following command (or that of your preferred package manager):

```
sudo apt-get install postgresql
```

In order to allow ownCloud access to the database, create a known password for the default user, `postgres`, which was added when the database was installed.

```
sudo -i -u postgres psql
postgres=# \password
Enter new password:
Enter it again:
postgres=# \q
exit
```

Oracle 11g

Oracle 11g is only supported for the ownCloud Enterprise edition.

Database Setup By ownCloud

Your database and PHP connectors must be installed before you run the Installation Wizard by clicking the “Finish setup” button. After you enter your temporary or root administrator login for your database, the installer creates a special database user with privileges limited to the ownCloud database.

Following this, ownCloud needs only this special ownCloud database user and drops the temporary or root database login. This new user is named from your ownCloud admin user, with an `oc_` prefix, and given a random password. The ownCloud database user and password are written into `config.php`:

For MySQL/MariaDB:

```
'dbuser' => 'oc_dbadmin',  
'dbpassword' => 'pX65Ty5DrHQkYPE5HRsDvyFH1ZZHcm',
```

For PostgreSQL:

```
'dbuser' => 'oc_postgres',  
'dbpassword' => 'pX65Ty5DrHQkYPE5HRsDvyFH1ZZHcm',
```

Click Finish Setup, and you're ready to start using your new ownCloud server.

4.6.3 Post-Installation Steps

Now we will look at some important post-installation steps. For hardened security we recommend setting the permissions on your ownCloud directories as strictly as possible, and for proper server operations. This should be done immediately after the initial installation and before running the setup.

Your HTTP user must own the `config/`, `data/`, `apps/` respectively the `apps-external/` directories so that you can configure ownCloud, create, modify and delete your data files, and install apps via the ownCloud Web interface.

You can find your HTTP user in your HTTP server configuration files, or you can use *PHP Version and Information* (Look for the **User/Group** line).

- The HTTP user and group in Debian/Ubuntu is `www-data`.
- The HTTP user and group in Fedora/CentOS is `apache`.
- The HTTP user and group in Arch Linux is `http`.
- The HTTP user in openSUSE is `wwwrun`, and the HTTP group is `www`.

Note: When using an NFS mount for the data directory, do not change its ownership from the default. The simple act of mounting the drive will set proper permissions for ownCloud to write to the directory. Changing ownership as above could result in some issues if the NFS mount is lost.

The easy way to set the correct permissions is to copy and run the script, below. The script sets proper permissions and ownership including the handling of necessary directories. The script also prepares for an `apps-external` directory, for details see `config.sample.php`:

- Replace the `ocpath` variable with the path to your ownCloud directory.
- Replace the `ocdata` variable with the path to your ownCloud data directory.
- Replace the `apps_external` variable with the path to your ownCloud apps-external directory.

In case you want to use links for the data and apps-external directory:

- Replace the `linkdata` variable with the path to your ownCloud linked data directory.

- Replace the `linkapps-external` variable with the path to your ownCloud linked apps-external directory.

Set the correct HTTP user and group according your needs:

- Replace the `htuser` and `htgroup` variables with your HTTP user and group.

In case of upgrading using tar:

- Replace the `oldocpath` variable with the path to your old ownCloud directory.

```
#!/bin/bash

ocpath='/var/www/owncloud'
ocdata='/var/www/owncloud/data'
ocapps_external='/var/www/owncloud/apps-external'
oldocpath='/var/www/owncloud.old'
linkdata="/var/mylinks/data"
linkapps-external="/var/mylinks/apps-external"
htuser='www-data'
htgroup='www-data'
rootuser='root'

# Because the data directory can be huge or on external storage, an automatic chmod/chown can take a
# Therefore this directory can be treated differently.
# If you have already created an external data and apps-external directory which you want to link,
# set the paths above accordingly. This script can link and set the proper rights and permissions
# depending what you enter when running the script.
# You have to run this script twice, one time to prepare installation and one time post installation

# Example input
# New install using mkdir:      n/n/n (create missing directories, setup permissions and ownership)
# Upgrade using mkdir:         n/n/n (you move/replace data, apps-external and config.php manually, s
# New install using links:     y/y/n (link existing directories, setup permissions and ownership)
# Upgrade using links:         y/n/y (link existing directories, copy config.php, permissions and ow
# Post installation/upgrade:    either n/n/n or y/y/n
# Reset all perm & own:        either n/n/n or y/y/n

echo
read -p "Do you want to use ln instead of mkdir for creating directories (y/N)? " -r -e answer
if echo "$answer" | grep -iq "^y"; then
    uselinks="y"
else
    uselinks="n"
fi

read -p "Do you also want to chmod/chown these links (y/N)? " -r -e answer
if echo "$answer" | grep -iq "^y"; then
    chmdir="y"
else
    chmdir="n"
fi

read -p "If you upgrade, do you want to copy an existing config.php file (y/N)? " -r -e answer
if echo "$answer" | grep -iq "^y"; then
    upgrdcfg="y"
else
    upgrdcfg="n"
fi

printf "\nCreating or linking possible missing directories \n"
```

```
mkdir -p $ocpath/updater
# check if directory creation is possible and create if ok
if [ "$uselinks" = "n" ]; then
  if [ -L ${ocdata} ]; then
    echo "Symlink for $ocdata found but mkdir requested. Exiting."
    echo
    exit
  else
    echo "mkdir $ocdata"
    echo
    mkdir -p $ocdata
  fi
  if [ -L ${ocapps_external} ]; then
    echo "Symlink for $ocapps_external found but mkdir requested. Exiting."
    echo
    exit
  else
    printf "mkdir $ocapps_external \n"
    mkdir -p $ocapps_external
  fi
else
  if [ -d ${ocdata} ]; then
    echo "Directory for $ocdata found but link requested. Exiting."
    echo
    exit
  else
    printf "ln $ocdata \n"
    ln -sf $linkdata $ocdata
  fi
  if [ -d ${ocapps_external} ]; then
    echo "Directory for $ocapps_external found but link requested. Exiting."
    echo
    exit
  else
    printf "ln $ocapps_external \n"
    ln -sf $linkapps-external $ocapps_external
  fi
fi

# Copy if requested an existing config.php
if [ "$upgrdcfg" = "y" ]; then
  if [ -f ${oldocpath}/config/config.php ]; then
    printf "\nCopy existing config.php file \n"
    cp ${oldocpath}/config/config.php ${ocpath}/config/config.php
  else
    printf "Skipping copy config.php, not found: ${oldocpath}/config/config.php \n"
  fi
fi

printf "\nchmod files and directories excluding data and apps-external directory \n"
find -L ${ocpath} -path ${ocdata} -prune -o -path ${ocapps_external} -prune -o -type f -print0 | xargs
find -L ${ocpath} -path ${ocdata} -prune -o -path ${ocapps_external} -prune -o -type d -print0 | xargs

# no error messages on empty directories
if [ "$schmdir" = "n" ] && [ "$uselinks" = "n" ]; then
  printf "chmod data and apps-external directory (mkdir) \n"
  if [ -n "$(ls -A $ocdata)" ]; then
    find ${ocdata}/ -type f -print0 | xargs -0 chmod 0640
```

```

fi
find ${ocdata}/ -type d -print0 | xargs -0 chmod 0750
if [ -n "$(ls -A $ocapps_external)" ]; then
    find ${ocapps_external}/ -type f -print0 | xargs -0 chmod 0640
fi
find ${ocapps_external}/ -type d -print0 | xargs -0 chmod 0750
fi

if [ "$schmdir" = "y" ] && [ "$uselinks" = "y" ]; then
    printf "chmod data and apps-external directory (linked) \n"
    if [ -n "$(ls -A $ocdata)" ]; then
        find -L ${ocdata}/ -type f -print0 | xargs -0 chmod 0640
    fi
    find -L ${ocdata}/ -type d -print0 | xargs -0 chmod 0750
    if [ -n "$(ls -A $ocapps_external)" ]; then
        find -L ${ocapps_external}/ -type f -print0 | xargs -0 chmod 0640
    fi
    find -L ${ocapps_external}/ -type d -print0 | xargs -0 chmod 0750
fi

printf "\nchown files and directories excluding data and apps-external directory \n"
find -L $ocpath -path ${ocdata} -prune -o -path ${ocapps_external} -prune -o -type d -print0 | xargs -0 chmod 0750
find -L $ocpath -path ${ocdata} -prune -o -path ${ocapps_external} -prune -o -type f -print0 | xargs -0 chmod 0640

# do only if the directories are present
if [ -d ${ocpath}/apps/ ]; then
    printf "chown apps directory \n"
    chown -R ${htuser}:${htgroup} ${ocpath}/apps/
fi
if [ -d ${ocpath}/config/ ]; then
    printf "chown config directory \n"
    chown -R ${htuser}:${htgroup} ${ocpath}/config/
fi
if [ -d ${ocpath}/updater/ ]; then
    printf "chown updater directory \n"
    chown -R ${htuser}:${htgroup} ${ocpath}/updater
fi

if [ "$schmdir" = "n" ] && [ "$uselinks" = "n" ]; then
    printf "chown data and apps-external directories (mkdir) \n"
    chown -R ${htuser}:${htgroup} ${ocapps_external}/
    chown -R ${htuser}:${htgroup} ${ocdata}/
fi
if [ "$schmdir" = "y" ] && [ "$uselinks" = "y" ]; then
    printf "chown data and apps-external directories (linked) \n"
    chown -R ${htuser}:${htgroup} ${ocapps_external}/
    chown -R ${htuser}:${htgroup} ${ocdata}/
fi

printf "\nchmod occ command to make it executable \n"
if [ -f ${ocpath}/occ ]; then
    chmod +x ${ocpath}/occ
fi

printf "chmod/chown .htaccess \n"
if [ -f ${ocpath}/.htaccess ]; then
    chmod 0644 ${ocpath}/.htaccess
    chown ${rootuser}:${htgroup} ${ocpath}/.htaccess
fi

```

```
fi
if [ -f ${ocdata}/.htaccess ];then
    chmod 0644 ${ocdata}/.htaccess
    chown ${rootuser}:${htgroup} ${ocdata}/.htaccess
fi
echo
```

If you have customized your ownCloud installation and your file paths are different than the standard installation, modify this script accordingly.

This summary lists the recommended modes and ownership for your ownCloud directories and files:

- All files should be read-write for the file owner, read-only for the group owner, and zero for the world
- All directories should be executable (because directories always need the executable bit set), read-write for the directory owner, and read-only for the group owner
- The `apps/` directory should be owned by `[HTTP user]:[HTTP group]`
- The `apps-external/` directory should be owned by `[HTTP user]:[HTTP group]`
- The `config/` directory should be owned by `[HTTP user]:[HTTP group]`
- The `data/` directory should be owned by `[HTTP user]:[HTTP group]`
- The `updater/` directory should be owned by `[HTTP user]:[HTTP group]`
- The `[ocpath]/.htaccess` file should be owned by `root:[HTTP group]`
- The `data/.htaccess` file should be owned by `root:[HTTP group]`
- Both `.htaccess` files are read-write file owner, read-only group and world

These strong permissions prevent upgrading your ownCloud server; see *Setting Permissions for Updating* for a script to quickly change permissions to allow upgrading.

4.7 Installing with Docker

ownCloud can be installed using Docker, using [the official ownCloud Docker image](#). This official image is designed to work with a data volume in the host filesystem and with separate *MariaDB* and *Redis* containers. The configuration:

- exposes port 8080, which allows for HTTP connections.
- mounts the data and MySQL data directories on the host for persistent storage.

4.7.1 Installation on a Local Machine

To use it, first create a new project directory and download `docker-compose.yml` from [the ownCloud Docker GitHub repository](#) into that new directory. Next, create a `.env` configuration file, which contains the required configuration settings. Only a few settings are required, these are:

Setting Name	Description	Example
<code>OWNCLOUD_VERSION</code>	The ownCloud version	<code>latest</code>
<code>OWNCLOUD_DOMAIN</code>	The ownCloud domain	<code>localhost</code>
<code>ADMIN_USERNAME</code>	The admin username	<code>admin</code>
<code>ADMIN_PASSWORD</code>	The admin user's password	<code>admin</code>
<code>HTTP_PORT</code>	The HTTP port to bind to	<code>8080</code>

Then, you can start the container, using your preferred Docker command-line tool. The example below shows how to use [Docker Compose](#).

Note: You can find instructions for using plain docker in the [GitHub repository](#).

```
# Create a new project directory
mkdir owncloud-docker-server

cd owncloud-docker-server

# Copy docker-compose.yml from the GitHub repository
wget https://raw.githubusercontent.com/owncloud-docker/server/master/docker-compose.yml

# Create the environment configuration file
cat << EOF > .env
OWNCLOUD_VERSION=10.0
OWNCLOUD_DOMAIN=localhost
ADMIN_USERNAME=admin
ADMIN_PASSWORD=admin
HTTP_PORT=8080
EOF

# Build and start the container
docker-compose up -d
```

When the process completes, then check that all the containers have successfully started, by running `docker-compose ps`. If they are all working correctly, you should expect to see output similar to that below:

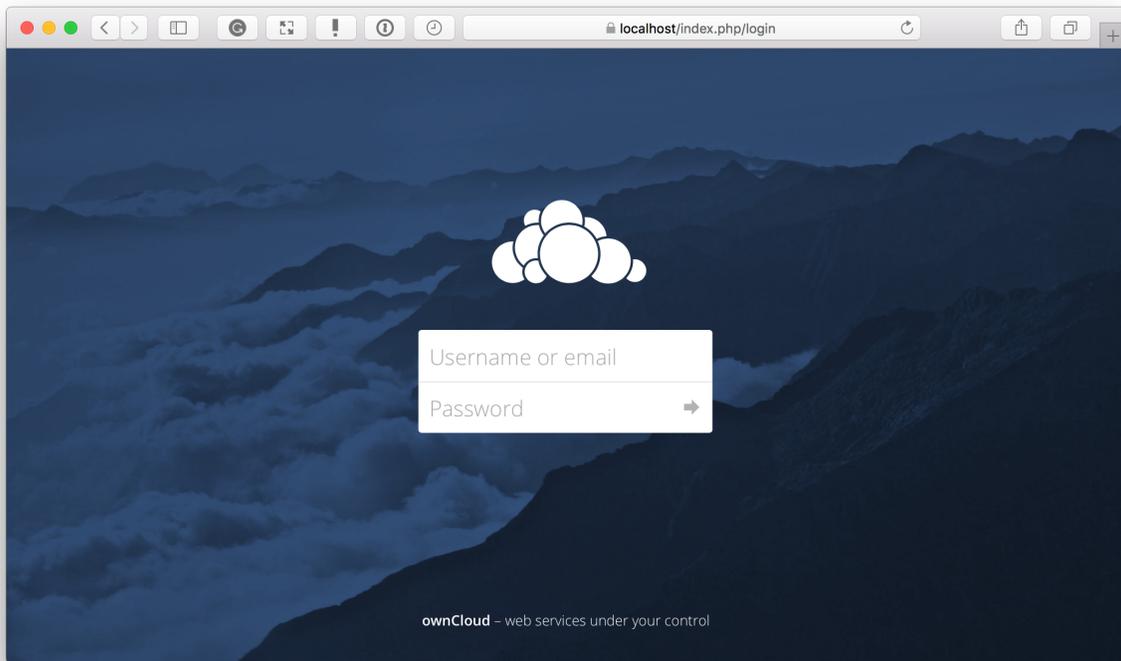
Name	Command	State	Ports
server_db_1	/usr/bin/entrypoint /bin/s ...	Up	3306/tcp
server_owncloud_1	/usr/local/bin/entrypoint ...	Up	0.0.0.0:8080->8080/tcp
server_redis_1	/bin/s6-svscan /etc/s6	Up	6379/tcp

In it, you can see that the database, ownCloud, and Redis containers are running, and that ownCloud is accessible via port 8080 on the host machine.

Note: Just because all the containers are running, it takes a few minutes for ownCloud to be fully functional. If you run `docker-compose logs --follow owncloud` and see a significant amount of information logging to the console, then please wait until it slows down to attempt to access the web UI.

Logging In

To log in to the ownCloud UI, open `http://localhost` in your browser of choice, where you see the standard ownCloud login screen, as in the image below.



The username and password are the admin username and password which you stored in `.env` earlier.

Stopping the Containers

Assuming you used `docker-compose`, as in the previous example, to stop the containers use `docker-compose stop`. Alternatively, use `docker-compose down` to stop and remove containers, along with the related networks, images, and volumes.

Upgrading ownCloud on Docker

When a new version of ownCloud gets released, you should update your instance. To do so, follow these simple steps.

First, go to your docker directory where your `.yaml` or `.env` file exists. Second, put ownCloud into maintenance mode; you can do so using the following command:

```
docker-compose exec server occ maintenance:mode --on
```

Third, create a backup in case something goes wrong during the upgrade process, using the following command:

```
docker-compose exec db backup
```

Note: This assumes that you are using [the default database container from Webhippie](#).

Fifth, shutdown the containers.

```
docker-compose down
```

Sixth, update the version number of ownCloud in your `.env` file or the YAML file. You can use `sed` for it, as in the following example.

```
# Make sure that you adjust the example to match your installation.
sed -i 's/^OWNCLOUD_VERSION=.*$/OWNCLOUD_VERSION=<newVersion>/' /compose/*.env
```

Seventh, view the file to ensure the changes has been implemented.

```
cat .env
```

Eighth, start your docker instance again.

```
docker-compose up -d
```

Now you should have the current ownCloud running with docker-compose.

4.8 Command Line Installation

ownCloud can be installed entirely from the command line. This is convenient for scripted operations and for systems administrators who prefer using the command line over a GUI. It involves five steps:

1. Ensure your server meets *the ownCloud prerequisites*
2. Download and unpack the source
3. Install using the `occ` command
4. Set the correct owner and permissions
5. Optional post#installation considerations

Let's begin. To install ownCloud, first [download the source](#) (whether community or enterprise) directly from ownCloud, and then unpack (decompress) the tarball into the appropriate directory.

With that done, you next need to set your webserver user to be the owner of your unpacked `owncloud` directory, as in the example below.

```
$ sudo chown -R www-data:www-data /var/www/owncloud/
```

With those steps completed, next use the `occ` command, from the root directory of the ownCloud source, to perform the installation. This removes the need to run the Graphical Installation Wizard. Here's an example of how to do it

```
# Assuming you've unpacked the source to /var/www/owncloud/
$ cd /var/www/owncloud/
$ sudo -u www-data php occ maintenance:install \
  --database "mysql" --database-name "owncloud" \
  --database-user "root" --database-pass "password" \
  --admin-user "admin" --admin-pass "password"
```

Note: You must run `occ` as your HTTP user. See [Run occ As Your HTTP User](#)

If you want to use a directory other than the default (which is `data` inside the root ownCloud directory), you can also supply the `--data-dir` switch. For example, if you were using the command above and you wanted the data directory to be `/opt/owncloud/data`, then add `--data-dir /opt/owncloud/data` to the command.

When the command completes, apply the correct permissions to your ownCloud files and directories (see [Set Strong Directory Permissions](#)). This is extremely important, as it helps protect your ownCloud installation and ensure that it will operate correctly. See [Command Line Installation](#) for more information.

4.9 Configuration Notes & Tips

4.9.1 SELinux

See *SELinux Configuration* for a suggested configuration for SELinux-enabled distributions such as Fedora and CentOS.

4.9.2 php.ini

Several core PHP settings must be configured correctly, otherwise ownCloud may not work properly. Known settings causing issues are listed here. Please note that, there might be other settings which cause unwanted behavior. In general, however, it is recommended to keep the `php.ini` settings at their defaults, except when you know exactly why the change is required, and its implications.

Note: Keep in mind that, changes to `php.ini` may have to be configured in more than one ini file. This can be the case, for example, for the `date.timezone` setting.

php.ini - Used by the Web server

For PHP version 7.0 onward, replace `php_version` with the version number installed, e.g., `7.0` in the following examples.

```
/etc/php/[php_version]/apache2/php.ini  
or  
/etc/php/[php_version]/fpm/php.ini  
or ...
```

php.ini - used by the php-cli and so by ownCloud CRON jobs

```
/etc/php/[php_version]/cli/php.ini
```

session.auto_start && enable_post_data_reading

Ensure that `session.auto_start` is set to `0` or `Off` and `enable_post_data_reading` to `1` or `On` in your configuration. If not, you may have issues logging in to ownCloud via the WebUI, where you see the error: “*Access denied. CSRF check failed*”.

session.save_path

In addition to setting `session.auto_start` and `enable_post_data_reading` correctly, ensure that, if `session.save_handler` is set to `files`, that `session.save_path` is set to a path on the filesystem which **only** the web server process (or process which PHP is running as) can read from and write to.

This is especially important if your ownCloud installation is using a shared-hosting arrangement. In these situations, [session poisoning](#) can occur if all of the session files are stored in the same location. Session poisoning is where one web application can manipulate data in the `$_SESSION` superglobal array of another.

When this happens, the original application has no way of knowing that this corruption has occurred and may not treat the data with any sense of suspicion. You can [read through a thorough discussion of local session poisoning](#) if you'd like to know more.

suhosin.session.cryptkey

When `suhosin.session.cryptkey` is enabled, session data will be transparently encrypted. If enabled, there is less of a concern in storing application session files in the same location, as discussed in `session.save_path`. Ideally, however, session files for each application should always be stored in a location specific to that application, and never stored collectively with any other.

Note: This is only relevant if you're using PHP 5.x.

post_max_size

Please ensure that you have `post_max_size` configured with *at least* the minimum amount of memory for use with ownCloud, which is 512 MB.

Important: Please be careful when you set this value if you use the byte value shortcut as it is very specific. Use *K* for kilobyte, *M* for megabyte and *G* for gigabyte. *KB*, *MB*, and *GB* **do not work!**

realpath_cache_size

This determines the size of the realpath cache used by PHP. This value should be increased on systems where PHP opens many files, to reflect the number of file operations performed. For a detailed description see [realpath-cache-size](#). This setting has been available since PHP 5.1.0. Prior to PHP 7.0.16 and 7.1.2, the default was 16 KB.

To see your current value, query your `phpinfo()` output for this key. It is recommended to set the value if it is currently set to the default of 16 KB. A good reading about the background can be found at [tideways.io](#).

How to get a working value

With the assumption of 112 bytes per file path needed, this would allow the cache to hold around 37.000 items with a cache size of 4096K (4M), but only about a hundred entries for a cache size of 16 KB.

Note: It's a good rule of thumb to always have a realpath cache that can hold entries for all your files paths in memory. If you use symlink deployment, then set it to double or triple the amount of files.

The easiest way to get the quantity of PHP files is to use `cloc`, which can be installed by running `sudo apt-get install cloc`. The `cloc` package is available for nearly all distributions.

```
sudo cloc /var/www/owncloud --exclude-dir=data --follow-links
 12179 text files.
 11367 unique files.
 73126 files ignored.
```

```
http://cloc.sourceforge.net v 1.60 T=1308.98 s (6.4 files/s, 1283.5 lines/s)
```

Language	files	blank	comment	code
PHP	4896	96509	285384	558135
...				

Taking the math from above and assuming a symlinked instance, using factor 3. For example: $4896 * 3 * 112 = 1.6\text{MB}$ This result shows that you can run with the PHP setting of 4M two instances of ownCloud.

Having the default of 16 KB means that only 1/100 of the existing PHP file paths can be cached and need continuous cache refresh slowing down performance. If you run more web services using PHP, you have to calculate accordingly.

4.9.3 PHP-FPM

System Environment Variables

When you are using `php-fpm`, system environment variables like `PATH`, `TMP` or others are not automatically populated in the same way as when using `php-cli`. A PHP call like `getenv('PATH')` can therefore return an empty result. So you may need to manually configure environment variables in the appropriate `php-fpm ini/config` file.

Here are some example root paths for these ini/config files:

Ubuntu/Mint /etc/php/[php_version]/fpm/	CentOS/Red Hat/Fedora /etc/php-fpm.d/
--------------------------------------------	------------------------------------------

In both examples, the `ini/config` file is called `www.conf`, and depending on the distribution or customizations which you have made, it may be in a sub-directory.

Usually, you will find some or all of the environment variables already in the file, but commented out like this:

```
;env[HOSTNAME] = $HOSTNAME
;env[PATH] = /usr/local/bin:/usr/bin:/bin
;env[TMP] = /tmp
;env[TMPDIR] = /tmp
;env[TEMP] = /tmp
```

Uncomment the appropriate existing entries. Then run `printenv PATH` to confirm your paths, for example:

```
$ printenv PATH
/home/user/bin:/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:
/sbin:/bin:/
```

If any of your system environment variables are not present in the file then you must add them.

When you are using shared hosting or a control panel to manage your ownCloud virtual machine or server, the configuration files are almost certain to be located somewhere else, for security and flexibility reasons, so check your documentation for the correct locations.

Please keep in mind that it is possible to create different settings for `php-cli` and `php-fpm`, and for different domains and Web sites. The best way to check your settings is with *PHP Version and Information*.

Maximum Upload Size

If you want to increase the maximum upload size, you will also have to modify your `php-fpm` configuration and increase the `upload_max_filesize` and `post_max_size` values. You will need to restart `php5-fpm` and your HTTP server in order for these changes to be applied.

.htaccess Notes for Apache

ownCloud comes with its own `owncloud/.htaccess` file. Because `php-fpm` can't read PHP settings in `.htaccess` these settings and permissions must be set in the `owncloud/.user.ini` file.

No basic authentication headers were found

This error is shown in your `data/owncloud.log` file. Some Apache modules like `mod_fastcgi`, `mod_fcgid` or `mod_proxy_fcgi` are not passing the needed authentication headers to PHP and so the login to ownCloud via WebDAV, CalDAV and CardDAV clients is failing. Information on how to correctly configure your environment can be found in the [forums](#) but we generally recommend against the use of these modules and recommend `mod_php` instead.

4.9.4 Other Web Servers

- Other HTTP servers
- Univention Corporate Server installation

4.10 Troubleshooting

4.10.1 Database Configuration Issues

If your ownCloud installation fails and you see the following error in your ownCloud log please refer to *MySQL / MariaDB with Binary Logging Enabled* for how to resolve it.

```
An unhandled exception has been thrown: exception 'PDOException' with message
'SQLSTATE[HY000]: General error: 1665 Cannot execute statement: impossible to
write to binary log since BINLOG_FORMAT = STATEMENT and at least one table
uses a storage engine limited to row-based logging. InnoDB is limited to
row-logging when transaction isolation level is READ COMMITTED or READ
UNCOMMITTED.'
```

4.11 Changing Your ownCloud URL

This admin manual assumes that the ownCloud server is already accessible under the route `/owncloud` (which is the default, e.g. `https://example.com/owncloud`). If you like, you can change this in your web server configuration, for example by changing it from `https://example.com/owncloud/` to `https://example.com/`.

To do so on Debian/Ubuntu Linux, you need to edit these files:

- `/etc/apache2/sites-enabled/owncloud.conf`
- `/var/www/owncloud/config/config.php`

Edit the `Alias` directive in `/etc/apache2/sites-enabled/owncloud.conf` to alias your ownCloud directory to the Web server root:

```
Alias / "/var/www/owncloud/"
```

Edit the `overwrite.cli.url` parameter in `/var/www/owncloud/config/config.php`:

```
'overwrite.cli.url' => 'http://localhost/',
```

When the changes have been made and the file saved, restart Apache. Now you can access ownCloud from either `https://example.com/` or `https://localhost/`.

Note: Note that you will not be able to run any other virtual hosts, as ownCloud is aliased to your web root. On CentOS/Fedora/Red Hat, edit `/etc/httpd/conf.d/owncloud.conf` and `/var/www/html/owncloud/config/config.php`, then restart Apache.

4.12 Installing and Managing Apps

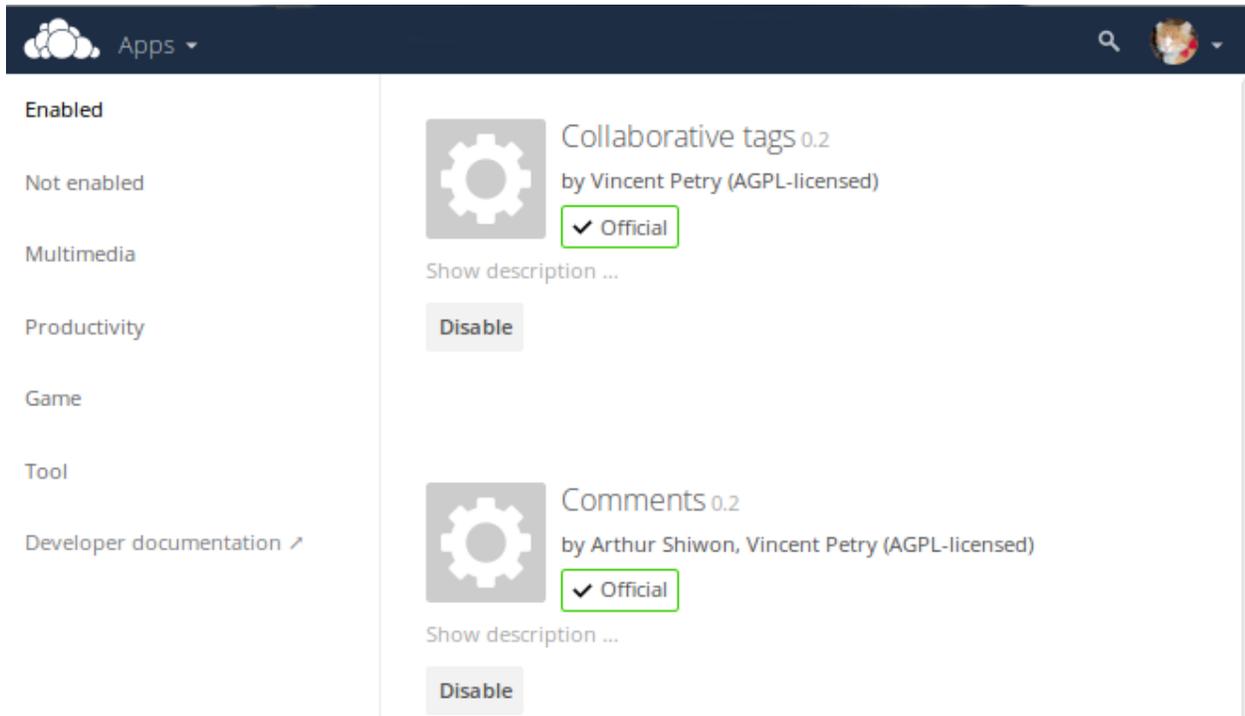
After installing ownCloud, you may provide added functionality by installing applications.

4.12.1 Supported Apps

See *Supported Apps in ownCloud* for a list of supported Enterprise edition apps.

4.12.2 Viewing Enabled Apps

During the ownCloud installation, some apps are installed and enabled by default, and some are able to be installed and enabled later on. To see the status of your installation's applications, go to your Apps page.



There, you will see which apps are currently: *enabled*, *not enabled*, and *recommended*. You'll also see additional filters, such as Multimedia, Productivity, and Tool for finding more apps quickly.

4.12.3 Managing Apps

In the Apps page, you can enable or disable applications. Some apps have configurable options on the Apps page, such as **Enable only for specific groups**, but mainly they are enabled or disabled here and are configured on your ownCloud *Admin page*, *Personal page*, or in `config.php`.

4.12.4 Adding Apps

Click the app name to view a description of the app and any of the app settings in the Application View field. Clicking the **Install** button installs the app. If the app is not part of your ownCloud installation, it will be downloaded from the ownCloud Marketplace, installed, and enabled.

Sometimes the installation of a third-party app fails silently, possibly because `'appcodechecker' => true`, is enabled in `config.php`. When `appcodechecker` is enabled it checks if third-party apps are using the private API, rather than the public API. If they are, then they will not be installed.

Note: If you would like to create or add your own ownCloud app, please refer to the [developer manual](#).

4.12.5 Using Custom App Directories

There are several reasons for using custom app directories instead of ownCloud's default. These are:

1. It separates ownCloud's core apps from user or admin downloaded apps. Doing so distinguishes which apps are core and which aren't, simplifying upgrades.
2. It eases manual upgrades. Downloaded apps must be manually copied. Having them in a separate directory makes it simpler to manage.
3. ownCloud may gain new core apps in newer versions. Doing so orphans deprecated apps, but doesn't remove them.

If you want to store apps in a custom directory, instead of ownCloud's default (`/app`), you need to modify the `apps_paths` element in `config/config.php`. There, you need to add a new associative array that contains three elements. These are:

- `path`: The absolute file system path to the custom app folder.
- `url`: The request path to that folder relative to the ownCloud web root, prefixed with `/`.
- `writable`: Whether users can install apps in that folder. After the configuration is added, new apps will only install in a directory where `writable` is set to `true`.

The configuration example below shows how to add a second directory, called `apps-external`.

```
<?php
$CONFIG = [
    'apps_paths' => [
        [
            'path' => OC::$SERVERROOT.'/apps',
            'url' => '/apps',
            'writable' => false,
        ],
        [
            'path' => OC::$SERVERROOT.'/apps-external',
            'url' => '/apps-external',
            'writable' => true,
        ],
    ],
    // remainder of the configuration
];
```

After you add a new directory configuration, you can then move apps from the original app directory to the new one. To do so, follow these steps:

1. *Enable maintenance mode.*

2. *Disable the apps* that you want to move.
3. Create a new apps directory and assign it the same user and group, and ownership permissions as the core apps directory.
4. Move the apps from the old apps directory to the new apps directory.
5. Add a new app directory in `config/config.php`.
6. If you're using a cache, such as Redis or Memcached, ensure that you clear the cache.
7. Re-enable the apps.
8. Disable maintenance mode.

4.12.6 Manually Installing Apps

To install an app manually instead of by using [the Marketplace](#), copy the app either into ownCloud's default app folder (`</path/to/owncloud>/apps`) or *a custom app folder*.

Be aware that the name of the app and its folder name **must be identical!** You can find these details in *the application's metadata file*, located in `<app directory>/appinfo/info.xml`.

Using the example below, both the app's name and directory name would be `yourappname`.

```
<?xml version="1.0"?>
<info>
  <id>yourappname</id>
  <name>Your App</name>
  <version>1.0</version>
</info>
```

4.13 Supported Apps in ownCloud

4.13.1 AGPL Apps

- Activity
- Anti-Virus
- Collaborative Tags
- Comments
- Encryption
- External Sites
- External Storage
- ownCloud WebDAV Endpoint (handles old and new webdav endpoints)
- Federated File Sharing (allows file sharing across ownCloud instances)
- Federation (allows username auto-complete across ownCloud instances)
- Files (cannot be disabled)
- Files PDF Viewer
- Files Sharing

- Files TextEditor
- Files Trashbin
- Files Versions
- Files VideoPlayer
- First Run Wizard
- Gallery
- Notifications
- Object Storage (Swift)
- Provisioning API
- Template Editor (for notification emails)
- Update Notifications
- User External
- User LDAP

4.13.2 Enterprise-Only Apps

- Auditing
- Collaborative Tags Management
- Enterprise License Key
- File Firewall
- LDAP Home Connector
- Object Storage Support
- Password Policy
- External Storage: SharePoint
- SAML/Shibboleth User Backend
- Windows Network Drives (requires External Storage)
- Workflows
- ownCloud X Enterprise Theme

4.14 SELinux Configuration

When you have SELinux enabled on your Linux distribution, you may run into permissions problems after a new ownCloud installation, and see `permission denied` errors in your ownCloud logs.

The following settings should work for most SELinux systems that use the default distro profiles. Run these commands as root, and remember to adjust the filepaths in these examples for your installation

```
semanage fcontext -a -t httpd_sys_rw_content_t '/var/www/html/owncloud/data(/.*)?'
semanage fcontext -a -t httpd_sys_rw_content_t '/var/www/html/owncloud/config(/.*)?'
semanage fcontext -a -t httpd_sys_rw_content_t '/var/www/html/owncloud/apps(/.*)?'
semanage fcontext -a -t httpd_sys_rw_content_t '/var/www/html/owncloud/.htaccess'
semanage fcontext -a -t httpd_sys_rw_content_t '/var/www/html/owncloud/.user.ini'

restorecon -Rv '/var/www/html/owncloud/'
```

If you uninstall ownCloud you need to remove the ownCloud directory labels. To do this execute the following commands as root after uninstalling ownCloud

```
semanage fcontext -d '/var/www/html/owncloud/data(/.*)?'
semanage fcontext -d '/var/www/html/owncloud/config(/.*)?'
semanage fcontext -d '/var/www/html/owncloud/apps(/.*)?'
semanage fcontext -d '/var/www/html/owncloud/.htaccess'
semanage fcontext -d '/var/www/html/owncloud/.user.ini'

restorecon -Rv '/var/www/html/owncloud/'
```

If you have customized SELinux policies and these examples do not work, you must give the HTTP server write access to these directories:

```
/var/www/html/owncloud/data
/var/www/html/owncloud/config
/var/www/html/owncloud/apps
```

4.14.1 Enable updates via the web interface

To enable updates via the ownCloud web interface, you may need this to enable writing to the ownCloud directories:

```
setsebool httpd_unified on
```

When the update is completed, disable write access:

```
setsebool -P httpd_unified off
```

4.14.2 Disallow write access to the whole web directory

For security reasons it's suggested to disable write access to all folders in /var/www/ (default):

```
setsebool -P httpd_unified off
```

4.14.3 Allow access to a remote database

An additional setting is needed if your installation is connecting to a remote database:

```
setsebool -P httpd_can_network_connect_db on
```

4.14.4 Allow access to LDAP server

Use this setting to allow LDAP connections:

```
setsebool -P httpd_can_connect_ldap on
```

4.14.5 Allow access to remote network

ownCloud requires access to remote networks for functions such as Server-to-Server sharing, external storages or the ownCloud Marketplace. To allow this access use the following setting:

```
setsebool -P httpd_can_network_connect on
```

4.14.6 Allow access to network memcache

This setting is not required if `httpd_can_network_connect` is already on:

```
setsebool -P httpd_can_network_memcache on
```

4.14.7 Allow access to SMTP/sendmail

If you want to allow ownCloud to send out e-mail notifications via sendmail you need to use the following setting:

```
setsebool -P httpd_can_sendmail on
```

4.14.8 Allow access to CIFS/SMB

If you have placed your datadir on a CIFS/SMB share use the following setting:

```
setsebool -P httpd_use_cifs on
```

4.14.9 Allow access to FuseFS

If your owncloud data folder resides on a Fuse Filesystem (e.g. EncFS etc), this setting is required as well:

```
setsebool -P httpd_use_fusefs on
```

4.14.10 Allow access to GPG for Rainloop

If you use a the rainloop webmail client app which supports GPG/PGP, you might need this:

```
setsebool -P httpd_use_gpg on
```

4.14.11 Troubleshooting

General Troubleshooting

For general Troubleshooting of SELinux and its profiles try to install the package `setroubleshoot` and run:

```
sealert -a /var/log/audit/audit.log > /path/to/mylogfile.txt
```

to get a report which helps you configuring your SELinux profiles.

Another tool for troubleshooting is to enable a single ruleset for your ownCloud directory:

```
semanage fcontext -a -t httpd_sys_rw_content_t '/var/www/html/owncloud(/.*)?'
restorecon -RF /var/www/html/owncloud
```

It is much stronger security to have a more fine-grained ruleset as in the examples at the beginning, so use this only for testing and troubleshooting. It has a similar effect to disabling SELinux, so don't use it on production systems.

See this [discussion on GitHub](#) to learn more about configuring SELinux correctly for ownCloud.

Redis on RHEL 7 & Derivatives

On RHEL 7 and its derivatives, if you are using Redis for both local server cache and file locking and Redis is configured to listen on a Unix socket instead of a TCP/IP port (*which is recommended if Redis is running on the same system as ownCloud*) you must instruct SELinux to allow daemons to enable cluster mode. You can do this using the following command:

```
setsebool -P daemons_enable_cluster_mode 1
```

4.15 NGINX Configuration

This page covers example NGINX configurations to use with running an ownCloud server. Note that NGINX is *not officially supported*, and this page is *community-maintained*. Thank you, contributors!

- Depending on your setup, you need to insert the code examples into your NGINX configuration file.
- Adjust **server_name**, **root**, **ssl_certificate**, **ssl_certificate_key** ect. to suit your needs.
- Make sure your SSL certificates are readable by the server (see [NGINX HTTP SSL Module documentation](#)).
- `add_header` statements are only valid in the current `location` block and are not derived or cascaded from or to a different `location` block. All necessary `add_header` statements **must** be defined in each `location` block needed.
- For better readability it is possible to move *common* `add_header` directives into a separate file and include that file wherever necessary. However, each `add_header` directive must be written in a single line to prevent connection problems with sync clients.
- The same is true for `map` directives which also can be collected into a single file and then be included.

4.15.1 Example Configurations

Note: Be careful about line breaks if you copy the examples, as long lines may be broken for page formatting.

You can use ownCloud over plain HTTP. However, *we strongly encourage you* to use SSL/TLS to encrypt all of your server traffic **and** to protect users' logins, and their data while it is in transit. To use plain HTTP:

1. Remove the server block containing the redirect
2. Change **listen 443 ssl http2** to **listen 80**;
3. Remove all **ssl_** entries.
4. Remove **fastcgi_params HTTPS on**;

Note 1

```
fastcgi_buffers 8 4K;
```

- Do not set the number of buffers to greater than 63. In our example, it is set to 8.
- If you exceed this maximum, big file downloads may consume a lot of system memory over time. This is especially problematic on low-memory systems.

Note 2

```
fastcgi_ignore_headers
X-Accel-Buffering
```

- From ownCloud version 10.0.4 on, a header will be sent to NGINX not to use buffers to avoid problems with problematic `fastcgi_buffers` values. See note above.
- If the values of `fastcgi_buffers` are properly set and no problems are expected, you can use this directive to reenble buffering **overriding** the sent header.
- In case you use an earlier version of ownCloud or can't change the buffers, or can't remove a existing ignore header directive, you can explicitly enable following directive in the location block `fastcgi_buffering off;`

Note: The directives `fastcgi_ignore_headers X-Accel-Buffering;` and `fastcgi_buffering off;` can be used separately but not together.

ownCloud in the web root of NGINX

The following config should be used when ownCloud is placed in the web root of your NGINX installation.

The configuration assumes that ownCloud is installed in

`/var/www/owncloud` and is accessed via `http(s)://cloud.example.com`.

```
upstream php-handler {
    server 127.0.0.1:9000;
    # Depending on your used PHP version
    #server unix:/var/run/php5-fpm.sock;
    #server unix:/var/run/php7-fpm.sock;
}

server {
    listen 80;
    server_name cloud.example.com;

    # For Lets Encrypt, this needs to be served via HTTP
    location /.well-known/acme-challenge/ {
        root /var/www/owncloud; # Specify here where the challenge file is placed
    }

    # enforce https
    location / {
        return 301 https://$server_name$request_uri;
    }
}
```

```
server {
    listen 443 ssl http2;
    server_name cloud.example.com;

    ssl_certificate /etc/ssl/nginx/cloud.example.com.crt;
    ssl_certificate_key /etc/ssl/nginx/cloud.example.com.key;

    # Example SSL/TLS configuration. Please read into the manual of NGINX before applying these.
    ssl_session_timeout 5m;
    ssl_protocols TLSv1 TLSv1.1 TLSv1.2;
    ssl_ciphers "-ALL:EECDH+AES256:EDH+AES256:AES256-SHA:EECDH+AES:EDH+AES:!ADH:!NULL:!aNULL:!eNULL";
    ssl_dhparam /etc/nginx/dh4096.pem;
    ssl_prefer_server_ciphers on;
    keepalive_timeout 70;
    ssl_stapling on;
    ssl_stapling_verify on;

    # Add headers to serve security related headers
    # Before enabling Strict-Transport-Security headers please read into this topic first.
    #add_header Strict-Transport-Security "max-age=15552000; includeSubDomains";
    add_header X-Content-Type-Options nosniff;
    add_header X-Frame-Options "SAMEORIGIN";
    add_header X-XSS-Protection "1; mode=block";
    add_header X-Robots-Tag none;
    add_header X-Download-Options noopen;
    add_header X-Permitted-Cross-Domain-Policies none;

    # Path to the root of your installation
    root /var/www/owncloud/;

    location = /robots.txt {
        allow all;
        log_not_found off;
        access_log off;
    }

    # The following 2 rules are only needed for the user_webfinger app.
    # Uncomment it if you're planning to use this app.
    #rewrite ^/.well-known/host-meta /public.php?service=host-meta last;
    #rewrite ^/.well-known/host-meta.json /public.php?service=host-meta-json last;

    location = /.well-known/carddav {
        return 301 $scheme://$host/remote.php/dav;
    }
    location = /.well-known/caldav {
        return 301 $scheme://$host/remote.php/dav;
    }

    # set max upload size
    client_max_body_size 512M;
    fastcgi_buffers 8 4K; # Please see note 1
    fastcgi_ignore_headers X-Accel-Buffering; # Please see note 2

    # Disable gzip to avoid the removal of the ETag header
    # Enabling gzip would also make your server vulnerable to BREACH
    # if no additional measures are done. See https://bugs.debian.org/cgi-bin/bugreport.cgi?bug=773
    gzip off;
```

```

# Uncomment if your server is build with the ngx_pagespeed module
# This module is currently not supported.
#pagespeed off;

error_page 403 /core/templates/403.php;
error_page 404 /core/templates/404.php;

location / {
    rewrite ^ /index.php$uri;
}

location ~ ^/(?:(build|tests|config|lib|3rdparty|templates|data)/ {
    return 404;
}
location ~ ^/(?!(\.|autotest|occ|issue|indie|db_|console) {
    return 404;
}

location ~ ^/(?:(index|remote|public|cron|core/ajax/update|status|ocs/v[12]|updater/.+|ocs-provider
    fastcgi_split_path_info ^(.+\.(php|\.))(/.*)$;
    include fastcgi_params;
    fastcgi_param SCRIPT_FILENAME $document_root$fastcgi_script_name;
    fastcgi_param SCRIPT_NAME $fastcgi_script_name; # necessary for owncloud to detect the cont
    fastcgi_param PATH_INFO $fastcgi_path_info;
    fastcgi_param HTTPS on;
    fastcgi_param modHeadersAvailable true; #Avoid sending the security headers twice
    fastcgi_param front_controller_active true;
    fastcgi_read_timeout 180; # increase default timeout e.g. for long running carddav/ caldav
    fastcgi_pass php-handler;
    fastcgi_intercept_errors on;
    fastcgi_request_buffering off; #Available since NGINX 1.7.11
}

location ~ ^/(?:(updater|ocs-provider)(?:$|/)) {
    try_files $uri $uri/ =404;
    index index.php;
}

# Adding the cache control header for js and css files
# Make sure it is BELOW the PHP block
location ~ \.(?:css|js)$ {
    try_files $uri /index.php$uri$is_args$args;
    add_header Cache-Control "max-age=15778463";
    # Add headers to serve security related headers (It is intended to have those duplicated to
    # Before enabling Strict-Transport-Security headers please read into this topic first.
    #add_header Strict-Transport-Security "max-age=15552000; includeSubDomains";
    add_header X-Content-Type-Options nosniff;
    add_header X-Frame-Options "SAMEORIGIN";
    add_header X-XSS-Protection "1; mode=block";
    add_header X-Robots-Tag none;
    add_header X-Download-Options noopen;
    add_header X-Permitted-Cross-Domain-Policies none;
    # Optional: Don't log access to assets
    access_log off;
}

location ~ \.(?:svg|gif|png|html|ttf|woff|ico|jpg|jpeg|map)$ {
    add_header Cache-Control "public, max-age=7200";
}

```

```
    try_files $uri /index.php$uri$is_args$args;
    # Optional: Don't log access to other assets
    access_log off;
}
}
```

ownCloud in a subdirectory of NGINX

The following config should be used when ownCloud is placed under a different context root of your NGINX installation such as `/owncloud` or `/cloud`.

The configuration assumes that ownCloud is installed in

`/var/www/owncloud` is accessed via `http(s)://example.com/owncloud`

and that you have `'overwriteweb root' => '/owncloud'`, set in your `config/config.php`.

```
upstream php-handler {
    server 127.0.0.1:9000;
    # Depending on your used PHP version
    #server unix:/var/run/php5-fpm.sock;
    #server unix:/var/run/php7-fpm.sock;
}

server {
    listen 80;
    server_name cloud.example.com;

    # For Lets Encrypt, this needs to be served via HTTP
    location /.well-known/acme-challenge/ {
        root /var/www/owncloud; # Specify here where the challenge file is placed
    }

    # enforce https
    location / {
        return 301 https://$server_name$request_uri;
    }
}

server {
    listen 443 ssl http2;
    server_name cloud.example.com;

    ssl_certificate /etc/ssl/nginx/cloud.example.com.crt;
    ssl_certificate_key /etc/ssl/nginx/cloud.example.com.key;

    # Example SSL/TLS configuration. Please read into the manual of NGINX before applying these.
    ssl_session_timeout 5m;
    ssl_protocols TLSv1 TLSv1.1 TLSv1.2;
    ssl_ciphers "-ALL:EECDH+AES256:EDH+AES256:AES256-SHA:EECDH+AES:EDH+AES:!ADH:!NULL:!aNULL:!eNULL";
    ssl_dhparam /etc/nginx/dh4096.pem;
    ssl_prefer_server_ciphers on;
    keepalive_timeout 70;
    ssl_stapling on;
    ssl_stapling_verify on;

    # Add headers to serve security related headers
```

```

# Before enabling Strict-Transport-Security headers please read into this topic first.
#add_header Strict-Transport-Security "max-age=15552000; includeSubDomains";
add_header X-Content-Type-Options nosniff;
add_header X-Frame-Options "SAMEORIGIN";
add_header X-XSS-Protection "1; mode=block";
add_header X-Robots-Tag none;
add_header X-Download-Options noopen;
add_header X-Permitted-Cross-Domain-Policies none;

# Path to the root of your installation
root /var/www/;

location = /robots.txt {
    allow all;
    log_not_found off;
    access_log off;
}

# The following 2 rules are only needed for the user_webfinger app.
# Uncomment it if you're planning to use this app.
#rewrite ^/.well-known/host-meta /owncloud/public.php?service=host-meta last;
#rewrite ^/.well-known/host-meta.json /owncloud/public.php?service=host-meta-json last;

location = /.well-known/carddav {
    return 301 $scheme://$host/owncloud/remote.php/dav;
}
location = /.well-known/caldav {
    return 301 $scheme://$host/owncloud/remote.php/dav;
}

location ^~ /owncloud {

    # set max upload size
    client_max_body_size 512M;
    fastcgi_buffers 8 4K; # Please see note 1
    fastcgi_ignore_headers X-Accel-Buffering; # Please see note 2

    # Disable gzip to avoid the removal of the ETag header
    # Enabling gzip would also make your server vulnerable to BREACH
    # if no additional measures are done. See https://bugs.debian.org/cgi-bin/bugreport.cgi?bu
    gzip off;

    # Uncomment if your server is build with the ngx_pagespeed module
    # This module is currently not supported.
    #pagespeed off;

    error_page 403 /owncloud/core/templates/403.php;
    error_page 404 /owncloud/core/templates/404.php;

    location /owncloud {
        rewrite ^ /owncloud/index.php$uri;
    }

    location ~ ^/owncloud/(?::build|tests|config|lib|3rdparty|templates|data)/ {
        return 404;
    }
    location ~ ^/owncloud/(?::\.|autotest|occ|issue|indie|db_|console) {

```

```
        return 404;
    }

    location ~ ^/owncloud/(? :index|remote|public|cron|core/ajax/update|status|ocs/v[12]|update) {
        fastcgi_split_path_info ^(.+\.(php))(/.*)$;
        include fastcgi_params;
        fastcgi_param SCRIPT_FILENAME $document_root$fastcgi_script_name;
        fastcgi_param SCRIPT_NAME $fastcgi_script_name; # necessary for owncloud to detect the
        fastcgi_param PATH_INFO $fastcgi_path_info;
        fastcgi_param HTTPS on;
        fastcgi_param modHeadersAvailable true; #Avoid sending the security headers twice
        # EXPERIMENTAL: active the following if you need to get rid of the 'index.php' in the U
        #fastcgi_param front_controller_active true;
        fastcgi_read_timeout 180; # increase default timeout e.g. for long running carddav/ cal
        fastcgi_pass php-handler;
        fastcgi_intercept_errors on;
        fastcgi_request_buffering off; #Available since NGINX 1.7.11
    }

    location ~ ^/owncloud/(? :updater|ocs-provider)(? :$|/) {
        try_files $uri $uri/ =404;
        index index.php;
    }

    # Adding the cache control header for js and css files
    # Make sure it is BELOW the PHP block
    location ~ /owncloud/.*\.(? :css|js) {
        try_files $uri /owncloud/index.php$uri$is_args$args;
        add_header Cache-Control "max-age=15778463";
        # Add headers to serve security related headers (It is intended to have those duplicat
        # Before enabling Strict-Transport-Security headers please read into this topic first.
        #add_header Strict-Transport-Security "max-age=15552000; includeSubDomains";
        add_header X-Content-Type-Options nosniff;
        add_header X-Frame-Options "SAMEORIGIN";
        add_header X-XSS-Protection "1; mode=block";
        add_header X-Robots-Tag none;
        add_header X-Download-Options noopen;
        add_header X-Permitted-Cross-Domain-Policies none;
        # Optional: Don't log access to assets
        access_log off;
    }

    location ~ /owncloud/.*\.(? :svg|gif|png|html|ttf|woff|ico|jpg|jpeg|map) {
        try_files $uri /owncloud/index.php$uri$is_args$args;
        add_header Cache-Control "public, max-age=7200";
        # Optional: Don't log access to other assets
        access_log off;
    }
}
}
```

4.15.2 Troubleshooting

JavaScript (.js) or CSS (.css) files not served properly

A standard issue with custom NGINX configurations is, that JavaScript (.js) or CSS (.css) files are not served properly, leading to a 404 (File Not Found) error on those files and a broken web interface.

- This could be caused by an improper sequence of `location` blocks.

The following sequence is correct:

```
location ~ /\.php(?:$|/) {
    ...
}

location ~ /\.(?:css|js)$ {
    ...
}
```

Other custom configurations like caching JavaScript (.js) or CSS (.css) files via `gzip` could also cause such issues.

Not all of my contacts are synchronized

Check for server timeouts! It turns out that CardDAV sync often fails silently if the request runs into timeouts. With PHP-FPM you might see a “CoreDAVHTTPStatusErrorDomain error 504” which is an “HTTP 504 Gateway timeout” error. To solve this, first check the `default_socket_timeout` setting in `/etc/php/7.0/fpm/php.ini` and increase the above `fastcgi_read_timeout` accordingly. Depending on your server’s performance a timeout of 180s should be sufficient to sync an address book of ~1000 contacts.

Windows: Error 0x80070043 “The network name cannot be found.” while adding a network drive

The windows native WebDAV client might fail with the following error message:

```
Error 0x80070043 "The network name cannot be found." while adding a network drive
```

A known workaround for this issue is to update your web server configuration.

Because NGINX does not allow nested `if` directives, you need to use the `map` directive. The position of the `location` directive is important for success.

1 Create a map directive outside your server block

```
# Fixes Windows WebDav client error 0x80070043 "The network name cannot be found."
map "$http_user_agent:$request_method" $WinWebDav {
    default                0;
    "DavClnt:OPTIONS"     1;
}
```

2 Inside your server block on top of your location directives

```
location = / {
    if ($WinWebDav) { return 401; }
}
```

4.15.3 Log Optimisation

Suppressing htaccessstest.txt and .ocdata Log Messages

If you are seeing meaningless messages in your logfile, for example `client denied by server configuration: /var/www/data/htaccessstest.txt`, or access to `.ocdata`, add this section to your NGINX configuration to suppress them:

```
location = /data/htaccessstest.txt {
    allow all;
    log_not_found off;
    access_log off;
}

location = /data/.ocdata {
    access_log off;
}
```

Prevent access log entries when accessing thumbnails

When using eg. the Gallery App, any access to a thumbnail of a picture will be logged. This can cause a massive log quantity making log reading challenging. With this approach, you can prevent access logging for those thumbnails.

1 Create a map directive outside your server block like

(Adopt the path queried according your needs.)

```
# do not access log to gallery thumbnails, flooding access logs only, error will be logged anyway
map $request_uri $loggable {
    default 1;
    ~*\apps\/gallery\/thumbnails 0;
}
```

2 Inside your server block where you define your logs

```
access_log /path-to-your-log-file combined if=$loggable;
```

If you want or need to log thumbnails access, you can easily add another logfile which only logs this access. You can easily enable / disable this kind of logging if you uncomment / comment the line starting with 0 in the following map directive.

Below the above map statement

```
# invert the $loggable variable
map $loggable $invertloggable {
    default 0;
    0 1;
}
```

Below the above access_log statement

```
access_log /var/log/nginx/<your-log-file-inverted> combined if=$invertloggable;
```

4.15.4 Performance Tuning

1 HTTP/2

To increase the performance of your NGINX installation, we recommend using either the SPDY or HTTP_V2 modules, depending on your installed NGINX version.

- nginx (<1.9.5) `ngx_http_spdy_module`
- nginx (+1.9.5) `ngx_http_v2_module`

To use HTTP_V2 for NGINX you have to check two things:

1. Be aware that this module may not be built in by default, due to a dependency to the OpenSSL version used on your system. It will be enabled with the `--with-http_v2_module` configuration parameter during compilation. The dependencies should be checked automatically. You can check the presence of `ngx_http_v2_module` by using the command: `nginx -V 2>&1 | grep http_v2 -o`. A description of how to compile NGINX to include modules can be found in [Compiling Modules](#).
2. When changing from **SPDY** to **HTTP v2**, the NGINX config has to be changed from `listen 443 ssl spdy;` to `listen 443 ssl http2;`

2 Caching Metadata

The `open_file_cache` directive can help you to cache file metadata information. This can increase performance on high loads respectively when using eg NFS as backend. That cache can store:

- Open file descriptors, their sizes and modification times;
- Information on existence of directories;
- File lookup errors, such as “file not found”, “no read permission”, and so on.

To configure metadata caching, add following directives either in your `http`, `server` or `location` block:

```
open_file_cache          max=10000 inactive=5m;
open_file_cache_valid   1m;
open_file_cache_min_uses 1;
open_file_cache_errors  on;
```

Configure NGINX to use caching for ownCloud internal images and thumbnails

This mechanism speeds up presentation as it shifts requests to NGINX and minimizes PHP invocations, which otherwise would take place for every thumbnail or internal image presented every time.

1 Preparation

- Create a directory where NGINX will save the cached thumbnails or internal images. Use any path that fits to your environment. Replace `/opt/cachezone` in this example with your path created:

```
sudo mkdir -p /opt/cachezone
sudo chown www-data:www-data /opt/cachezone
```

2 Configuration

1. **Define when to skip the cache:**

- **Option 1:** `map`

This is the preferred method. In the `http{}` block, but *outside* the `server{}` block:

```
# skip_cache, default skip
map $request_uri $skip_cache {
    default          1;
    ~*\thumbnail.php 0;
    ~*\apps/gallery/ 0;
```

```
    ~*\/core\/img\/    0;
}
```

- **Option 2:** `if`

In the `server{}` block, above the location block mentioned below:

```
set $skip_cache 1;
if ($request_uri ~* "thumbnail.php")    { set $skip_cache 0; }
if ($request_uri ~* "/apps/gallery/")    { set $skip_cache 0; }
if ($request_uri ~* "/core/img/")       { set $skip_cache 0; }
```

2. General Config:

In case you want to have multiple cache paths with different cache keys, follow the NGINX documentation where to place the directives. For the sake of simplicity, we both add them to the `http{}` block.

- Add *inside* the `http{}` block:

```
fastcgi_cache_path /opt/cache levels=1:2 keys_zone=cachezone:100m
                    max_size=500m inactive=60m use_temp_path=off;
fastcgi_cache_key $http_cookie$request_method$host$request_uri;
```

- Add *inside* the `server{}` block the following FastCGI caching directives, as an example of a configuration:

```
location ~ \.php(?:$/) {
    fastcgi_split_path_info ^(.+\.(php))(/.+)$;

    include fastcgi_params;
    # ...

    ## Begin - FastCGI caching
    fastcgi_ignore_headers    "Cache-Control"
                              "Expires"
                              "Set-Cookie";
    fastcgi_cache_use_stale   error
                              timeout
                              updating
                              http_429
                              http_500
                              http_503;
    fastcgi_cache_background_update on;
    fastcgi_no_cache          $skip_cache;
    fastcgi_cache_bypass      $skip_cache;
    fastcgi_cache              cachezone;
    fastcgi_cache_valid        60m;
    fastcgi_cache_methods     GET HEAD;
    ## End - FastCGI caching
}
```

3 Test the configuration

```
sudo nginx -t
sudo service nginx reload
```

- Open your browser and clear your cache.
- Logon to your ownCloud instance, open the gallery app, move thru your folders and watch while the thumbnails are generated for the first time.

- You may also watch with eg. `htop` your system load while the thumbnails are processed.
- Go to another app or logout and relogin.
- Open the gallery app again and browse to the folders you accessed before. Your thumbnails should appear more or less immediately.
- `htop` will not show up additional load while processing, compared to the high load before.

4.16 Using Let's Encrypt SSL Certificates

This page covers how to configure your web server to use [Let's Encrypt](#) as the certificate authority for your own-Cloud server. Note that Let's Encrypt is *not officially supported*, and this page is *community-maintained*. Thank you, contributors!

- For ease of handling, SSL-specific directives have been moved into a separately included file. This can help for first-time certificate issuance as well as for reusing configurations.
- The examples shown are based on Ubuntu 17.10.
- Read the [Certbot user guide](#) for details of the commands.
- Let's Encrypt CA issues short-lived certificates valid for 90 days. Make sure you renew the certificates at least once in this period, because expired certificates need reissuing. A certificate is due for renewal earliest 30 days before expiring. Certbot can be forced to renew via options at any time as long the certificate is valid.

Excellent introductions to strong SSL security measures can be found here: [Apache](#) and [NGINX](#).

1. [Requirements & Dependencies](#)
2. [Install Let's Encrypt's Certbot client](#)
3. [Register your email address](#)
4. [Create Let's Encrypt's config files](#)
5. [Create an SSL certificate](#)
6. [Web Server setup](#)
7. [Test the setup](#)
8. [‘Certificate renewal’_](#)

4.16.1 Requirements & Dependencies

- You require a domain name with a valid [A record](#) pointing back to your servers IP address. In case your server is behind a firewall, take the necessary measures to ensure that your server is accessible, worldwide, from the internet, by adding the required firewall and port forward rules.

4.16.2 Install Let's Encrypt's Certbot client

The latest [Certbot](#) client can be installed in two ways:

1. *From source.*
2. With the Ubuntu *ppa repository*.

Via GitHub

```
sudo apt-get update
sudo apt-get install -y git
sudo git clone https://github.com/certbot/certbot /opt/letsencrypt
```

To run Certbot use the following command:

```
sudo /opt/letsencrypt/certbot-auto
```

Note: For the sake of simplicity, the path chosen for the installation is `/opt/letsencrypt`. You can use any path that fits your needs.

Note: Unless explicitly denied, Certbot will auto-update on each run.

As part of the first run, `certbot-auto` will install any missing dependencies.

Via Apt

To install Certbot via the PPA repository, run the following commands. These will add the repository, update Apt's cache, and install Certbot.

```
sudo apt-get install certbot
```

Note: If you're using a version of Ubuntu prior to 17.10, you may need to run the following commands before you can install Certbot:

```
sudo apt-get update
sudo apt-get install software-properties-common
sudo add-apt-repository ppa:certbot/certbot
```

To run Certbot use the following command:

```
sudo /usr/bin/certbot
```

```
# Alternatively, you could run the following instead
sudo certbot
```

Note: Depending on how you installed Let's Encrypt, `certbot` may also be named `letsencrypt` or `certbot-auto`. However, this guide will refer to it as `certbot`. Please bear that in mind, and update the `../examples` and scripts used in this guide to reflect your Certbot installation.

4.16.3 Updating Certbot

If you need to update Certbot at a later date, run `sudo apt-get install --only-upgrade certbot`.

4.16.4 Register your email address

Now that Certbot is installed, register your email address for urgent renewal and security notifications. This command also prepares Certbot's environment if it's not already installed. To do this, run the following command:

```
sudo certbot register --agree-tos --email <your-email-address>
```

When it executes, you'll see the following question, which you can answer "Yes" or "No" to:

Saving debug log to /var/log/letsencrypt/letsencrypt.log

```
-----
Would you be willing to share your email address with the Electronic Frontier
Foundation, a founding partner of the Let's Encrypt project and the non-profit
organization that develops Certbot? We'd like to send you email about EFF and
our work to encrypt the web, protect its users and defend digital rights.
-----
```

```
(Y)es/(N)o:
```

When that completes, you'll see a message similar to the following:

IMPORTANT NOTES:

1. Your account credentials have been saved in your Certbot configuration directory at /etc/letsencrypt. You should make a secure backup of this folder now. This configuration directory will also contain certificates and private keys obtained by Certbot so making regular backups of this folder is ideal.

Please, **strongly**, consider following its recommendation.

4.16.5 Create Let's Encrypt's config files

- Create following files in the Let's Encrypt directory. They will help to maintain your certificates.
- Replace the path to Certbot and the Certbot script name based on your installation. You can find it by running `which certbot`.
- Rename `<your-domain-name>.sh` with the name of the domain(s) you want to issue a certificate for. As an example, the script could be renamed to `your-domain-name.com.sh`.
- Make all files executable except `cli.ini` by running `sudo chmod +x <script-name>`.

Note: All scripts have to be executed with `sudo`.

```
cd /etc/letsencrypt
touch cli.ini list.sh renew.sh renew-cron.sh delete.sh <your-domain-name>.sh
```

cli.ini

This file defines some settings used by Certbot. Use the email address you registered with. Comment / un-comment the post-hook parameter according which web server you use.

```
rsa-key-size = 4096
email = <your-email-address>
agree-tos = True
authenticator = webroot
webroot-path = /var/www/letsencrypt/
post-hook = service nginx reload
# post-hook = service apache2 reload
```

list.sh

This script lists all your issued certificates.

```
#!/bin/bash

LE_PATH="/usr/bin"
LE_CB="certbot"

"$LE_PATH/$LE_CB" certificates
```

renew.sh

This script:

1. Renews all your issued certificates.
2. Updates Certbot, when using Git as the installation source.
3. Reloads the web server configuration automatically if a certificate has been renewed.

```
#!/bin/bash

LE_PATH="/usr/bin"
LE_CB="certbot"

"$LE_PATH/$LE_CB" renew
```

renew-cron.sh

This script:

- Renews all your issued certificates but does not upgrade Certbot.
- Reloads the web server configuration automatically if a certificate has been renewed.

Note: It is intended for use via Cron.

```
#!/bin/bash

LE_PATH="/usr/bin"
LE_CB="certbot"

"$LE_PATH/$LE_CB" renew --no-self-upgrade --noninteractive
```

delete.sh

This script deletes an issued certificate. Use the `list.sh` script to list issued certificates.

```
#!/bin/bash

LE_PATH="/usr/bin"
LE_CB="certbot"

##
## Retrieve and print a list of the installed Let's Encrypt SSL certificates.
```

```
##
function get_certificate_names()
{
    "$LE_PATH/$LE_CB" certificates | grep -iE "certificate name" | awk -F: '{gsub(/\s+/, ""); print $2}'
}

echo "Available Certificates:"

get_certificate_names
echo

read -p "Which certificate do you want to delete: " -r -e answer
if [ -n "$answer" ]; then
    "$LE_PATH/$LE_CB" delete --cert-name "$answer"
fi
```

<your-domain-name>.sh

As an example, this script creates a certificate for following domain / sub-domains. You can add or remove sub-domains as necessary. Use your domain / sub-domain names. The first (sub)domain name used in the script is taken for naming the directories created by Certbot.

Note: You can create different certificates for different sub-domains, such as `mydom.tld`, `www.mydom.tld`, and `sub.mydom.tld`, by creating different scripts. You can see an example script here below:

```
#!/bin/bash
# export makes the variable available for all subprocesses

LE_PATH="/usr/bin"
LE_CB="certbot"

# Assumes that mydom.tld www.mydom.tld and sub.mydom.tld are the domains that you want a certificate
export DOMAINS="-d mydom.tld -d www.mydom.tld -d sub.mydom.tld"

"$LE_PATH/$LE_CB" certonly --config /etc/letsencrypt/cli.ini "$DOMAINS" # --dry-run
```

Note: You can enable the `--dry-run` option which does a test run of the client only.

4.16.6 Create an SSL certificate

With all the scripts created, to create an SSL certificate, run the following command:

```
sudo /etc/letsencrypt/<your-domain-name>.sh
```

After you run the script, you will see output similar to the following:

```
Saving debug log to /var/log/letsencrypt/letsencrypt.log
Obtaining a new certificate
Performing the following challenges:
http-01 challenge for your-domain-name.com
Using the webroot path /var/www/html for all unmatched domains.
Waiting for verification...
Cleaning up challenges
Running post-hook command: service apache2 reload
```

IMPORTANT NOTES:

1. Congratulations! Your certificate and chain have been saved at:
/etc/letsencrypt/live/your-domain-name.com/fullchain.pem
Your key file has been saved at:
/etc/letsencrypt/live/your-domain-name.com/privkey.pem
Your cert will expire on 2018-06-18. To obtain a new or tweaked version of this certificate in the future, simply run certbot again. To non-interactively renew *all* of your certificates, run "certbot renew"
2. If you like Certbot, please consider supporting our work by:

Donating to ISRG / Let's Encrypt: <https://letsencrypt.org/donate>
Donating to EFF: <https://eff.org/donate-le>

You can see that the SSL certificate's been successfully created, and that it will expire on 2018-06-18.

4.16.7 Listing Existing Certificates

If you want to list (view) the existing SSL certificates, use `list.sh`, which can be run as follows:

```
sudo /etc/letsencrypt/list.sh
```

Depending on the number of certificates, you can expect to see output similar to the following:

```
-----  
Found the following certs:  
Certificate Name: your-domain-name.com  
Domains: your-domain-name.com  
Expiry Date: 2018-06-18 10:57:18+00:00 (VALID: 82 days)  
Certificate Path: /etc/letsencrypt/live/your-domain-name.com/fullchain.pem  
Private Key Path: /etc/letsencrypt/live/your-domain-name.com/privkey.pem  
-----
```

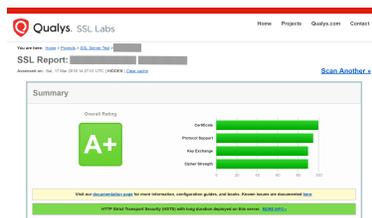
4.16.8 Web Server setup

Follow the links to set up your web server and issue a certificate.

- [apache](#)
- [nginx](#)

4.16.9 Test the setup

After you have setup and configured the web server and installed the SSL certificate using Certbot, you should now test the security of your new configuration. To do so, you can use the free service of [SSL Labs](#). See an example screenshot of a test run below.



4.16.10 Renewing Certificates

As Let's Encrypts certificates expire every 90 days, you should ensure you renew them before that time. There are two ways to do so: manually and automatically.

Manual renewal

If you have provided your email address, you will receive reminder notifications.

```
sudo /etc/letsencrypt/renew.sh
```

If the certificate is not yet due for renewal, you can expect to see output similar to that below:

```
-----  
Processing /etc/letsencrypt/renewal/your-domain-name.com.conf  
-----  
Cert not yet due for renewal
```

```
The following certs are not due for renewal yet:  
  /etc/letsencrypt/live/your-domain-name.com/fullchain.pem (skipped)  
No renewals were attempted.  
No hooks were run.
```

Automatic renewal via crontab

Certificates are only renewed if they are due, so you can schedule Cron jobs to renew your SSL certificates on a more frequent basis. However, a weekly check is sufficient.

To add a new Cron job to auto-renew your certificates, firstly run the following command to edit the job list.

```
sudo crontab -e
```

Note: It is essential to use `sudo` to derive proper permissions.

Then, add the following at the end of the existing configuration:

```
30 03 * * 6 /etc/letsencrypt/renew-cron.sh
```

After you save and exit the file, the new job will have been added to the Cron job scheduler.

Note: If you want to use own values, you can check them at crontab.guru or modify the script for other options.

4.16.11 Add extra domains to the certificate

If you want to add an extra domain, like `test.mydom.tld`, to your certificate, add the domain in the domain shell script above, re-run it and reload the web server config. This can be useful when migrating from a sub-directory to sub-domain access.

Note: This also implies that you need to comment the `include` directive (please refer to the relevant *web server setup*) and follow the steps afterward.

4.16.12 Deleting SSL Certificates

If you want to delete an SSL certificate, use the `delete.sh` script, running it as follows:

```
sudo /etc/letsencrypt/delete.sh
```

It will start off, as below, by displaying a list of the currently available SSL certificate domain names, and then prompt you to supply the certificate that you want to delete.

```
Available Certificates:
```

```
1. your-domain-name.com
```

```
Which certificate do you want to delete:
```

Provide the SSL certificate name that you want to delete and click enter, and the certificate and all of its related files will be deleted. After that you should expect to see a confirmation, as in the example output below.

```
-----  
Deleted all files relating to certificate your-domain-name.com.  
-----
```

UPGRADING

5.1 Upgrade PHP on RedHat 7 and Centos 7

You should, almost, always upgrade to the latest version of PHP, if and where possible. And if you're on a version of PHP older than 5.6 you need to upgrade. This guide steps you through upgrading your installation of PHP to version 5.6 or 7.0 if you're on RedHat or Centos 7.

- *Upgrade PHP to version 5.6*
- *Upgrade PHP to version 7.0*

5.1.1 Upgrade PHP to version 5.6

Note: You should really be upgrading to PHP 7, as version 5.6 is **no longer actively supported**, and security support ends on 31 Dec, 2018.

You will first need to subscribe to the Red Hat Software Collections channel repository to be able to download and install the PHP 5.6 package in RHEL 7. To do that, run the following command:

```
subscription-manager repos --enable rhel-server-rhsc1-7-rpms
```

Note: To know more about registering and subscribing a system to the Red Hat Customer Portal using the Red Hat Subscription-Manager, please refer to [the official documentation](#).

When that's completed, then proceed by installing PHP 5.6, along with *the other required PHP packages*.

```
yum install rh-php56 rh-php56-php rh-php56-php-gd rh-php56-php-mbstring rh-php56-php-mysqlnd rh-php56
```

Once they're all installed, you next need to enable PHP 5.6 system-wide. To do this, run the following command:

```
cp /opt/rh/rh-php56/enable /etc/profile.d/rh-php56.sh source /opt/rh/rh-php56/enable
```

With PHP 5.6 enabled system-wide, you next need to disable the loading the previous version of PHP 5.4. For this example, we'll assume that you're upgrading from PHP 5.4. Here, you disable it from loading by renaming it's Apache configuration files.

```
mv /etc/httpd/conf.d/php.conf /etc/httpd/conf.d/php54.off  
mv /etc/httpd/conf.modules.d/10-php.conf /etc/httpd/conf.modules.d/10-php54.off
```

Note: You could also delete the files if you prefer.

Next, you need to enable loading of the PHP 5.6 Apache shared-object file. This you do by copying the shared object along with its two Apache configuration files, as in the command below.

```
cp /opt/rh/httpd24/root/etc/httpd/conf.d/rh-php56-php.conf /etc/httpd/conf.d/  
cp /opt/rh/httpd24/root/etc/httpd/conf.modules.d/10-rh-php56-php.conf /etc/httpd/conf.modules.d/  
cp /opt/rh/httpd24/root/etc/httpd/modules/librh-php56-php5.so /etc/httpd/modules/
```

With all that done, you lastly need to restart Apache.

```
service httpd restart
```

5.1.2 Upgrade PHP to version 7.0

As with *upgrading to PHP 5.6*, to upgrade to PHP 7 you will first need to subscribe to the Red Hat Software Collections channel repository to download and install the PHP 7 package in RHEL 7 (if you've not done this already). This uses the same command as you will find there.

Note: This section assumes that you're upgrading from PHP 5.6.

Then, proceed by installing the required PHP 7 modules. You can use the command below to save you time.

```
yum install rh-php70 rh-php70-php rh-php70-php-gd rh-php70-php-mbstring rh-php70-php-mysqlnd rh-php70-
```

Next, you need to enable PHP 7 and disable PHP 5.6 system-wide. To enable PHP 7 system-wide, run the following command:

```
cp /opt/rh/rh-php70/enable /etc/profile.d/rh-php70.sh source /opt/rh/rh-php70/enable
```

Then, you need to disable loading of the PHP 5.6 Apache modules. You can do this either by changing their names, as in the example below, or deleting the files.

```
mv /etc/httpd/conf.d/php.conf /etc/httpd/conf.d/php56.off  
mv /etc/httpd/conf.modules.d/10-php.conf /etc/httpd/conf.modules.d/10-php56.off
```

With that done, you next need to copy the PHP 7 Apache modules into place; that being the two Apache configuration files and the shared object file.

```
cp /opt/rh/httpd24/root/etc/httpd/conf.d/rh-php70-php.conf /etc/httpd/conf.d/  
cp /opt/rh/httpd24/root/etc/httpd/conf.modules.d/15-rh-php70-php.conf /etc/httpd/conf.modules.d/  
cp /opt/rh/httpd24/root/etc/httpd/modules/librh-php70-php7.so /etc/httpd/modules/
```

Finally, you need to restart Apache to make the changes permanent, as in the command below.

```
service httpd restart
```

5.2 Upgrade Marketplace Applications

To upgrade Marketplace applications, please refer to the documentation below, as applicable for your ownCloud setup.

5.2.1 Single-Server Environment

To upgrade Marketplace applications when running ownCloud in a single server environment, you can use the *Market app*, specifically by running `market:upgrade`. This will install new versions of your installed apps if updates are available in the marketplace.

Note: The user running the update command, which will likely be your webserver user, needs write permission for the /apps folder. If they don't have write permission, the command may report that the update was successful, however it may silently fail.

5.2.2 Clustered/Multi-Server Environment

The *Market app*, both the UI and command line, are not, *currently*, designed to operate on clustered installations. Given that, you will have to update the applications on each server in the cluster individually. There are several ways to do this. But here is a concise approach:

1. Download the latest server release (whether [the tarball](#) or [the zip archive](#)).
2. Download your installed apps from *the ownCloud marketplace*.
3. Combine them together into one installation source, such as *a Docker or VM image*, or *an Ansible script*, etc.
4. Apply the combined upgrade across all the cluster nodes in your ownCloud setup.

CONFIGURATION

6.1 Database Configuration

6.1.1 Converting Database Type

SQLite is good for testing ownCloud, as well as small, single-user, ownCloud servers. But, **it does not scale** for large, multi-user sites. If you have an existing ownCloud installation which uses SQLite, and you want to convert to a better performing database, such as *MySQL*, *MariaDB* or *PostgreSQL*, you can use *the ownCloud command line tool: occ*.

Note: ownCloud Enterprise edition does not support SQLite.

Preparation

Add the following to your ownCloud `config/config.php`.

```
'mysql.utf8mb4' => true,
```

Add, or adjust, the following in `/etc/mysql/mariadb.conf.d/50-server.cnf`.

Note: You can do the same for MySQL by replacing `mariadb.conf.d/50-server.cnf` with `mysql.conf.d/mysqld.cnf`

```
key_buffer_size          = 32M
table_cache              = 400
query_cache_size        = 128M
```

```
#innoDB:
innodb_flush_method=O_DIRECT
innodb_flush_log_at_trx_commit=1
innodb_log_file_size=256M
innodb_log_buffer_size = 128M
innodb_buffer_pool_size=2048M
innodb_buffer_pool_instances=3
innodb_read_io_threads=4
innodb_write_io_threads=4
innodb_io_capacity = 500
innodb_thread_concurrency=2
innodb_file_format=Barracuda
innodb_file_per_table=ON
innodb_large_prefix = 1
```

```
character-set-server = utf8mb4
collation-server    = utf8mb4_general_ci
```

Restart the Database Server

When you have changed the database parameters, restart your database by running following command:

```
sudo service mysql restart
```

Run the Conversion

After you have restarted the database, run the following occ command in your ownCloud root folder, to convert the database to the new format:

```
sudo -uwww-data ./occ db:convert-type [options] type username hostname database
```

Note: The converter searches for apps in your configured app folders and uses the schema definitions in the apps to create the new table. As a result, tables of removed apps will not be converted — even with option `--all-apps`

For example

```
sudo -uwww-data ./occ db:convert-type --all-apps mysql oc_mysql_user 127.0.0.1 new_db_name
```

To successfully proceed with the conversion, you must type `yes` when prompted with the question `Continue with the conversion?` On success the converter will automatically configure the new database in your ownCloud config `config.php`.

Unconvertible Tables

If you updated your ownCloud installation then the old tables, which are not used anymore, might still exist. The converter will tell you which ones.

The following tables will not be converted:

```
oc_permissions
```

You can ignore these tables. Here is a list of known old tables:

- `oc_calendar_calendars`
- `oc_calendar_objects`
- `oc_calendar_share_calendar`
- `oc_calendar_share_event`
- `oc_fscache`
- `oc_log`
- `oc_media_albums`
- `oc_media_artists`
- `oc_media_sessions`
- `oc_media_songs`
- `oc_media_users`

- oc_permissions
- oc_queuedtasks
- oc_sharing

6.1.2 Database Configuration

ownCloud requires a database in which administrative data is stored. The following databases are currently supported:

- *MySQL / MariaDB*
- *PostgreSQL*
- *Oracle* (ownCloud Enterprise edition only)

The MySQL or MariaDB databases are the recommended database engines.

Requirements

Choosing to use MySQL / MariaDB, PostgreSQL, or Oracle (ownCloud Enterprise edition only) as your database requires that you install and set up the server software first. (Oracle users, see *Oracle Database Setup*.)

Note: The steps for configuring a third party database are beyond the scope of this document. Please refer to the documentation for your specific database choice for instructions.

MySQL / MariaDB with Binary Logging Enabled

ownCloud is currently using a `TRANSACTION_READ_COMMITTED` transaction isolation to avoid data loss under high load scenarios (e.g., by using the sync client with many clients/users and many parallel operations). This requires a disabled or correctly configured binary logging when using MySQL or MariaDB. Your system is affected if you see the following in your log file during the installation or update of ownCloud:

```
An unhandled exception has been thrown: exception 'PDOException' with message 'SQL-STATE[HY000]: General error: 1665 Cannot execute statement: impossible to write to binary log since BINLOG_FORMAT = STATEMENT and at least one table uses a storage engine limited to row-based logging. InnoDB is limited to row-logging when transaction isolation level is READ COMMITTED or READ UNCOMMITTED.'
```

There are two solutions. One is to disable binary logging. Binary logging records all changes to your database, and how long each change took. The purpose of binary logging is to enable replication and to support backup operations.

The other is to change the `BINLOG_FORMAT = STATEMENT` in your database configuration file, or possibly in your database startup script, to `BINLOG_FORMAT = MIXED` or `BINLOG_FORMAT = ROW`. See [Overview of the Binary Log](#) and [The Binary Log](#) for detailed information.

MySQL / MariaDB “READ COMMITTED” transaction isolation level

As discussed above ownCloud is using the `TRANSACTION_READ_COMMITTED` transaction isolation level. Some database configurations are enforcing other transaction isolation levels. To avoid data loss under high load scenarios (e.g., by using the sync client with many clients/users and many parallel operations) you need to configure the transaction isolation level accordingly. Please refer to the [MySQL manual](#) for detailed information.

MySQL / MariaDB storage engine

Since ownCloud 7 only InnoDB is supported as a storage engine. There are some shared hosts who do not support InnoDB and only MyISAM. Running ownCloud on such an environment is not supported.

Parameters

For setting up ownCloud to use any database, use the instructions in *The Installation Wizard*. You should not have to edit the respective values in the `config/config.php`. However, in special cases (for example, if you want to connect your ownCloud instance to a database created by a previous installation of ownCloud), some modification might be required.

Configuring a MySQL or MariaDB Database

If you decide to use a MySQL or MariaDB database, ensure the following:

- That you have installed and enabled the `pdo_mysql` extension in PHP
- That the `mysql.default_socket` points to the correct socket (if the database runs on the same server as ownCloud).

Note: MariaDB is backwards compatible with MySQL. All instructions work for both, so you will not need to replace or revise any, existing, MySQL client commands.

The PHP configuration in `/etc/php5/conf.d/mysql.ini` could look like this:

```
# configuration for PHP MySQL module
extension=pdo_mysql.so

[mysql]
mysql.allow_local_infile=On
mysql.allow_persistent=On
mysql.cache_size=2000
mysql.max_persistent=-1
mysql.max_links=-1
mysql.default_port=
mysql.default_socket=/var/lib/mysql/mysql.sock # Debian squeeze: /var/run/mysqld/mysqld.sock
mysql.default_host=
mysql.default_user=
mysql.default_password=
mysql.connect_timeout=60
mysql.trace_mode=Off
```

Now you need to create a database user and the database itself by using the MySQL command line interface. The database tables will be created by ownCloud when you login for the first time.

To start the MySQL command line mode use:

```
mysql -uroot -p
```

Then a `mysql>` or `MariaDB [root]>` prompt will appear. Now enter the following lines and confirm them with the `enter` key:

```
CREATE DATABASE IF NOT EXISTS owncloud;
GRANT ALL PRIVILEGES ON owncloud.* TO 'username'@'localhost' IDENTIFIED BY 'password';
```

You can quit the prompt by entering:

```
quit
```

An ownCloud instance configured with MySQL would contain the hostname on which the database is running, a valid username and password to access it, and the name of the database. The `config/config.php` as created by the *The Installation Wizard* would therefore contain entries like this:

```
<?php

"dbtype"          => "mysql",
"dbname"          => "owncloud",
"dbuser"          => "username",
"dbpassword"      => "password",
"dbhost"          => "localhost",
"dbtableprefix"  => "oc_",
```

Configure MySQL for 4-byte Unicode Support For supporting such features as emoji, you have to enable 4-byte Unicode support in MySQL (instead of the default 3) *and* in ownCloud. If you have a new installation, you don't need to do anything, as mb4 support is checked during setup, and used if available. If it's available, ownCloud is configured to use it.

However, if you have an existing installation that you need to convert to use 4-byte Unicode support, then you need to do two things:

1. In your MySQL configuration, add the configuration settings below. If you already have them configured, update them to reflect the values specified:

```
[mysqld]
innodb_large_prefix=ON
innodb_file_format=Barracuda
innodb_file_per_table=ON
```

Then, run the following command:

```
./occ db:convert-mysql-charset
```

When this is done, tables will be created with a:

- `utf8mb4` character set.
- `utf8mb4_bin` collation.
- `row_format` of compressed.

For more information, please either refer to lines 1126 to 1156 in `config/config.sample.php`, or have a read through the following links:

- https://dev.mysql.com/doc/refman/5.7/en/innodb-parameters.html#sysvar_innodb_large_prefix
- https://mariadb.com/kb/en/mariadb/xtradbinnodb-server-system-variables/#innodb_large_prefix
- <http://www.tocker.ca/2013/10/31/benchmarking-innodb-page-compression-performance.html>
- <http://mechanics.flite.com/blog/2014/07/29/using-innodb-large-prefix-to-avoid-error-1071/>
- <http://dev.mysql.com/doc/refman/5.7/en/charset-unicode-utf8mb4.html>

Note: This is not required for new installations, only existing ones, as mb4 support is checked during setup, and used if available.

PostgreSQL Database

If you decide to use a PostgreSQL database make sure that you have installed and enabled the PostgreSQL extension in PHP. The PHP configuration in `/etc/php5/conf.d/pgsql.ini` could look like this:

```
# configuration for PHP PostgreSQL module
extension=pdo_pgsql.so
extension=pgsql.so

[PostgreSQL]
pgsql.allow_persistent = On
pgsql.auto_reset_persistent = Off
pgsql.max_persistent = -1
pgsql.max_links = -1
pgsql.ignore_notice = 0
pgsql.log_notice = 0
```

The default configuration for PostgreSQL (at least in Ubuntu 14.04) is to use the peer authentication method. Check `/etc/postgresql/9.3/main/pg_hba.conf` to find out which authentication method is used in your setup. To start the postgres command line mode use:

```
sudo -u postgres psql -d template1
```

Then a **template1=#** prompt will appear. Now enter the following lines and confirm them with the enter key:

```
CREATE USER username CREATEDB;
CREATE DATABASE owncloud OWNER username;
```

You can quit the prompt by entering:

```
\q
```

An ownCloud instance configured with PostgreSQL would contain the path to the socket on which the database is running as the hostname, the system username the php process is using, and an empty password to access it, and the name of the database. The `config/config.php` as created by the *The Installation Wizard* would therefore contain entries like this:

```
<?php
    "dbtype"         => "pgsql",
    "dbname"        => "owncloud",
    "dbuser"        => "username",
    "dbpassword"    => "",
    "dbhost"        => "/var/run/postgresql",
    "dbtableprefix" => "oc_,"
```

Note: The host actually points to the socket that is used to connect to the database. Using localhost here will not work if PostgreSQL is configured to use peer authentication. Also note, that no password is specified, because this authentication method doesn't use a password.

If you use another authentication method (not peer), you'll need to use the following steps to get the database setup: Now you need to create a database user and the database itself by using the PostgreSQL command line interface. The database tables will be created by ownCloud when you login for the first time.

To start the PostgreSQL command line mode use:

```
psql -hlocalhost -Upostgres
```

Then a **postgres=#** prompt will appear. Now enter the following lines and confirm them with the enter key:

```
CREATE USER username WITH PASSWORD 'password';
CREATE DATABASE owncloud TEMPLATE template0 ENCODING 'UNICODE';
ALTER DATABASE owncloud OWNER TO username;
GRANT ALL PRIVILEGES ON DATABASE owncloud TO username;
```

You can quit the prompt by entering:

```
\q
```

An ownCloud instance configured with PostgreSQL would contain the hostname on which the database is running, a valid username and password to access it, and the name of the database. The `config/config.php` as created by the *The Installation Wizard* would therefore contain entries like this:

```
<?php
```

```
"dbtype"          => "pgsql",
"dbname"          => "owncloud",
"dbuser"          => "username",
"dbpassword"      => "password",
"dbhost"          => "localhost",
"dbtableprefix"  => "oc_",
```

Troubleshooting

How to workaround General error: 2006 MySQL server has gone away

The database request takes too long and therefore the MySQL server times out. Its also possible that the server is dropping a packet that is too large. Please refer to the manual of your database for how to raise the configuration options `wait_timeout` and/or `max_allowed_packet`.

Some shared hosts are not allowing the access to these config options. For such systems ownCloud is providing a `dbdriveroptions` configuration option within your `config/config.php` where you can pass such options to the database driver. Please refer to *Core Config.php Parameters* for an example.

How can I find out if my MySQL/PostgreSQL server is reachable?

To check the server's network availability, use the ping command on the server's host name (db.server.com in this example):

```
ping db.server.dom
```

```
PING db.server.dom (ip-address) 56(84) bytes of data.
64 bytes from your-server.local.lan (192.168.1.10): icmp_req=1 ttl=64 time=3.64 ms
64 bytes from your-server.local.lan (192.168.1.10): icmp_req=2 ttl=64 time=0.055 ms
64 bytes from your-server.local.lan (192.168.1.10): icmp_req=3 ttl=64 time=0.062 ms
```

For a more detailed check whether the access to the database server software itself works correctly, see the next question.

How can I find out if a created user can access a database?

The easiest way to test if a database can be accessed is by starting the command line interface:

MySQL:

Assuming the database server is installed on the same system you're running the command from, use:

```
mysql -uUSERNAME -p
```

To access a MySQL installation on a different machine, add the `-h` option with the respective host name:

```
mysql -uUSERNAME -p -h HOSTNAME
```

```
mysql> SHOW VARIABLES LIKE "version";
```

```
+-----+-----+
| Variable_name | Value |
+-----+-----+
| version      | 5.1.67 |
+-----+-----+
```

```
1 row in set (0.00 sec)
```

```
mysql> quit
```

PostgreSQL:

Assuming the database server is installed on the same system you're running the command from, use:

```
psql -Username -downcloud
```

To access a MySQL installation on a different machine, add the `-h` option with the respective host name:

```
psql -Username -downcloud -h HOSTNAME
```

```
postgres=# SELECT version();
```

```
PostgreSQL 8.4.12 on i686-pc-linux-gnu, compiled by GCC gcc (GCC) 4.1.3 20080704 (prerelease), 32-bit
(1 row)
```

```
postgres=# \q
```

Useful SQL commands

Show Database Users:

```
MySQL      : SELECT User,Host FROM mysql.user;
```

```
PostgreSQL: SELECT * FROM pg_user;
```

Show available Databases:

```
MySQL      : SHOW DATABASES;
```

```
PostgreSQL: \l
```

Show ownCloud Tables in Database:

```
MySQL      : USE owncloud; SHOW TABLES;
```

```
PostgreSQL: \c owncloud; \d
```

Quit Database:

```
MySQL      : quit
```

```
PostgreSQL: \q
```

6.2 File Sharing and Management

6.2.1 File Sharing

The sharing policy is configured on the Admin page in the “*Sharing*” section.

Sharing *i*

- Allow apps to use the Share API
- Allow users to share via link
 - Allow public uploads
 - Enforce password protection
 - Set default expiration date
 - Allow users to send mail notification for shared files
 - Allow users to share file via social media
- Allow resharing
- Allow sharing with groups
 - Restrict users to only share with users in their groups
 - Allow users to send mail notification for shared files to other users
 - Exclude groups from sharing
- Allow username autocompletion in share dialog. If this is disabled the full username needs to be entered.
 - Restrict enumeration to group members

From this section, ownCloud users can:

- Share files with their ownCloud groups and other users on the same ownCloud server
- Share files with ownCloud users on *other ownCloud servers*
- Create public shares for people who are not ownCloud users.

You have control of a number of user permissions on file shares:

- Allow users to share files
- Allow users to create public shares
- Require a password on public shares
- Allow public uploads to public shares
- Require an expiration date on public share links
- Allow resharing
- Restrict sharing to group members only
- Allow email notifications of new public shares

- Exclude groups from creating shares

Note: ownCloud Enterprise includes a Share Link Password Policy app; see [the Password Policy documentation](#).

Settings Explained

Allow apps to use the Share API

Check this option to enable users to share files. If this is not checked, no users can create file shares.

Allow users to share via link

Check this option to enable creating public shares for people who are not ownCloud users via hyperlink.

Enforce password protection

Check this option to force users to set a password on all public share links. This does not apply to local user and group shares.

Allow public uploads

Check this option to allow anyone to upload files to public shares.

Allow users to send mail notification for shared files

Check this option to enable sending notifications from ownCloud. When clicked, the administrator can choose the language for public mail notifications for shared files.

Allow users to send mail notification for shared files

Language used for public mail notifications for shared files Owner language ▼

What this means is that email notifications will be sent in the language of the user that shared an item. By default the language is the share owner's language. However, it can be changed to any of the currently available languages. It is also possible to change this setting on the command-line by using [the `occ config:app:set` command](#), as in this example:

```
sudo -u www-data php occ config:app:set core shareapi_public_notification_lang --value '<language code>'
```

Note: In the above example “<language code>” is an ISO 3166-1 alpha-2 two-letter country code, such as *ru*, *gb*, *us*, and *au*.

Note: To use this functionality, your ownCloud server must be configured to send mail.

Allow users to share file via social media

Check this option to enable displaying of a set of links that allow for quickly sharing files and share links via *Twitter*, *Facebook*, *Google+*, *Diaspora*, and email.

**Set default expiration date**

Check this option to set a default expiration date on public shares.

Allow resharing

Check this option to enable users to re-share files shared with them.

Restrict users to only share with users in their groups

Check this option to confine sharing within group memberships.

Note: This setting does not apply to the Federated Cloud sharing feature. If *Federated Cloud Sharing* is enabled, users can still share items with any users on any instances (including the one they are on) via a remote share.

Allow users to send mail notification for shared files

Check this option to enable users to send an email notification to every ownCloud user that the file is shared with.

Exclude groups from sharing

Check this option to prevent members of specific groups from creating any file shares in those groups. When you check this, you'll get a dropdown list of all your groups to choose from. Members of excluded groups can still receive shares, but not create any.

Allow username autocompletion in share dialog

Check this option to enable auto-completion of ownCloud usernames.

Restrict enumeration to group members

Check this option to restrict auto-completion of ownCloud usernames to only those users who are members of the same group(s) that the user is in.

Note: ownCloud does not preserve the mtime (modification time) of directories, though it does update the mtimes on files. See [Wrong folder date when syncing](#) for discussion of this.

Blacklist Groups From Receiving Shares

Sometimes it's necessary or desirable to block groups from receiving shares. For example, if a group has a significant number of users (> 5,000) or if it's a system group, then it can be advisable to block it from receiving shares. In these cases, ownCloud administrators can blacklist one or more groups, so that they do not receive shares.

To blacklist one or more groups, via the Web UI, under “**Admin -> Settings -> Sharing**”, add one or more groups to the “*Files Sharing*” list. As you type the group's name, if it exists, it will appear in the drop down list, where you can select it.

Files Sharing

Exclude groups from receiving shares.

These groups will not receive shares. Members of the group can still send and receive shares outside of the group.

Transferring Files to Another User

You may transfer files from one user to another with `occ`. The command transfers either all or a limited set of files from one user to another. It also transfers the shares and metadata info associated with those files (*shares*, *tags*, and *comments*, etc). This is useful when you have to transfer a user's files to another user before you delete them.

Important: Trashbin contents are not transferred.

Here is an example of how to transfer all files from one user to another.

```
occ files:transfer-ownership <source-user> <destination-user>
```

Here is an example of how to transfer *a limited group* a single folder from one user to another. In it, `folder/to/move`, and any file and folder inside it will be moved to `<destination-user>`.

```
sudo -u www-data php occ files:transfer-ownership --path="folder/to/move" <source-user> <destination-user>
```

When using this command keep two things in mind:

1. The directory provided to the `--path` switch **must** exist inside `data/<source-user>/files`.
2. The directory (and its contents) won't be moved as is between the users. It'll be moved inside the destination user's `files` directory, and placed in a directory which follows the format: transferred from `<source-user>` on `<timestamp>`. Using the example above, it will be stored under: `data/<destination-user>/files/transferred from <source-user> on 20170426_124510/`

(See [Using occ core commands](#) for a complete `occ` reference.)

Creating Persistent File Shares

When a user is deleted, their files are also deleted. As you can imagine, this is a problem if they created file shares that need to be preserved, because these disappear as well. In ownCloud files are tied to their owners, so whatever happens to the file owner also happens to the files.

One solution is to create persistent shares for your users. You can retain ownership of them, or you could create a special user for the purpose of establishing permanent file shares. Simply create a shared folder in the usual way, and share it with the users or groups who need to use it. Set the appropriate permissions on it, and then no matter which users come and go, the file shares will remain. Because all files added to the share, or edited in it, automatically become owned by the owner of the share regardless of who adds or edits them.

Create Shares Programmatically

If you need to create new shares using command-line scripts, there are two available options.

- `occ files_external:create`
- `occ files_external:import`

`occ files_external:create`

This command provides for the creation of both personal (for a specific user) and general shares. The command's configuration options can be provided either as individual arguments or collectively, as a JSON object. For more information about the command, refer to the *the occ documentation*.

Personal Share

```
sudo -u www-data php occ files_external:create /my_share_name windows_network_drive \
password::logincredentials \
--config={host=127.0.0.1, share='home', root='$user', domain='owncloud.local'} \
--user someuser
```

```
sudo -u www-data php occ files_external:create /my_share_name windows_network_drive \
password::logincredentials \
--config host=127.0.0.1 \
--config share='home' \
--config root='$user' \
--config domain='somedomain.local' \
--user someuser
```

General Share

```
sudo -u www-data php occ files_external:create /my_share_name windows_network_drive \
password::logincredentials \
--config={host=127.0.0.1, share='home', root='$user', domain='owncloud.local'}
```

```
sudo -u www-data php occ files_external:create /my_share_name windows_network_drive \
password::logincredentials \
--config host=127.0.0.1 \
--config share='home' \
--config root='$user' \
--config domain='somedomain.local'
```

occ files_external:import

You can create general and personal shares passing the configuration details via JSON files, using the `occ files_external:import` command.

General Share

```
sudo -u www-data php occ files_external:import /import.json
```

Personal Share

```
sudo -u www-data php occ files_external:import /import.json --user someuser
```

In the two examples above, here is a sample JSON file, showing all of the available configuration options that the command supports.

```
{
  "mount_point": "\/my_share_name",
  "storage": "OCA\\windows_network_drive\\lib\\WND",
  "authentication_type": "password::logincredentials",
  "configuration": {
    "host": "127.0.0.1",
    "share": "home",
    "root": "$user",
    "domain": "owncloud.local"
  },
  "options": {
    "enable_sharing": false
  },
  "applicable_users": [],
  "applicable_groups": []
}
```

6.2.2 Configuring Federation Sharing

Federated Cloud Sharing is now managed by the Federation app (9.0+), and is now called Federation sharing. When you enable the Federation app you can easily and securely link file shares between ownCloud servers, in effect creating a cloud of ownClouds.

For security reasons federated sharing **strictly requires HTTPS (SSL/TLS)**.

Sharing With ownCloud 8 and Older

Direct Federation shares (*Creating a new Federation Share (9.0+ only)*) are not supported in ownCloud 8 and older, so you must create Federation shares with public links (*Creating Federation Shares via Public Link Share*).

Creating a new Federation Share (9.0+ only)

Follow these steps to create a new Federation share between two ownCloud 9.0+ servers. This requires no action by the user on the remote server; all it takes is a few steps on the originating server.

1. Enable the Federation app.
2. Go to your ownCloud Admin page and scroll to the Sharing section. Verify that **Allow users on this server to send shares to other servers** and **Allow users on this server to receive shares from other servers** are enabled.

- Now go to the Federation section. By default, **Add server automatically once a federated share was created successfully** is checked. The Federation app supports creating a list of trusted ownCloud servers, which allows the trusted servers to exchange user directories and auto-complete the names of external users when you create shares. If you do not want this enabled, then un-check it.

Federation

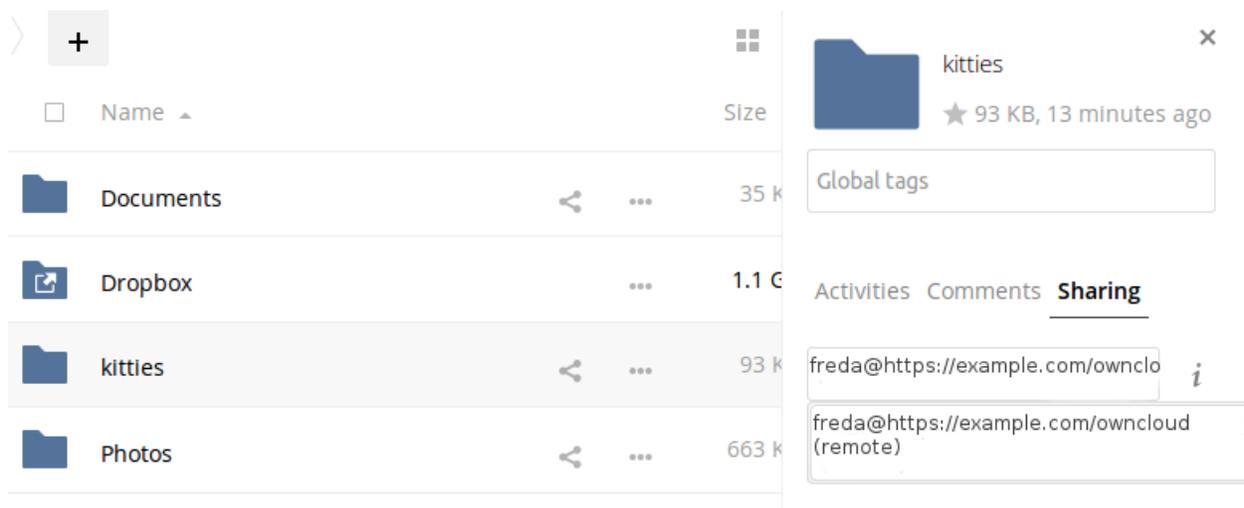
ownCloud Federation allows you to connect with other trusted ownClouds to exchange the user directory. For example this will be used to auto-complete external users for federated sharing.

- Add server automatically once a federated share was created successfully

Trusted ownCloud Servers

[+ Add ownCloud server](#)

- Then, go to your Files page and select a folder to share. Click the share icon, and then enter the username and URL of the user on the remote ownCloud server. In this example, that is `freda@https://example.com/owncloud`. When ownCloud verifies the link, it displays it with the **(remote)** label. Click on this label to establish the link.

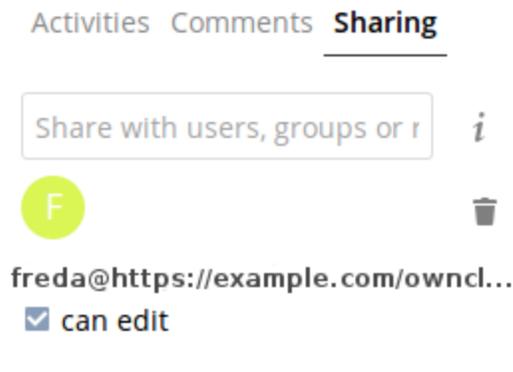


- When the link is successfully completed, you have a single share option, and that is **can edit**.

You may disconnect the share at any time by clicking the trash can icon.

Configuring Trusted ownCloud Servers

You may create a list of trusted ownCloud servers for Federation sharing. This allows your linked ownCloud servers to share user directories, and to auto-fill user names in share dialogs. If **Add server automatically once a federated share was created successfully** is enabled on your Admin page, servers will be automatically added to your trusted list when you create new Federation shares.



You may also enter ownCloud server URLs in the **Add ownCloud Server** field. The yellow light indicates a successful connection, with no user names exchanged. The green light indicates a successful connection with user names exchanged. A red light means the connection failed.

Federation

ownCloud Federation allows you to connect with other trusted ownClouds to exl

Add server automatically once a federated share was created successfully

Trusted ownCloud Servers

+ Add ownCloud server

 http://localhost/federation/

 https://server2

 https://server3

Creating Federation Shares via Public Link Share

You'll need to use a Public Link Share to create Federation shares with ownCloud 8.x and older.

Check the **Share Link** checkbox to expose more sharing options (which are described more fully in *File Sharing*). You may create a Federation share by allowing ownCloud to create a public link for you, and then email it to the person you want to create the share with.

You may optionally set a password and expiration date on it. When your recipient receives your email they must click the link, or copy it to a Web browser. They will see a page displaying a thumbnail of the file, with a button to **Add to your ownCloud**.

Your recipient should click the **Add to your ownCloud** button. On the next screen your recipient needs to enter the URL to their ownCloud server, and then press the return key.

Share link

Password protect

Set expiration date

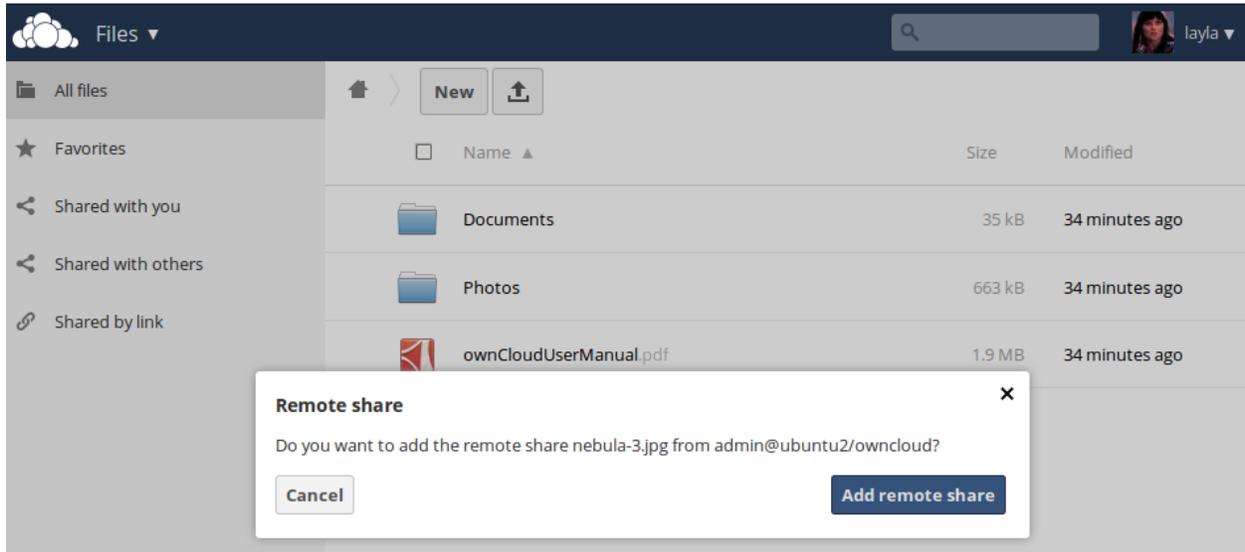




Direct link



Your recipient has to take one more step, and that is to confirm creating the federated cloud share link by clicking the **Add remote share** button.



Un-check the `Share Link` checkbox to disable any federated cloud share created this way.

Configuration Tips

The Sharing section on your Admin page allows you to control how your users manage federated cloud shares:

- Check `Enforce password protection` to require passwords on link shares.
- Check `Set default expiration date` to require an expiration date on link shares.
- Check `Allow public uploads` to allow two-way file sharing.

Your Apache Web server must have `mod_rewrite` enabled, and you must have `trusted_domains` correctly configured in `config.php` to allow external connections (see [The Installation Wizard](#)). Consider also enabling SSL to encrypt all traffic between your servers .

Your ownCloud server creates the share link from the URL that you used to log into the server, so make sure that you log into your server using a URL that is accessible to your users. For example, if you log in via its LAN IP address, such as `http://192.168.10.50`, then your share URL will be something like `http://192.168.10.50/owncloud/index.php/s/jWfCfTVztG1WTJe`, which is not accessible outside of your LAN. This also applies to using the server name; for access outside of your LAN you need to use a fully-qualified domain name such as `http://myserver.example.com`, rather than `http://myserver`.

6.2.3 Uploading big files > 512MB

The default maximum file size for uploads, in ownCloud, is 512MB. You can increase this limit up to the maximum file size which your filesystem, operating system, or other software allows, for example:

- < 2GB on a 32Bit OS-architecture
- < 2GB with IE6 - IE8
- < 4GB with IE9 - IE11

64-bit filesystems have much higher limits. Please consult the documentation for your filesystem.

Note: The ownCloud sync client itself however is able to upload files of any size, as it uploads files by transmitting them in small chunks. But, it can never exceed the maximum file size limits of the remote host.

System Configuration

- Make sure that the latest version of PHP (at least 5.6) is installed
- Disable user quotas, which makes them unlimited
- Your temp file or partition has to be big enough to hold multiple parallel uploads from multiple users; e.g. if the max upload size is 10GB and the average number of users uploading at the same time is 100: temp space has to hold at least 10x100 GB

Configuring Your Web server

Note: ownCloud comes with its own `owncloud/.htaccess` file. Because `php-fpm` can't read PHP settings in `.htaccess` these settings must be set in the `owncloud/.user.ini` file.

Set the following two parameters inside the corresponding `php.ini` file (see the **Loaded Configuration File** section of *PHP Version and Information* to find your relevant `php.ini` files)

```
php_value upload_max_filesize = 16G
php_value post_max_size = 16G
```

Adjust these values for your needs. If you see PHP timeouts in your logfiles, increase the timeout values, which are in seconds:

```
php_value max_input_time 3600
php_value max_execution_time 3600
```

The `mod_reqtimeout` Apache module could also stop large uploads from completing. If you're using this module and getting failed uploads of large files either disable it in your Apache config or raise the configured `RequestReadTimeout` timeouts.

There are also several other configuration options in your Web server config which could prevent the upload of larger files. Please see the manual of your Web server for how to configure those values correctly:

Apache

- `LimitRequestBody`
- `SSLRenegBufferSize`

Apache with `mod_fcgid`

- `FcgidMaxRequestInMem`
- `FcgidMaxRequestLen`

Note: If you are using Apache/2.4 with `mod_fcgid`, as of February/March 2016, `FcgidMaxRequestInMem` still needs to be significantly increased from its default value to avoid the occurrence of segmentation faults when uploading big files. This is not a regular setting but serves as a workaround for Apache with `mod_fcgid` bug #51747.

Setting `FcgidMaxRequestInMem` significantly higher than normal may no longer be necessary, once bug #51747 is fixed.

NGINX

- `client_max_body_size`
- `fastcgi_read_timeout`
- `client_body_temp_path`

Since NGINX 1.7.11 a new config option `fastcgi_request_buffering` is available. Setting this option to `fastcgi_request_buffering off;` in your NGINX config might help with timeouts during the upload. Furthermore it helps if you're running out of disc space on the `/tmp` partition of your system.

For more info how to configure NGINX to raise the upload limits see also [this](#) wiki entry.

Note: Make sure that `client_body_temp_path` points to a partition with adequate space for your upload file size, and on the same partition as the `upload_tmp_dir` or `tempdirectory` (see below). For optimal performance, place these on a separate hard drive that is dedicated to swap and temp storage.

If your site is behind a NGINX frontend (for example a loadbalancer):

By default, downloads will be limited to 1GB due to `proxy_buffering` and `proxy_max_temp_file_size` on the frontend.

- If you can access the frontend's configuration, disable `proxy_buffering` or increase `proxy_max_temp_file_size` from the default 1GB.
- If you do not have access to the frontend, set the `X-Accel-Buffering` header to `add_header X-Accel-Buffering no;` on your backend server.

Configuring PHP

If you don't want to use the ownCloud `.htaccess` or `.user.ini` file, you may configure PHP instead. Make sure to comment out any lines `.htaccess` pertaining to upload size, if you entered any.

If you are running ownCloud on a 32-bit system, any `open_basedir` directive in your `php.ini` file needs to be commented out.

Set the following two parameters inside `php.ini`, using your own desired file size values:

```
upload_max_filesize = 16G
post_max_size = 16G
```

Tell PHP which temp file you want it to use:

```
upload_tmp_dir = /var/big_temp_file/
```

Output Buffering must be turned off in `.htaccess` or `.user.ini` or `php.ini`, or PHP will return memory-related errors:

- `output_buffering = 0`

Configuring ownCloud

As an alternative to the `upload_tmp_dir` of PHP (e.g., if you don't have access to your `php.ini`) you can also configure a temporary location for uploaded files by using the `tempdirectory` setting in your `config.php` (See *Core Config.php Parameters*).

If you have configured the `session_lifetime` setting in your `config.php` (See *Core Config.php Parameters*) file then make sure it is not too low. This setting needs to be configured to at least the time (in seconds) that the longest upload will take. If unsure remove this completely from your configuration to reset it to the default shown in the `config.sample.php`.

Configuring upload limits within the GUI

If all prerequisites described in this documentation are in place an admin can change the upload limits on demand by using the `File handling` input box within the administrative backend of ownCloud.

File handling

Maximum upload size

With PHP-FPM this value may take up to 5 minutes to take effect after saving.

Save

Depending on your environment you might get an insufficient permissions message shown for this input box.

File handling

Maximum upload size

Can not be edited from here due to insufficient permissions.

To be able to use this input box you need to make sure that:

- Your Web server is able to use the `.htaccess` file shipped by ownCloud (Apache only)
- The user your Web server is running as has write permissions to the files `.htaccess` and `.user.ini`

Set Strong Directory Permissions might prevent write access to these files. As an admin you need to decide between the ability to use the input box and a more secure ownCloud installation where you need to manually modify the upload limits in the `.htaccess` and `.user.ini` files described above.

General upload issues

Various environmental factors could cause a restriction of the upload size. Examples are:

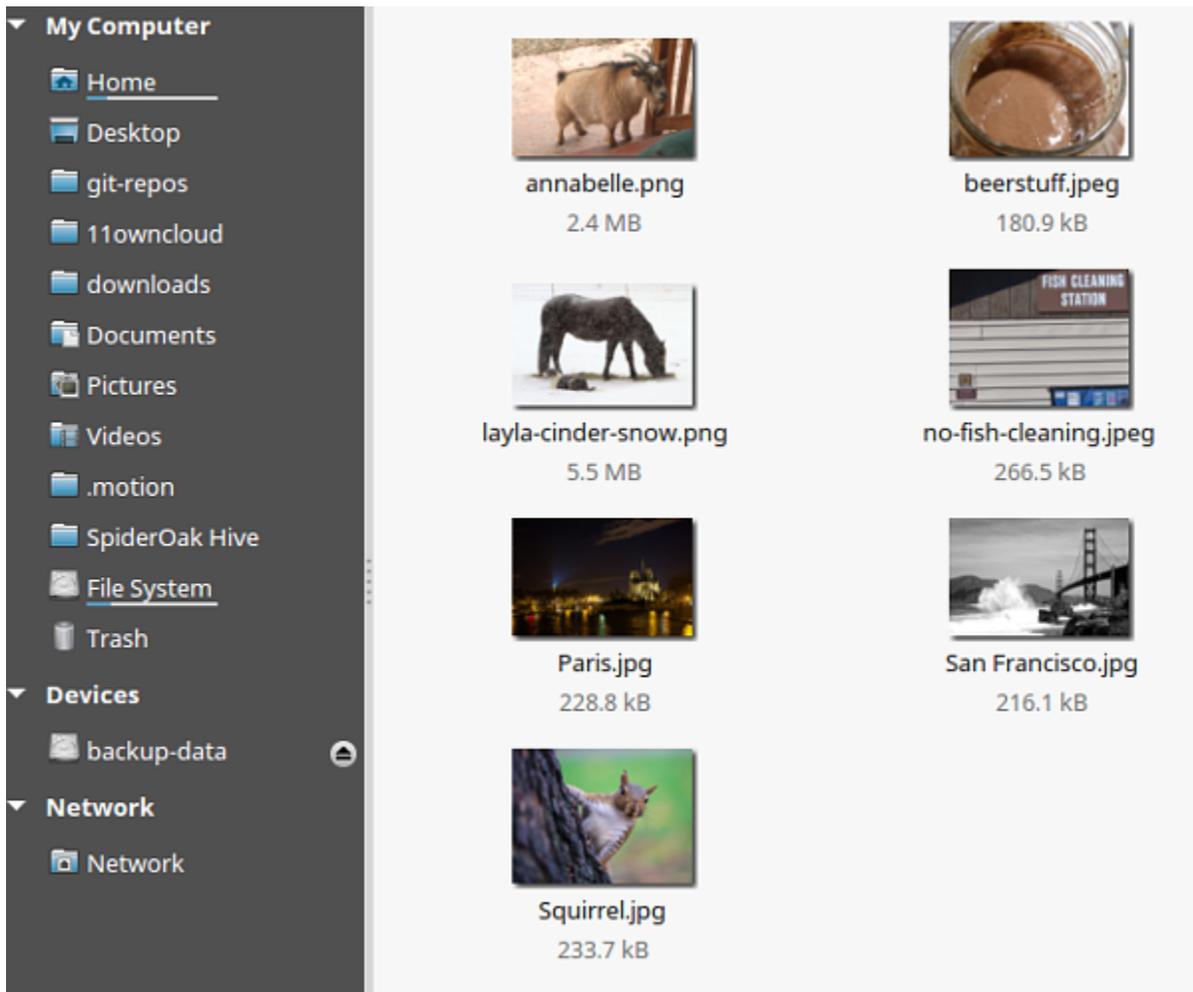
- The LVE Manager of CloudLinux which sets a `I/O limit`

- Some services like Cloudflare are also known to cause uploading issues
- Upload limits enforced by proxies used by your clients
- Other webserver modules like described in *General Troubleshooting*

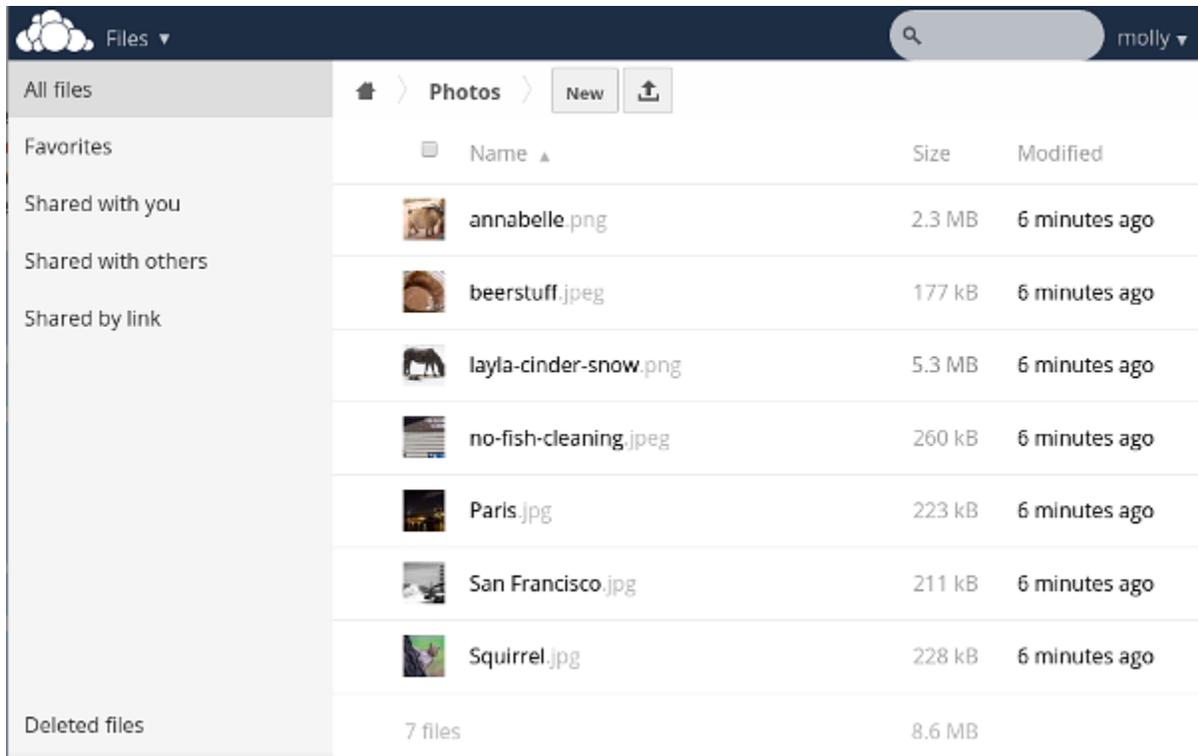
6.2.4 Providing Default Files

You may distribute a set of default files and folders to all users by placing them in the `owncloud/core/skeleton` directory on your ownCloud server. These files appear only to new users after their initial login, and existing users will not see files that are added to this directory after their first login. The files in the `skeleton` directory are copied into the users' data directories, so they may change and delete the files without affecting the originals.

This screenshot shows a set of photos in the `skeleton` directory.



They appear on the user's ownCloud Files page just like any other files.



Additional Configuration

The configuration option `skeletondirectory` available in your `config.php` (See *Core Config.php Parameters*) allows you to configure the directory where the skeleton files are located. These files will be copied to the data directory of new users. Leave empty to not copy any skeleton files.

6.2.5 Configuring External Storage (GUI)

The External Storage Support application enables you to mount external storage services and devices as secondary ownCloud storage devices. You may also allow users to mount their own external storage services.

ownCloud 9.0 introduces a new set of *occ commands for managing external storage*.

Also new in 9.0 is an option for the ownCloud admin to enable or disable sharing on individual external mountpoints (see *Mount Options*). Sharing on such mountpoints is disabled by default.

Enabling External Storage Support

Tick the check box under Settings > Storage > “Enable External Storage”.

Storage Configuration

To create a new external storage mount, select an available backend from the dropdown **Add storage**. Each backend has different required options, which are configured in the configuration fields.

Each backend may also accept multiple authentication methods. These are selected with the dropdown under **Authentication**. Different backends support different authentication mechanisms; some specific to the backend, others are more generic. See *External Storage Authentication mechanisms* for more detailed information.

The screenshot shows the 'Settings' page in ownCloud. The 'Settings' menu item is highlighted with a red box. The left sidebar is divided into 'Personal' and 'Admin' sections. Under 'Personal', 'Storage' is highlighted with a red box. The main content area is titled 'External Storage' and shows a checkbox for 'Enable external storage' which is unchecked. Below it, a message states: 'External storage has been disabled by the administrator'.

The screenshot shows the 'Settings' page in ownCloud with 'External Storage' enabled. The 'Storage' menu item in the sidebar is highlighted with a red box. The 'Enable external storage' checkbox is checked. A message states: 'External storage has been disabled by the administrator'. Below this is a table with columns for 'Folder name', 'External storage', and 'Authentication'. The 'Folder name' column has a text input field with 'Folder name' as a placeholder. The 'External storage' column has a dropdown menu labeled 'Add storage' which is open, showing a list of options: Amazon S3, Google Drive, OpenStack Object Storage, ownCloud, SFTP, SMB / CIFS, and WebDAV. There is also an unchecked checkbox for 'Allow users to mount external s'.

When you select an authentication mechanism, the configuration fields change as appropriate for the mechanism. The SFTP backend, for one example, supports **username and password**, **Log-in credentials, save in session**, and **RSA public key**.

External Storage

Folder name	External storage	Authentication	Configuration
SFTP	SFTP	Username and password Username and password Log-in credentials, save in session RSA public key	Host Root Username Password

Required fields are marked with a red border. When all required fields are filled, the storage is automatically saved. A green dot next to the storage row indicates the storage is ready for use. A red or yellow icon indicates that ownCloud could not connect to the external storage, so you need to re-check your configuration and network availability.

If there is an error on the storage, it will be marked as unavailable for ten minutes. To re-check it, click the colored icon or reload your Admin page.

User and Group Permissions

A storage configured in a user's Personal settings is available only to the user that created it. A storage configured in the Admin settings is available to all users by default, and it can be restricted to specific users and groups in the **Available for** field.

Available for

✕ guest0
✕ admin (group)

- BlueDragon
- rootA
- test1
- test2

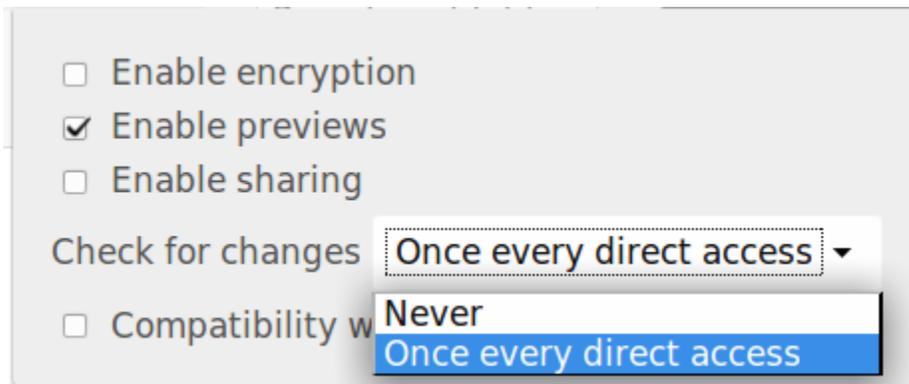
Mount Options

Hover your cursor to the right of any storage configuration to expose the settings button and trashcan. Click the trashcan to delete the mountpoint. The settings button allows you to configure each storage mount individually with the following options:

- Encryption
- Previews
- Enable Sharing
- Filesystem check frequency (Never, Once per direct access)

The **Encryption** checkbox is visible only when the Encryption app is enabled.

Enable Sharing allows the ownCloud admin to enable or disable sharing on individual mountpoints. When sharing is disabled the shares are retained internally, so that you can re-enable sharing and the previous shares become available again. Sharing is disabled by default.



Using Self-Signed Certificates

When using self-signed certificates for external storage mounts the certificate must be imported into ownCloud. Please refer to *Importing System-wide and Personal SSL Certificates* for more information.

Available storage backends

The following backends are provided by the external storages app. Other apps may provide their own backends, which are not listed here.

Amazon S3

To connect your Amazon S3 buckets to ownCloud, you will need:

- S3 access key
- S3 secret key
- Bucket name

In the **Folder name** field enter a local folder name for your S3 mountpoint. If this does not exist it will be created.

In the **Available for** field enter the users or groups who have permission to access your S3 mount.

The `Enable SSL` checkbox enables HTTPS connections; using HTTPS is always highly-recommended.

External Storage

Folder name	External storage	Configuration	Available for
 AmazonS3	Amazon S3 and compliant	<input type="text" value="AKIAIOSHDC77WFI"/> <input type="text" value="....."/> <input type="text" value="oc-files-wc"/> <input type="text" value="Hostname (optional)"/> <input type="text" value="Port (optional)"/> <input type="text" value="Region (optional)"/> <input checked="" type="checkbox"/> Enable SSL <input checked="" type="checkbox"/> <input type="checkbox"/> Enable Path Style	<input type="text" value="All Users x"/>

Optionally, you can override the hostname, port and region of your S3 server, which is required for non-Amazon servers such as Ceph Object Gateway.

Enable path style is usually not required (and is, in fact, incompatible with newer Amazon datacenters), but can be used with non-Amazon servers where the DNS infrastructure cannot be controlled. Ordinarily, requests will be made with `http://bucket.hostname.domain/`, but with path style enabled, requests are made with `http://hostname.domain/bucket` instead.

See *Configuring External Storage (GUI)* for additional mount options and information.

See *External Storage Authentication mechanisms* for more information on authentication schemes.

Dropbox

To connect Dropbox to your ownCloud installation requires four steps to be completed.

1. *Install the “External Storage: Dropbox” app from the ownCloud Marketplace*
2. *Create a Dropbox app*
3. *Create a Dropbox storage share*
4. *Use the Dropbox share*

Step One - Install the “External Storage: Dropbox” app from the ownCloud Marketplace

1. Click **Market** in the ownCloud web UI dropdown menu on the left side
2. Go to the **Storage** category
3. select **External Storage: Dropbox App**
4. Click **INSTALL**


```
``http(s)://<<Server_Address>>/index.php/settings/personal?sectionid=storage``
```

Step Three - Create a Dropbox Share To create a Dropbox share, under “admin -> Settings -> Admin -> Storage”, check the “Enable external storage” checkbox, if it’s not already checked. Then, in the dropdown list under “External storage”, click the first “Dropbox” option.

Note: There are two Dropbox options in the dropdown list, as Dropbox functionality is currently part of ownCloud’s core. However, the internal Dropbox functionality should be removed in ownCloud 10.0.4.

Then, you need to provide a name for the folder in the “Folder name” field, and a “client key” and “client secret”, located in the “Configuration” column. The client key and client secret values are the “App key” and “App secret” fields which you saw earlier in your Dropbox app’s configuration settings page.

After you have added these three settings, click “Grant access”. ownCloud then interacts with Dropbox’s API to set up the new shared folder. If the process is successful, a green circle icon appears, at the far left-hand side of the row, next to the folder’s name.

External Storage

Enable external storage

Folder name	External storage	Authentication	Configuration	Available for
<input type="text" value="Dropbox"/>	Dropbox	OAuth2	<input type="text" value="client key"/> <input type="text" value="client secret"/>	<input type="text" value="All users. Type to select user or group."/>
<input type="text" value="Folder name"/>	<input type="button" value="Add storage"/>		<input type="button" value="Grant access"/>	<input type="button" value="Settings"/> <input type="button" value="Delete"/>

Other Options If you want to restrict access to the share to a select list of users and groups, you can add them to the field in the “Available for” column.

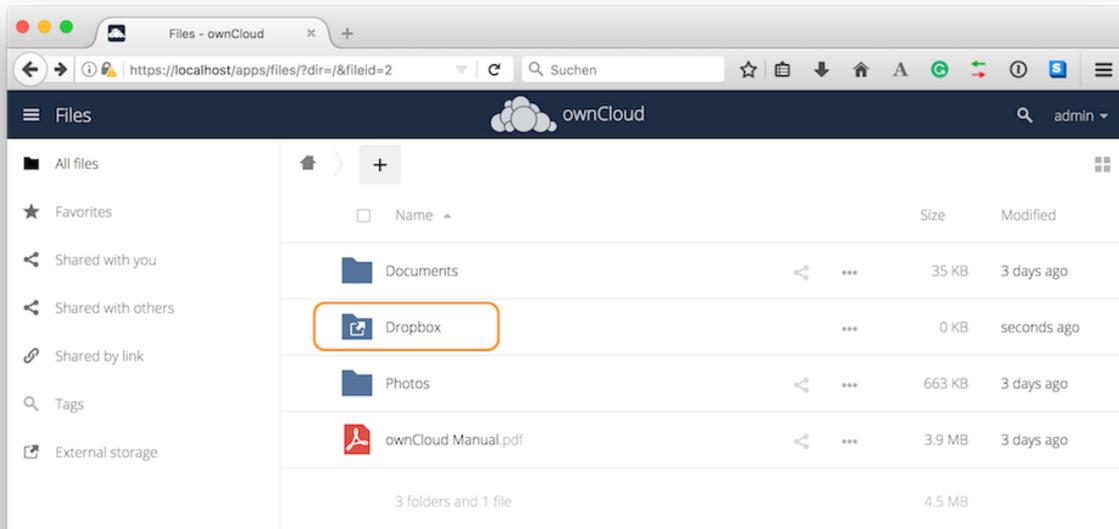
Step Four - Using the Dropbox Share After a Dropbox-backed share is created, a new folder is available under “All Files”. It has the name that you gave it when you created the share, and it is represented by an external share folder icon, as in the image below.

External Storage

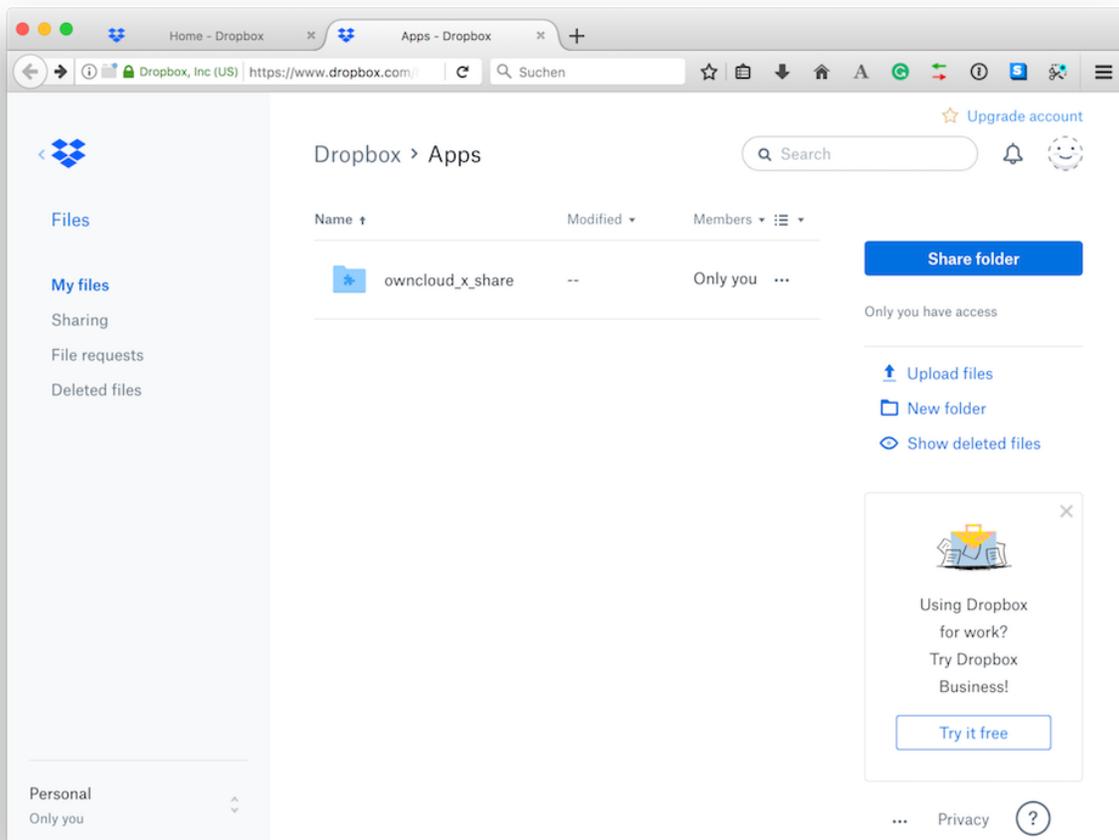
Enable external storage

Folder name	External storage	Authentication	Configuration	Available for
<input type="text" value="Dropbox"/>	Dropbox	OAuth2	<input type="text" value="client key"/> <input type="text" value="client secret"/>	<input type="text" value="All users. Type to select user or group."/>
<input type="text" value="Folder name"/>	<input type="button" value="Add storage"/>		<input type="button" value="Grant access"/>	<input type="button" value="Settings"/> <input type="button" value="Delete"/>

This links to a new folder in your Dropbox account, under “Dropbox > Apps”, with the name of the Dropbox app that you created.



Now, if you add files and folders in either the new Dropbox folder or the new ownCloud folder, after being synced, they will be visible inside the other.



FTP/FTPS

If you want to mount an FTP Storage, please install the [FTP Storage Support](#) app from the ownCloud Marketplace.

The screenshot shows the ownCloud Marketplace interface. On the left, a sidebar menu lists various categories, with 'External plugins' highlighted in a red box. The main content area displays the 'FTP storage support' app page. At the top of the app page, there is a header with the app name and a star rating. Below this is a large image of the ownCloud logo. Underneath the image, the text 'FTP backend for files_external' is displayed. A table provides details about the app:

DEVELOPER	VERSION	RELEASE DATE	LICENSE
ownCloud	0.2.0	Apr 25, 2017	GNU Affero General Public License

At the bottom right of the app page, there is a blue 'INSTALL' button.

To connect to an FTP server, you will need:

- A folder name for your local mountpoint; the folder will be created if it does not exist
- The URL of the FTP server
- Port number (default: 21)
- Username and password to access the resource
- Remote Subfolder, the FTP directory to mount in ownCloud. ownCloud defaults to the root directory. If you specify a subfolder you must leave off the leading slash. For example, `public_html/images`

Your new mountpoint is available to all users by default, and you may restrict access by entering specific users or groups in the **Available for** field.

Optionally, ownCloud can use FTPS (FTP over SSL) by checking **Secure ftps://**. This requires additional configuration with your root certificate if the FTP server uses a self-signed certificate (See *Importing System-wide and Personal SSL Certificates*).

External Storage

Folder name	External storage	Configuration	Available for
<input type="checkbox"/> FTP	FTP	<input type="text" value="ftp.example.com:22"/> <input type="text" value="username"/> <input type="password" value="●●●●●●●●"/> <input type="text" value="public.html"/> <input checked="" type="checkbox"/> Secure ftps://	<input type="button" value="x support(group)"/>

Note: The external storage FTP/FTPS needs the `allow_url_fopen` PHP setting to be set to 1. When having connection problems make sure that it is not set to 0 in your `php.ini`. See *PHP Version and Information* to learn how to find the right `php.ini` file to edit.

See *Configuring External Storage (GUI)* for additional mount options and information.

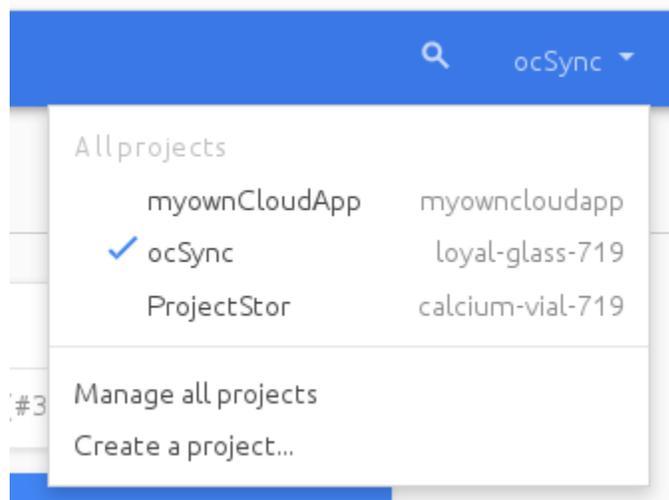
FTP uses the password authentication scheme; see *External Storage Authentication mechanisms* for more information on authentication schemes. .. Links

Google Drive

ownCloud uses OAuth 2.0 to connect to Google Drive. This requires configuration through Google to get an app ID and app secret, as ownCloud registers itself as an app.

All applications that access a Google API must be registered through the [Google Cloud Console](#). Follow along carefully because the Google interface is a bit of a maze and it's easy to get lost.

If you already have a Google account, such as Groups, Drive, or Mail, you can use your existing login to log into the Google Cloud Console. After logging in click the **Create Project** button.



Give your project a name, and either accept the default **Project ID** or create your own, then click the **Create** button.

You'll be returned to your dashboard.

New Project

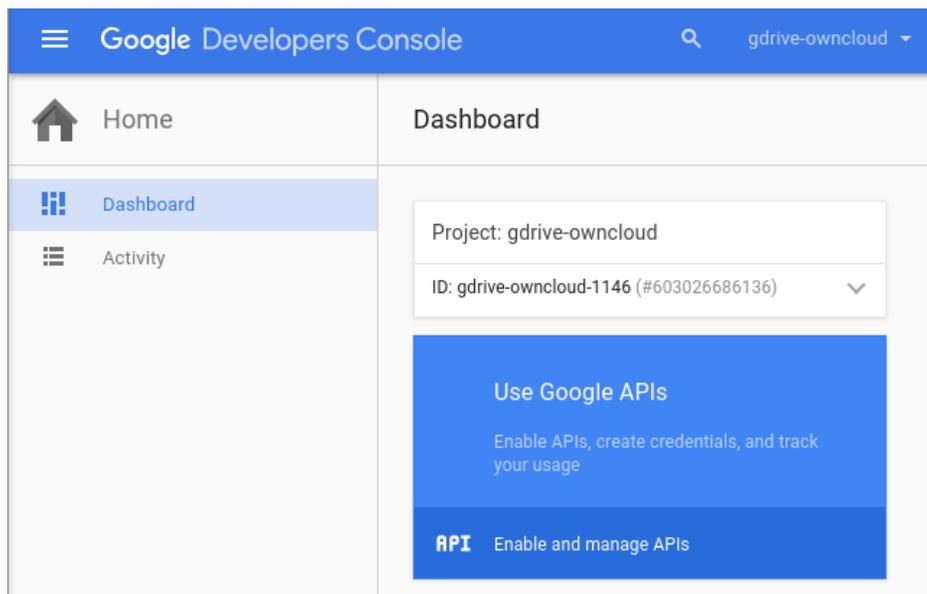
Project name [?](#)

gdrive-owncloud

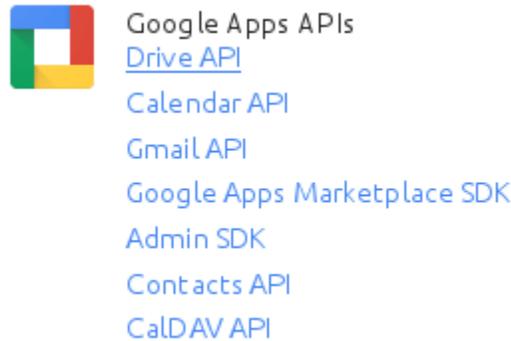
Your project ID will be gdrive-owncloud-1146 [?](#) [Edit](#)

[Show advanced options...](#)

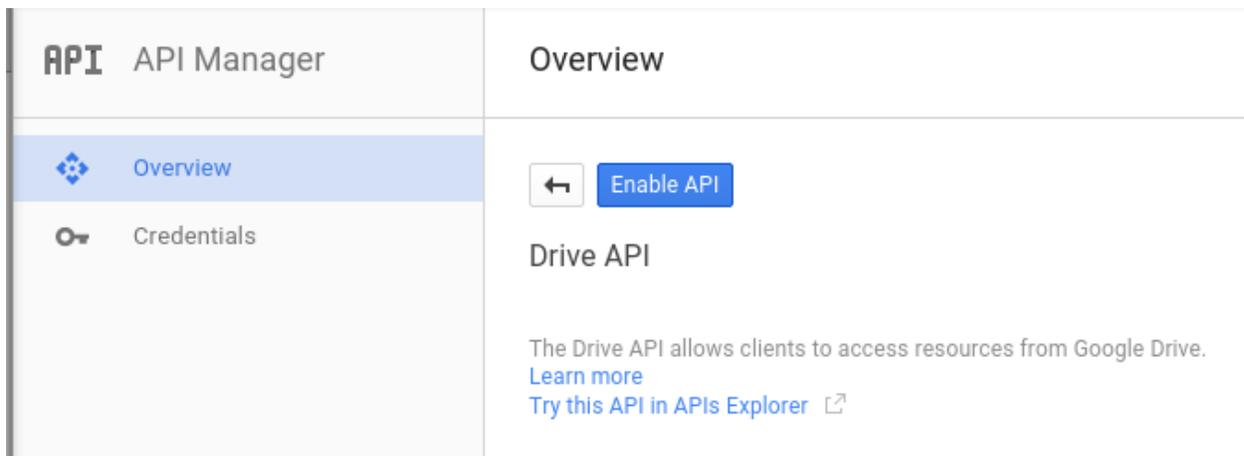
[Create](#) [Cancel](#)



Google helpfully highlights your next step in blue, the **Use Google APIs** box. Make sure that your new project is selected, click on **Use Google APIs**, and it takes you to Google's APIs screen. There are many Google APIs; look for the **Google Apps APIs** and click **Drive API**.



Drive API takes you to the API Manager overview. Click the blue **Enable API** button.



Now you must create your credentials, so click on **Go to credentials**.

For some reason Google warns us again that we need to create credentials. We will use OAuth 2.0.

Now we have to create a consent screen. This is the information in the screen Google shows you when you connect your new Google app to ownCloud the first time. Click **Configure consent screen**. Then fill in the required form fields. Your logo must be hosted, as you cannot upload it, so enter its URL. When you're finished click **Save**.

The next screen that opens is **Create Client ID**. Check **Web Application**, then enter your app name. **Authorized JavaScript Origins** is your root domain, for example `https://example.com`, without a trailing slash. You need two **Authorized Redirect URIs**, and they must be in this form:

```
https://example.com/owncloud/index.php/settings/personal?sectionid=storage
https://example.com/owncloud/index.php/settings/admin?sectionid=storage
```

Replace `https://example.com/owncloud/` with your own ownCloud server URL, then click **Create**.

Now Google reveals to you your **Client ID** and **Client Secret**. Click **OK**.

You can see these anytime in your Google console; just click on your app name to see complete information.

Overview

[←](#) [Disable API](#)

Drive API

 This API is enabled, but you can't use it in your project until you create credentials. Click "Go to Credentials" to do this now (strongly recommended).

[Go to Credentials](#)

Credentials

[Credentials](#) [OAuth consent screen](#) [Domain verification](#)

APIs Credentials

You need credentials to access APIs. [Enable the APIs you plan to use](#) and then create the credentials they require. Depending on the API, you need an API key, a service account, or an OAuth 2.0 client ID. [Refer to the API documentation](#) for details.

[Add credentials](#) ▾

API key

Identifies your project using a simple API key to check quota and access. For APIs like Google Translate.

OAuth 2.0 client ID

Requests user consent so your app can access the user's data. For APIs like Google Calendar.

Service account

Enables server-to-server, app-level authentication using robot accounts. For use with Google Cloud APIs.

Credentials

Credentials [OAuth consent screen](#) Domain verification

Email address [?](#)

dev@gmail.com

Product name shown to users

MyGoogleDriveApp

Homepage URL (Optional)

https://example.com

Product logo URL (Optional) [?](#)

https://owncloud.org/imggs



This is how your logo will look to end users
Max size: 120x120 px

Privacy policy URL (Optional)

https://example.com/privacy

Terms of service URL (Optional)

https://example.com/tos

Save

Cancel

Credentials



Create client ID

Application type

- Web application
- Android [Learn more](#)
- Chrome App [Learn more](#)
- iOS [Learn more](#)
- PlayStation 4
- Other

Name

Authorized JavaScript origins

Enter JavaScript origins here or redirect URIs below (or both) [?](#)

Cannot contain a wildcard (http://*.example.com) or a path (<http://example.com/subdir>).



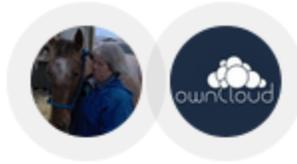
Authorized redirect URIs

Must have a protocol. Cannot contain URL fragments or relative paths. Cannot be a public IP address.



Now you have everything you need to mount your Google Drive in ownCloud.

Go to the External Storage section of your Admin page, create your new folder name, enter the Client ID and Client Secret. If you wish limit access to a single folder, simply enter the path to the desired folder, separated by '/'. Finally, click **Grant Access**. Your consent page appears when ownCloud makes a successful connection. Click **Allow**.



MyGoogleDriveApp would like to:

 View and manage the files in your Google Drive 

By clicking Allow, you allow this app and Google to use your information in accordance with their respective [terms of service](#) and [privacy policies](#). You can change this and other [Account Permissions](#) at any time.

Deny

Allow

When you see the green light confirming a successful connection you're finished.



See *Configuring External Storage (GUI)* for additional mount options and information.

See *External Storage Authentication mechanisms* for more information on authentication schemes. 603026686136-qnv9oocacrkrl1vs0cht83eprgm2sbb.apps.googleusercontent.com

Local

Local storage provides the ability to mount any directory on your ownCloud server that is:

- Outside of your ownCloud `data/` directory
- Both readable and writable by your HTTP server user

Since this is a significant security risk, Local storage is only configurable via the ownCloud admin settings. Non-admin users cannot create Local storage mounts.

Note: See *Set Strong Directory Permissions* for information on correct file permissions, and find your HTTP user

PHP Version and Information.

To manage Local storage, navigate to `admin`, and then to `Storage`. You can see an example in the screenshot below.

External Storage

Folder name	External storage	Configuration	Available for
 Local	Local	/shared/projects	All Users x

In the **Folder name** field enter the folder name that you want to appear on your ownCloud Files page. In the **Configuration** field enter the full file path of the directory you want to mount. In the **Available for** field enter the users or groups who have permission to access the mount; by default all users have access.

In addition to these steps, you have to ensure that Local storage is enabled in your ownCloud installation's `config/config.php` file. It should have the following configuration:

```
'files_external_allow_create_new_local' => 'true',
```

Note: See *Configuring External Storage (GUI)* for additional mount options and information, and *External Storage Authentication mechanisms* for more information on authentication schemes.

OpenStack Object Storage

OpenStack Object Storage is used to connect to an OpenStack Swift server, or to Rackspace. Two authentication mechanisms are available: one is the generic OpenStack mechanism, and the other is used exclusively for Rackspace, a provider of object storage that uses the OpenStack Swift protocol.

The OpenStack authentication mechanism uses the OpenStack Keystone v2 protocol. Your ownCloud configuration needs:

- **Bucket.** This is user-defined; think of it as a subdirectory of your total storage. The bucket will be created if it does not exist.
- **Username** of your account.
- **Password** of your account.
- **Tenant name** of your account. (A tenant is similar to a user group.)
- **Identity Endpoint URL**, the URL to log in to your OpenStack account.

The Rackspace authentication mechanism requires:

- **Bucket**
- **Username**
- **API key.**

You must also enter the term **cloudFiles** in the **Service name** field.

It may be necessary to specify a **Region**. Your region should be named in your account information, and you can read about Rackspace regions at [About Regions](#).

Folder name	External storage	Authentication	Configuration	A
OpenStackObjectSt	OpenStack Object Storage	OpenStack ▼	<input type="text" value="Service name"/> <input type="text" value="Region"/> <input type="text" value="myfiles"/> <input type="text" value="Request timeout (seconds)"/> <input type="text" value="molly"/> <input type="text" value="....."/> <input type="text" value="foobar"/> <input type="text" value="http://devstack:5001"/>	[

Folder name	External storage	Authentication	Configuration	A
OpenStackObjectSt	OpenStack Object Storage	Rackspace ▼	<input type="text" value="cloudFiles"/> <input type="text" value="Region"/> <input type="text" value="myfiles"/> <input type="text" value="Request timeout (seconds)"/> <input type="text" value="molly"/> <input type="text" value="....."/>	[

The timeout of HTTP requests is set in the **Request timeout** field, in seconds.

See *Configuring External Storage (GUI)* for additional mount options and information.

See *External Storage Authentication mechanisms* for more information on authentication schemes.

ownCloud

An ownCloud storage is a specialized *WebDAV* storage, with optimizations for ownCloud-ownCloud communication. See the *WebDAV* documentation to learn how to configure an ownCloud external storage.

When filling in the **URL** field, use the path to the root of the ownCloud installation, rather than the path to the WebDAV endpoint. So, for a server at `https://example.com/owncloud`, use `https://example.com/owncloud` and not `https://example.com/owncloud/remote.php/dav`.

See *Configuring External Storage (GUI)* for additional mount options and information.

See *External Storage Authentication mechanisms* for more information on authentication schemes.

SFTP

ownCloud's SFTP (FTP over an SSH tunnel) backend supports both password and public key authentication.

The **Host** field is required; a port can be specified as part of the **Host** field in the following format: `hostname.domain:port`. The default port is 22 (SSH).

For public key authentication, you can generate a public/private key pair from your **SFTP with secret key login** configuration.

External Storage

Folder name	External storage	Authentication	Configuration
<input type="text" value="SFTP"/>	<input type="text" value="SFTP"/>	<input type="text" value="Username and password"/> <input type="text" value="Username and password"/> <input type="text" value="Log-in credentials, save in session"/> <input type="text" value="RSA public key"/>	<input type="text" value="Host"/> <input type="text" value="Root"/> <input type="text" value="Username"/> <input type="text" value="Password"/>

After generating your keys, you need to copy your new public key to the destination server to `.ssh/authorized_keys`. ownCloud will then use its private key to authenticate to the SFTP server.

The default **Remote Subfolder** is the root directory (`/`) of the remote SFTP server, and you may enter any directory you wish.

See *Configuring External Storage (GUI)* for additional mount options and information.

See *External Storage Authentication mechanisms* for more information on authentication schemes.

SMB/CIFS

ownCloud can connect to Windows file servers or other SMB-compatible servers with the SMB/CIFS backend.

Note: ownCloud's SMB/CIFS backend requires either [the libsmbclient-php module](#) (version 0.8.0+) or [the smbclient command](#) (and its dependencies) to be installed on the ownCloud server. We highly recommend libsmbclient-php, but it isn't required. If installed, however, smbclient won't be needed. Most Linux distributions provide libsmbclient-php and, typically, name it `php-smbclient`.

You also need the Samba client installed on your Linux system. This is included in all Linux distributions; on Debian, Ubuntu, and other Debian derivatives this is `smbclient`. On SUSE, Red Hat, CentOS, and other Red Hat derivatives it is `samba-client`. You also need `which` and `stdbuf`, which should be included in most Linux distributions.

You need the following information:

- Folder name for your local mountpoint.
- Host: The URL of the Samba server.
- Username: The username or domain/username used to login to the Samba server.
- Password: the password to login to the Samba server.
- Share: The share on the Samba server to mount.
- Remote Subfolder: The remote subfolder inside the Samba share to mount (optional, defaults to `/`). To assign the ownCloud logon username automatically to the subfolder, use `$user` instead of a particular subfolder name.
- And finally, the ownCloud users and groups who get access to the share.

Optionally, you can specify a `Domain`. This is useful in cases where the SMB server requires a domain and a username, and an advanced authentication mechanism like session credentials is used so that the username cannot be modified. This is concatenated with the username, so the backend gets `domain\username`

See [Configuring External Storage \(GUI\)](#) for additional mount options and information.

See [External Storage Authentication mechanisms](#) for more information on authentication schemes.

WebDAV

Use this backend to mount a directory from any WebDAV server, or another ownCloud server.

You need the following information:

- Folder name: The name of your local mountpoint.
- The URL of the WebDAV or ownCloud server.
- Username and password for the remote server
- Secure `https://`: We always recommend `https://` for security, though you can leave this unchecked for `http://`.

Optionally, a `Remote Subfolder` can be specified to change the destination directory. The default is to use the whole root.

Note: CPANEL users should install [Web Disk](#) to enable WebDAV functionality.

See [Configuring External Storage \(GUI\)](#) for additional mount options and information.

oc-remote ownCloud

https://remoteserve

admin

.....

↑

Secure https://

All Users x

See *External Storage Authentication mechanisms* for more information on authentication schemes.

Note: A non-blocking or correctly configured SELinux setup is needed for these backends to work. Please refer to the *SELinux Configuration*.

Allow Users to Mount External Storage

Check “*Allow users to mount external storage*” to allow your users to mount storages on external services. Then enable the backends you want to allow.

Allow users to mount external storage

Allow users to mount the following external storage

- WebDAV
- ownCloud
- SFTP
- Amazon S3
- Dropbox
- Google Drive
- OpenStack Object Storage
- SMB / CIFS

Warning: Be careful with the choices that you enable, as it allows a user to make potentially arbitrary connections to other services on your network!

Setting Up Google Drive and Dropbox Connections

When an external storage is created which uses either Google Drive or Dropbox, a link to the respective configuration page is available, next to the service name.

Folder name	External storage	Authentication	Configuration		Grant access	Available for
GoogleDrive	Google Drive	OAuth2	Client ID	Client secret	Grant access	All users. Type to select user or group.
Dropbox	Dropbox	OAuth1	App key	App secret	Grant access	All users. Type to select user or group.
Folder name	Add storage					

In the screenshot above, you can see that two external storage connections have been created, but not configured. One goes to Google Drive, the other to Dropbox. If you click the cog icon next to the name of either, the respective app configuration page will open in a new tab, or a new window. From there, you can manage the configuration and obtain the respective credentials needed for configuring the connection.

Detecting Files Added to External Storages

We recommend configuring the background job **Webcron** or **Cron** (see [Background Jobs](#)) to enable ownCloud to automatically detect files added to your external storages.

Note: You cannot scan/detect changed files on external storage mounts when you select the **Log-in credentials, save in session** authentication mechanism. However, there is a workaround, and that is to use Ajax cron mode. See [Password-based Mechanisms](#) for more information.

ownCloud may not always be able to find out what has been changed remotely (files changed without going through ownCloud), especially when it's very deep in the folder hierarchy of the external storage.

You might need to setup a cron job that runs `sudo -u www-data php occ files:scan --all` (or replace “--all” with the user name, see also [Using occ core commands](#)) to trigger a rescan of the user's files periodically (for example every 15 minutes), which includes the mounted external storage.

FTP

If you want to mount a FTP Storage, please install the app `FTP Storage Support` from ownCloud market.

6.2.6 Configuring External Storage (Configuration File)

Starting with ownCloud 9.0, the `data/mount.json` file for configuring external storages has been removed, and replaced with a set of [occ commands](#).

6.2.7 External Storage Authentication mechanisms

ownCloud storage backends accept one or more authentication schemes such as passwords, OAuth, or token-based, to name a few examples. Each authentication scheme may be implemented by multiple authentication mechanisms. Different mechanisms require different configuration parameters, depending on their behaviour.

The screenshot shows the ownCloud Market interface. On the left is a sidebar menu with the following items: 'Market', 'Show all', 'App Bundles', 'CATEGORIES', 'Automation', 'Collaboration', 'Customization', 'External plugins' (highlighted with a red box), 'Games', 'Integration', 'Multimedia', 'Productivity', 'Security', 'Storage', 'Tools', 'SETTINGS', 'Edit API Key', and 'Clear cache'. The main content area displays the 'FTP storage support' plugin, which is categorized under 'external-plugins'. It features a dark blue banner with the ownCloud logo. Below the banner, the text reads 'FTP backend for files_external'. A table provides the following details:

DEVELOPER	VERSION	RELEASE DATE	LICENSE
ownCloud	0.2.0	Apr 25, 2017	GNU Affero General Public License

An 'INSTALL' button is located at the bottom right of the plugin details.

Special Mechanisms

The **None** authentication mechanism requires no configuration parameters, and is used when a backend requires no authentication.

The **Built-in** authentication mechanism itself requires no configuration parameters, but is used as a placeholder for legacy storages that have not been migrated to the new system and do not take advantage of generic authentication mechanisms. The authentication parameters are provided directly by the backend.

Password-based Mechanisms

The **Username and password** mechanism requires a manually-defined username and password. These get passed directly to the backend.

The **Log-in credentials, save in session** mechanism uses the ownCloud login credentials of the user to connect to the storage. These are not stored anywhere on the server, but rather in the user session, giving increased security. The drawbacks are that sharing is disabled when this mechanism is in use, as ownCloud has no access to the storage credentials, and background file scanning does not work.

Note: There is a workaround that allows background file scanning when using **Log-in credentials, save in session**, and that is using Ajax cron mode. (See [Background Jobs](#).) Be aware that the Ajax cron mode is triggered by browsing the ownCloud Web GUI.

Known Limitations

Please be aware that any operations must be performed by the logged-in mount owner, as credentials are not stored anywhere. As a result, there are three known limitations, for both admin and personal mounts where both have the “log-in credentials, save in session” option. These are:

1. Directly sharing the storage or any of its sub-folders will go through, but the recipient will not see the share mounted. This is because the mount cannot be set up due to missing credentials. Federated sharing is also affected, because it works on a “public link share token” basis, which itself doesn’t contain the user’s storage password. As a result, the storage cannot be mounted in this case either.
2. Any background task operating on the storage, such as background scanning.
3. Any *occ command* that operates on the storage, such as `occ files:scan`, will have no effect.

Note: Enterprise Users Only

The enterprise version has a mode called “Save in DB” where the credentials are saved, in encrypted form, in the database (via *the WND app*). In this mode, all of the above operations work.

Public-key Mechanisms

Currently only the RSA mechanism is implemented, where a public/private keypair is generated by ownCloud and the public half shown in the GUI. The keys are generated in the SSH format, and are currently 1024 bits in length. Keys can be regenerated with a button in the GUI.

OAuth

OAuth 1.0 and OAuth 2.0 are both implemented, but currently limited to the Dropbox and Google Drive backends respectively. These mechanisms require additional configuration at the service provider, where an app ID and app secret

Authentication	Configuration			
RSA public key	Host	Root	Username	ssh-rsa AAAAB3NzaC1:
	Generate keys			

are provided and then entered into ownCloud. Then ownCloud can perform an authentication request, establishing the storage connection.

sharedropbox	Dropbox	rt	Access granted
		All Users x

If ownCloud client's are unable to connect to your ownCloud server, check that the bearer authorization header *is not being stripped out*.

6.2.8 Encryption Configuration Quick Guide

Encryption Types

ownCloud provides two encryption types:

- **Master Key:** there is only one key (or key pair) and all files are encrypted using that key pair. This is **highly recommended** for **new** instances to avoid **restrictions** in functionality of user key encryption.
- **User-specific Key:** every user has their own private/public key pairs; the private key is protected by the user's password. This **will be removed in future a release**.

Master Key

- The **recommended** type of encryption.
- Best to activate on new instances with no data.
- If you have existing data, use **encrypt all** command. Depending on the amount of existing data, this operation can take a long time.

Activation

```
occ maintenance:singleuser --on
occ app:enable encryption
occ encryption:enable
occ encryption:select-encryption-type masterkey -y
occ encryption:encrypt-all
occ maintenance:singleuser --off
```

Status

```
occ encryption:status
```

Decryption Depending on the amount of existing data, this operation can take a long time.

```
occ maintenance:singleuser --on
occ encryption:decrypt-all
occ maintenance:singleuser --off
```

Deactivation

```
occ encryption:disable
# ignore the "already disabled" message
occ app:disable encryption
```

If the master key has been compromised or exposed, you can recreate it. You will need the current master key for it.

```
occ encryption:recreate-master-key
```

User-Specific Key

Activation

```
occ maintenance:singleuser --on
occ app:enable encryption
occ encryption:enable
occ encryption:select-encryption-type user-keys
occ encryption:encrypt-all
occ maintenance:singleuser --off
```

After User-specific encryption is enabled, users must log out and log back in to trigger the automatic personal encryption key generation process.

Recovery Key

- Go to the “_Encryption_” section of your Admin page.
- Set a recovery key password.
- Ask the users to opt-in to the recovery key.

If a user decides not to opt-in to the recovery key and forgets or loses their password, **the user’s data cannot be decrypted**. This leads to **permanent data loss**.

They need to:

- Go to the “**Personal**” page
- Enable the Recovery Key

Status

```
occ encryption:status
```

Decrypt

```
occ maintenance:singleuser --on
occ encryption:decrypt-all
#enter **Recovery Key** for **each user**
# Recovery Key is a password set by the admin
occ maintenance:singleuser --off
```

Deactivation

```
occ encryption:disable
# ignore the "already disabled" message
occ app:disable encryption
```

6.2.9 Encryption Configuration

Background information

The primary purpose of the ownCloud server-side encryption is to protect users' files when they're located on remote storages, such as Dropbox and Google Drive, and to do it smoothly and seamlessly from within ownCloud.

From ownCloud 9.0, server-side encryption for local and remote storages can operate independently of each other. By doing so, you can encrypt a remote storage *without* also having to encrypt your home storage on your ownCloud server.

Note: Starting with ownCloud 9.0 we support Authenticated Encryption for all newly encrypted files. See <https://hackerone.com/reports/108082> for more technical information about the impact.

For maximum security make sure to configure external storage with “*Check for changes: Never.*” This will let ownCloud ignore new files not added via ownCloud. By doing so, a malicious external storage administrator cannot add new files to the storage without your knowledge. However, this is not wise *if* your external storage is subject to legitimate external changes.

ownCloud's server-side encryption encrypts files stored on the ownCloud server and files on remote storages that are connected to your ownCloud server. Encryption and decryption are performed on the ownCloud server. All files sent to remote storage will be encrypted by the ownCloud server and decrypted before serving them to you or anyone whom you have shared them with.

Note: Encrypting files increases their size by roughly 35%. Remember to take this into account when you are both provisioning storage and setting storage quotas. Secondly, user quotas are based on the *unencrypted* file size — **not** the encrypted size.

When files on an external storage are encrypted in ownCloud, you cannot share them directly from the external storage services, only through ownCloud sharing. This is because the key to decrypt the data **never** leaves the ownCloud server.

ownCloud's server-side encryption generates a strong encryption key, which is unlocked by users' passwords. As a result, your users don't need to track an extra password. All they need to do is log in as they normally would. ownCloud, transparently, encrypts only the contents of files, and not filenames and directory structures.

Important: You should regularly backup all encryption keys to prevent permanent data loss.

The encryption keys are stored in the following directories:

Directory	Description
data/<user>/files_encryption	Users' private keys and all other keys necessary to decrypt the users' files.
data/files_encryption	Private keys and all other keys necessary to decrypt the files stored on a system wide external storage.

Note: You can move the keys to a different location. To do so, refer to the [Move Key Location](#) section of the documentation.

When encryption is enabled, all files are encrypted and decrypted by the ownCloud application, and stored encrypted on your remote storage. This protects your data on externally hosted storage. The ownCloud admin and the storage admin will see only encrypted files when browsing backend storage.

Warning: Encryption keys are stored only on the ownCloud server, eliminating exposure of your data to third-party storage providers. The encryption application does **not** protect your data if your ownCloud server is compromised, and it does not prevent ownCloud administrators from reading users' files. This would require client-side encryption, which this application does not provide. If your ownCloud server is not connected to any external storage services, it is better to use other encryption tools, such as file-level or whole-disk encryption.

Important: SSL terminates at or before Apache on the ownCloud server. Consequently, all files are in an unencrypted state between the SSL connection termination and the ownCloud code that encrypts and decrypts them. This is, potentially, exploitable by anyone with administrator access to your server. For more information, read: [How ownCloud uses encryption to protect your data](#).

Encryption Types

ownCloud provides two encryption types:

- **User-Key:** every user has their own private/public key pairs, and the private key is protected by the user's password.
- **Master Key:** there is only one key (or key pair) and all files are encrypted using that key pair.

Before Enabling Encryption

Plan very carefully before enabling encryption, because it is **not reversible** via the ownCloud Web interface. If you lose your encryption keys, your files are **not recoverable**. Always have backups of your encryption keys stored in a safe location, and consider enabling all recovery options.

You have more options via the `occ` command (see [Enabling Master Key Based Encryption from the Command-Line](#))

Warning: You can't manage encryption without access to the command line. If your ownCloud installation is on a hosted environment and you don't have access to the command line, you won't be able to run `occ commands`. In this case, **don't enable encryption!**

Enabling Master Key Based Encryption from the Command-Line

To enable master key based encryption:

1. Enable the default encryption module app, using the following command

```
occ app:enable encryption
```

2. Then enable encryption, using the following command

```
occ encryption:enable
```

3. Then enable the master key, using the following command

```
occ encryption:select-encryption-type masterkey
```

Note: The master key mode has to be set up in a newly created instance.

4. Encrypt all data

```
occ encryption:encrypt-all
```

Note: This is not typically required, as the master key is often enabled at install time. As a result, when enabling it, there should be no data to encrypt. But, in case it's being enabled after install, and the installation does have files which are unencrypted, encrypt-all can be used to encrypt them.

View Current Encryption Status

Get the current encryption status and the loaded encryption module:

```
occ encryption:status
```

This is equivalent to checking **Enable server-side encryption** on your Admin page:

```
occ encryption:enable
Encryption enabled
```

```
Default module: OC_DEFAULT_MODULE
```

Recreating an Existing Master Key

If the master key needs replacing, for example, because it has been compromised, an occ command is available. The command is *encryption:recreate-master-key*. It replaces existing master key with new one and encrypts the files with the new key.

Decrypt Master-Key Encryption

You must first put your ownCloud server into single-user mode to prevent any user activity until encryption is completed

```
occ maintenance:singleuser --on
Single user mode is currently enabled
```

Decrypt all user data files, or optionally a single user:

```
occ encryption:decrypt-all [username]
```

Disabling Encryption

To disable encryption, put your ownCloud server into single-user mode, and then disable your encryption module with these commands:

```
occ maintenance:singleuser --on
occ encryption:disable
```

Take it out of single-user mode when you are finished, by using the following command:

```
occ maintenance:singleuser --off
```

Important: You may only disable encryption by using the ‘**occ Encryption Commands**‘. Make sure you have backups of all encryption keys, including those for all your users.

Enabling User-Key Based Encryption From the Command-line

To enable User-Key based encryption:

To be safe, put your server in single user mode, to avoid any issues on a running instance

```
occ maintenance:singleuser --on
```

1. Enable the default encryption module app, using the following command

```
occ app:enable encryption
```

2. Then enable encryption, using the following command

```
occ encryption:enable
```

3. Then enable the user-key, using the following command

```
occ encryption:select-encryption-type user-key
```

4. Encrypt all data

```
occ encryption:encrypt-all
```

Now you can turn off the singleuser mode

```
occ maintenance:singleuser --off
```

How To Enable Users File Recovery Keys

Once a user has encrypted their files, if they lose their ownCloud password, then they lose access to their encrypted files, as their files will be unrecoverable. It is not possible, when user files are encrypted, to reset a user’s password using the standard reset process.

If so, you’ll see a yellow banner warning:

Please provide an admin recovery password; otherwise, all user data will be lost.

To avoid all this, create a Recovery Key. To do so, go to the Encryption section of your Admin page and set a recovery key password.

You then need to ask your users to opt-in to the Recovery Key. For the users to do this, they need to go to the “**Personal**” page and enable the recovery key. This signals that they are OK that the admin might have a way to decrypt their data for recovery reasons. If they do *not* do this, then the Recovery Key won’t work for them.

For users who have enabled password recovery, give them a new password and recover access to their encrypted files, by supplying the Recovery Key on the Users page.

You may change your recovery key password.

Server-side encryption *i*

Enable server-side encryption

Select default encryption module:

Default encryption module

Enable recovery key

The recovery key is an extra encryption key that is used to encrypt files. It allows recovery of a user's files if the user forgets his or her password.

Disable recovery key

Encryption

Enable password recovery:

Enabling this option will allow you to reobtain access to your encrypted files in case of password loss

Enabled

Disabled

File recovery settings updated

Admin Recovery Password		
Group Admin	Quota	Storage Location
Group Admin ▼	Default ▼	/var/www/owncloud.

Enter the recovery password in order to recover the users files during password change

Change recovery key password:

Old Recovery key password

New Recovery key password

Repeat New Recovery key password

Note: Sharing a recovery key with a user group is **not** supported. This is only supported with *the master key*.

Changing The Recovery Key Password

If you have misplaced your recovery key password and need to replace it, here's what you need to do:

1. Delete the recovery key from both `data/owncloud_private_keys` and `data/public-keys`
2. Edit your database table `oc_appconfig` and remove the rows with the config keys `recoveryKeyId` and `recoveryAdminEnabled` for the appid `files_encryption`
3. Login as admin and activate the recovery key again with a new password. This will generate a new key pair
4. All users who used the original recovery key will need to disable it and enable it again. This deletes the old recovery share keys from their files and encrypts their files with the new recovery key

Note: You can only change the recovery key password if you know the original. This is by design, as only admins who know the recovery key password should be able to change it. If not, admins could hijack the recovery key from each other

Warning: Replacing the recovery key will mean that all users will lose the possibility to recover their files until they have applied the new recovery key

Decrypt User-Key Encryption

You must first put your ownCloud server into single-user mode to prevent any user activity until encryption is completed

```
occ maintenance:singleuser --on
Single user mode is currently enabled
```

Decrypt all user data files, or optionally a single user:

```
occ encryption:decrypt-all [username]
```

Disabling Encryption

You may disable encryption only with `occ`. Make sure you have backups of all the encryption keys, including those for all users. When you do, put your ownCloud server into single-user mode, and then disable your encryption module with this command:

```
occ maintenance:singleuser --on
occ encryption:disable
```

Warning: Encryption cannot be disabled without the user's password or *file recovery key*. If you don't have access to at least one of these then there is no way to decrypt all files.

Then, take it out of single-user mode when you are finished with this command:

```
occ maintenance:singleuser --off
```

It is possible to disable encryption with the file recovery key, *if* every user uses them. If so, "*decrypt all*" will use it to decrypt all files.

Note: It is **not** planned to move this to the next user login or a background job. If that was done, then login passwords would need to be stored in the database, which could be a security issue.

Move Key Location

View current location of keys:

```
occ encryption:show-key-storage-root
Current key storage root: default storage location (data/)
```

Move keys to a different root folder, either locally or on a different server. The folder must already exist, be owned by root and your HTTP group, and be restricted to root and your HTTP group. This example is for Ubuntu Linux. Note that the new folder is relative to your `occ` directory:

```
mkdir /etc/keys
chown -R root:www-data /etc/keys
chmod -R 0770 /etc/keys
occ encryption:change-key-storage-root ../../etc/keys
Start to move keys:
  4 [=====]
Key storage root successfully changed to ../../etc/keys
```

Files Not Encrypted

Only the data in the files in `data/user/files` are encrypted, and not the filenames or folder structures. These files are never encrypted:

- Existing files in the trash bin & Versions. Only new and changed files after encryption is enabled are encrypted.

- Existing files in Versions
- Image thumbnails from the Gallery app
- Previews from the Files app
- The search index from the full-text search app
- Third-party app data

There may be other files that are not encrypted; only files that are exposed to third-party storage providers are guaranteed to be encrypted.

LDAP and Other External User Back-ends

If you use an external user back-end, such as an LDAP or Samba server, and you change a user's password on that back-end, the user will be prompted to change their ownCloud login to match on their next ownCloud login. The user will need both their old and new passwords to do this. If you have enabled the recovery key then you can change a user's password in the ownCloud Users panel to match their back-end password and then — of course — notify the user and give them their new password.

Encrypting External Mountpoints

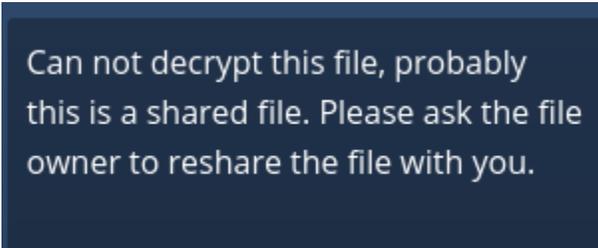
You and your users can encrypt individual external mount points. You must have external storage enabled on your Admin page, and enabled for your users. Encryption settings can be configured in the mount options for an external storage mount; see *Mount Options (Configuring External Storage (GUI))*

Sharing Encrypted Files

After encryption is enabled, your users must also log out and log back in to generate their personal encryption keys. They will see a yellow warning banner that says *“Encryption App is enabled, but your keys are not initialized. Please log-out and log-in again.”*

Also, share owners may need to re-share files after encryption is enabled. Users who are trying to access the share will see a message advising them to ask the share owner to re-share the file with them.

For individual shares, un-share and re-share the file. For group shares, share with any individuals who can't access the share. This updates the encryption, and then the share owner can remove the individual shares.



Can not decrypt this file, probably this is a shared file. Please ask the file owner to reshare the file with you.

How To Enable Encryption From the Web-UI

1. First, you must enable the encryption app, and then select an encryption type. Go to the **Apps** section of your Admin page, click on **Show disabled Apps** and enable **Default encryption module**.
2. After that go to the encryption section of your Admin page, and check the checkbox “Enable server-side encryption”.

3. Then select an encryption Type. Masterkey and User-key are the options. Masterkey is recommended.
4. Now you **must** log out and then log back in to initialize your encryption keys.

6.2.10 Transactional File Locking

ownCloud's Transactional File Locking mechanism locks files to avoid file corruption during normal operation. It performs these functions:

- Operates at a higher level than the filesystem, so you don't need to use a filesystem that supports locking
- Locks parent directories so they cannot be renamed during any activity on files inside the directories
- Releases locks after file transactions are interrupted, for example when a sync client loses the connection during an upload
- Manages locking and releasing locks correctly on shared files during changes from multiple users
- Manages locks correctly on external storage mounts
- Manages encrypted files correctly

Transactional File locking will not prevent multiple users from editing the same document, nor give notice that other users are working on the same document. Multiple users can open and edit a file at the same time and Transactional File locking does not prevent this. Rather, it prevents simultaneous file saving.

Note: Transactional file locking is in ownCloud core, and replaces the old File Locking app. The File Locking app was removed from ownCloud in version 8.2.1. If your ownCloud server still has the File Locking app, you **must** visit your Apps page to verify that it is disabled; the File Locking app and Transactional File Locking cannot both operate at the same time.

File locking is enabled by default, using the database locking backend. This places a significant load on your database. Using `memcache.locking` relieves the database load and improves performance. Admins of ownCloud servers with heavy workloads should install *a memory cache*.

6.2.11 Previews Configuration

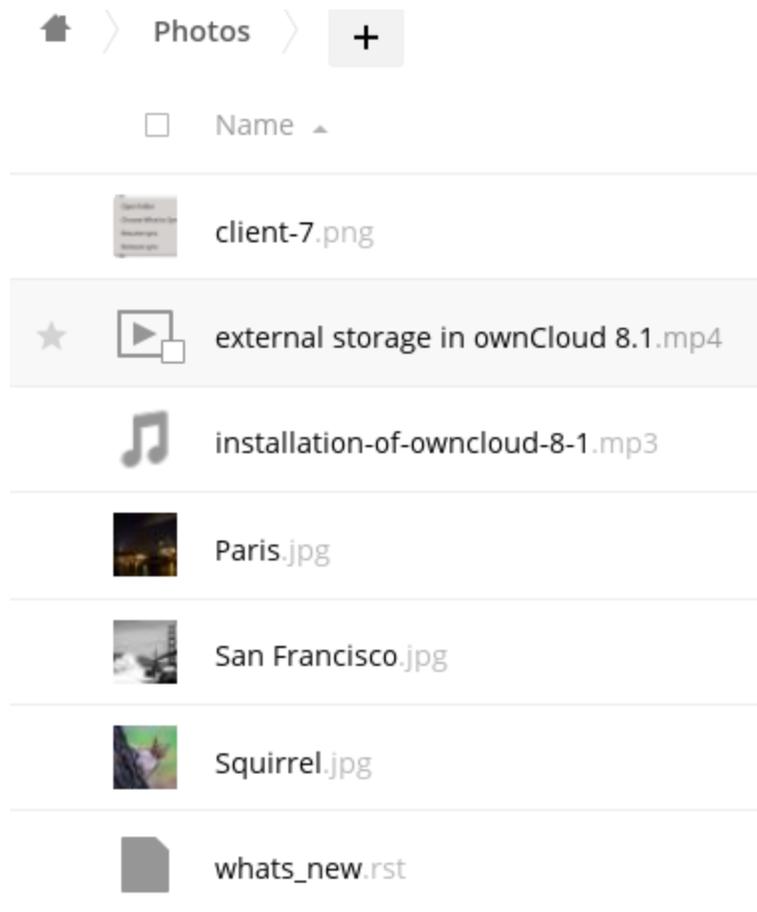
The ownCloud thumbnail system generates previews of files for all ownCloud apps that display files, such as Files and Gallery.

The following image shows some examples of previews of various file types.

By default, ownCloud can generate previews for the following filetypes:

- Images files
- Cover of MP3 files
- Text documents

Note: Older versions of ownCloud also supported the preview generation of other file types such as PDF, SVG or various office documents. Due to security concerns those providers have been disabled by default and are considered unsupported. While those providers are still available, we discourage enabling them, and they are not documented.



Parameters

Please notice that the ownCloud preview system comes already with sensible defaults, and therefore it is usually unnecessary to adjust those configuration values.

Disabling previews

Under certain circumstances, for example if the server has limited resources, you might want to consider disabling the generation of previews. Note that if you do this all previews in all apps are disabled, including the Gallery app, and will display generic icons instead of thumbnails.

Set the configuration option `enable_previews` in `config.php` to `false`:

```
<?php
    'enable_previews' => false,
```

Maximum preview size

There are two configuration options for setting the maximum size (in pixels) of a preview. These are `preview_max_x` which represents the x-axis and `preview_max_y` which represents the y-axis. In `config/config.sample.php`, which you can see below, both options are set to a default of 2048.

```
<?php
    'preview_max_x' => 2048,
    'preview_max_y' => 2048,
```

The following example would limit previews to a maximum size of 100 px × 100 px:

```
<?php
    'preview_max_x' => 100,
    'preview_max_y' => 100,
```

Note: If you want no limit applied for one or both of these values then set them to `null`.

Maximum scale factor

If a lot of small pictures are stored on the ownCloud instance and the preview system generates blurry previews, you might want to consider setting a maximum scale factor. By default, pictures are upscaled to 10 times the original size:

```
<?php
    'preview_max_scale_factor' => 10,
```

If you want to disable scaling at all, you can set the config value to `'1'`:

```
<?php
    'preview_max_scale_factor' => 1,
```

If you want to disable the maximum scaling factor, you can set the config value to `'null'`:

```
<?php
    'preview_max_scale_factor' => null,
```

6.2.12 Controlling File Versions and Aging

The Versions app (`files_versions`) expires old file versions automatically to ensure that users don't exceed their storage quotas. This is the default pattern used to delete old versions:

- For the first second we keep one version
- For the first 10 seconds ownCloud keeps one version every 2 seconds
- For the first minute ownCloud keeps one version every 10 seconds
- For the first hour ownCloud keeps one version every minute
- For the first 24 hours ownCloud keeps one version every hour
- For the first 30 days ownCloud keeps one version every day
- After the first 30 days ownCloud keeps one version every week

The versions are adjusted along this pattern every time a new version is created.

The Versions app never uses more than 50% of the user's storage quota. If the stored versions exceed this limit, ownCloud deletes the oldest file versions until it meets the disk space limit again.

You may alter the default pattern in `config.php`. The default setting is `auto`, which sets the default pattern:

```
'versions_retention_obligation' => 'auto',
```

Additional options are:

- **D, auto** Keep versions at least for D days, apply expiration rules to all versions that are older than D days
- **auto, D** Delete all versions that are older than D days automatically, delete other versions according to expiration rules
- **D1, D2** Keep versions for at least D1 days and delete when they exceed D2 days.
- **disabled** Disable Versions; no files will be deleted.

Enterprise File Retention

Enterprise customers have additional tools for managing file retention policies; see [Advanced File Tagging With the Workflow App](#).

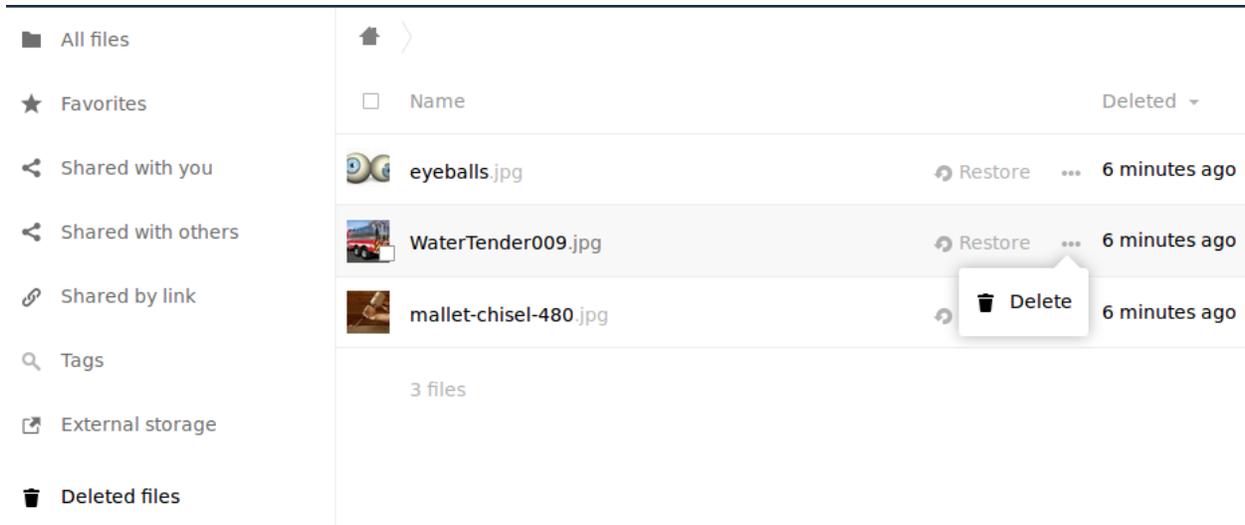
6.2.13 Managing the Trashbin

The ownCloud Trashbin (`files_trashbin`) permanently deletes files according to users' storage quotas and file ages. When a user deletes a file it is not immediately removed from your ownCloud server, but goes into the Trashbin. Then the user has the options to un-delete the file, or to delete it permanently.

As the ownCloud server administrator, you have two `occ` commands for permanently deleting files from the Trashbin manually, without waiting for the normal aging-out process:

```
trashbin
trashbin:cleanup  Remove deleted files
trashbin:expire   Expires the users trashbin
```

The `trashbin:cleanup` command removes the deleted files of all users, or you may specify certain users in a space-delimited list. This example removes all the deleted files of all users:



```
sudo -u www-data php occ trashbin:cleanup
Remove all deleted files
Remove deleted files for users on backend Database
user1
user2
user3
user4
```

This example removes the deleted files of user2 and user4:

```
sudo -u www-data php occ trashbin:cleanup user2 user4
Remove deleted files of user2
Remove deleted files of user4
```

`trashbin:expire` deletes only expired files according to the `trashbin_retention_obligation` setting in `config.php`. The default setting is `auto`, which keeps files in the Trashbin for 30 days, then deletes the oldest files as space is needed to keep users within their storage quotas. Files may not be deleted if the space is not needed.

The default is to delete expired files for all users, or you may list users in a space-delimited list:

```
sudo -u www-data php occ trashbin:cleanup user1 user2
Remove deleted files of user1
Remove deleted files of user2
```

See the **Deleted Files** section in *Core Config.php Parameters*, and the *Trashbin* section of *Using occ core commands*.

6.3 How To Install and Configure an LDAP Proxy-Cache Server

6.3.1 Background

To reduce network traffic overhead and avoid problems either logging in or performing user searches while sharing, it's an excellent idea to implement an LDAP proxy cache.

An LDAP proxy cache server, similar to other kinds of caching servers, is a special type of LDAP replica. It can cache a range of LDAP records, often resulting in improved LDAP server performance.

Specifically, the records which need to be cached, for improved ownCloud performance, are:

- Users that are allowed to log in
- Groups (limited to the allowed users)
- Search fields (e.g., sAMAccountName, cn, sn, givenName, and displayName)

6.3.2 How To Setup the Server

There's not that much to it, just the following five steps:

1. Install OpenLDAP
2. Configure the server
3. Edit the default configuration directory
4. Perform a test search
5. Check the logs
6. Configure ownCloud LDAP app

Let's begin.

6.3.3 1. Install OpenLDAP

There are a number of [LDAP server implementations](#) available. The one used in this guide is [OpenLDAP](#).

Note: While OpenLDAP does work on any operating system, for the purposes of this guide, we'll be using a Debian-based Linux distribution.

Firstly, log in as root, and update your system, to ensure that you're using the latest packages.:

```
apt-get update && apt-get upgrade -y
```

Next, install OpenLDAP and its associated packages.:

```
apt-get install slapd ldap-utils -y
```

6.3.4 2. Configure the Server

With OpenLDAP installed and running, you now need to configure the server. One way of doing so, is to create a configuration file. So, create `/etc/ldap/slapd.conf` with your text editor of choice, and add the following configuration to it.

```
# This an example of a config file:

# See slapd.conf(5)

# Global Directives:

# Schema and objectClass definitions

include          /etc/ldap/schema/core.schema
include          /etc/ldap/schema/cosine.schema
include          /etc/ldap/schema/nis.schema
include          /etc/ldap/schema/inetorgperson.schema
```

```
# Where the pid file is put. The init.d script
# will not stop the server if you change this.

pidfile          /var/run/slapd/slapd.pid

# List of arguments that were passed to the server

argsfile         /var/run/slapd/slapd.args

# Read slapd.conf(5) for possible values
# Change loglevel to "any" if you want to see everything.

loglevel         none

# Where the dynamically loaded modules are stored

modulepath       /usr/lib/ldap

# Here are the recommended modules:

# module for the target ldap-server

moduleload       back_ldap.la

# module for your local database

moduleload       back_hdb.la

# module for rewriting attributes

moduleload       rwm

# caching module

moduleload       pcache.la

# module to enable memberof in LDAP

moduleload memberof.la

# The maximum number of entries that is returned for a search operation

sizelimit 500

# The tool-threads parameter sets the actual amount of cpu's that is used
# for indexing.

tool-threads 1

# Type of backend, for example "ldap"

backend          ldap

# Type of database

database         ldap
```

```
# If you only have read access, set this to "yes"
readonly          yes

# Set which protocol to use, we suggest "3"
protocol-version  3

# remember bind credentials
rebind-as-user

# If you want to save time and don't want to list all the refferals, set to "yes"
norefs           yes

# Same as above
chase-referrals  no

# Specify the URL of your ldap server and the port.
# For unencrypted access use the port 389, for encrypted 636
# If you have to use 636, you will also probably have to import
# the certificate of your target server. restart your webserver after you do.
uri "ldap://192.168.178.2:389"

# The base of your directory in database, for example "dc=ldap01,dc=com"
suffix           "dc=ldap01,dc=com"

# rootdn directive for specifying a superuser on the database.
# If you don't have access to the admin user, use the one you have.
rootdn           "cn=admin,dc=ldap01,dc=com"

# Now we start initialising the modules
# First the rewrite module
overlay          rwm

# Now we rewrite the attributes
rwm-map          attribute uid sAMAccountName
rwm-map          attribute dn distinguishedName

# Next one is optional, if you want memberof, for the groups,
# you have to load it.
overlay          memberof

# Now we load the caching module
overlay pcache

# The directive enables proxy caching
# See slapo-pcache
```

```
# pcache <database> <max_entries> <numattrsets> <entry_limit> <cc_period>
# Parameters:
#
# <database> for cached entries.
# <max_entries> when reached - cache replacement is invoked
# <numattrsets> = pcacheAttrset
# <entry_limit> limit to the number of entries returned
# <cc_period> Consistency check time to wait

pcache hdb 100000 3 1000 100

# pcachePersist { TRUE | FALSE }
# Write cached results into the database
# Results remain in database after restart

pcachePersist TRUE

# Where the database file are physically stored for database #1

directory      "/var/lib/ldap"

# Caching templates for general search

# pcacheAttrset <index> <attrs...>
# First set the index number
# Then set the attribute to cache

pcacheAttrset  0 1.1

# pcacheTemplate <template_string> <attrset_index> <ttl>
# First define the query sting to cache
# Then reference the Attrset
# Last set the time-to-live

pcacheTemplate (&(|(objectClass=))) 0 3600

pcacheTemplate (objectClass=*) 0 3600

# User Name Field (Advanced Tab)

pcacheAttrset  1 displayname
pcacheTemplate (objectClass=*) 1 3600

# Group Field

pcacheAttrset  2 memberOf
pcacheTemplate (objectClass=*) 2 3600

# This an example of a config file:

# See slapd.conf(5)

# Global Directives:

# Schema and objectClass definitions

include        /etc/ldap/schema/core.schema
```

```
include          /etc/ldap/schema/cosine.schema
include          /etc/ldap/schema/nis.schema
include          /etc/ldap/schema/inetorgperson.schema

# Where the pid file is put. The init.d script
# will not stop the server if you change this.

pidfile          /var/run/slapd/slapd.pid

# List of arguments that were passed to the server

argsfile         /var/run/slapd/slapd.args

# Read slapd.conf(5) for possible values
# Change loglevel to "any" if you want to see everything.

loglevel         none

# Where the dynamically loaded modules are stored

modulepath       /usr/lib/ldap

# Here are the recommended modules:

# module for the target ldap-server

moduleload       back_ldap.la

# module for your local database

moduleload       back_hdb.la

# module for rewriting attributes

moduleload       rwm

# caching module

moduleload       pcache.la

# module to enable memberof in LDAP

moduleload       memberof.la

# The maximum number of entries that is returned for a search operation

sizelimit 500

# The tool-threads parameter sets the actual amount of cpu's that is used
# for indexing.

tool-threads 1

# Type of backend, for example "ldap"

backend          ldap
```

```
# If you only have read access, set this to "yes"
readonly          yes

# Set which protocol to use, we suggest "3"
protocol-version  3

# remember bind credentials
rebind-as-user

# If you want to save time and don't want to list all the refferals, set to "yes"
norefs           yes

# Same as above
chase-referrals  no

# Specify the URL of your ldap server and the port.
# For unencrypted access use the port 389, for encrypted 636
# If you have to use 636, you will also probably have to import
# the certificate of your target server.
# Restart your webserver after you do.
uri "ldap://192.168.178.2:389"

# The base of your directory in database, for example "dc=ldap01,dc=com"
suffix           "dc=ldap01,dc=com"

# rootdn directive for specifying a superuser on the database.
# If you don't have access to the admin user, use the one you have.
rootdn           "cn=admin,dc=ldap01,dc=com"

# Now we start initialising the modules
# First the rewrite module
overlay          rwm

# Now we rewrite the attributes
rwm-map          attribute uid sAMAccountName
rwm-map          attribute dn distinguishedName

# Next one is optional, if you want memberof, for the groups,
# you have to load it.
overlay          memberof

# Now we load the caching module
overlay pcache

# The directive enables proxy caching
# See slapd-pcache
```

```
# pcache <database> <max_entries> <numattrsets> <entry_limit> <cc_period>
# Parameters:
#
# <database> for cached entries.
# <max_entries> when reached - cache replacement is invoked
# <numattrsets> = pcacheAttrset
# <entry_limit> limit to the number of entries returned
# <cc_period> Consistency check time to wait

pcache hdb 100000 3 1000 100

# pcachePersist { TRUE | FALSE }
# Write cached results into the database
# Results remain in database after restart

pcachePersist TRUE

# Where the database file are physically stored for database #1

directory      "/var/lib/ldap"

# Caching templates for general search

# pcacheAttrset <index> <attrs...>
# First set the index number
# Then set the attribute to cache

pcacheAttrset  0 1.1

# pcacheTemplate <template_string> <attrset_index> <ttl>
# First define the query string to cache
# Then reference the Attrset
# Last set the time-to-live

pcacheTemplate (&(|(objectClass=))) 0 3600

pcacheTemplate (objectClass=*) 0 3600

# User Name Field (Advanced Tab)

pcacheAttrset  1 displayname
pcacheTemplate (objectClass=*) 1 3600

# Group Field

pcacheAttrset  2 memberOf
pcacheTemplate (objectClass=*) 2 3600
```

Note: This configuration only caches queries from a single Active Directory server. To cache queries from multiple Active Directory servers, a configuration is available below.

After you've done that, save the file, test that there are no errors in the configuration by running:

```
slaptest -f /etc/ldap/slapd.conf
```

Note: If you see warnings in the console output, they are not crucial.

6.3.5 3. Enable the configuration file

Next, we need to tell OpenLDAP to use our configuration. To do so, open `/etc/default/slapd` and add the following line to it:

```
SLAPD_CONF=/etc/ldap/slapd.conf
```

With that done, restart OpenLDAP by running the following command:

```
service slapd restart
```

6.3.6 4. Open the log

Open another terminal and see the systemlog with the following command.:

```
tail -f /var/log/syslog | grep QUERY
```

If there is no such file, you need to install rsyslog with.

```
apt install rsyslog
```

6.3.7 5. Perform a test search

Now that the server's installed, configured, and running, we next need to perform a search. This will check that records are being correctly cached. To do so, update the command below with values from your Active Directory server configuration, and then run it.:

```
ldapsearch -h localhost -x -LLL -D "cn=admin,cn=users,dc=example,dc=com" -b "cn=users,dc=example,dc=com"
```

or

```
ldapsearch -H ldaps://localhost:636 -x -LLL -D "cn=admin,cn=users,dc=example,dc=com" -b "cn=users,dc=example,dc=com" -W "(cn=Administrator)" name
```

`-h` = host address (Example: localhost or 192.168.1.1) `-H` = host address (Example: ldap:// or ldaps:// hostname or ip and port :389 or :636) `-x` = simple authentication `-b` = Search Base, (Example: "cn=Users,dc=example,dc=com") `-D` = User with permissions (Example: "cn=Admin,dc=example,dc=com") `-LLL` = Show only results, no extra information `-w` = Password ("Password") `-W` = Password, will ask for password and hide your input `"(cn=Administrator)"` = Filter the search name = Show only this attributes

If you see results including: "Query cachable" and "Query answered (x) times", then the setup works.

6.3.8 6. Configure ownCloud LDAP App

Login as ownCloud admin in your ownCloud server.

Click on the dropdown menu in the top-left corner next to "Files", then on Apps.

Click on "Not enabled", and enable the "LDAP user and group backend" App.

Go to the admin dropdown menu in the top-right corner, select "Admin".

In the administration section, click on the left side on "LDAP".

Configure Server-Tab

First enter the server address, either IP or DN.

You can click on the button to detect your servers port or enter it manually.

Next, enter the dn of the user, you want to log in with and in the next line enter the password.

Then you can click on “detect base dn” or enter it manually. then click on “test base dn”.

If you fulfill all the requirements you should get a green light and “configuration ok” message.

Configure Users

Select the objectclass for the users, for example “user”.

Verify your settings; where you will see the number of users being found.

Configure Login Attributes

A configuration appears by default, adjusted it to your users configuration.

If required, adjust the login parameters additional login attributes.

You can check users with any of the allowed login options. You can adjust them or leave them the way they are.

Configure Groups

Select all the objectclasses for your groups, for example “group”. Verify your settings.

Configure Advanced

Configuration Active should be selected.

Adjust the Cache TTL (time to live) value as required.

ownCloud usually autoselects the best settings for each AD configuration.

Check if the Group-Member association is “Member (AD)”. That’s important for the users being shown in their respective groups.

Select “Nested groups”, if you have them.

Configure Expert

“Internal Username Attribute”

Here we need to set “cn” for the users being shown with their unique name. If you leave that field empty, each user will get a unique uid as a string of numbers and letters.

Clear the Username and Groupname Mapping and test your configuration by clicking on the buttons below.

Navigate to Admin -> Users and check if all your users are listed properly, and shown in the right groups.

Go to the homepage of your ownCloud server and try to share something with one of your users

If everything is set up correctly, you now have an LDAP proxy server to your active directory that will reduce the network traffic by caching the searches your perform.

6.3.9 Cache Multiple Active Directory Servers

If you have more than one that you want to cache, in `/etc/ldap/slapd.conf` add the following configuration instead, adjusting as necessary. The ownCloud LDAP app settings are the same as in section 6.

```
# This an example of a config file:
```

```
# See slapd.conf(5)
```

```
# Global Directives:
```

```
# Schema and objectClass definitions

include      /etc/ldap/schema/core.schema
include      /etc/ldap/schema/cosine.schema
include      /etc/ldap/schema/nis.schema
include      /etc/ldap/schema/inetorgperson.schema
include      /etc/ldap/schema/misc.schema

# Where the pid file is put. The init.d script
# will not stop the server if you change this.

pidfile      /var/run/slapd/slapd.pid

# List of arguments that were passed to the server

argsfile     /var/run/slapd/slapd.args

# Read slapd.conf(5) for possible values
# Change loglevel to "any" if you want to see everything.

loglevel     none

# Where the dynamically loaded modules are stored

modulepath   /usr/lib/ldap

# Here are the recommended modules:

# module for meta-database

moduleload   back_meta.la

# module for the target ldap-server

moduleload   back_ldap.la

# module for your local database

moduleload   back_hdb.la

# module for rewriting attributes

moduleload   rwm

# caching module

moduleload   pcache.la

# module to enable memberof in ldap

moduleload   memberof.la

# The maximum number of entries that is returned for a search operation

sizelimit    500

# The tool-threads parameter sets the actual amount of cpu's that is used
```

```
# for indexing.

tool-threads 1

# If you want to save time and don't want to list all the referrals, set "yes"

norefs yes

# Same as above

chase-referrals no

# See slapd-meta

# database type, for multiple ADS "meta" is required

database meta

# now we create a local ldap tree

# in our tree we put the multiple ADS on different branches

# we need a suffix, an admin, and a password

suffix "dc=owncloud,dc=com"

rootdn "cn=Administrator,cn=Users,dc=example,dc=com"

rootpw "Password"

# now we specify our ADS

# First-AD

# uri <protocol>://[<host>]/<naming context>

uri "ldap://first.ad.com:389/
cn=users,dc=first,dc=example,dc=com"

# here we need to set the virtual name to the real name

# the virtual name is a branch in our new created ldap tree

# suffixmassage <virtual naming context> <real naming context>

suffixmassage "cn=users,dc=first,dc=example,dc=com" "cn=users,dc=first,dc=ad,dc=com"

# authentication parameters

idassert-bind bindmethod=simple
binddn="cn=user01,cn=users,dc=first,dc=owncloud,dc=com"
credentials="Password01"

# Second-AD

uri "ldaps://second.ad.com:636/cn=users,dc=second,dc=example,dc=com"
suffixmassage "cn=users,dc=second,dc=example,dc=com" "cn=users,dc=second,dc=ad,dc=com"
```

```
idassert-bind    bindmethod=simple
                 binddn="cn=user02,cn=users,dc=second,dc=owncloud,dc=com"
                 credentials="Password02"

# Now we start initialising the modules
# First the rewrite module

overlay          rwm

# Now we rewrite the attributes

rwm-map          attribute uid sAMAccountName
rwm-map          attribute dn distinguishedName

# Next one is optional, if you want memberof, for the groups,
# you have to load it.

overlay          memberof

# Now we load the caching module

overlay pcache

# The directive enables proxy caching
# See slapo-pcache

# pcache <database> <max_entries> <numattrsets> <entry_limit> <cc_period>
# Parameters:
#
# <database> for cached entries.
# <max_entries> when reached - cache replacement is invoked
# <numattrsets> = pcacheAttrset
# <entry_limit> limit to the number of entries returned
# <cc_period> Consistency check time to wait

pcache hdb 100000 3 1000 100

# pcachePersist { TRUE | FALSE }
# Write cached results into the database
# Results remain in database after restart

pcachePersist TRUE

# Where the database files are physically stored for database #1

directory        "/var/lib/ldap"

# Caching templates for general search

# pcacheAttrset <index> <attrs...>
# First set the index number
# Then set the attribute to cache

pcacheAttrset    0 1.1

# pcacheTemplate <template_string> <attrset_index> <ttl>
# First define the query sting to cache
```

```

# Then reference the Attrset
# Last set the time-to-live

pccacheTemplate (&(|(objectClass=))) 0 3600

pccacheTemplate (objectClass=*) 0 3600

# User Name Field (Advanced Tab)

pccacheAttrset 1 displayname
pccacheTemplate (objectClass=*) 1 3600

# Group Field

pccacheAttrset 2 memberOf
pccacheTemplate (objectClass=*) 2 3600

```

6.4 Mimetypes Management

ownCloud allows you to create aliases for mimetypes and map file extensions to a mimetype. These allow administrators the ability to change the existing icons that ownCloud uses to represent certain file types and folders, as well as to use custom icons for mimetypes and file extensions which ownCloud doesn't natively support. This is handy in a variety of situations, such as when you might want a custom audio icon for audio mimetypes, instead of the default file icon.

6.4.1 Mimetype Aliases

ownCloud's default mimetype configuration is defined in `owncloud/resources/config/mimetypealiases.dist.json`, which you can see a snippet of below. The mimetype's on the left, and the icon used to represent that mimetype is on the right.

```

{
  "application/coreldraw": "image",
  "application/font-sfnt": "image",
  "application/font-woff": "image",
  "application/illustrator": "image",
  "application/epub+zip": "text",
  "application/javascript": "text/code",
}

```

Stepping through that file, you can see that:

- the image icon is used to represent Corel Draw, SFNT and WOFF font files, and Adobe Illustrator files.
- ePub files are represented by the text file icon.
- JavaScript files are represented by the text/code icon.

Changing Existing Icons and Using Custom Icons

If you want to change one or more of the existing icons which ownCloud uses, or if you want to expand the available list, here's how to do so.

First, create a copy of `resources/config/mimetypealiases.dist.json`, naming it `mimetypealiases.json` and storing it in `config/`. This is required for two reasons:

1. It will take precedence over the default file.
2. The original file will get replaced on each ownCloud upgrade.

Then, either override one or more existing definitions or add new, custom, aliases as required.

Note: Please refer to [the ownCloud theming documentation](#) for where to put the new image files.

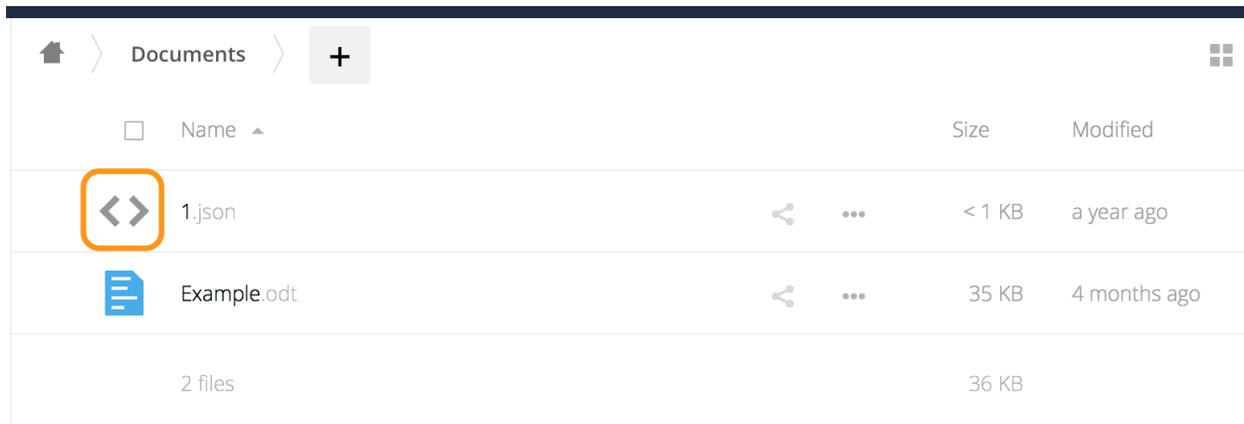
Some common mimetypes that may be useful in creating aliases are:

Mimetype	Description
image	Generic image
image/vector	Vector image
audio	Generic audio file
x-office/document	Word processed document
x-office/spreadsheet	Spreadsheet
x-office/presentation	Presentation
text	Generic text document
text/code	Source code

Once you have made changes to `config/mimetypealiases.json`, use *the occ command* to propagate the changes throughout your ownCloud installation. Here is an example for Ubuntu Linux:

```
$ sudo -u www-data php occ maintenance:mimetype:update-js
```

Example - Changing the JSON File Icon



Let's step through an example, from start to finish, of changing the icon that ownCloud uses to represent JSON files, which you can see above.

1. From the root directory of your ownCloud installation, copy `resources/config/mimetypealiases.dist.json` to `/config/mimetypealiases.json`.
2. Update the alias for `application/json`, which you should find on line 8, to match the following, and save the file:

```
"application/json": "text/json",
```

3. Copy a new SVG icon to represent JSON files to `core/img/filetypes`, calling it `text-json.svg`.

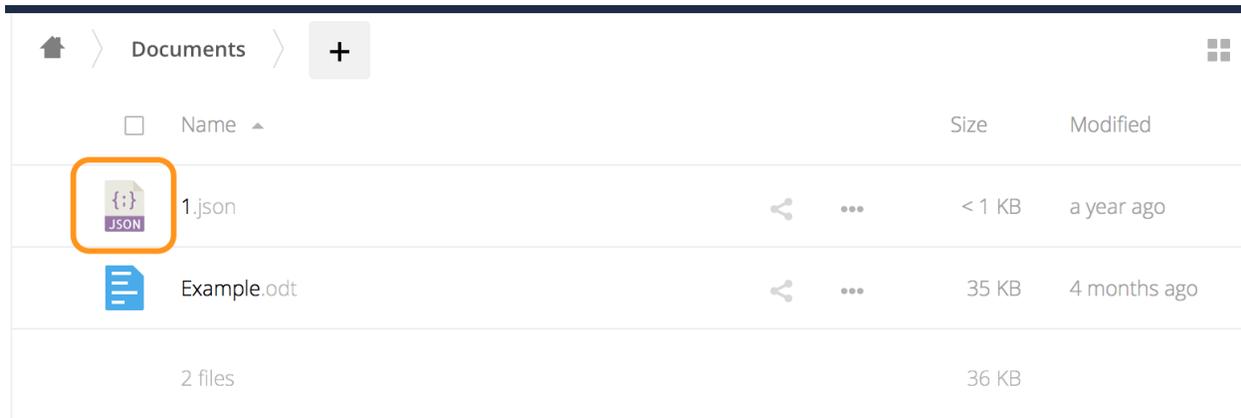
Note: The name and location of the file are important. The location is because the `core/img/filetypes`

directory stores the mimetype file icons. The name is important as it's a rough mapping between the alias name and the icon's file name, i.e., `text/json` becomes `text-json`.

4. Run the following command to update the mimetype alias database.

```
$ sudo -u www-data php occ maintenance:mimetype:update-js
```

After doing so, whenever you view a folder that contains JSON files or upload one, your new icon file will be used to represent the file, as in the image below.



6.4.2 Mimetype Mapping

ownCloud allows administrators to map a file extension to a mimetype, e.g., such as mapping files ending in `mp3` to `audio/mpeg`. Which then, in turn, allows ownCloud to show the audio icon.

The default file extension to mimetype mapping configuration is stored in `resources/config/mimetypermapping.dist.json`. This is similar to `resources/config/mimetypealiases.dist.json`, and also returns a basic JSON array.

```
{
  "3gp": ["video/3gpp"],
  "7z": ["application/x-7z-compressed"],
  "accdb": ["application/msaccess"],
  "ai": ["application/illustrator"],
  "apk": ["application/vnd.android.package-archive"],
  "arw": ["image/x-dcraw"],
  "avi": ["video/x-msvideo"],
  "bash": ["text/x-shellscript"],
  "json": ["application/json", "text/plain"],
}
```

In the example above, you can see nine mimetypes mapped to file extensions. Each of them, except the last (`json`), maps a file extension to a mimetype. Now take a look at the JSON example.

In this case, ownCloud will first check if a mimetype alias is defined for `application/json`, in `mimetypealiases.json`. If it is, it will use that icon. If not, then ownCloud will fall back to using the icon for `text/plain`.

If you want to update or extend the existing mapping, as with updating the mimetype aliases, create a copy of `resources/config/mimetypermapping.dist.json` and name it `mimetypermapping.json` and storing it in `config/`. Then, in this new file, make any changes required.

Note: Please refer to [the ownCloud theming documentation](#) for where to put the new image files.

6.4.3 Icon retrieval

When an icon is retrieved for a mimetype, if the full mimetype cannot be found, the search will fallback to looking for the part before the slash. Given a file with the mimetype `image/my-custom-image`, if no icon exists for the full mimetype, the icon for `image` will be used instead. This allows specialized mimetypes to fallback to generic icons when the relevant icons are unavailable.

6.5 Server Configuration

6.5.1 Warnings on Admin Page

Your ownCloud server has a built-in configuration checker, and it reports its findings at the top of your Admin page. These are some of the warnings you might see, and what to do about them.

Security & setup warnings

- **No memory cache has been configured. To enhance your performance please configure a memcache if available. Further information can be found in our documentation.**
- **You are accessing this site via HTTP. We strongly suggest you configure your server to require using HTTPS instead.**

Please double check the [installation guides](#) ↗, and check for any errors or warnings in the [log](#).

Cache Warnings

“No memory cache has been configured. To enhance your performance please configure a memcache if available.” ownCloud supports multiple php caching extensions:

- APCu
- Memcached
- Redis (minimum required PHP extension version: 2.2.6)

You will see this warning if you have no caches installed and enabled, or if your cache does not have the required minimum version installed; older versions are disabled because of performance problems.

If you see “*{Cache}* below version *{Version}* is installed. for stability and performance reasons we recommend to update to a newer *{Cache}* version” then you need to upgrade, or, if you’re not using it, remove it.

You are not required to use any caches, but caches improve server performance. See [Memory Caching](#).

Transactional file locking is disabled

“Transactional file locking is disabled, this might lead to issues with race conditions.”

Please see [Transactional File Locking](#) for how to correctly configure your environment for transactional file locking.

You are accessing this site via HTTP

“You are accessing this site via HTTP. We strongly suggest you configure your server to require using HTTPS instead.” Please take this warning seriously; using HTTPS is a fundamental security measure. You must configure your Web server to support it, and then there are some settings in the **Security** section of your ownCloud Admin page to enable. The following pages describe how to enable HTTPS on the Apache and Nginx Web servers.

Enable SSL (on Apache)

Use HTTPS

The test with getenv(“PATH”) only returns an empty response

Some environments are not passing a valid PATH variable to ownCloud. The *PHP-FPM* provides the information about how to configure your environment.

The “Strict-Transport-Security” HTTP header is not configured

“The “Strict-Transport-Security” HTTP header is not configured to least “15552000” seconds. For enhanced security we recommend enabling HSTS as described in our security tips.”

The HSTS header needs to be configured within your Web server by following the *Enable HTTP Strict Transport Security* documentation

/dev/urandom is not readable by PHP

“/dev/urandom is not readable by PHP which is highly discouraged for security reasons. Further information can be found in our documentation.”

This message is another one which needs to be taken seriously. Please have a look at the *Give PHP read access to /dev/urandom* documentation.

Your Web server is not yet set up properly to allow file synchronization

“Your web server is not yet set up properly to allow file synchronization because the WebDAV interface seems to be broken.”

At the ownCloud community forums a larger [FAQ](#) is maintained containing various information and debugging hints.

Outdated NSS / OpenSSL version

“cURL is using an outdated OpenSSL version (OpenSSL/\$version). Please update your operating system or features such as installing and updating apps via the ownCloud Marketplace or Federated Cloud Sharing will not work reliably.”

“cURL is using an outdated NSS version (NSS/\$version). Please update your operating system or features such as installing and updating apps via the ownCloud Marketplace or Federated Cloud Sharing will not work reliably.”

There are known bugs in older OpenSSL and NSS versions leading to misbehaviour in combination with remote hosts using SNI. A technology used by most of the HTTPS websites. To ensure that ownCloud will work properly you need to update OpenSSL to at least 1.0.2b or 1.0.1d. For NSS the patch version depends on your distribution and an heuristic is running the test which actually reproduces the bug. There are distributions such as RHEL/CentOS which have this backport still [pending](#).

Your Web server is not set up properly to resolve `/.well-known/caldav/` or `/.well-known/carddav/`

Both URLs need to be correctly redirected to the DAV endpoint of ownCloud. Please refer to *Service discovery* for more info.

Some files have not passed the integrity check

Please refer to the *Fixing Invalid Code Integrity Messages* documentation how to debug this issue.

Your database does not run with “READ COMMITTED” transaction isolation level

“Your database does not run with “READ COMMITTED” transaction isolation level. This can cause problems when multiple actions are executed in parallel.”

Please refer to *MySQL / MariaDB “READ COMMITTED” transaction isolation level* how to configure your database for this requirement.

6.5.2 Importing System-wide and Personal SSL Certificates

Modern Web browsers try to keep us safe, and so they blast us with scary warnings when sites have the smallest errors in their SSL certificates, or when they use self-signed SSL certificates. ownCloud admins encounter this when creating Federation shares, or setting up external storage mounts. There is no reason against using self-signed certificates on your own networks; they’re fast, free, and easy.

Importing Personal SSL Certificates

ownCloud has several methods for importing self-signed certificates so that you don’t have to hassle with Web browser warnings. When you allow your users to create their own external storage mounts or Federation shares, they can import SSL certificates for those shares on their Personal pages.

SSL Root Certificates

A rectangular button with a light gray background and a dark gray border. The text "Import root certificate" is centered on the button in a bold, dark gray font.

Click the **Import root certificate** button to open a file picker. You can distribute copies of your SSL certificates to your users (via an ownCloud share!), or users can download them from their Web browsers. Click on the little padlock icon and click through until you see a **View Certificate** button, then keep going until you can download it. In Firefox and Chromium there is an **Export** button for downloading your own copy of a site’s SSL certificate.

Site-wide SSL Import

The personal imports only work for individual users. You can enable site-wide SSL certificates for all of your users on your ownCloud admin page. To enable this, you must add this line to your `config.php` file:

```
'enable_certificate_management' => true,
```

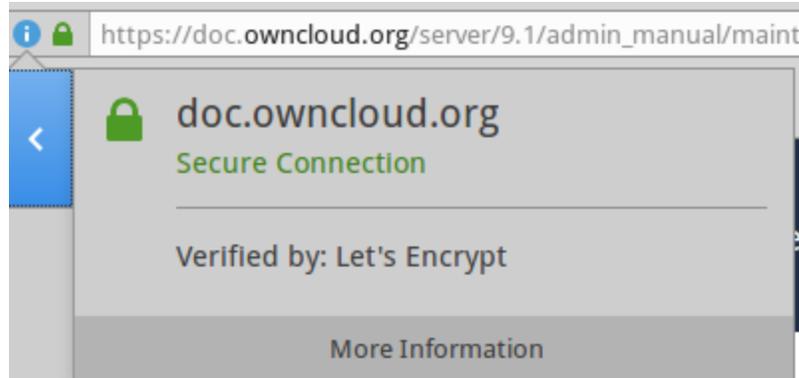


Figure 6.1: Click “More information” in Firefox to import SSL certificate

Then you’ll have a **Import root certificate** button on your admin page, just like the one on your personal page. Navigate to it by clicking “*admin -> Settings -> (Admin) General*” and then scroll almost to the bottom, where you will find the “*SSL Root Certificates*” section.

Using OCC to Import and Manage SSL Certificates

The `occ` command has options for listing and managing your SSL certificates:

```
security:certificates          list trusted certificates
security:certificates:import  import trusted certificate
security:certificates:remove  remove trusted certificate
```

See *Using occ core commands* to learn about how to use `occ`.

6.5.3 Using occ core commands

This command description references to ownCloud core commands only.

ownCloud’s `occ` command (ownCloud console) is ownCloud’s command-line interface. You can perform many common server operations with `occ`, such as installing and upgrading ownCloud, managing users and groups, encryption, passwords, LDAP setting, and more.

`occ` is in the `owncloud/` directory; for example `/var/www/owncloud` on Ubuntu Linux. `occ` is a PHP script. **You must run it as your HTTP user** to ensure that the correct permissions are maintained on your ownCloud files and directories.

occ Command Directory

- *Run occ As Your HTTP User*
- *Commands managing Apps*
- *Background Jobs Selector*
- *Config Commands*
- *Dav Commands*
- *Database Conversion*
- *Encryption*

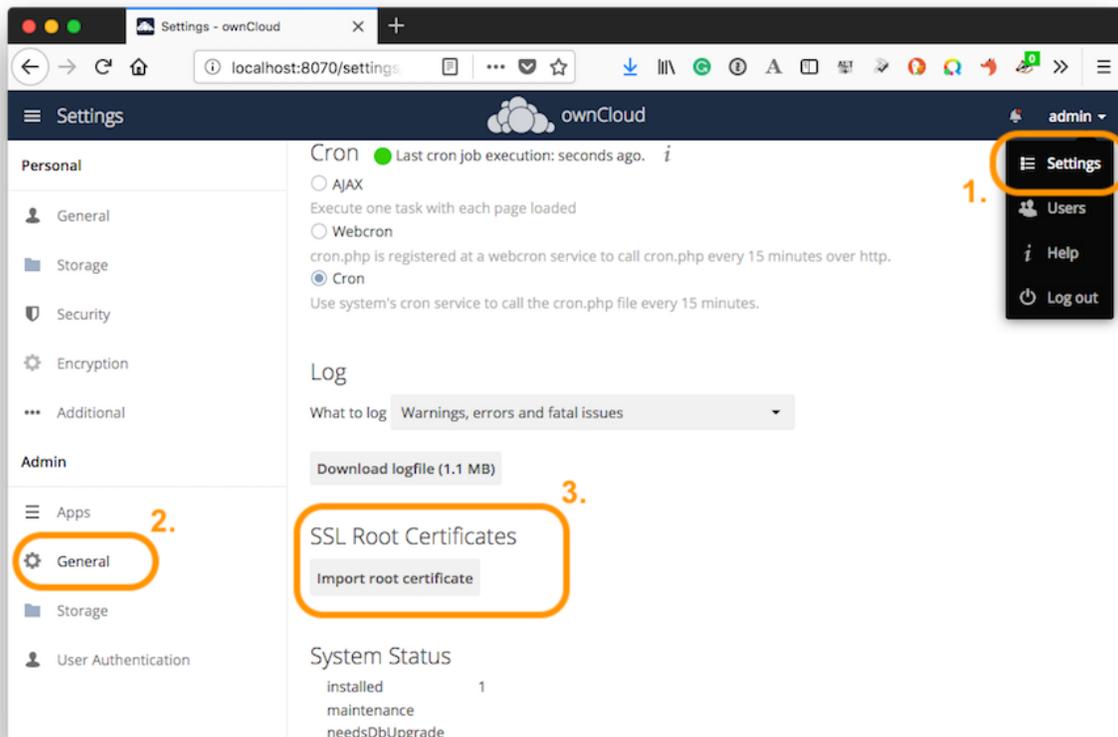


Figure 6.2: Site-wide SSL Root Certificate Import

- *Federation Sync*
- *File Operations*
- *Files External*
- *Group Commands*
- *Integrity Check*
- *l10n, Create Javascript Translation Files for Apps*
- *Logging Commands*
- *Maintenance Commands*
- *Security*
- *Trashbin*
- *User Commands*
- *Versions*
- *Command Line Installation*
- *Command Line Upgrade*
- *Disable Users*

Run occ As Your HTTP User

The HTTP user is different on the various Linux distributions. See *Set Strong Directory Permissions* to learn how to find your HTTP user.

- The HTTP user and group in Debian/Ubuntu is www-data.
- The HTTP user and group in Fedora/CentOS is apache.
- The HTTP user and group in Arch Linux is http.
- The HTTP user in openSUSE is wwwrun, and the HTTP group is www.

If your HTTP server is configured to use a different PHP version than the default (`/usr/bin/php`), `occ` should be run with the same version. For example, in CentOS 6.5 with SCL-PHP54 installed, the command looks like this:

```
sudo -u apache /opt/rh/php54/root/usr/bin/php /var/www/html/owncloud/occ
```

The following examples are based on Ubuntu.

Running `occ` with no options lists all commands and options

```
sudo -u www-data php occ
ownCloud version 10.0.8
```

Usage:

```
command [options] [arguments]
```

Options:

```
-h, --help           Display this help message
-q, --quiet          Do not output any message
-V, --version        Display this application version
    --ansi           Force ANSI output
    --no-ansi        Disable ANSI output
-n, --no-interaction Do not ask any interactive question
```

```
    --no-warnings      Skip global warnings, show command output only
-v|vv|vvv, --verbose  Increase the verbosity of messages: 1 for normal output,
                      2 for more verbose output and 3 for debug
```

Available commands:

```
check      Check dependencies of the server environment
help      Displays help for a command
list      Lists commands
status    Show some status information
upgrade   Run upgrade routines after installation of
          a new release. The release has to be installed before
```

This is the same as `sudo -u www-data php occ list`.

General syntax help

Run `occ` with the `-h` option for syntax help

```
sudo -u www-data php occ -h
```

Display your ownCloud version

```
sudo -u www-data php occ -V
ownCloud version 10.0.8
```

Query your ownCloud server status

```
sudo -u www-data php occ status
- installed: true
- version: 10.0.8.5
- versionstring: 10.0.8
- edition: Community
```

Command syntax help

Get detailed information on individual commands with the `help` command, like this example for the `maintenance:mode` command

```
sudo -u www-data php occ --help maintenance:mode
Usage:
maintenance:mode [options]
```

Options:

```
    --on              Enable maintenance mode
    --off            Disable maintenance mode
    --output[=OUTPUT] Output format (plain, json or json_pretty, default is plain) [default: "plain"]
-h, --help          Display this help message
-q, --quiet         Do not output any message
-V, --version       Display this application version
    --ansi          Force ANSI output
    --no-ansi       Disable ANSI output
-n, --no-interaction Do not ask any interactive question
```

```
--no-warnings      Skip global warnings, show command output only
-v|vv|vvv, --verbose  Increase the verbosity of messages: 1 for normal output,
                      2 for more verbose output and 3 for debug
```

Options and Arguments

occ has *options*, *commands*, and *arguments*. Commands are required. Options are optional. Arguments can be required *or* optional. The, generic, syntax is

```
occ [options] command [arguments]
```

The status command from above has an option to define the output format.

The default is plain text, but it can also be json

```
sudo -u www-data php occ status --output=json
{"installed":true,"version":"9.0.0.19","versionstring":"9.0.0","edition":""}
```

or json_pretty

```
sudo -u www-data php occ status --output=json_pretty
{
  "installed": true,
  "version": "10.0.8.5",
  "versionstring": "10.0.8",
  "edition": "Community"
}
```

This output option is available on all list and list-like commands, which include status, check, app:list, config:list, encryption:status and encryption:list-modules.

Usage of parameters in Options

In case an option requires parameters, following format should be used for short or long Options forms

The following example command has an option in -p (short) form and --path (long) form.

Parameters for long form options will be written after a blank or equal sign

```
sudo -u www-data ./occ files:scan --path="user_x/files/folder"
```

Parameters for short form options will be written either directly after the option or after a blank. Do not use the equal sign as this could be interpreted as part of the parameter.

```
sudo -u www-data ./occ files:scan -p "user_x/files/folder"
```

Commands managing Apps

The app commands list, enable, and disable apps

```
app
app:check-code    check code to be compliant
app:disable      disable an app
app:enable       enable an app
app:getpath      Get an absolute path to the app directory
app:list         List all available apps
```

List all of your installed apps or optionally provide a search pattern to restrict the list of apps to those whose name matches the given regular expression. The output shows whether they are enabled or disabled

```
sudo -u www-data php occ app:list [<search-pattern>]
```

Enable an app, for example the Market app

```
sudo -u www-data php occ app:enable market
market enabled
```

Disable an app

```
sudo -u www-data php occ app:disable market
market disabled
```

Note: Be aware that the following apps cannot be disabled: *DAV*, *FederatedFileSharing*, *Files* and *Files_External*.

`app:check-code` has multiple checks: it checks if an app uses ownCloud's public API (OCP) or private API (OC_), and it also checks for deprecated methods and the validity of the `info.xml` file. By default all checks are enabled. The Activity app is an example of a correctly-formatted app

```
sudo -u www-data php occ app:check-code notifications
App is compliant - awesome job!
```

If your app has issues, you'll see output like this

```
sudo -u www-data php occ app:check-code foo_app
Analysing /var/www/owncloud/apps/files/foo_app.php
4 errors
  line 45: OCP\Response - Static method of deprecated class must not be
  called
  line 46: OCP\Response - Static method of deprecated class must not be
  called
  line 47: OCP\Response - Static method of deprecated class must not be
  called
  line 49: OC_Util - Static method of private class must not be called
```

You can get the full file path to an app

```
sudo -u www-data php occ app:getpath notifications
/var/www/owncloud/apps/notifications
```

Note: Please see the command set `market` for managing apps (install, uninstall ect) from the marketplace

Background Jobs Selector

Use the `background` command to select which scheduler you want to use for controlling *background jobs*, *Ajax*, *Webcron*, or *Cron*. This is the same as using the **Cron** section on your ownCloud Admin page.

```
background
background:ajax      Use ajax to run background jobs
background:cron      Use cron to run background jobs
background:webcron   Use webcron to run background jobs
```

This example selects Ajax:

```
sudo -u www-data php occ background:ajax
Set mode for background jobs to 'ajax'
```

The other two commands are:

- background:cron
- background:webcron

See *Background Jobs* to learn more.

Config Commands

The `config` commands are used to configure the ownCloud server.

```
config
config:app:delete    Delete an app config value
config:app:get       Get an app config value
config:app:set       Set an app config value
config:import        Import a list of configuration settings
config:list          List all configuration settings
config:system:delete Delete a system config value
config:system:get    Get a system config value
config:system:set    Set a system config value
```

You can list all configuration values with one command:

```
sudo -u www-data php occ config:list
```

By default, passwords and other sensitive data are omitted from the report, so the output can be posted publicly (e.g., as part of a bug report). In order to generate a full backport of all configuration values the `--private` flag needs to be set:

```
sudo -u www-data php occ config:list --private
```

The exported content can also be imported again to allow the fast setup of similar instances. The `import` command will only add or update values. Values that exist in the current configuration, but not in the one that is being imported are left untouched.

```
sudo -u www-data php occ config:import filename.json
```

It is also possible to import remote files, by piping the input:

```
sudo -u www-data php occ config:import < local-backup.json
```

Note: While it is possible to update/set/delete the versions and installation statuses of apps and ownCloud itself, it is **not** recommended to do this directly. Use the `occ app:enable`, `occ app:disable` and `occ update` commands instead.

Getting a Single Configuration Value

These commands get the value of a single app or system configuration:

```
sudo -u www-data php occ config:system:get version
10.0.8.5
```

```
sudo -u www-data php occ config:app:get activity installed_version
2.2.1
```

Setting a Single Configuration Value

These commands set the value of a single app or system configuration:

```
sudo -u www-data php occ config:system:set logtimezone
  --value="Europe/Berlin"
System config value logtimezone set to Europe/Berlin
```

```
sudo -u www-data php occ config:app:set files_sharing
incoming_server2server_share_enabled --value="yes" --type=boolean
Config value incoming_server2server_share_enabled for app files_sharing set to yes
```

The `config:system:set` command creates the value, if it does not already exist. To update an existing value, set `--update-only`:

```
sudo -u www-data php occ config:system:set doesnotexist --value="true"
  --type=boolean --update-only
Value not updated, as it has not been set before.
```

Note that in order to write a boolean, float, JSON, or integer value to the configuration file, you need to specify the type on your command. This applies only to the `config:system:set` command. The following values are known:

- boolean
- integer
- float
- json
- string (default)

Examples Disable the maintenance mode:

```
sudo -u www-data php occ config:system:set maintenance \
  --value=false
  --type=boolean
```

```
ownCloud is in maintenance mode - no app have been loaded
System config value maintenance set to boolean false
```

Create the `app_paths` config setting (using a JSON payload):

```
sudo -u www-data php occ config:system:set apps_paths \
  --type=json \
  --value=' [{"path":"/var/www/owncloud/apps", "url":"apps", "writable":1}, {"path":"/var/www/owncloud/a
```

Setting an Array of Configuration Values

Some configurations (e.g., the trusted domain setting) are an array of data. In order to set (and also get) the value of one key, you can specify multiple `config` names separated by spaces:

```
sudo -u www-data php occ config:system:get trusted_domains localhost owncloud.local sample.tld
```

To replace `sample.tld` with `example.com` `trusted_domains => 2` needs to be set:

```
sudo -u www-data php occ config:system:set trusted_domains 2
--value=example.com
System config value trusted_domains => 2 set to string example.com

sudo -u www-data php occ config:system:get trusted_domains localhost owncloud.local example.com
```

Deleting a Single Configuration Value

These commands delete the configuration of an app or system configuration:

```
sudo -u www-data php occ config:system:delete maintenance:mode
System config value maintenance:mode deleted

sudo -u www-data php occ config:app:delete appname provisioning_api
Config value provisioning_api of app appname deleted
```

The delete command will by default not complain if the configuration was not set before. If you want to be notified in that case, set the `--error-if-not-exists` flag.

```
sudo -u www-data php occ config:system:delete doesnotexist --error-if-not-exists
Config provisioning_api of app appname could not be deleted because it did not exist
```

Dav Commands

A set of commands to create address books, calendars, and to migrate address books:

```
dav
dav:cleanup-chunks           Cleanup outdated chunks
dav:create-addressbook      Create a dav address book
dav:create-calendar         Create a dav calendar
dav:sync-birthday-calendar  Synchronizes the birthday calendar
dav:sync-system-addressbook Synchronizes users to the system address book
```

Note: These commands are not available in *single-user (maintenance) mode*.

`dav:cleanup-chunks` cleans up outdated chunks (uploaded files) more than a certain number of days old. By default, the command cleans up chunks more than 2 days old. However, by supplying the number of days to the command, the range can be increased. For example, in the example below, chunks older than 10 days will be removed.

```
sudo -u www-data php occ dav:cleanup-chunks 10

# example output
Cleaning chunks older than 10 days(2017-11-08T13:13:45+00:00)
Cleaning chunks for admin
  0 [>-----]
```

The syntax for `dav:create-addressbook` and `dav:create-calendar` is `dav:create-addressbook [user] [name]`. This example creates the addressbook `mollybook` for the user `molly`:

```
sudo -u www-data php occ dav:create-addressbook molly mollybook
```

This example creates a new calendar for `molly`:

```
sudo -u www-data php occ dav:create-calendar molly mollycal
```

Molly will immediately see these on her Calendar and Contacts pages. Your existing calendars and contacts should migrate automatically when you upgrade. If something goes wrong you can try a manual migration. First delete any partially-migrated calendars or address books. Then run this command to migrate user's contacts:

```
sudo -u www-data php occ dav:migrate-addressbooks [user]
```

Run this command to migrate calendars:

```
sudo -u www-data php occ dav:migrate-calendars [user]
```

`dav:sync-birthday-calendar` adds all birthdays to your calendar from address books shared with you. This example syncs to your calendar from user `bernie`:

```
sudo -u www-data php occ dav:sync-birthday-calendar bernie
```

`dav:sync-system-addressbook` synchronizes all users to the system addressbook.

```
sudo -u www-data php occ dav:sync-system-addressbook
```

Database Conversion

The SQLite database is good for testing, and for ownCloud servers with small single-user workloads that do not use sync clients, but production servers with multiple users should use MariaDB, MySQL, or PostgreSQL. You can use `occ` to convert from SQLite to one of these other databases.

```
db
db:convert-type          Convert the ownCloud database to the newly configured one
db:generate-change-script Generates the change script from the current
                        connected db to db_structure.xml
```

You need:

- Your desired database and its PHP connector installed.
- The login and password of a database admin user.
- The database port number, if it is a non-standard port.

This is example converts SQLite to MySQL/MariaDB:

```
sudo -u www-data php occ db:convert-type mysql oc_dbuser 127.0.0.1 oc_database
```

For a more detailed explanation see [Converting Database Type](#).

Encryption

`occ` includes a complete set of commands for managing encryption.

```
encryption
encryption:change-key-storage-root  Change key storage root
encryption:decrypt-all             Disable server-side encryption and decrypt all files
encryption:disable                  Disable encryption
encryption:enable                    Enable encryption
encryption:encrypt-all             Encrypt all files for all users
encryption:list-modules              List all available encryption modules
encryption:migrate                  initial migration to encryption 2.0
encryption:recreate-master-key      Replace existing master key with new one. Encrypt the file system
```

```

newly created master key
encryption:select-encryption-type  Select the encryption type. The encryption types available are:
user-keys. There is also no way to disable it again.
encryption:set-default-module      Set the encryption default module
encryption:show-key-storage-root   Show current key storage root
encryption:status                  Lists the current status of encryption

```

`encryption:status` shows whether you have active encryption, and your default encryption module. To enable encryption you must first enable the Encryption app, and then run `encryption:enable`:

```

sudo -u www-data php occ app:enable encryption
sudo -u www-data php occ encryption:enable
sudo -u www-data php occ encryption:status
- enabled: true
- defaultModule: OC_DEFAULT_MODULE

```

`encryption:change-key-storage-root` is for moving your encryption keys to a different folder. It takes one argument, `newRoot`, which defines your new root folder. The folder must exist, and the path is relative to your root ownCloud directory.

```
sudo -u www-data php occ encryption:change-key-storage-root ../../etc/oc-keys
```

You can see the current location of your keys folder:

```
sudo -u www-data php occ encryption:show-key-storage-root
Current key storage root: default storage location (data/)
```

`encryption:list-modules` displays your available encryption modules. You will see a list of modules only if you have enabled the Encryption app. Use `encryption:set-default-module [module name]` to set your desired module.

`encryption:encrypt-all` encrypts all data files for all users. You must first put your ownCloud server into *single-user mode* to prevent any user activity until encryption is completed.

`encryption:decrypt-all` decrypts all user data files, or optionally a single user:

```
sudo -u www-data php occ encryption:decrypt freda
```

Users must have enabled recovery keys on their Personal pages. You must first put your ownCloud server into *single-user mode* to prevent any user activity until decryption is completed.

Use `encryption:disable` to disable your encryption module. You must first put your ownCloud server into *single-user mode* to prevent any user activity.

`encryption:migrate` migrates encryption keys after a major ownCloud version upgrade. You may optionally specify individual users in a space-delimited list. See [Encryption Configuration](#) to learn more.

`encryption:recreate-master-key` decrypts the ownCloud file system, replaces the existing master key with a new one, and encrypts the entire ownCloud file system with the new master key. Given the size of your ownCloud filesystem, this may take some time to complete. However, if your filesystem is quite small, then it will complete quite quickly. The `-y` switch can be supplied to automate acceptance of user input.

Federation Sync

Synchronize the address books of all federated ownCloud servers.

```
federation:sync-addressbooks  Synchronizes address books of all federated clouds
```

Servers connected with federation shares can share user address books, and auto-complete usernames in share dialogs. Use this command to synchronize federated servers:

```
sudo -u www-data php occ federation:sync-addressbooks
```

Note: This command is only available when the “Federation” app (`federation`) is enabled.

File Operations

`occ` has three commands for managing files in ownCloud.

```
files
files:checksums:verify    Get all checksums in filecache and compares them by
                           recalculating the checksum of the file.
files:cleanup             Deletes orphaned file cache entries.
files:scan                Rescans the filesystem.
files:transfer-ownership All files and folders are moved to another user
                           - outgoing shares are moved as well (incoming shares are
                           not moved as the sharing user holds the ownership of the respective files)
```

Note: These commands are not available in *single-user (maintenance) mode*.

The `files:checksums:verify` command

ownCloud supports file integrity checking, by computing and matching checksums. Doing so ensures that transferred files arrive at their target in the exact state as they left their origin.

In some rare cases, wrong checksums are written to the database which leads to synchronization issues, such as with the Desktop Client. To mitigate such problems a new command is available: `occ files:checksums:verify`.

Executing the command recalculates checksums, either for all files of a user or within a specified filesystem path on the designated storage. It then compares them with the values in the database. The command also offers an option to repair incorrect checksum values (`-r`, `--repair`).

Note: Executing this command might take some time depending on the file count.

Below is sample output that you can expect to see when using the command.

```
./occ files:checksums:verify
This operation might take very long.
Mismatch for files/welcome.txt:
  Filecache:  SHA1:eeb2c08011374d8ad4e483a4938e1aa1007c089d MD5:368e3a6cb99f88c3543123931d786e21 ADL
  Actual:     SHA1:da39a3ee5e6b4b0d3255bfe95601890afd80709 MD5:d41d8cd98f00b204e9800998ecf8427e ADL
Mismatch for thumbnails/9/2048-2048-max.png:
  Filecache:  SHA1:2634fed078d1978f24f71892bf4ee0e4bd0c3c99 MD5:dd249372f7a68c551f7e6b2615d49463 ADL
  Actual:     SHA1:da39a3ee5e6b4b0d3255bfe95601890afd80709 MD5:d41d8cd98f00b204e9800998ecf8427e ADL
```

The `files:cleanup` command

`files:cleanup` tidies up the server’s file cache by deleting all file entries that have no matching entries in the storage table.

The files:scan command

The `files:scan` command

- Scans for new files.
- Scans not fully scanned files.
- Repairs file cache holes.
- Updates the file cache.

File scans can be performed per-user, for a space-delimited list of users, for groups of users, and for all users.

```
sudo -u www-data php occ files:scan --help
```

Usage:

```
files:scan [options] [--] [<user_id>]...
```

Arguments:

```
user_id          Will rescan all files of the given user(s)
```

Options:

```
--output[=OUTPUT] Output format (plain, json or json_pretty, default is plain) [default: "plain"]
-p, --path=PATH    Limit rescan to this path, eg. --path="/alice/files/Music", the user_id is
-g, --groups=GROUPS Scan user(s) under the group(s). This option can be used as --groups=foo,bar
-q, --quiet        Do not output any message
--all             Will rescan all files of all known users
--repair         Will repair detached filecache entries (slow)
--unscanned      Only scan files which are marked as not fully scanned
-h, --help        Display this help message
-V, --version     Display this application version
--ansi           Force ANSI output
--no-ansi        Disable ANSI output
-n, --no-interactive Do not ask any interactive question
--no-warnings     Skip global warnings, show command output only
-v|vv|vvv, --verbose Increase the verbosity of messages: 1 for normal output, 2 for more verbose
```

Note: If not using `--quiet`, statistics will be shown at the end of the scan.

The `--path` Option

When using the `--path` option, the path must be in one of the following formats:

```
"user_id/files/path"
"user_id/files/mount_name"
"user_id/files/mount_name/path"
```

For example:

```
--path="/alice/files/Music"
```

In the example above, the `user_id` `alice` is determined implicitly from the path component given.

To get a list of scannable mounts for a given user, use following command:

```
sudo -u www-data php occ files_external:list user_id
```

Note: Mounts are only scannable at the point of origin. Scanning of shares including federated shares is not necessary

on the receiver side and therefore not possible.

The `--path`, `--all`, `--groups` and `[user_id]` parameters are exclusive - only one must be specified.

The `--repair` Option

As noted above, repairs can be performed for individual users, groups of users, and for all users in an ownCloud installation. What's more, repair scans can be run even if no files are known to need repairing and if one or more files are known to be in need of repair. Two examples of when files need repairing are:

- If folders have the same entry twice in the web UI (known as a “*ghost folder*”), this can also lead to strange error messages in the desktop client.
- If entering a folder doesn't seem to lead into that folder.

The repair command needs to be run in single user mode. The following commands show how to enable single user mode, run a repair file scan, and then disable single user mode.

```
sudo -u www-data php occ maintenance:singleuser --on
sudo -u www-data php occ files:scan --all --repair
sudo -u www-data php occ maintenance:singleuser --off
```

Note: We strongly suggest that you backup the database before running this command.

The `files:transfer-ownership` command You may transfer all files and shares from one user to another. This is useful before removing a user. For example, to move all files from `<source-user>` to `<destination-user>`, use the following command:

```
sudo -u www-data php occ files:transfer-ownership <source-user> <destination-user>
```

You can also move a limited set of files from `<source-user>` to `<destination-user>` by making use of the `--path` switch, as in the example below. In it, `folder/to/move`, and any file and folder inside it will be moved to `<destination-user>`.

```
sudo -u www-data php occ files:transfer-ownership --path="folder/to/move" <source-user> <destination-user>
```

When using this command, please keep in mind:

1. The directory provided to the `--path` switch **must** exist inside `data/<source-user>/files`.
2. The directory (and its contents) won't be moved as is between the users. It'll be moved inside the destination user's `files` directory, and placed in a directory which follows the format: transferred from `<source-user>` on `<timestamp>`. Using the example above, it will be stored under: `data/<destination-user>/files/transferred from <source-user> on 20170426_124510/`
3. Currently file versions can't be transferred. Only the latest version of moved files will appear in the destination user's account.

Files External

These commands replace the `data/mount.json` configuration file used in ownCloud releases before 9.0.

Commands for managing external storage.

```

files_external
files_external:applicable  Manage applicable users and groups for a mount
files_external:backends   Show available authentication and storage backends
files_external:config     Manage backend configuration for a mount
files_external:create     Create a new mount configuration
files_external:delete     Delete an external mount
files_external:export     Export mount configurations
files_external:import     Import mount configurations
files_external:list       List configured mounts
files_external:option     Manage mount options for a mount
files_external:verify     Verify mount configuration

```

These commands replicate the functionality in the ownCloud Web GUI, plus two new features: `files_external:export` and `files_external:import`.

Use `files_external:export` to export all admin mounts to stdout, and `files_external:export [user_id]` to export the mounts of the specified ownCloud user.

Note: These commands are only available when the “External storage support” app (`files_external`) is enabled. It is not available in *single-user (maintenance) mode*.

`files_external:list`

List configured mounts.

Usage:

```
files_external:list [--show-password] [--full] [-a|--all] [--] [<user_id>]
```

Arguments:

<code>user_id</code>	User ID to list the personal mounts for, if no user is provided admin mounts will be listed.
----------------------	----------------------------------------------------------------------------------------------

Example:

```
sudo -u www-data php occ files_external:list -- user1
```

`files_external:applicable`

Manage applicable users and groups for a mount.

Usage:

```

files_external:applicable
[--add-user      ADD-USER]
[--remove-user   REMOVE-USER]
[--add-group     ADD-GROUP]
[--remove-group  REMOVE-GROUP]
[--remove-all]
[--output       [OUTPUT]]
[--]
<mount_id>

```

Arguments:

<code>mount_id</code>	The ID of the mount to edit
-----------------------	-----------------------------

Options:

<code>--add-user</code>	user to add as applicable (multiple values allowed)
<code>--remove-user</code>	user to remove as applicable (multiple values allowed)
<code>--add-group</code>	group to add as applicable (multiple values allowed)
<code>--remove-group</code>	group to remove as applicable (multiple values allowed)
<code>--remove-all</code>	Set the mount to be globally applicable
<code>--output</code>	The output format to use (plain, json or json_pretty, default is plain).

files_external:backends

Show available authentication and storage backends.

Usage:

```
files_external:backends [options]
[--]
[<type>]
[<backend>]
```

Arguments:

type	Only show backends of a certain type. Possible values are authentication or storage.
backend	Only show information of a specific backend.

Options:

<code>--output</code>	The output format to use (plain, json or json_pretty, default is plain).
-----------------------	--------------------------------------------------------------------------

files_external:config

Manage backend configuration for a mount.

Usage:

```
files_external:config [options]
[--]
<mount_id>
<key>
[<value>]
```

Arguments:

mount_id	The ID of the mount to edit.
key	Key of the config option to set/get.
value	Value to set the config option to, when no value is provided the existing value will be printed.

Options:

<code>--output</code>	The output format to use (plain, json or json_pretty, default is plain).
-----------------------	--------------------------------------------------------------------------

files_external:create

Create a new mount configuration.

Usage:

```
files_external:create [options]
[--]
<mount_point>
<storage_backend>
<authentication_backend>
```

Arguments	mount_point	Mount point for the new mount.
	storage_backend	Storage backend identifier for the new mount, see <i>occ files_external:backends</i> for possible values.
	authentication_backend	Authentication backend identifier for the new mount, see <i>occ files_external:backends</i> for possible values.

Options	--user [=USER]	User to add the mount configurations for, if not set the mount will be added as system mount.
	-c,	Mount configuration option in <i>key=value</i> format (multiple values allowed).
	--config=CONFIG	
	--dry	Don't save the imported mounts, only list the new mounts.
--output	The output format to use (plain, json or json_pretty, default is plain).	

Storage Backend	Identifier
Windows Network Drive	windows_network_drive
WebDav	dav
Local	local
ownCloud	owncloud
SFTP	sftp
Amazon S3	amazons3
Dropbox	dropbox
Google Drive	googledrive
OpenStack Object Storage	swift
SMB / CIFS	smb

Authentication method	Identifier, name, configuration
Log-in credentials, save in session	password::sessioncredentials
Log-in credentials, save in database	password::logincredentials
User entered, store in database	password::userprovided (*)
Global Credentials	password::global
None	null::null
Builtin	builtin::builtin
Username and password	password::password
OAuth1	oauth1::oauth1 (*)
OAuth2	oauth2::oauth2 (*)
RSA public key	publickey::rsa (*)
OpenStack	openstack::openstack (*)
Rackspace	openstack::rackspace (*)
Access key (Amazon S3)	amazons3::accesskey (*)

(*) - Authentication methods require additional configuration.

Note: Each Storage Backend needs its corresponding authentication methods.

files_external:delete

Delete an external mount.

Usage:

```
files_external:delete [options] [--] <mount_id>
```

Arguments:

mount_id	The ID of the mount to edit.
----------	------------------------------

Options:

-y, --yes	Skip confirmation.
--output	The output format to use (plain, json or json_pretty, default is plain).

files_external:export

Usage:

```
files_external:export [options] [--] [<user_id>]
```

Arguments:

user_id	User ID to export the personal mounts for, if no user is provided admin mounts will be exported.
---------	--------------------------------------------------------------------------------------------------

Options:

-a, --all	Show both system wide mounts and all personal mounts.
-----------	-------------------------------------------------------

files_external:import

Import mount configurations.

Usage:

```
files_external:import [options] [--] <path>
```

Arguments:

path	Path to a json file containing the mounts to import, use - to read from stdin.
------	--------------------------------------------------------------------------------

Options:

--user[=USER]	User to add the mount configurations for, if not set the mount will be added as system mount.
--dry	Don't save the imported mounts, only list the new mounts.
--output	The output format to use (plain, json or json_pretty, default is plain).

files_external:list

List configured mounts.

Usage:

```
files_external:list [--show-password] [--full] [-a|--all] [--] [<user_id>]
```

Arguments:

user_id	User ID to list the personal mounts for, if no user is provided admin mounts will be listed.
---------	----------------------------------------------------------------------------------------------

Options:

--show-password	User to add the mount configurations for, if not set the mount will be added as system mount.
--full	Don't save the imported mounts, only list the new mounts.
-a, --all	Show both system wide mounts and all personal mounts.
--output	The output format to use (plain, json or json_pretty, default is plain).

Example:

```
sudo -u www-data php occ files_external:list -- user1
```

files_external:option

Manage mount options for a mount.

Usage:: files_external:option <mount_id> <key> [<value>]

Arguments:

mount_id	The ID of the mount to edit.
key	Key of the mount option to set/get.
value	Value to set the mount option to, when no value is provided the existing value will be printed.

files_external:verify

Verify mount configuration.

Usage:

```
files_external:verify [options] [--] <mount_id>
```

Arguments:

mount_id	The ID of the mount to check.
----------	-------------------------------

Options:

-c,	Additional config option to set before checking in key=value pairs, required for certain
--config=CONF	both backends such as login credentials (multiple values allowed).
--output	The output format to use (plain, json or json_pretty, default is plain).

Group Commands

The group commands provide a range of functionality for managing ownCloud groups. This includes creating and removing groups and managing group membership. Group names are case-sensitive, so “Finance” and “finance” are two different groups.

The full list of commands is:

```
group
  group:add           Adds a group
  group:add-member   Add members to a group
  group:delete       Deletes the specified group
  group:list         List groups
```

```
group:list-members          List group members
group:remove-member        Remove member(s) from a group
```

Creating Groups

You can create a new group with the `group:add` command. The syntax is:

```
group:add groupname
```

This example adds a new group, called “Finance”:

```
sudo -u www-data php occ group:add Finance
Created group "Finance"
```

Listing Groups

You can list the names of existing groups with the `group:list` command. The syntax is:

```
group:list [options] [<search-pattern>]
```

Groups containing the `search-pattern` string are listed. Matching is not case-sensitive. If you do not provide a `search-pattern` then all groups are listed.

Options:

```
--output[=OUTPUT] Output format (plain, json or json_pretty, default is plain) [default: "plain"]
```

This example lists groups containing the string “finance”.

```
sudo -u www-data php occ group:list finance
- All-Finance-Staff
- Finance
- Finance-Managers
```

This example lists groups containing the string “finance” formatted with `json_pretty`.

```
sudo -u www-data php occ group:list --output=json_pretty finance
[
  "All-Finance-Staff",
  "Finance",
  "Finance-Managers"
]
```

Listing Group Members

You can list the user IDs of group members with the `group:list-members` command. The syntax is:

```
group:list-members [options] <group>
```

Options:

```
--output[=OUTPUT] Output format (plain, json or json_pretty, default is plain) [default: "plain"]
```

This example lists members of the “Finance” group.

```
sudo -u www-data php occ group:list-members Finance
- aaron: Aaron Smith
- julie: Julie Jones
```

This example lists members of the Finance group formatted with `json_pretty`.

```
sudo -u www-data php occ group:list-members --output=json_pretty Finance
{
  "aaron": "Aaron Smith",
  "julie": "Julie Jones"
}
```

Adding Members to Groups

You can add members to an existing group with the `group:add-member` command. Members must be existing users. The syntax is

```
group:add-member [-m|--member [MEMBER]] <group>
```

This example adds members “aaron” and “julie” to group “Finance”:

```
sudo -u www-data php occ group:add-member --member aaron --member julie Finance
User "aaron" added to group "Finance"
User "julie" added to group "Finance"
```

You may attempt to add members that are already in the group, without error. This allows you to add members in a scripted way without needing to know if the user is already a member of the group. For example:

```
sudo -u www-data php occ group:add-member --member aaron --member julie --member fred Finance
User "aaron" is already a member of group "Finance"
User "julie" is already a member of group "Finance"
User fred" added to group "Finance"
```

Removing Members from Groups

You can remove members from a group with the `group:remove-member` command. The syntax is:

```
group:remove-member [-m|--member [MEMBER]] <group>
```

This example removes members “aaron” and “julie” from group “Finance”.

```
sudo -u www-data php occ group:remove-member --member aaron --member julie Finance
Member "aaron" removed from group "Finance"
Member "julie" removed from group "Finance"
```

You may attempt to remove members that have already been removed from the group, without error. This allows you to remove members in a scripted way without needing to know if the user is still a member of the group. For example:

```
sudo -u www-data php occ group:remove-member --member aaron --member fred Finance
Member "aaron" could not be found in group "Finance"
Member "fred" removed from group "Finance"
```

Deleting a Group

To delete a group, you use the `group:delete` command, as in the example below:

```
sudo -u www-data php occ group:delete Finance
```

Integrity Check

Apps which have an official tag **MUST** be code signed. Unsigned official apps won't be installable anymore. Code signing is optional for all third-party applications.

```
integrity
  integrity:check-app           Check app integrity using a signature.
  integrity:check-core         Check core integrity using a signature.
  integrity:sign-app           Signs an app using a private key.
  integrity:sign-core          Sign core using a private key
```

After creating your signing key, sign your app like this example:

```
sudo -u www-data php occ integrity:sign-app --privateKey=/Users/karlmay/contacts.key --certificate=/U
```

Verify your app:

```
sudo -u www-data php occ integrity:check-app --path=/pathto/app appname
```

When it returns nothing, your app is signed correctly. When it returns a message then there is an error. See [Code Signing](#) in the Developer manual for more detailed information.

`integrity:sign-core` is for ownCloud core developers only.

See [Code Signing](#) to learn more.

l10n, Create Javascript Translation Files for Apps

This command creates JavaScript and JSON translation files for ownCloud applications.

Note: The command does not update existing translations if the source translation file has been updated. It only creates translation files when none are present for a given language.

```
l10n
  l10n:createjs                Create Javascript translation files for a given app
```

The command takes two parameters; these are:

- `app`: the name of the application.
- `lang`: the output language of the translation files; more than one can be supplied.

To create the two translation files, the command reads translation data from a source PHP translation file.

A Working Example

In this example, we'll create Austrian German translations for the Gallery app.

Note: This example assumes that the ownCloud directory is `/var/www/owncloud/` and that it uses ownCloud's standard apps directory, `app`.

First, create a source translation file in `/var/www/owncloud/apps/gallery/l10n`, called `de_AT.php`. In it, add the required translation strings, as in the following example. Refer to the developer documentation on [creating translation files](#), if you're not familiar with creating them.

```
<?php
// The source string is the key, the translated string is the value.
$TRANSLATIONS = [
    "Share" => "Freigegeben"
];
$PLURAL_FORMS = "nplurals=2; plural=(n != 1);";
```

After that, run the following command to create the translation.

```
sudo -u www-data php occ l10n:createjs gallery de_AT
```

This will generate two translation files, `de_AT.js` and `de_AT.json`, in `/var/www/owncloud/apps/gallery/l10n`.

Create Translations in Multiple Languages

To create translations in multiple languages simultaneously, supply multiple languages to the command, as in the following example:

```
sudo -u www-data php occ l10n:createjs gallery de_AT de_DE hu_HU es fr
```

Logging Commands

These commands view and configure your ownCloud logging preferences.

```
log
log:manage      Manage logging configuration
log:owncloud    Manipulate ownCloud logging backend
```

Run `log:owncloud` to see your current logging status:

```
sudo -u www-data php occ log:owncloud
Log backend ownCloud: enabled
Log file: /opt/owncloud/data/owncloud.log
Rotate at: disabled
```

Options for `log:owncloud`:

```
--enable          Enable this logging backend
--file=FILE       Set the log file path
--rotate-size=ROTATE-SIZE Set the file size for log rotation, 0 = disabled
```

Use the `--enable` option to turn on logging. Use `--file` to set a different log file path. Set your rotation by log file size in bytes with `--rotate-size`; 0 disables rotation.

Run `log:manage` to set your logging backend, log level, and timezone:

The defaults are `owncloud`, `Warning`, and `UTC`.

Options for `log:manage`:

```
--backend=BACKEND set the logging backend [owncloud, syslog, errorlog]
--level=LEVEL     set the log level [debug, info, warning, error, fatal]
```

Log level can be adjusted by entering the number or the name:

```
sudo -u www-data php occ log:manage --level 4
sudo -u www-data php occ log:manage --level error
```

Note: Setting the log level to debug (0) can be used for finding the cause of an error, but should not be the standard as it increases the log file size.

Maintenance Commands

Use these commands when you upgrade ownCloud, manage encryption, perform backups and other tasks that require locking users out until you are finished.

```
maintenance
maintenance:data-fingerprint      Update the systems data-fingerprint after a backup is restored
maintenance:mimetype:update-db    Update database mimetypes and update filecache
maintenance:mimetype:update-js    Update mimetypelist.js
maintenance:mode                  Set maintenance mode
maintenance:repair                Repair this installation
maintenance:singleuser            Set single user mode
maintenance:update:htaccess       Updates the .htaccess file
```

`maintenance:mode` locks the sessions of all logged-in users, including administrators, and displays a status screen warning that the server is in maintenance mode. Users who are not already logged in cannot log in until maintenance mode is turned off. When you take the server out of maintenance mode logged-in users must refresh their Web browsers to continue working.

```
sudo -u www-data php occ maintenance:mode --on
sudo -u www-data php occ maintenance:mode --off
```

Putting your ownCloud server into single-user mode allows admins to log in and work, but not ordinary users. This is useful for performing maintenance and troubleshooting on a running server.

```
sudo -u www-data php occ maintenance:singleuser --on
Single user mode enabled
```

Turn it off when you're finished:

```
sudo -u www-data php occ maintenance:singleuser --off
Single user mode disabled
```

Run `maintenance:data-fingerprint` to tell desktop and mobile clients that a server backup has been restored. Users will be prompted to resolve any conflicts between newer and older file versions.

Run `maintenance:data-fingerprint` to tell desktop and mobile clients that a server backup has been restored. This command changes the ETag for all files in the communication with sync clients, informing them that one or more files were modified. After the command completes, users will be prompted to resolve any conflicts between newer and older file versions.

The `maintenance:repair` command runs automatically during upgrades to clean up the database, so while you can run it manually there usually isn't a need to.

```
sudo -u www-data php occ maintenance:repair
```

`maintenance:mimetype:update-db` updates the ownCloud database and file cache with changed mimetypes found in `config/mimetypermapping.json`. Run this command after modifying `config/mimetypermapping.json`. If you change a mimetype, run `maintenance:mimetype:update-db --repair-filecache` to apply the change to existing files.

Security

Use these commands when you manage security related tasks

Routes displays all routes of ownCloud. You can use this information to grant strict access via firewalls, proxies or loadbalancers etc.

```
security:routes [options]
```

Options:

```
--output          Output format (plain, json or json-pretty, default is plain)
--with-details    Adds more details to the output
```

Example 1:

```
sudo -uwww-data ./occ security:routes
```

```
+-----+-----+
| Path                                     | Methods |
+-----+-----+
| /apps/federation/auto-add-servers       | POST    |
| /apps/federation/trusted-servers       | POST    |
| /apps/federation/trusted-servers/{id}  | DELETE  |
| /apps/files/                             | GET     |
| /apps/files/ajax/download.php          |         |
...

```

Example 2:

```
sudo -uwww-data ./occ security:routes --output=json-pretty
```

```
[
  {
    "path": "\apps\federation\auto-add-servers",
    "methods": [
      "POST"
    ]
  },
  ...
]
```

Example 3:

```
sudo -uwww-data ./occ security:routes --with-details
```

```
+-----+-----+-----+
| Path                                     | Methods | Controller |
+-----+-----+-----+
| /apps/files/api/v1/sorting               | POST    | OCA\Files\Controller\ApiController::update |
| /apps/files/api/v1/thumbnail/{x}/{y}/{file} | GET     | OCA\Files\Controller\ApiController::getThur |
...

```

The following commands manage server-wide SSL certificates. These are useful when you create federation shares with other ownCloud servers that use self-signed certificates.

```
security:certificates      List trusted certificates
security:certificates:import  Import trusted certificate
security:certificates:remove  Remove trusted certificate
```

This example lists your installed certificates:

```
sudo -u www-data php occ security:certificates
```

Import a new certificate:

```
sudo -u www-data php occ security:certificates:import /path/to/certificate
```

Remove a certificate:

```
sudo -u www-data php occ security:certificates:remove [certificate name]
```

Sharing

This is an occ command to cleanup orphaned remote storages. To explain why this is necessary, a little background is required. While shares are able to be deleted as a normal matter of course, remote storages with “shared::” are not included in this process.

This might not, normally, be a problem. However, if a user has re-shared a remote share which has been deleted it will. This is because when the original share is deleted, the remote re-share reference is not. Internally, the fileid will remain in the file cache and storage for that file will not be deleted.

As a result, any user(s) who the share was re-shared with will now get an error when trying to access that file or folder. That’s why the command is available.

So, to cleanup all orphaned remote storages, run it as follows:

```
sudo -u www-data php occ sharing:cleanup-remote-storages
```

You can also set it up to run as *a background job*

Note: These commands are not available in *single-user (maintenance) mode*.

Trashbin

Note: These commands are only available when the “Deleted files” app (files_trashbin) is enabled. These commands are not available in *single-user (maintenance) mode*.

```
trashbin
trashbin:cleanup  Remove deleted files
trashbin:expire   Expires the users trash bin
```

The `trashbin:cleanup` command removes the deleted files of the specified users in a space-delimited list, or all users if none are specified. This example removes all the deleted files of all users:

```
sudo -u www-data php occ trashbin:cleanup
Remove all deleted files
Remove deleted files for users on backend Database
freda
molly
stash
```

```
rosa
edward
```

This example removes the deleted files of users “molly” and “freda”:

```
sudo -u www-data php occ trashbin:cleanup molly freda
Remove deleted files of  molly
Remove deleted files of  freda
```

`trashbin:expire` deletes only expired files according to the `trashbin_retention_obligation` setting in `config.php` (see the Deleted Files section in *Core Config.php Parameters*). The default is to delete expired files for all users, or you may list users in a space-delimited list.

User Commands

The `user` commands provide a range of functionality for managing ownCloud users. This includes: creating and removing users, resetting user passwords, displaying a report which shows how many users you have, and when a user was last logged in.

The full list, of commands is:

```
user
user:add                Adds a user
user:delete             Deletes the specified user
user:disable            Disables the specified user
user:enable             Enables the specified user
user:inactive           Reports users who are known to owncloud,
                        but have not logged in for a certain number of days
user:lastseen           Shows when the user was logged in last time
user:list               List users
user:list-groups        List groups for a user
user:modify             Modify user details
user:report             Shows how many users have access
user:resetpassword      Resets the password of the named user
user:setting            Read and modify user application settings
user:sync               Sync local users with an external backend service
```

Creating Users

You can create a new user with the `user:add` command. This command lets you set the following attributes:

- **uid:** The `uid` is the user’s username and their login name
- **display name:** This corresponds to the **Full Name** on the Users page in your ownCloud Web UI
- **email address**
- **group**
- **login name**
- **password**

The command’s syntax is:

```
user:add [--password-from-env] [--display-name [DISPLAY-NAME]] [--email [EMAIL]] [-g|--group [GROUP]]
```

This example adds new user Layla Smith, and adds her to the `users` and `db-admins` groups. Any groups that do not exist are created.

```
sudo -u www-data php occ user:add --display-name="Layla Smith" \  
  --group="users" --group="db-admins" --email=layla.smith@example.com layla  
Enter password:  
Confirm password:  
The user "layla" was created successfully  
Display name set to "Layla Smith"  
Email address set to "layla.smith@example.com"  
User "layla" added to group "users"  
User "layla" added to group "db-admins"
```

After the command completes, go to your Users page, and you will see your new user.

Setting a User's Password

`password-from-env` allows you to set the user's password from an environment variable. This prevents the password from being exposed to all users via the process list, and will only be visible in the history of the user (root) running the command. This also permits creating scripts for adding multiple new users.

To use `password-from-env` you must run as “real” root, rather than `sudo`, because `sudo` strips environment variables. This example adds new user Fred Jones:

```
export OC_PASS=newpassword  
su -s /bin/sh www-data -c 'php occ user:add --password-from-env  
  --display-name="Fred Jones" --group="users" fred'  
The user "fred" was created successfully  
Display name set to "Fred Jones"  
User "fred" added to group "users"
```

You can reset any user's password, including administrators (see [Resetting a Lost Admin Password](#)):

```
sudo -u www-data php occ user:resetpassword layla  
Enter a new password:  
Confirm the new password:  
Successfully reset password for layla
```

You may also use `password-from-env` to reset passwords:

```
export OC_PASS=newpassword  
sudo -u www-data php occ user:resetpassword --password-from-env layla  
Successfully reset password for layla
```

Deleting A User

To delete a user, you use the `user:delete` command, as in the example below:

```
sudo -u www-data php occ user:delete fred
```

Expiring a User's Password

Note: This command is only available when ‘**the Password Policy app**’ is installed.

```
sudo -u www-data php user:expire-password <uid> [<expiredate>]
```

To expire a user's password at a specific date and time, use the `user:expire-password` command. The command accepts two arguments, the user's uid and an expiry date. The expiry date can be provided using any of [PHP's supported date and time formats](#).

If an expiry date is not supplied, the password will expire with immediate effect. This is because the password will be set as being expired 24 hours before the command was run. For example, if the command was run at "2018-07-12 13:15:28 UTC", then the password's expiry date will be set to "2018-07-11 13:15:28 UTC".

After the command completes, console output, similar to that below, confirms when the user's password is set to expire.

```
The password for frank is set to expire on 2018-07-12 13:15:28 UTC.
```

Command Examples

```
# The password for user "frank" will be set as being expired 24 hours before the command was run.
sudo -u www-data php occ user:expire-password frank
```

```
# Expire the user "frank"'s password in 2 days time.
sudo -u www-data php occ user:expire-password frank '+2 days'
```

```
# Expire the user "frank"'s password on the 15th of August 2005, at 15:52:01 in the local timezone.
sudo -u www-data php occ user:expire-password frank '2005-08-15T15:52:01+00:00'
```

```
# Expire the user "frank"'s password on the 15th of August 2005, at 15:52:01 UTC.
sudo -u www-data php occ user:expire-password frank '15-Aug-05 15:52:01 UTC'
```

Caveats Please be aware of the following implications of enabling or changing the password policy's "*days until user password expires*" option.

- Administrators need to run the `occ user:expire-password` command to initiate expiry for new users.
- Passwords will never expire for users who have *not* changed their initial password, because they do not have a password history. To force password expiration use the `occ user:expire-password` command.
- A password expiration date will be set after users change their password for the first time. To force password expiration use the `occ user:expire-password` command.
- Passwords changed for the first time, will expire based on the *active* password policy. If the policy is later changed, it will not update the password's expiry date to reflect the new setting.
- Password expiration dates of users where the administrator has run the `occ user:expire-password` command *won't* automatically update to reflect the policy change. In these cases, Administrators need to run the `occ user:expire-password` command again and supply a new expiry date.

Listing Users

You can list existing users with the `user:list` command. The syntax is

```
user:list [options] [<search-pattern>]
```

User IDs containing the `search-pattern` string are listed. Matching is not case-sensitive. If you do not provide a `search-pattern` then all users are listed.

Options:

```
--output[=OUTPUT]           Output format (plain, json or json-pretty, default is plain)
-a, --attributes[=ATTRIBUTES] Adds more details to the output
```

Allowed attributes, multiple values possible

```
uid, displayName, email, quota, enabled, lastLogin, home,
backend, cloudId, searchTerms [default: ["displayName"]]
```

This example lists user IDs containing the string “aron”

```
sudo -u www-data php occ user:list ron
- aaron: Aaron Smith
```

The output can be formatted in JSON with the output option `json` or `json_pretty`.

```
sudo -u www-data php occ user:list --output=json_pretty
{
  "aaron": "Aaron Smith",
  "herbert": "Herbert Smith",
  "julie": "Julie Jones"
}
```

This example lists all users including the attribute “enabled”.

```
sudo -u www-data php occ user:list -a enabled
- admin: true
- foo: true
```

Listing Group Membership of a User

You can list the group membership of a user with the `user:list-groups` command. The syntax is

```
user:list-groups [options] <uid>
```

This example lists group membership of user `julie`:

```
sudo -u www-data php occ user:list-groups julie
- Executive
- Finance
```

The output can be formatted in JSON with the output option `json` or `json_pretty`:

```
sudo -u www-data php occ user:list-groups --output=json_pretty julie
[
  "Executive",
  "Finance"
]
```

Finding The User’s Last Login

To view a user’s most recent login, use the `user:lastseen` command, as in the example below:

```
sudo -u www-data php occ user:lastseen layla
layla’s last login: 09.01.2015 18:46
```

User Application Settings

To manage application settings for a user, use the `user:setting` command. This command provides the ability to:

- Retrieve all settings for an application

- Retrieve a single setting
- Set a setting value
- Delete a setting

If you run the command and pass the help switch (`--help`), you will see the following output, in your terminal:

```
Usage:
  user:setting [options] [--] <uid> [<app>] [<key>]

Arguments:
  uid      User ID used to login
  app      Restrict the settings to a given app [default: ""]
  key      Setting key to set, get or delete [default: ""]
```

```
sudo -u www-data php occ user:setting --help
```

If you're new to the `user:setting` command, the descriptions for the `app` and `key` arguments may not be completely transparent. So, here's a lengthier description of both.

Argument	Description
<code>app</code>	When an value is supplied, <code>user:setting</code> limits the settings displayed, to those for that, specific, application — assuming that the application is installed, and that there are settings available for it. Some example applications are “core”, “files_trashbin”, and “user_ldap”. A complete list, unfortunately, cannot be supplied, as it is impossible to know the entire list of applications which a user could, potentially, install.
<code>key</code>	This value specifies the setting key to be manipulated (set, retrieved, or deleted) by the <code>user:setting</code> command.

Retrieving User Settings

To retrieve all settings for a user, you need to call the `user:setting` command and supply the user's username, as in the example below.

```
sudo -u www-data php occ user:setting layla
- core:
  - lang: en
- login:
  - lastLogin: 1465910968
- settings:
  - email: layla@example.tld
```

Here, we see that the user has settings for the application `core`, when they last logged in, and what their email address is.

To retrieve the user's settings for a specific application, you have to supply the username and the application's name, which you want to retrieve the settings for; such as in the example below:

```
sudo -u www-data php occ user:setting layla core
- core:
  - lang: en
```

In the output, you can see that one setting is in effect, `lang`, which is set to `en`. To retrieve the value of a single application for a user, use the `user:setting` command, as in the example below.

```
sudo -u www-data php occ user:setting layla core lang
```

This will display the value for that setting, such as `en`.

Setting a Setting

To set a setting, you need to supply four things; these are:

- the username
- the application (or setting category)
- the `--value` switch
- the, quoted, value for that setting

Here's an example of how you would set the email address of the user `layla`.

```
sudo -u www-data php occ user:setting layla settings email --value "new-layla@example.tld"
```

Deleting a Setting

Deleting a setting is quite similar to setting a setting. In this case, you supply the username, application (or setting category) and key as above. Then, in addition, you supply the `--delete` flag.

```
sudo -u www-data php occ user:setting layla settings email --delete
```

Modify user details New in version 10.0.8.

This command modifies either the users username or email address.

```
user:modify [options] [--] <uid> <key> <value>
```

Arguments:

<code>uid</code>	User ID used to login
<code>key</code>	Key to be changed. Valid keys are: <code>displayname</code> , <code>email</code>
<code>value</code>	The new value of the key

All three arguments are mandatory and can not be empty.

Example to set the email address:

```
sudo -u www-data php occ user:modify carla email foobar@foo.com
```

The email address of `carla` is updated to `foobar@foo.com`

Generating a User Count Report Generate a simple report that counts all users, including users on external user authentication servers such as LDAP.

```
sudo -u www-data php occ user:report
```

```
+-----+-----+
| User Report      |     |
+-----+-----+
| Database         | 12  |
| LDAP             | 86  |
|                 |     |
| total users      | 98  |
|                 |     |
| user directories | 2   |
+-----+-----+
```

Syncing User Accounts This command syncs users stored in external backend services, such as *LDAP*, *Shibboleth*, and *Samba*, with ownCloud's, internal, user database. However, it's not essential to run it regularly, unless you have a large number of users whose account properties have changed in a backend outside of ownCloud. When run, it will pick up changes from alternative user backends, such as LDAP where properties like `cn` or `display name` have changed, and sync them with ownCloud's user database. If accounts are found that no longer exist in the external backend, you are given the choice of either removing or disabling the accounts.

Note: It's also *one of the commands* that you should run on a regular basis to ensure that your ownCloud installation is running optimally.

Note: This command replaces the old `show-remnants` functionality, and brings the LDAP feature more in line with the rest of ownCloud's functionality.

Usage:

```
user:sync [options] [--] [<backend-class>]
```

Arguments:

backend-class

The quoted PHP class name for the backend, eg

- LDAP: "OCA\User_LDAP\User_Proxy"
- Samba: "OCA\User\SMB"
- Shibboleth: "OCA\User_Shibboleth\UserBacker"

Options:

-l, --list

List all enabled backend classes

-u, --uid=UID

Sync only the user with the given user id

-s, --seenOnly

Sync only seen users

-c, --showCount

Calculate user count before syncing

-m, --missing-account-action=MISSING-ACCOUNT-ACTION

Action to take if the account isn't connected

-r, --re-enable

When syncing multiple accounts re-enable accou

-h, --help

Display this help message

-q, --quiet

Do not output any message

-V, --version

Display this application version

--ansi

Force ANSI output

--no-ansi

Disable ANSI output

-n, --no-interaction

Do not ask any interactive question

--no-warnings

Skip global warnings, show command output only

-v|vv|vvv, --verbose

Increase the verbosity of messages: 1 for normal

Help:

Synchronize users from a given backend to the accounts table.

Below are examples of how to use the command with different backends:

LDAP

```
sudo -u www-data ./occ user:sync "OCA\User_LDAP\User_Proxy"
```

Samba

```
sudo -u www-data ./occ user:sync "OCA\User\SMB"
```

Shibboleth

```
sudo -u www-data ./occ user:sync "OCA\User_Shibboleth\UserBackend"
```

Below are examples of how to use the command with the *LDAP* backend along with example console output.

Example 1:

```
sudo ./occ user:sync "OCA\User_LDAP\User_Proxy" -m disable -r
Analysing all users ...
 6 [=====]
```

No removed users have been detected.

No existing accounts to re-enable.

```
Insert new and update existing users ...
 4 [=====]
```

Example 2:

```
sudo ./occ user:sync "OCA\User_LDAP\User_Proxy" -m disable -r
Analysing all users ...
 6 [=====]
```

Following users are no longer known with the connected backend.

Disabling accounts:

```
9F625F70-08DD-4838-AD52-7DE1F72DBE30, Bobbie, bobbie@example.org disabled
53CDB5AC-B02E-4A49-8FEF-001A13725777, David, dave@example.org disabled
34C3F461-90FE-417C-ADC5-CE97FE5B8E72, Carol, carol@example.org disabled
```

No existing accounts to re-enable.

```
Insert new and update existing users ...
 1 [=====]
```

Example 3:

```
sudo ./occ user:sync "OCA\User_LDAP\User_Proxy" -m disable -r
Analysing all users ...
 6 [=====]
```

Following users are no longer known with the connected backend.

Disabling accounts:

```
53CDB5AC-B02E-4A49-8FEF-001A13725777, David, dave@example.org skipped, already disabled
34C3F461-90FE-417C-ADC5-CE97FE5B8E72, Carol, carol@example.org skipped, already disabled
B5275C13-6466-43FD-A129-A12A6D3D9A0D, Alicia3, alicia3@example.org disabled
```

Re-enabling accounts:

```
9F625F70-08DD-4838-AD52-7DE1F72DBE30, Bobbie, bobbie@example.org enabled
```

```
Insert new and update existing users ...
 1 [=====]
```

Example 4:

```
sudo ./occ user:sync "OCA\User_LDAP\User_Proxy" -m disable -r
Analysing all users ...
 6 [=====]
```

No removed users have been detected.

Re-enabling accounts:

```
53CDB5AC-B02E-4A49-8FEF-001A13725777, David, dave@example.org enabled
34C3F461-90FE-417C-ADC5-CE97FE5B8E72, Carol, carol@example.org enabled
B5275C13-6466-43FD-A129-A12A6D3D9A0D, Alicia3, alicia3@example.org enabled
```

Insert new and update existing users ...

```
4 [=====]
```

Syncing via cron job

Here is an example for syncing with LDAP four times a day on Ubuntu:

```
crontab -e -u www-data
```

```
* */6 * * * /usr/bin/php /var/www/owncloud/occ user:sync -vvv --missing-account-action="disable" -n
```

Versions

versions

```
versions:cleanup    Delete versions
versions:expire     Expires the users file versions
```

`versions:cleanup` can delete all versioned files, as well as the `files_versions` folder, for either specific users, or for all users. The example below deletes all versioned files for all users:

```
sudo -u www-data php occ versions:cleanup
Delete all versions
Delete versions for users on backend Database
  freda
  molly
  stash
  rosa
  edward
```

You can delete versions for specific users in a space-delimited list:

```
sudo -u www-data php occ versions:cleanup freda molly
Delete versions of  freda
Delete versions of  molly
```

`versions:expire` deletes only expired files according to the `versions_retention_obligation` setting in `config.php` (see the File versions section in *Core Config.php Parameters*). The default is to delete expired files for all users, or you may list users in a space-delimited list.

Note: These commands are only available when the “Versions” app (`files_versions`) is enabled. These commands are not available in *single-user (maintenance) mode*.

Command Line Installation

ownCloud can be installed entirely from the command line. After downloading the tarball and copying ownCloud into the appropriate directories, or after installing ownCloud packages (See *Linux Package Manager Installation and Manual Installation on Linux*) you can use `occ` commands in place of running the graphical Installation Wizard.

Note: These instructions assume that you have a fully working and configured webserver. If not, please refer to the documentation on *configuring the Apache web server* for detailed instructions.

Apply correct permissions to your ownCloud directories; see *Set Strong Directory Permissions*. Then choose your `occ` options. This lists your available options:

```
sudo -u www-data php occ
ownCloud is not installed - only a limited number of commands are available
ownCloud version 10.0.8
```

Usage:

```
[options] command [arguments]
```

Options:

```
--help (-h)           Display this help message
--quiet (-q)          Do not output any message
--verbose (-v|vv|vvv) Increase the verbosity of messages: 1 for normal output,
                      2 for more verbose output and 3 for debug
--version (-V)        Display this application version
--ansi                Force ANSI output
--no-ansi              Disable ANSI output
--no-interaction (-n) Do not ask any interactive question
```

Available commands:

```
check                Check dependencies of the server environment
help                 Displays help for a command
list                 Lists commands
status               Show some status information
app
  app:check-code     Check code to be compliant
l10n
  l10n:createjs      Create javascript translation files for a given app
maintenance
  maintenance:install Install ownCloud
```

Display your `maintenance:install` options

```
sudo -u www-data php occ help maintenance:install
ownCloud is not installed - only a limited number of commands are available
Usage:
```

```
maintenance:install [--database="..."] [--database-name="..."]
[--database-host="..."] [--database-user="..."] [--database-pass[="..."]]
[--database-table-prefix[="..."]] [--admin-user="..."] [--admin-pass="..."]
[--data-dir="..."]
```

Options:

```
--database            Supported database type (default: "sqlite")
--database-name       Name of the database
--database-host       Hostname of the database (default: "localhost")
--database-user       User name to connect to the database
--database-pass       Password of the database user
--database-table-prefix Prefix for all tables (default: oc_)
--admin-user          User name of the admin account (default: "admin")
--admin-pass          Password of the admin account
--data-dir            Path to data directory (default: "/var/www/owncloud/data")
--help (-h)           Display this help message
--quiet (-q)          Do not output any message
```

```

--verbose (-v|vv|vvv)  Increase the verbosity of messages: 1 for normal output,
                        2 for more verbose output and 3 for debug
--version (-V)          Display this application version
--ansi                  Force ANSI output
--no-ansi               Disable ANSI output
--no-interaction (-n)  Do not ask any interactive question

```

This example completes the installation:

```

cd /var/www/owncloud/
sudo -u www-data php occ maintenance:install --database
"mysql" --database-name "owncloud" --database-user "root" --database-pass
"password" --admin-user "admin" --admin-pass "password"
ownCloud is not installed - only a limited number of commands are available
ownCloud was successfully installed

```

Supported databases are:

- sqlite (SQLite3 - ownCloud Community edition only)
- mysql (MySQL/MariaDB)
- pgsql (PostgreSQL)
- oci (Oracle - ownCloud Enterprise edition only)

Command Line Upgrade

These commands are available only after you have downloaded upgraded packages or tar archives, and before you complete the upgrade. List all options, like this example on CentOS Linux:

```

sudo -u www-data php occ upgrade -h
Usage:

```

```

upgrade [options]

```

Options:

```

--no-app-disable  Skips the disable of third party apps
-h, --help        Display this help message
-q, --quiet        Do not output any message
-V, --version      Display this application version
--ansi            Force ANSI output
--no-ansi         Disable ANSI output
-n, --no-interaction Do not ask any interactive question
--no-warnings      Skip global warnings, show command output only
-v|vv|vvv, --verbose Increase the verbosity of messages: 1 for normal output, 2 for more verbose output

```

Help:

```

run upgrade routines after installation of a new release. The release has to be installed before.

```

When you are performing an update or upgrade on your ownCloud server (see the Maintenance section of this manual), it is better to use `occ` to perform the database upgrade step, rather than the Web GUI, in order to avoid timeouts. PHP scripts invoked from the Web interface are limited to 3600 seconds. In larger environments this may not be enough, leaving the system in an inconsistent state. After performing all the preliminary steps (see [How to Upgrade Your ownCloud Server](#)) use this command to upgrade your databases, like this example on CentOS Linux:

```

sudo -u www-data php occ upgrade
ownCloud or one of the apps require upgrade - only a limited number of
commands are available
Turned on maintenance mode

```

```
Checked database schema update
Checked database schema update for apps
Updated database
Updating <gallery> ...
Updated <gallery> to 0.6.1
Updating <activity> ...
Updated <activity> to 2.1.0
Update successful
Turned off maintenance mode
```

Note how it details the steps. Enabling verbosity displays timestamps:

```
sudo -u www-data php occ upgrade -v
ownCloud or one of the apps require upgrade - only a limited number of commands are available
2017-06-23T09:06:15+0000 Turned on maintenance mode
2017-06-23T09:06:15+0000 Checked database schema update
2017-06-23T09:06:15+0000 Checked database schema update for apps
2017-06-23T09:06:15+0000 Updated database
2017-06-23T09:06:15+0000 Updated <files_sharing> to 0.6.6
2017-06-23T09:06:15+0000 Update successful
2017-06-23T09:06:15+0000 Turned off maintenance mode
```

If there is an error it throws an exception, and the error is detailed in your ownCloud logfile, so you can use the log output to figure out what went wrong, or to use in a bug report.

```
Turned on maintenance mode
Checked database schema update
Checked database schema update for apps
Updated database
Updating <files_sharing> ...
Exception
ServerNotAvailableException: LDAP server is not available
Update failed
Turned off maintenance mode
```

Disable Users

Admins can disable users via the occ command too:

```
sudo -u www-data php occ user:disable <username>
```

Use the following command to enable the user again:

```
sudo -u www-data php occ user:enable <username>
```

Note: Once users are disabled, their connected browsers will be disconnected.

Finding Inactive Users

To view a list of users who've not logged in for a given number of days, use the `user:inactive` command. The example below searches for users inactive for five days, or more.

```
sudo -u www-data php occ user:inactive 5
```

Options

`--output[=OUTPUT]` Output format (plain, json or json_pretty, default is plain) [default: "plain"]

By default, this will generate output in the following format:

```
- 0:
  - uid: admin
  - displayName: admin
  - inactiveSinceDays: 5
```

You can see the user's user id, display name, and the number of days they've been inactive. If you're passing or piping this information to another application for further processing, you can also use the `--output` switch to change its format.

Using the output option `json` will render the output formatted as follows.

```
[{"uid": "admin", "displayName": "admin", "inactiveSinceDays": 5}]
```

Using the output option `json_pretty` will render the output formatted as follows.

```
[
  {
    "uid": "admin",
    "displayName": "admin",
    "inactiveSinceDays": 5
  }
]
```

6.5.4 Using occ apps commands

Note: This command reference covers the ownCloud maintained apps commands.

ownCloud's `occ` command (ownCloud console) is ownCloud's command-line interface. You can perform common server operations with `occ`, including installing and upgrading ownCloud, managing users and groups, encryption, passwords, and LDAP setting.

`occ` is in the `owncloud/` directory; for example `/var/www/owncloud` on Ubuntu Linux. `occ` is a PHP script. **You must run it as your HTTP user** to ensure that your ownCloud files and directories retain the correct permissions.

occ Command Directory

- *Run occ As Your HTTP User*
- *Calendar Commands*
- *Contacts Commands*
- *S3 Objectstore Commands*
- *LDAP Commands*
- *Market*
- *Notifications*
- *Password Policy*
- *Reports*
- *Ransomware Protection*

- *Shibboleth Modes (Enterprise Edition only)*
- *Two-factor Authentication*

Run occ As Your HTTP User

The HTTP user is different on the various Linux distributions. See *Set Strong Directory Permissions* to learn how to find your HTTP user.

- The HTTP user and group in Debian/Ubuntu is www-data.
- The HTTP user and group in Fedora/CentOS is apache.
- The HTTP user and group in Arch Linux is http.
- The HTTP user in openSUSE is wwwrun, and the HTTP group is www.

If your HTTP server is configured to use a different PHP version than the default (`/usr/bin/php`), `occ` should be run with the same version. For example, in CentOS 6.5 with SCL-PHP54 installed, the command looks like this:

```
sudo -u apache /opt/rh/php54/root/usr/bin/php /var/www/html/owncloud/occ
```

The following examples are based on Ubuntu.

Running `occ` with no options lists all commands and options

```
sudo -u www-data php occ
ownCloud version 10.0.8
```

Usage:

```
command [options] [arguments]
```

Options:

```
-h, --help           Display this help message
-q, --quiet          Do not output any message
-V, --version        Display this application version
--ansi              Force ANSI output
--no-ansi           Disable ANSI output
-n, --no-interaction Do not ask any interactive question
--no-warnings        Skip global warnings, show command output only
-v|vv|vvv, --verbose Increase the verbosity of messages: 1 for normal output,
                    2 for more verbose output and 3 for debug
```

Available commands:

```
check               Check dependencies of the server environment
help                Displays help for a command
list                Lists commands
status              Show some status information
upgrade             Run upgrade routines after installation of
                    a new release. The release has to be installed before
```

This is the same as `sudo -u www-data php occ list`.

General syntax help

Run `occ` with the `-h` option for syntax help

```
sudo -u www-data php occ -h
```

Display your ownCloud version

```
sudo -u www-data php occ -V
ownCloud version 10.0.8
```

Query your ownCloud server status

```
sudo -u www-data php occ status
- installed: true
- version: 10.0.8.5
- versionstring: 10.0.8
- edition: Community
```

Command syntax help

Get detailed information on individual commands with the `help` command, like this example for the `maintenance:mode` command

```
sudo -u www-data php occ --help maintenance:mode
Usage:
maintenance:mode [options]
```

Options:

```
--on           Enable maintenance mode
--off          Disable maintenance mode
--output[=OUTPUT] Output format (plain, json or json_pretty, default is plain) [default: "plain"]
-h, --help    Display this help message
-q, --quiet   Do not output any message
-V, --version Display this application version
--ansi        Force ANSI output
--no-ansi     Disable ANSI output
-n, --no-interactive Do not ask any interactive question
--no-warnings Skip global warnings, show command output only
-v|vv|vvv, --verbose Increase the verbosity of messages: 1 for normal output,
2 for more verbose output and 3 for debug
```

Options and Arguments

`occ` has *options*, *commands*, and *arguments*. Commands are required. Options are optional. Arguments can be required *or* optional. The, generic, syntax is

```
occ [options] command [arguments]
```

The `status` command from above has an option to define the output format.

The default is plain text, but it can also be `json`

```
sudo -u www-data php occ status --output=json
{"installed":true,"version":"9.0.0.19","versionstring":"9.0.0","edition":""}
```

or `json_pretty`

```
sudo -u www-data php occ status --output=json_pretty
{
  "installed": true,
  "version": "10.0.8.5",
  "versionstring": "10.0.8",
  "edition": "Community"
}
```

This output option is available on all list and list-like commands, which include `status`, `check`, `app:list`, `config:list`, `encryption:status` and `encryption:list-modules`.

Usage of parameters in Options

In case an option requires parameters, following format should be used for short or long Options forms

The following example command has an option in `-p` (short) form and `--path` (long) form.

Parameters for long form options will be written after a blank or equal sign

```
sudo -u www-data ./occ files:scan --path="user_x/files/folder"
```

Parameters for short form options will be written either directly after the option or after a blank. Do not use the equal sign as this could be interpreted as part of the parameter.

```
sudo -u www-data ./occ files:scan -p "user_x/files/folder"
```

Calendar Commands

For commands for managing the calendar, please see the DAV Command section in the occ core command set.

Contacts Commands

For commands for managing contacts, please see the DAV Command section in the occ core command set.

S3 Objectstore Commands

List objects, buckets or versions of an object

```
sudo -u www-data occ s3:list
```

Arguments:

<code>bucket</code>	Name of the bucket; it's objects will be listed
<code>object</code>	Key of the object; it's versions will be listed

Create a bucket as necessary to be used

```
sudo -u www-data occ s3:create-bucket
```

Arguments:

<code>bucket</code>	Name of the bucket to be created
---------------------	----------------------------------

Options:

update-configuration	If the bucket exists the configuration will be updated
accept-warning	No warning about the usage of this command will be displayed

LDAP Commands

Note: These commands are only available when the “LDAP user and group backend” app (`user_ldap`) is enabled.

These LDAP commands appear only when you have enabled the LDAP app. Then you can run the following LDAP commands with `occ`:

```
ldap
ldap:check-user           Checks whether a user exists on LDAP.
ldap:create-empty-config Creates an empty LDAP configuration
ldap:delete-config       Deletes an existing LDAP configuration
ldap:search               Executes a user or group search
ldap:set-config           Modifies an LDAP configuration
ldap:show-config          Shows the LDAP configuration
ldap:test-config          Tests an LDAP configuration
ldap:update-group         Update the specified group membership
                          Information stored locally
```

Search for an LDAP user, using this syntax:

```
sudo -u www-data php occ ldap:search [--group] [--offset="..."]
[--limit="..."] search
```

Searches match at the beginning of the attribute value only. This example searches for `givenNames` that start with “rob”:

```
sudo -u www-data php occ ldap:search "rob"
```

This will find `_robbie_`, `_roberta_`, and `_robin_`. Broaden the search to find, for example, `jeroboam` with the asterisk wildcard:

```
sudo -u www-data php occ ldap:search "*rob"
```

User search attributes are set with `ldap:set-config` (below). For example, if your search attributes are `givenName` and `sn` you can find users by first name + last name very quickly. For example, you’ll find “Terri Hanson” by searching for `te ha`. Trailing whitespace is ignored.

Check if an LDAP user exists. This works only if the ownCloud server is connected to an LDAP server.

```
sudo -u www-data php occ ldap:check-user robert
```

`ldap:check-user` will not run a check when it finds a disabled LDAP connection. This prevents users that exist on disabled LDAP connections from being marked as deleted. If you know for sure that the user you are searching for is not in one of the disabled connections, and exists on an active connection, use the `--force` option to force it to check all active LDAP connections.

```
sudo -u www-data php occ ldap:check-user --force robert
```

`ldap:create-empty-config` creates an empty LDAP configuration. The first one you create has no `configID`, like this example:

```
sudo -u www-data php occ ldap:create-empty-config
Created new configuration with configID ''
```

This is a holdover from the early days, when there was no option to create additional configurations. The second, and all subsequent, configurations that you create are automatically assigned IDs.

```
sudo -u www-data php occ ldap:create-empty-config
Created new configuration with configID 's01'
```

Then you can list and view your configurations:

```
sudo -u www-data php occ ldap:show-config
```

And view the configuration for a single configID:

```
sudo -u www-data php occ ldap:show-config s01
```

`ldap:delete-config [configID]` deletes an existing LDAP configuration.

```
sudo -u www-data php occ ldap:delete s01
Deleted configuration with configID 's01'
```

The `ldap:set-config` command is for manipulating configurations, like this example that sets search attributes:

```
sudo -u www-data php occ ldap:set-config s01 ldapAttributesForUserSearch
"cn;givenname;sn;displayname;mail"
```

The command takes the following format:

```
ldap:set-config <configID> <configKey> <configValue>
```

All of the available keys, along with default values for *configValue*, are listed in the table below.

Configuration	Setting
hasMemberOfFilterSupport	
hasPagedResultSupport	
homeFolderNamingRule	
lastJpegPhotoLookup	0
ldapAgentName	<i>cn=admin,dc=owncloudqa,dc=com</i>
ldapAgentPassword	*
ldapAttributesForGroupSearch	
ldapAttributesForUserSearch	
ldapBackupHost	
ldapBackupPort	
ldapBase	<i>dc=owncloudqa,dc=com</i>
ldapBaseGroups	<i>dc=owncloudqa,dc=com</i>
ldapBaseUsers	<i>dc=owncloudqa,dc=com</i>
ldapCacheTTL	600
ldapConfigurationActive	1
ldapDynamicGroupMemberURL	
ldapEmailAttribute	
ldapExperiencedAdmin	0
ldapExpertUUIDGroupAttr	
ldapExpertUUIDUserAttr	
ldapExpertUsernameAttr	<i>ldapGroupDisplayName cn</i>
ldapGroupFilter	<i>ldapGroupFilterGroups</i>
ldapGroupFilterMode	0
ldapGroupFilterObjectclass	
ldapGroupMemberAssocAttr	<i>uniqueMember</i>
ldapHost	<i>ldap://host</i>

Continued on next page

Table 6.1 – continued from previous page

Configuration	Setting
ldapIgnoreNamingRules	
ldapLoginFilter	<i>(&((objectclass=inetOrgPerson))(uid=%uid))</i>
ldapLoginFilterAttributes	
ldapLoginFilterEmail	0
ldapLoginFilterMode	0
ldapLoginFilterUsername	1
ldapNestedGroups	0
ldapOverrideMainServer	
ldapPagingSize	500
ldapPort	389
ldapQuotaAttribute	
ldapQuotaDefault	
ldapTLS	0
ldapUserDisplayName	<i>displayName</i>
ldapUserDisplayName2	
ldapUserFilter	<i>((objectclass=inetOrgPerson))</i>
ldapUserFilterGroups	
ldapUserFilterMode	0
ldapUserFilterObjectclass	<i>inetOrgPerson</i>
ldapUuidGroupAttribute	<i>auto</i>
ldapUuidUserAttribute	<i>auto</i>
turnOffCertCheck	0
useMemberOfToDetectMembership	1

`ldap:test-config` tests whether your configuration is correct and can bind to the server.

```
sudo -u www-data php occ ldap:test-config s01
The configuration is valid and the connection could be established!
```

`ldap:update-group` updates the specified group membership information stored locally.

The command takes the following format:

```
ldap:update-group <groupID> <groupID <groupID> ...>
```

The command allows for running a manual group sync on one or more groups, instead of having to wait for group syncing to occur. If users have been added or removed from these groups in LDAP, ownCloud will update its details. If a group was deleted in LDAP, ownCloud will also delete the local mapping info about this group.

Note: New groups in LDAP won't be synced with this command. The LDAP TTL configuration (by default 10 minutes) still applies. This means that recently deleted groups from LDAP might be considered as “active” and might not be deleted in ownCloud immediately.

Configuring the LDAP Refresh Attribute Interval

You can configure the LDAP refresh attribute interval, but not with the `ldap` commands. Instead, you need to use the `config:app:set` command, as in the following example, which takes a number of seconds to the `--value` switch.

```
sudo -u www-data php occ config:app:set user_ldap updateAttributesInterval --value=7200
```

In the example above, the interval is being set to 7200 seconds. Assuming the above example was used, the command would output the following:

Config value `updateAttributesInterval` for app `user_ldap` set to 7200

If you want to reset (or unset) the setting, then you can use the following command:

```
sudo -u www-data php occ config:app:delete user_ldap updateAttributesInterval
```

Market

The market commands *install*, *uninstall*, *list*, and *upgrade* applications from *the ownCloud Marketplace*.

```
market
  market:install    Install apps from the marketplace. If already installed and
                   an update is available the update will be installed.
  market:uninstall  Uninstall apps from the marketplace.
  market:list       Lists apps as available on the marketplace.
  market:upgrade    Installs new app versions if available on the marketplace
```

Note: The user running the update command, which will likely be your webserver user, requires write permission for the `/apps` folder. If they don't have write permission, the command may report that the update was successful, but it may silently fail.

Note: These commands are not available in *single-user (maintenance) mode*. For more details please see the Maintenance Commands section in the `occ core` command set.

Install an Application

Applications can be installed both from [the ownCloud Marketplace](#) and from a local file archive.

Install Apps From The Marketplace

To install an application from the Marketplace, you need to supply the app's id, which can be found in the app's Marketplace URL. For example, the URL for *Two factor backup codes* is https://marketplace.owncloud.com/apps/twofactor_backup_codes. So its app id is `twofactor_backup_codes`.

Install Apps From a File Archive

To install an application from a local file archive, you need to supply the path to the archive, and that you pass the `-l` switch. Only `zip`, `gzip`, and `bzip2` archives are supported.

Usage Example

```
# Install an app from the marketplace.
sudo -u www-data occ market:install twofactor_backup_codes

# Install an app from a local archive.
sudo -u www-data occ market:install -l /mnt/data/richdocuments-2.0.0.tar.gz
```

Notifications

If you want to send notifications to users or groups use the following command.

```
notifications
  notifications:generate  Generates a notification.
```

Options and Arguments:

```
notifications:generate [-u|--user USER] [-g|--group GROUP] [-l|--link <linktext>] [--] <subject> [<message>]
```

Options:

```
-u --user          User id to whom the notification shall be sent
-g --group        Group id to whom the notification shall be sent
-l --link         A link associated with the notification
```

Arguments:

```
subject          The notification subject - maximum 255 characters
message          A more extended message - maximum 4000 characters
linktext         A link to an HTML page
```

At least one user or group must be set.

A link can be useful for notifications shown in client apps.

Example:

```
sudo -u www-data php occ notifications:generate -g Office "Emergency Alert" "Rebooting in 5min"
```

Password Policy

Command to expire a users password

```
sudo -u www-data occ user:expire-password
```

Arguments:

expiredate	The date and time when a password expires, e.g. "2019-01-01 14:00:00 CET" or -1 days
------------	--------------------------------------------------------------------------------------

Options:

-a, --all	Will add password expiry to all known users. uid and group option are discarded if the option is provided by user
-u, --uid	The user's uid is used. This option can be used as -uid "Alice" -uid Bob"
-g, --group	Add password expiry to user(s) under group(s). This option can be used as -group "foo" -group "bar" to add expiry passwords for users in group foo and bar. If uid option (eg: -uid "user1") is passed with group, then uid will also be processed

Reports

If you're working with ownCloud support and need to send them a configuration summary, you can generate it using the `configreport:generate` command. This command generates the same JSON-based report as the Admin Config Report, which you can access under `admin -> Settings -> Admin -> General -> Generate Config Report -> Download ownCloud config report`.

From the command-line in the root directory of your ownCloud installation, run it as your webserver user as follows, (assuming your webserver user is `www-data`):

```
sudo -u www-data occ configreport:generate
```

This generates the report and send it to `STDOUT`. You can optionally pipe the output to a file and then attach it to an email to ownCloud support, by running the following command:

```
sudo -u www-data occ configreport:generate > generated-config-report.txt
```

Alternatively, you could generate the report and email it all in one command, by running:

```
sudo -u www-data occ configreport:generate | mail -s "configuration report" \  
-r <the email address to send from> \  
support@owncloud.com
```

Note: These commands are not available in *single-user (maintenance) mode*.

Ransomware Protection

Use these commands to help users recover from a Ransomware attack. You can find more information about the application *in the documentation*.

Note: Ransomware Protection (which is an Enterprise app) needs to be installed and enabled to be able to use these commands.

```
occ ransomguard:scan <timestamp> <user>      Report all changes in a user's account, starting from time  
occ ransomguard:restore <timestamp> <user>  Revert all operations in a user account after a point in  
occ ransomguard:lock <user>                 Set a user account as read-only for ownCloud and other W  
clients when malicious activity is suspected.  
occ ransomguard:unlock <user>               Unlock a user account after ransomware issues have been r
```

Shibboleth Modes (Enterprise Edition only)

```
shibboleth:mode sets your Shibboleth mode to notactive, autoprovision, or ssoonly  
shibboleth:mode [mode]
```

Note: These commands are only available when the “Shibboleth user backend” app (`user_shibboleth`) is enabled.

Two-factor Authentication

If a two-factor provider app is enabled, it is enabled for all users by default (though the provider can decide whether or not the user has to pass the challenge). In the case of an user losing access to the second factor (e.g., a lost phone with two-factor SMS verification), the admin can temporarily disable the two-factor check for that user via the `occ` command:

```
sudo -u www-data php occ twofactor:disable <username>
```

To re-enable two-factor authentication again, use the following command:

```
sudo -u www-data php occ twofactor:enable <username>
```

6.5.5 Configuring the Activity App

You can configure your ownCloud server to automatically send out e-mail notifications to your users for various events like:

- A file or folder has been shared
- A new file or folder has been created
- A file or folder has been changed
- A file or folder has been deleted

Users can see actions (delete, add, modify) that happen to files they have access to. Sharing actions are only visible to the sharer and recipient.

Enabling the Activity App

The Activity App is shipped and enabled by default. If it is not enabled simply go to your ownCloud Apps page to enable it.

Configuring your ownCloud for the Activity App

To configure your ownCloud to send out e-mail notifications a working *Email Configuration* is mandatory.

Furthermore it is recommended to configure the background job `Webcron` or `Cron` as described in *Background Jobs*.

There is also a configuration option `activity_expire_days` available in your `config.php` (See *Core Config.php Parameters*) which allows you to clean-up older activities from the database.

6.5.6 Virus Scanner Support

Overview

ClamAV is the only *officially* supported virus scanner available for use with ownCloud. It:

- Operates on all major operating systems, including *Windows*, *Linux*, and *Mac*
- Detects all forms of malware including *Trojan horses*, *viruses*, and *worms*
- Scans *compressed files*, *executables*, *image files*, *Flash*, *PDF*, as well as many others

What's more, *ClamAV's Freshclam daemon* automatically updates its malware signature database at scheduled intervals. However, other scanners can be used, so long as they:

1. Can receive data streams via pipe on the command-line and return an exit code
2. Return a parsable result on stdout

How ClamAV Works With ownCloud

Before you install and configure ClamAV, here is a bit of background which may be handy to know. ownCloud integrates with anti-virus tools by connecting to them via:

- A URL and port
- A socket
- Streaming the data from the command-line via a pipe with a configured executable

In the case of ClamAV, ownCloud's Antivirus extension sends files as streams to a ClamAV service (which can be on the same ownCloud server or another server within the same network) which in turn scans them and returns a result to stdout.

Note: Individual chunks are **not** scanned. The whole file is scanned when it is moved to the final location.

The information is then parsed or an exit code is evaluated if no result is available to determine the response from the scan. Based on ownCloud's evaluation of the response (or exit code) an appropriate action is then taken, such as recording a log message or deleting the file.

Note: Scanner exit status rules are used to handle errors when ClamAV is run in CLI mode. Scanner output rules are used in daemon/socket mode.

Things To Note

1. Files are checked when they are uploaded or updated (whether because they were edited or saved) but *not* when they are downloaded.
2. ownCloud doesn't support a cache of previously scanned files.
3. If the app is either not configured or is misconfigured, then it rejects file uploads.
4. If ClamAV is unavailable, then the app rejects file uploads.
5. A file size limit applies both to background jobs and to file uploads.

Configuring the ClamAV Antivirus Scanner

You can configure your ownCloud server to automatically run a virus scan on newly-uploaded files using the [Antivirus App for Files](#).

Note: ClamAV must be installed before installing and configuring Antivirus App for Files.

Installing ClamAV

As always, Linux distributions install and configure ClamAV in different ways. Below you can find the instructions for installing it on Debian or Red Hat-based distributions.

Debian, Ubuntu, Linux Mint

On Debian, Ubuntu, and their many variants, install ClamAV with the following command:

```
sudo apt-get install clamav clamav-daemon
```

This automatically creates the default configuration files and launches the `clamd` and `freshclam` daemons. You shouldn't have to do anything else, though it is a good idea to review the ClamAV documentation, as well ClamAV's settings in `/etc/clamav/`.

Red Hat 7 and CentOS 7

On Red Hat 7 and related systems, you must install the "Extra Packages for Enterprise Linux (EPEL)" repository, and then install ClamAV. To do so, run the following commands:

```
yum install epel-release
yum install clamav clamav-scanner clamav-scanner-systemd clamav-server
clamav-server-systemd clamav-update
```

Note: Regardless of your operating system, we recommend that you enable verbose logging in both `clamd.conf` and `freshclam.conf` until you get any kinks with your ClamAV installation worked out.

Configuring and Running ClamAV

After installing ClamAV and the related tools, you will now have two configuration files: `/etc/freshclam.conf` and `/etc/clamd.d/scan.conf`. You must edit both of these before you can run ClamAV. Both files are well commented. Running either `man clamd.conf` or `man freshclam.conf` will provide detailed information on all the available configuration options.

Note: Refer to `/etc/passwd` and `/etc/group` when you need to verify the ClamAV user and group.

When you're finished editing the configuration files, you must enable the `clamd` service file and start `clamd`. You can do so using the following commands:

```
systemctl enable clamav-daemon.service
systemctl start clamav-daemon.service
```

That should take care of everything.

Note: Enable verbose logging in `scan.conf` and `freshclam.conf` until it is running the way you want.

Automating ClamAV Virus Database Updates

To update your malware database and get the latest malware signatures, you need to run `freshclam` frequently. Do this by running `freshclam` or `sudo freshclam` on Debian-based distributions.

We recommend you do this, post-installation, to download your first set of malware signatures. If you want to adjust `freshclam`'s behavior, edit `/etc/clamav/freshclam.conf` and make any changes you believe are necessary.

After that, create a [cron job](#) to automate the process. For example, to run it every hour at 47 minutes past the hour, add the following in the applicable user's crontab:

```
# m h dom mon dow command
47 * * * * /usr/bin/freshclam --quiet
```

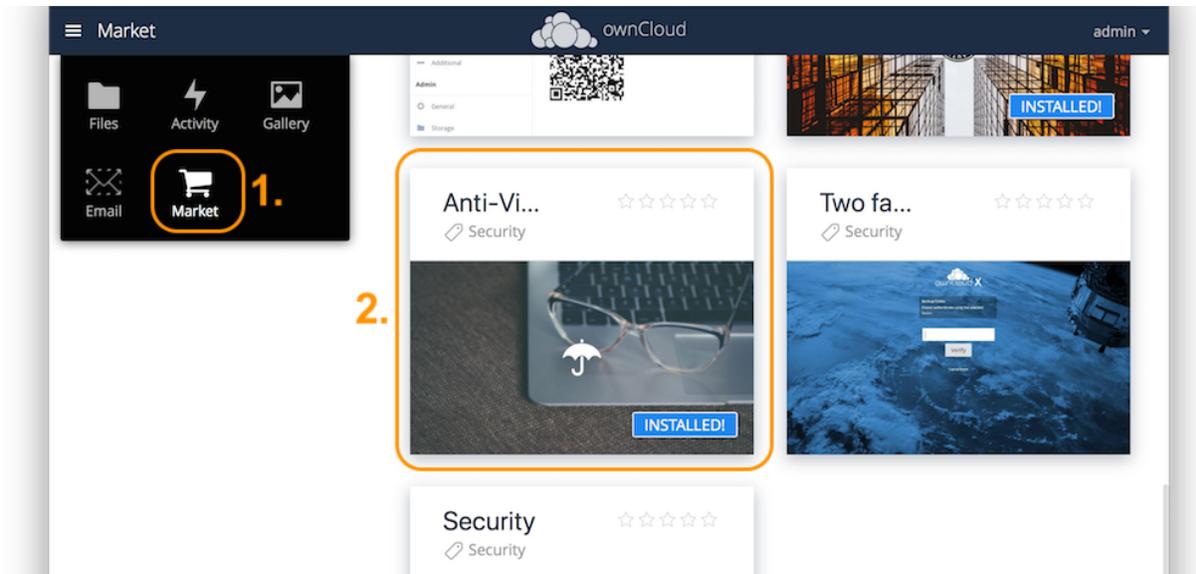
Note: Please avoid any multiples of 10, because those are when the ClamAV servers are hit the hardest for updates.

Install the Anti-Virus App

The Anti-Virus app needs to be installed from the ownCloud Market, under “*Security*”. You can access the ownCloud Market via the App Menu (or App Switcher).

Configuring ClamAV within ownCloud

Once it is installed, go to your ownCloud Admin page and set your ownCloud logging level to `Everything`.



Log

Log level **Everything (fatal issues, errors, warnings, info, debug)**

Now, navigate to `Settings -> Admin -> Security`, where you'll find the “**Antivirus Configuration**” panel. There, as below, you'll see the configuration options which ownCloud will pass to ClamAV.

Configuration Warnings

The Antivirus App for Files will show one of three warnings if it is either misconfigured, or ClamAV is not available. You can see an example of all three below.

Mode Configuration

ClamAV runs in one of three modes: `Daemon (Socket)`, `Daemon`, and `Executable`.

Daemon (Socket)

In this mode, ClamAV runs in the background on the same server as the ownCloud installation. When there is no activity `clamd` places a minimal load on your system. However, if your users upload large volumes of files, you will see high CPU usage. Please keep this in mind.

ownCloud should detect your `clamd` socket and fill in the `Socket` field. This is the `LocalSocket` option in `clamd.conf`. You can run `netstat` to verify:

```
netstat -a|grep clam
unix 2 [ ACC ] STREAM LISTENING 15857 /var/run/clamav/clamdctl
```

The `Stream Length` value sets the number of bytes to read in one pass. 10485760 bytes, or ten megabytes, is the default. This value should be no larger than the PHP `memory_limit` settings or physical memory if `memory_limit` is set to `-1` (no limit).

Antivirus Configuration

Mode

Stream Length bytes

Path to clamscan

Extra command line options (comma-separated)

File size limit, -1 means no limit bytes

When infected files were found during a background scan

Antivirus app is misconfigured or antivirus inaccessible. Could not connect to host "localhost" on port 999 ✕

Antivirus app is misconfigured or antivirus inaccessible. The antivirus executable could not be found at path "/usr/bin/clamsfcan" ✕

Antivirus app is misconfigured or antivirus inaccessible. Could not connect to socket "/var/run/clamav/cslamd-socket": No such file or directory (code 2) ✕

Antivirus Configuration

Mode

Socket

Stream Length bytes

File size limit, -1 means no limit bytes

When infected files were found during a background scan

Action for infected files found while scanning gives you the choice of logging any alerts without deleting the files or immediately deleting infected files.

Daemon

In this mode, ClamAV runs on a different server. This is a good option for ownCloud servers with high volumes of file uploads. For the Daemon option, you need the hostname or IP address of the remote server running ClamAV and the server's port number.

Antivirus Configuration

The screenshot shows the 'Antivirus Configuration' interface. The 'Mode' is set to 'Daemon (Socket)'. The 'Socket' is '/var/run/clamav/clamd'. The 'Stream Length' is '26214400 bytes'. The 'File size limit, -1 means no limit' is '-1 bytes'. Below these fields, there is a dropdown menu for 'When infected files were found during a background scan' with two options: 'Only log' (selected) and 'Delete file'. A 'Save' button is located at the bottom left of the configuration area.

Executable

In this mode, ClamAV runs on the same server as the ownCloud installation, and the `clamscan` command only runs when a file is uploaded. `clamscan` is slow and not always reliable for on-demand usage; it is better to use one of the daemon modes.

This option requires the path to `clamscan`, which is the interactive ClamAV scanning command. ownCloud should find it automatically.

When you are satisfied with how ClamAV is operating, you might want to go back and change all of your logging to less verbose levels.

Rule Configuration

ownCloud provides the ability to customize how it reacts to the response given by an anti-virus scan. To do so, under *Admin -> Antivirus Configuration -> Advanced*, which you can see in the screenshot below, you can view and change the existing rules. You can also add new ones.

Rules can match on either an exit status (e.g., `0`, `1`, or `40`) or a pattern in the string returned from ClamAV (e.g., `/. * : (. *) FOUND$/`).

Here are some points to bear in mind about rules:

- Scanner exit status rules are used to handle errors when ClamAV is run in CLI mode while

Antivirus Configuration

Mode

Stream Length bytes

Path to clamscan

Extra command line options (comma-separated)

File size limit, -1 means no limit bytes

When infected files were found during a background scan

Match by	The exit status code returned by ClamAV to match against	A human-readable description of what the status code means	The action to take when that status is returned
<input checked="" type="checkbox"/>	Scanner exit status - 0		Clean <input type="button" value="🗑️"/>
<input checked="" type="checkbox"/>	Scanner exit status - 1		Infected <input type="button" value="🗑️"/>
<input checked="" type="checkbox"/>	Scanner exit status - 40	Unknown option passed.	Unchecked <input type="button" value="🗑️"/>
<input checked="" type="checkbox"/>	Scanner exit status - 50	Database initialization error.	Unchecked <input type="button" value="🗑️"/>
<input checked="" type="checkbox"/>	Scanner output - /.* OKS/	Scanned successfully	Clean <input type="button" value="🗑️"/>
<input checked="" type="checkbox"/>	Scanner output - /.* (.*?) FOUNDS/	FOUND virus	Infected <input type="button" value="🗑️"/>
<input checked="" type="checkbox"/>	Scanner output - /.* (.*?) ERRORS/	Error scanning file	Unchecked <input type="button" value="🗑️"/>

Annotations:

- Whether to match on the exit status or scanner output (points to Match by)
- The exit status code returned by ClamAV to match against (points to Scanner exit status)
- A human-readable description of what the status code means (points to Description)
- The action to take when that status is returned (points to Mark as)
- Delete an existing rule (points to trash icon)
- Confirm the new rule or existing rule changes (points to checked checkboxes)
- A regular expression to match against the search response text returned by ClamAv (points to Scanner output)

- scanner output rules are used in daemon/socket mode.
- Daemon output is parsed by regexp.
- In case there are no matching rules, the status is: *Unknown*, and a warning will be logged.

Default Ruleset

The default rule set for ClamAV is populated automatically with the following rules:

Exit Status or Signature	Description	Marks File As
0		Clean
1		Infected
40	Unknown option passed	Unchecked
50	Database initialization error	Unchecked
52	Not supported file type	Unchecked
53	Can't open directory	Unchecked
54	Can't open file	Unchecked
55	Error reading file	Unchecked
56	Can't stat input file	Unchecked
57	Can't get absolute path name of current working directory	Unchecked
58	I/O error	Unchecked
62	Can't initialize logger	Unchecked
63	Can't create temporary files/directories	Unchecked
64	Can't write to temporary directory	Unchecked
70	Can't allocate memory (calloc)	Unchecked
71	Can't allocate memory (malloc)	Unchecked
/. *: OK\$/		Clean
/. *: (.*) FOUND\$/		Infected
/. *: (.*) ERROR\$/		Unchecked

The rules are always checked in the following order:

1. Infected
2. Error
3. Clean

In case there are no matching rules, the status would be *Unknown* and a warning would be logged.

Update An Existing Rule To match on an exit status, change the “**Match by**” dropdown list to “**Scanner exit status**” and in the “**Scanner exit status or signature to search**” field, add the status code to match on.

To match on the scanner’s output, change the “**Match by**” dropdown list to “**Scanner output**” and in the “**Scanner exit status or signature to search**” field, add the regular expression to match against the scanner’s output.

Then, while not mandatory, add a description of what the status or scan output means. After that, set what ownCloud should do when the exit status or regular expression you set matches the value returned by ClamAV. To do so change the value of the dropdown in the “**Mark as**” column.

The dropdown supports the following three options:

Option	Description
Clean	The file is clean, and contains no viruses
Infected	The file contains a virus
Unchecked	No action should be taken

With all these changes made, click the check mark on the lefthand side of the “**Match by**” column, to confirm the change to the rule.

Add A New Rule To add a new rule, click the button marked “Add a rule” at the bottom left of the rules table. Then follow the process outlined in *Update An Existing Rule*.

Delete An Existing Rule To delete an existing rule, click the rubbish bin icon on the far right-hand side of the rule that you want to delete.

6.5.7 Memory Caching

You can significantly improve ownCloud server performance by using memory caching. This is the process of storing frequently-requested objects in-memory for faster retrieval later. There are two types of memory caching available:

A PHP opcode Cache (OPcache): An opcode cache stores compiled PHP scripts so they don’t need to be re-compiled every time they are called. These compiled PHP scripts are stored in-memory, on the server on which they’re compiled.

A Data Cache: A data cache stores copies of *data*, *templates*, and other types of *information-based files*. Depending on the cache implementation, it can be either *local*, or specific, to one server, or *distributed* across multiple servers. This cache type is ideal when you have a scale-out installation.

Supported Caching Backends

The caching backends supported by ownCloud are:

- *APCu*: This is a local cache for systems running PHP 5.6 and up. APCu 4.0.6 and up is required. Alternatively you can use *the Zend OPcache*. However, **it is not a data cache**, only an opcode cache.
- *Redis*: This is a distributed cache for multi-server ownCloud installations. Version 2.2.6 or higher of the PHP Redis extension is required.
- *Memcached*: This is a distributed cache for multi-server ownCloud installations.

Note: You may use *both* a local and a distributed cache. The recommended ownCloud caches are APCu and Redis.

Note: If you do not install and enable a local memory cache you will see a warning on your ownCloud admin page. If you enable only a distributed cache in your `config.php` (`memcache.distributed`) and not a local cache (`memcache.local`) you will still see the cache warning.

Cache Directory Location

The cache directory defaults to `data/$user/cache` where `$user` is the current user. You may use the `'cache_path'` directive in `config.php` (See *Core Config.php Parameters*) to select a different location.

Cache Types

APCu

PHP 5.6 and up include the Zend OPcache in core, and on most Linux distributions it is enabled by default. However, it *does not* bundle a data cache. Given that, we recommend that you use APCu instead. APCu is a data cache *and* is available in most Linux distributions.

Installing APCu

```
# On RedHat/CentOS/Fedora systems running PHP 5.6
yum install rh-php56-php-devel
pecl install apcu
```

```
# On RedHat/CentOS/Fedora systems running PHP 7.0
yum install rh-php70-php-devel
pecl install apcu
```

```
# On Debian/Ubuntu/Mint systems
apt-get install php-apcu
```

Note: On Ubuntu 14.04 LTS, the APCu version is 4.0.2. This is too old to use with ownCloud, which requires ownCloud 4.0.6+. You can install 4.0.7 from Ubuntu backports with the following command:

```
apt-get install php5-apcu/trusty-backports
```

After APCu's installed, enable the extension by creating a configuration file for it, using the following commands.

```
cat << EOF > /etc/opt/rh/rh-php70/php.d/20-apcu.ini
; APCu php extension
extension=apcu.so
EOF
```

With that done, assuming that you don't encounter any errors, restart Apache and the extension is ready to use.

Redis

Redis is an excellent modern memory cache to use for both distributed caching and as a local cache for *Transactional File Locking*, because it guarantees that cached objects are available for as long as they are needed.

The Redis PHP module must be at least version 2.2.6 or higher. If you are running a Linux distribution that does not package the supported versions of this module — or does not package Redis at all — see *Installing Redis on other distributions*.

Note: Debian Jessie users, please see this [GitHub discussion](#) if you have problems with LDAP authentication when using Redis.

Installing Redis on Debian-based Distributions On Debian/Ubuntu/Mint run the following command:

```
apt-get install redis-server php5-redis
```

If you have Ubuntu 16.04 or higher:

```
apt install redis-server php-redis
```

The installer will automatically launch Redis and configure it to launch at startup.

Note: If you're running ownCloud on Ubuntu 14.04, which does not package the required version of `php5-redis`, then work through [this guide on Tech and Me](#) to see how to install and configure it.

Installing Redis on RedHat, CentOS, and Fedora On RedHat, CentOS, and Fedora run the following commands to install Redis:

```
yum install rh-php70-php-devel rh-redis32-redis
pecl install redis
```

Unlike on Debian-based distributions, Redis will not start automatically on *RedHat*, *Centos*, and *Fedora*. Given that, you must use your service manager to both start Redis, and to launch it at boot time as a daemon. To do so, run the following commands:

```
systemctl start rh-redis32-redis
systemctl enable rh-redis32-redis
```

You can verify that the Redis daemon is running using either of the following two commands:

```
ps ax | grep redis
netstat -tlnp | grep redis
```

When it's running, enable the Redis extension by creating a configuration file for it, using the following commands.

```
cat << EOF > /etc/opt/rh/rh-php70/php.d/20-redis.ini
; Redis php extension
extension=redis.so
EOF
```

After that, assuming that you don't encounter any errors, restart Apache and the extension is ready to use.

Additional notes for Redis vs. APCu on Memory Caching APCu is faster at local caching than Redis. If you have enough memory, use APCu for memory caching and Redis for file locking. If you are low on memory, use Redis for both.

Installing Redis on other distributions These instructions are adaptable for any distribution that does not package the supported version, or that does not package Redis at all, such as SUSE Linux Enterprise Server and RedHat Enterprise Linux.

Note: The [Redis PHP module](#) must be at least version 2.2.6.

On Debian/Mint/Ubuntu Use `apt-cache` to see the available `php5-redis` version, or the version of your installed package:

```
apt-cache policy php5-redis
```

On CentOS and Fedora The `yum` command shows available and installed version information:

```
yum search php-pecl-redis
```

Clearing the Redis Cache The Redis cache can be flushed from the command-line using the [redis-cli tool](#), as in the following example:

```
sudo redis-cli
SELECT <dbIndex>
FLUSHDB
```

<dbIndex> is the number of Redis database where the cache is stored. It is zero by default at ownCloud. To check what yours is currently set to, check the `dbindex` value in `config/config.php`. Here's an example of what to look for:

```
'redis' => [
  'host' => 'localhost', // Can also be a unix domain socket => '/tmp/redis.sock'
  'port' => 6379,
  'timeout' => 0,
  'password' => '', // Optional, if not defined no password will be used.
  'dbindex' => 0 // Optional, if undefined SELECT will not run and will
                // use Redis Server's default DB Index.
],
```

Further Reading

- <https://redis.io/commands/select>
- <https://redis.io/commands/flushdb>

Memcached

Memcached is a reliable old-timer for shared caching on distributed servers. It performs well with ownCloud with one exception: it is not suitable to use with *Transactional File Locking*. This is because it does not store locks, and data can disappear from the cache at any time. Given that, Redis is the best memory cache to use.

Note: Be sure to install the **memcached** PHP module, and not *memcache*, as in the following examples. ownCloud supports only the **memcached** PHP module.

Installing Memcached

On Debian/Ubuntu/Mint On Debian/Ubuntu/Mint run the following command:

```
apt-get install memcached php5-memcached
```

Note: The installer will automatically start *memcached* and configure it to launch at startup.

On RedHat/CentOS/Fedora On RedHat/CentOS/Fedora run the following command:

```
yum install memcached php-pecl-memcache
```

It will not start Memcached automatically after the installation or on subsequent reboots as a daemon, so you must do so yourself. To do so, run the following command:

```
systemctl start memcached
systemctl enable memcached
```

You can verify that the Memcached daemon is running using one of the following commands:

```
ps ax | grep memcached
netstat -tlnp | grep memcached
```

With the extension installed, you now need to configure it, by creating a configuration file for it. You can do so using the command below, substituting `FILE_PATH` with one from the list below the command.

```
cat << EOF > FILE_PATH
; Memcached PHP extension
extension=memcached.so
EOF
```

Configuration File Paths	PHP Version	Filename
	5.6	/etc/opt/rh/rh-php56/php.d/25-memcached.ini
	7.0	/etc/opt/rh/rh-php70/php.d/25-memcached.ini

After that, assuming that you don't encounter any errors:

1. Restart your Web server
2. Add the appropriate entries to `config.php` (which you can find an example of below)
3. Refresh your ownCloud admin page

Clearing the Memcached Cache The Memcached cache can be flushed from the command-line using a range of common Linux/UNIX tools, including netcat and telnet. The following example uses telnet to login, run the `flush_all` command, and logout:

```
telnet localhost 11211
flush_all
quit
```

For more information see:

- <https://github.com/memcached/memcached/wiki/Commands#flushall>

Configuring Memory Caching

Memory caches must be explicitly configured in ownCloud by:

1. Installing and enabling your desired cache (whether that be the PHP extension and/or the caching server).
2. Adding the appropriate entry to ownCloud's `config.php`.

See *Core Config.php Parameters* for an overview of all possible config parameters. After installing and enabling your chosen memory cache, verify that it is active by running *PHP Version and Information*.

APCu Configuration

To use APCu, add this line to `config.php`:

```
'memcache.local' => '\OC\Memcache\APCu',
```

With that done, refresh your ownCloud admin page, and the cache warning should disappear.

Redis Configuration

This example `config.php` configuration uses Redis for the local server cache:

```
'memcache.local' => '\OC\Memcache\Redis',
'redis' => [
    'host' => 'localhost',
    'port' => 6379,
```

```
],  
'memcache.locking' => '\OC\Memcache\Redis', // Add this for best performance
```

If you want to connect to Redis configured to listen on an Unix socket, which is recommended if Redis is running on the same system as ownCloud, use this example configuration:

```
'memcache.local' => '\OC\Memcache\Redis',  
'redis' => [  
    'host' => '/var/run/redis/redis.sock',  
    'port' => 0,  
],
```

Redis is very configurable; consult [the Redis documentation](#) to learn more.

Memcached Configuration

This example uses APCu for the local cache, Memcached as the distributed memory cache, and lists all the servers in the shared cache pool with their port numbers:

```
'memcache.local' => '\OC\Memcache\APCu',  
'memcache.distributed' => '\OC\Memcache\Memcached',  
'memcached_servers' => [  
    ['localhost', 11211],  
    ['server1.example.com', 11211],  
    ['server2.example.com', 11211],  
],
```

Configuration Recommendations Based on Type of Deployment

Small/Private Home Server

```
// Only use APCu  
'memcache.local' => '\OC\Memcache\APCu',
```

Small Organization, Single-server Setup Use APCu for local caching, Redis for file locking

```
'memcache.local' => '\OC\Memcache\APCu',  
'memcache.locking' => '\OC\Memcache\Redis',  
'redis' => [  
    'host' => 'localhost',  
    'port' => 6379,  
],
```

Large Organization, Clustered Setup Use Redis for everything except a local memory cache. Use the server's IP address or hostname so that it is accessible to other hosts:

```
'memcache.distributed' => '\OC\Memcache\Redis',  
'memcache.locking' => '\OC\Memcache\Redis',  
'memcache.local' => '\OC\Memcache\APCu',  
'redis' => [  
    'host' => 'server1', // hostname example  
    'host' => '12.34.56.78', // IP address example  
    'port' => 6379,  
],
```

Configuring Transactional File Locking

Transactional File Locking prevents simultaneous file saving. To use it, you have to enable it in `config.php` as in the following example, which uses Redis as the cache backend:

```
'filelocking.enabled' => true,
'memcache.locking' => '\OC\Memcache\Redis',
'redis' => [
    'host' => 'localhost',
    'port' => 6379,
    'timeout' => 0.0,
    'password' => '', // Optional, if not defined no password will be used.
],
```

Note: For enhanced security it is recommended to configure Redis to require a password. See <http://redis.io/topics/security> for more information.

Caching Exceptions

If ownCloud is configured to use either Memcached or Redis as a memory cache, please be aware that you may encounter issues with functionality. When these occur, it is usually a result of PHP being incorrectly configured, or the relevant PHP extension not being available.

In the table below, you can see all of the known reasons for reduced or broken functionality related to caching.

Setup/Configuration	Result
If file locking is enabled, but the locking cache class is missing, then an exception will appear in the web UI	The application will not be usable
If file locking is enabled and the locking cache is configured, but the PHP module missing.	There will be a white page/exception in web UI. It will be a full page issue, and the application will not be usable
All enabled, but the Redis server is not running	The application will be usable. But any file operation will return a “500 Redis went away” exception
If Memcache is configured for “local” and “distributed”, but the class is missing	There will be a white page and an exception written to the logs, This is because autoloading needs the missing class. So there is no way to show a page

6.5.8 Background Jobs

A system like ownCloud sometimes requires tasks to be done on a regular basis without requiring user interaction or hindering ownCloud’s performance. For that reason, as a system administrator, you can configure background jobs (for example, database clean-ups) to be executed without any user interaction.

These jobs are typically referred to as **Cron Jobs**. Cron jobs are commands or shell-based scripts that are scheduled to periodically run at fixed times, dates, or intervals. `cron.php` is an ownCloud internal process that runs such background jobs on demand.

ownCloud plug-in applications can register actions with `cron.php` automatically to take care of typical housekeeping operations. These actions can include garbage collecting of temporary files or checking for newly updated files using `files_scan()` on externally mounted file systems.

You can decide how often jobs get processed, we recommend an interval of one minute.

Cron Jobs

You can schedule Cron jobs in three ways: [Cron](#), [Webcron](#), or [AJAX](#). These can all be configured in the admin settings menu. However, the recommended method is to use Cron. The following sections describe the differences between each method.

There are a number of things to keep in mind when choosing an automation option:

Firstly, while the default method is AJAX, though the preferred way is to use Cron. The reason for this distinction is that AJAX is easier to get up and running. As a result, it makes sense (often times) to accept it in the interests of expediency.

However, doing so is known to cause issues, such as backlogs and potentially not running every job on a heavily-loaded system. What's more, an increasing amount of ownCloud automation has been migrated from Ajax to Cron in recent versions. For this reason, we encourage you to not use it for too long — especially if your site is rapidly growing.

Secondly, while Webcron is better than Ajax, it too has limitations. For example, running Webcron will only remove a single item from the job queue, not all of them. Cron, however, will clear the entire queue.

Note: It's for this reason that we encourage you to use Cron — if at all possible.

Cron

Using the operating system Cron feature is the preferred method for executing regular tasks. This method enables the execution of scheduled jobs without the inherent limitations which the web server might have.

For example, to run a Cron job on a *nix system every minute, under the default web server user (often, `www-data` or `wwwrun`) you must set up the following Cron job to call the **`cron.php`** script:

```
# crontab -u www-data -e
* * * * * /usr/bin/php -f /path/to/your/owncloud/cron.php
```

You can verify if the cron job has been added and scheduled by executing:

```
# crontab -u www-data -l
* * * * * /usr/bin/php -f /path/to/your/owncloud/cron.php
```

Note: You have to make sure that `php` is found by `cron`, hence why we've deliberately added the full path to the PHP binary above (`/usr/bin/php`). On some systems it might be necessary to use **`php-cli`** instead of **`php`**.

Please refer to the [crontab man page](#) for the exact command syntax if you don't want to have it run every minute.

Note: There are other methods to invoke programs by the system regularly, e.g. [systemd timers](#)

Webcron

By registering your ownCloud `cron.php` script address as an external webcron service (for example, [easyCron](#)), you ensure that background jobs are executed regularly. To use this type of service, your external webcron service must be able to access your ownCloud server using the Internet. For example:

URL to call: `http[s]://<domain-of-your-server>/owncloud/cron.php`

AJAX

The AJAX scheduling method is the default option. However, it is also the *least* reliable. Each time a user visits the ownCloud page, a single background job is executed. The advantage of this mechanism, however, is that it does not require access to the system nor registration with a third party service. The disadvantage of this mechanism, when compared to the [Webcron](#) service, is that it requires regular visits to the page for it to be triggered.

Note: Especially when using the Activity App or external storages, where new files are added, updated, or deleted one of the other methods should be used.

Parallel Task Execution

Regardless of the approach which you take, since ownCloud 9.1, Cron jobs can be run in parallel. This is done by running `cron.php` multiple times. Depending on the process which you're automating, this may not be necessary. However, for longer-running tasks, such as those which are LDAP related, it may be very beneficial.

There is no way to do so via the ownCloud UI. But, the most direct way to do so, is by opening three console tabs and in each one run `php cron.php`. Each of these processes would acquire their own list of jobs to process without overlapping any other.

Available Background Jobs

A number of existing background jobs are available to be run just for specific tasks.

Note: These jobs are generally only needed on large instances and can be run as background jobs. If the number of users in your installation ranges between 1,000 and 3,000, or if you're using LDAP and it becomes a bottleneck, then admins can delete several entries in the `oc_jobs` table and replace them with the corresponding `occ` command, which you can see here:

- `OCA\\DAV\\CardDAV\\SyncJob -> occ dav:sync-system-addressbook`
- `OCA\\Federation\\SyncJob -> occ federation:sync-addressbooks`
- `OCA\\Files_Trashbin\\BackgroundJob\\ExpireTrash -> occ trashbin:expire`
- `OCA\\Files_Versions\\BackgroundJob\\ExpireVersions -> occ versions:expire`

If used, these should be scheduled to run on a daily basis.

While not exhaustive, these include:

CleanupChunks The CleanupChunks command, `occ dav:cleanup-chunks`, will clean up outdated chunks (uploaded files) more than a certain number of days old and needs to be added to your crontab.

Note: There is no matching background job to delete from the `oc_jobs` table.

ExpireTrash The ExpireTrash job, contained in `OCA\\Files_Trashbin\\BackgroundJob\\ExpireTrash`, will remove any file in the ownCloud trash bin which is older than the specified maximum file retention time. It can be run, as follows, using the OCC command:

```
occ trashbin:expire
```

ExpireVersions The ExpireVersions job, contained in `OCA\Files_Versions\BackgroundJob\ExpireVersions`, will expire versions of files which are older than the specified maximum version retention time. It can be run, as follows, using the OCC command:

```
occ versions:expire
```

Warning: Please take care when adding ExpireTrash and ExpireVersions as Cron jobs. Make sure that they're not started in parallel on multiple machines. Running in parallel on a single machine is fine. But, currently, there isn't sufficient locking in place to prevent them from conflicting with each other if running in parallel across multiple machines.

SyncJob (CardDAV) The CardDAV SyncJob, contained in `OCA\DAV\CardDAV\SyncJob`, syncs the local system address book, updating any existing contacts, and deleting any expired contacts. It can be run, as follows, using the OCC command:

```
occ dav:sync-system-addressbook
```

SyncJob (Federation) `OCAFederationSyncJob`

It can be run, as follows, using the OCC command:

```
occ federation:sync-addressbooks
```

6.5.9 Core Config.php Parameters

ownCloud uses the `config/config.php` file to control server operations. `config/config.sample.php` lists all the configurable parameters within ownCloud, along with example or default values. This document provides a more detailed reference. Most options are configurable on your Admin page, so it is usually not necessary to edit `config/config.php`.

Note: The installer creates a configuration containing the essential parameters. Only manually add configuration parameters to `config/config.php` if you need to use a special value for a parameter. **Do not copy everything from `config/config.sample.php`. Only enter the parameters you wish to modify!**

ownCloud supports loading configuration parameters from multiple files. You can add arbitrary files ending with `.config.php` in the `config/` directory, for example you could place your email server configuration in `email.config.php`. This allows you to easily create and manage custom configurations, or to divide a large complex configuration file into a set of smaller files. These custom files are not overwritten by ownCloud, and the values in these files take precedence over `config.php`.

Default Parameters

These parameters are configured by the ownCloud installer, and are required for your ownCloud server to operate.

```
'instanceid' => '',
```

This is a unique identifier for your ownCloud installation, created automatically by the installer. This example is for documentation only, and you should never use it because it will not work. A valid `instanceid` is created when you install ownCloud.

```
'instanceid' => 'd3c944a9a',
```

```
'passwordsalt' => '',
```

The salt used to hash all passwords, auto-generated by the ownCloud installer. (There are also per-user salts.) If you lose this salt you lose all your passwords. This example is for documentation only, and you should never use it.

```
'trusted_domains' =>
  array (
    'demo.example.org',
    'otherdomain.example.org',
  ),
```

Your list of trusted domains that users can log into. Specifying trusted domains prevents host header poisoning. Do not remove this, as it performs necessary security checks. Please consider that for backend processes like background jobs or occ commands, the url parameter in key `overwrite.cli.url` is used. For more details please see that key.

```
'cors.allowed-domains' => [
    'https://foo.example.org',
],
```

The global list of CORS domains. All users can use tools running CORS requests from the listed domains.

```
'datadirectory' => '/var/www/owncloud/data',
```

Where user files are stored; this defaults to `data/` in the ownCloud directory. The SQLite database is also stored here, when you use SQLite.

(SQLite is not available in ownCloud Enterprise Edition)

```
'version' => '',
```

The current version number of your ownCloud installation. This is set up during installation and update, so you shouldn't need to change it.

```
'version.hide' => false,
```

While hardening an ownCloud instance hiding the version information in `status.php` can be a legitimate step. Please consult the documentation before enabling this.

```
'show_server_hostname' => false,
```

Optionally, show the hostname of the server in `status.php`. Defaults to hidden

```
'dbtype' => 'sqlite',
```

Identifies the database used with this installation. See also config option `supportedDatabases`

Available:

- `sqlite` (SQLite3 - Not in Enterprise Edition)
- `mysql` (MySQL/MariaDB)
- `pgsql` (PostgreSQL)
- `oci` (Oracle - Enterprise Edition Only)

```
'dbhost' => '',
```

Your host server name, for example `localhost`, `hostname`, `hostname.example.com`, or the IP address. To specify a port use `hostname:####`; to specify a Unix socket use `localhost:/path/to/socket`.

```
'dbname' => 'owncloud',
```

The name of the ownCloud database, which is set during installation. You should not need to change this.

```
'dbuser' => '',
```

The user that ownCloud uses to write to the database. This must be unique across ownCloud instances using the same SQL database. This is set up during installation, so you shouldn't need to change it.

```
'dbpassword' => '',
```

The password for the database user. This is set up during installation, so you shouldn't need to change it.

```
'dbtableprefix' => '',
```

Prefix for the ownCloud tables in the database.

```
'installed' => false,
```

Indicates whether the ownCloud instance was installed successfully; `true` indicates a successful installation, and `false` indicates an unsuccessful installation.

Default config.php Examples

When you use SQLite as your ownCloud database, your `config.php` looks like this after installation. The SQLite database is stored in your ownCloud `data/` directory. SQLite is a simple, lightweight embedded database that is good for testing and for simple installations, but for production ownCloud systems you should use MySQL, MariaDB, or PostgreSQL.

```
<?php

$CONFIG = [
    'instanceid' => 'occ6f7365735',
    'passwordsalt' => '2c5778476346786306303',
    'trusted_domains' => [
        0 => 'localhost',
        1 => 'studio',
    ],
    'datadirectory' => '/var/www/owncloud/data',
    'dbtype' => 'sqlite3',
    'version' => '7.0.2.1',
    'installed' => true,
    'operation.mode' => 'single-instance',
];
```

This example is from a new ownCloud installation using MariaDB

```
<?php

$CONFIG = [
    'instanceid' => 'oc8c0fd71e03',
    'passwordsalt' => '515a13302a6b3950a9d0fdb970191a',
    'trusted_domains' => [
        0 => 'localhost',
        1 => 'studio',
        2 => '192.168.10.155'
    ],
    'datadirectory' => '/var/www/owncloud/data',
    'dbtype' => 'mysql',
];
```

```

    'version' => '7.0.2.1',
    'dbname' => 'owncloud',
    'dbhost' => 'localhost',
    'dbtableprefix' => 'oc_',
    'dbuser' => 'oc_carla',
    'dbpassword' => '67336bcdf7630dd80b2b81a413d07',
    'installed' => true,
    'operation.mode' => 'single-instance',
];

```

User Experience

These optional parameters control some aspects of the user interface. Default values, where present, are shown.

```
'default_language' => 'en_GB',
```

This sets the default language on your ownCloud server, using ISO_639-1 language codes such as `en` for English, `de` for German, and `fr` for French. It overrides automatic language detection on public pages like login or shared items. User's language preferences configured under “personal -> language” override this setting after they have logged in.

```
'defaultapp' => 'files',
```

Set the default app to open on login. Use the app names as they appear in the URL after clicking them in the Apps menu, such as `documents`, `calendar`, and `gallery`. You can use a comma-separated list of app names, so if the first app is not enabled for a user then ownCloud will try the second one, and so on. If no enabled apps are found it defaults to the Files app.

```
'knowledgebaseenabled' => true,
```

`true` enables the Help menu item in the user menu (top right of the ownCloud Web interface). `false` removes the Help item.

```
'enable_avatars' => true,
```

`true` enables avatars, or user profile photos. These appear on the User page, on user's Personal pages and are used by some apps (contacts, mail, etc). `false` disables them.

```
'allow_user_to_change_display_name' => true,
```

`true` allows users to change their display names (on their Personal pages), and `false` prevents them from changing their display names.

```
'remember_login_cookie_lifetime' => 60*60*24*15,
```

Lifetime of the remember login cookie, which is set when the user clicks the `remember` checkbox on the login screen. The default is 15 days, expressed in seconds.

```
'session_lifetime' => 60 * 60 * 24,
```

The lifetime of a session after inactivity; the default is 24 hours, expressed in seconds.

```
'session_keepalive' => true,
```

Enable or disable session keep-alive when a user is logged in to the Web UI.

Enabling this sends a “heartbeat” to the server to keep it from timing out.

```
'token_auth_enforced' => false,
```

Enforces token only authentication for apps and clients connecting to ownCloud.

If enabled, all access requests using the users password are blocked for enhanced security. Users have to generate special app-passwords (tokens) for their apps or clients in their personal settings which are further used for app or client authentication. Browser logon is not affected.

```
'login.alternatives' => [],
```

Allows to specify additional login buttons on the logon screen for e.g. SSO integration

```
'login.alternatives' => [ ['href' => 'https://www.testshib.org/Shibboleth.sso/ProtectNetwork?target=https%3A%2F%2Fmy.owncloud.tld%2Flogin%2Fsso-saml%2F', 'name' => 'ProtectNetwork', 'img' => '/img/PN_sign-in.gif'], ['href' => 'https://www.testshib.org/Shibboleth.sso/OpenIdP.org?target=https%3A%2F%2Fmy.owncloud.tld%2Flogin%2Fsso-saml%2F', 'name' => 'OpenIdP.org', 'img' => '/img/openidp.png'], ]
```

```
'csrf.disabled' => false,
```

Disable ownCloud's built-in CSRF protection mechanism.

In some specific setups CSRF protection is handled in the environment, e.g., running F5 ASM. In these cases the built-in mechanism is not needed and can be disabled. Generally speaking, however, this config switch should be left unchanged.

WARNING: leave this as is if you're not sure what it does

```
'skeletondirectory' => '/path/to/owncloud/core/skeleton',
```

The directory where the skeleton files are located. These files will be copied to the data directory of new users. Leave empty to not copy any skeleton files.

```
'user_backends' => array(
    array(
        'class' => 'OC_User_IMAP',
        'arguments' => array('{imap.gmail.com:993/imap/ssl}INBOX')
    )
),
```

The `user_backends` app (which needs to be enabled first) allows you to configure alternate authentication backends. Supported backends are: IMAP (OC_User_IMAP), SMB (OC_User_SMB), and FTP (OC_User_FTP).

```
'lost_password_link' => 'https://example.org/link/to/password/reset',
```

If your user backend does not allow password resets (e.g. when it's a read-only user backend like LDAP), you can specify a custom link, where the user is redirected to, when clicking the "reset password" link after a failed login-attempt.

In case you do not want to provide any link, replace the url with 'disabled'

```
'accounts.enable_medial_search' => true,
```

Allow medial search on account properties like display name, user id, email, and other search terms. Allows finding 'Alice' when searching for 'lic'.

May slow down user search. Disable this if you encounter slow username search in the sharing dialog.

```
'user.search_min_length' => 2,
```

Defines the minimum characters entered before a search returns results for users or groups in the share autocomplete form. Lower values increase search time especially for large backends.

Any exact matches to a user or group will be returned, even though less than the minimum characters have been entered. The search is case insensitive. e.g. entering “tom” will always return “Tom” if there is an exact match.

Mail Parameters

These configure the email settings for ownCloud notifications and password resets.

```
'mail_domain' => 'example.com',
```

The return address that you want to appear on emails sent by the ownCloud server, for example `oc-admin@example.com`, substituting your own domain, of course.

```
'mail_from_address' => 'owncloud',
```

FROM address that overrides the built-in `sharing-noreply` and `lostpassword-noreply` FROM addresses.

```
'mail_smtpdebug' => false,
```

Enable SMTP class debugging.

```
'mail_smtpmode' => 'sendmail',
```

Which mode to use for sending mail: `sendmail`, `smtp`, `qmail` or `php`.

If you are using local or remote SMTP, set this to `smtp`.

If you are using PHP mail you must have an installed and working email system on the server. The program used to send email is defined in the `php.ini` file.

For the `sendmail` option you need an installed and working email system on the server, with `/usr/sbin/sendmail` installed on your Unix system.

For `qmail` the binary is `/var/qmail/bin/sendmail`, and it must be installed on your Unix system.

```
'mail_smtphost' => '127.0.0.1',
```

This depends on `mail_smtpmode`. Specify the IP address of your mail server host. This may contain multiple hosts separated by a semi-colon. If you need to specify the port number append it to the IP address separated by a colon, like this: `127.0.0.1:24`.

```
'mail_smtpport' => 25,
```

This depends on `mail_smtpmode`. Specify the port for sending mail.

```
'mail_smtptimeout' => 10,
```

This depends on `mail_smtpmode`. This sets the SMTP server timeout, in seconds. You may need to increase this if you are running an anti-malware or spam scanner.

```
'mail_smtpsecure' => '',
```

This depends on `mail_smtpmode`. Specify when you are using `ssl` or `tls`, or leave empty for no encryption.

```
'mail_smtpauth' => false,
```

This depends on `mail_smtpmode`. Change this to `true` if your mail server requires authentication.

```
'mail_smtpauthtype' => 'LOGIN',
```

This depends on `mail_smtpmode`. If SMTP authentication is required, choose the authentication type as `LOGIN` (default) or `PLAIN`.

```
'mail_smtpname' => '',
```

This depends on `mail_smtpauth`. Specify the username for authenticating to the SMTP server.

```
'mail_smtppassword' => '',
```

This depends on `mail_smtpauth`. Specify the password for authenticating to the SMTP server.

Proxy Configurations

```
'overwritehost' => '',
```

The automatic hostname detection of ownCloud can fail in certain reverse proxy and CLI/cron situations. This option allows you to manually override the automatic detection; for example `www.example.com`, or specify the port `www.example.com:8080`.

```
'overwriteprotocol' => '',
```

When generating URLs, ownCloud attempts to detect whether the server is accessed via `https` or `http`. However, if ownCloud is behind a proxy and the proxy handles the `https` calls, ownCloud would not know that `ssl` is in use, which would result in incorrect URLs being generated.

Valid values are `http` and `https`.

```
'overwritewebroot' => '',
```

ownCloud attempts to detect the webroot for generating URLs automatically.

For example, if `www.example.com/owncloud` is the URL pointing to the ownCloud instance, the webroot is `/owncloud`. When proxies are in use, it may be difficult for ownCloud to detect this parameter, resulting in invalid URLs.

```
'overwritecondaddr' => '',
```

This option allows you to define a manual override condition as a regular expression for the remote IP address. The keys `overwritewebroot`, `overwriteprotocol`, and `overwritehost` are subject to this condition.

For example, defining a range of IP addresses starting with `10.0.0.` and ending with `1` to `3`: `*^10\.0\.0\.[1-3]$`

```
'overwrite.cli.url' => '',
```

Use this configuration parameter to specify the base URL for any URLs which are generated within ownCloud using any kind of command line tools (cron or occ). The value should contain the full base URL: `https://www.example.com/owncloud` As an example, alerts shown in the browser to upgrade an app are triggered by a cron background process and therefore uses the url of this key, even if the user has logged on via a different domain defined in key `trusted_domains`. When the user clicks an alert like this, he will be redirected to that URL and must logon again.

```
'htaccess.RewriteBase' => '/',
```

To have clean URLs without `/index.php` this parameter needs to be configured.

This parameter will be written as “RewriteBase” on update and installation of ownCloud to your `.htaccess` file. While this value is often simply the URL path of the ownCloud installation it cannot be set automatically properly in every scenario and needs thus some manual configuration.

In a standard Apache setup this usually equals the folder that ownCloud is accessible at. So if ownCloud is accessible via “`https://mycloud.org/owncloud`” the correct value would most likely be “`/owncloud`”. If ownCloud is running under “`https://mycloud.org`” then it would be “`/`”.

Note that the above rule is not valid in every case, as there are some rare setup cases where this may not apply. However, to avoid any update problems this configuration value is explicitly opt-in.

After setting this value run `occ maintenance:update:htaccess`. Now, when the following conditions are met ownCloud URLs won't contain `index.php`:

- `mod_rewrite` is installed
- `mod_env` is installed

```
'proxy' => '',
```

The URL of your proxy server, for example `proxy.example.com:8081`.

```
'proxyuserpwd' => '',
```

The optional authentication for the proxy to use to connect to the internet.

The format is: `username:password`.

Deleted Items (trash bin)

These parameters control the Deleted files app.

```
'trashbin_retention_obligation' => 'auto',
```

If the trash bin app is enabled (default), this setting defines the policy for when files and folders in the trash bin will be permanently deleted.

The app allows for two settings, a minimum time for trash bin retention, and a maximum time for trash bin retention. Minimum time is the number of days a file will be kept, after which it may be deleted. Maximum time is the number of days at which it is guaranteed to be deleted. Both minimum and maximum times can be set together to explicitly define file and folder deletion. For migration purposes, this setting is installed initially set to “auto”, which is equivalent to the default setting in ownCloud 8.1 and before.

Available values:

- **auto** default setting. Keeps files and folders in the deleted files for up to 30 days, automatically deleting them (at any time) if space is needed. Note: files may not be removed if space is not required.
- **D, auto** keeps files and folders in the trash bin for D+ days, delete anytime if space needed (note: files may not be deleted if space is not needed)
- **auto, D** delete all files in the trash bin that are older than D days automatically, delete other files anytime if space needed
- **D1, D2** keep files and folders in the trash bin for at least D1 days and delete when exceeds D2 days
- **disabled** trash bin auto clean disabled, files and folders will be kept forever

File versions

These parameters control the Versions app.

```
'versions_retention_obligation' => 'auto',
```

If the versions app is enabled (default), this setting defines the policy for when versions will be permanently deleted.

The app allows for two settings, a minimum time for version retention, and a maximum time for version retention. Minimum time is the number of days a version will be kept, after which it may be deleted. Maximum time is the number of days at which it is guaranteed to be deleted. Both minimum and maximum times can be set together to

explicitly define version deletion. For migration purposes, this setting is installed initially set to “auto”, which is equivalent to the default setting in ownCloud 8.1 and before.

Available values:

- **auto** default setting. Automatically expire versions according to expire rules. Please refer to `../configuration/files/file_versioning` for more information.
- **D, auto** keep versions at least for D days, apply expire rules to all versions that are older than D days
- **auto, D** delete all versions that are older than D days automatically, delete other versions according to expire rules
- **D1, D2** keep versions for at least D1 days and delete when exceeds D2 days
- **disabled** versions auto clean disabled, versions will be kept forever

ownCloud Verifications

ownCloud performs several verification checks. There are two options, `true` and `false`.

```
'updatechecker' => true,
```

Check if ownCloud is up-to-date and shows a notification if a new version is available. This option is only applicable to ownCloud core. It is not applicable to app updates.

```
'updater.server.url' => 'https://updates.owncloud.com/server/',
```

URL that ownCloud should use to look for updates

```
'has_internet_connection' => true,
```

Is ownCloud connected to the Internet or running in a closed network?

```
'check_for_working_wellknown_setup' => true,
```

Allows ownCloud to verify a working `.well-known` URL redirects. This is done by attempting to make a request from JS to `https://your-domain.com/.well-known/caldav/`

```
'config_is_read_only' => false,
```

In certain environments it is desired to have a read-only configuration file.

When this switch is set to `true` ownCloud will not verify whether the configuration is writable. However, it will not be possible to configure all options via the Web interface. Furthermore, when updating ownCloud it is required to make the configuration file writable again for the update process.

```
'operation.mode' => 'single-instance',
```

This defines the mode of operations. The default value is ‘single-instance’ which means that ownCloud is running on a single node, which might be the most common operations mode. The only other possible value for now is ‘clustered-instance’ which means that ownCloud is running on at least 2 nodes. The mode of operations has various impact on the behavior of ownCloud.

Logging

These parameters configure the logging options. For additional information or advanced configuration, please see the logging section in the documentation.

```
'log_type' => 'owncloud',
```

By default the ownCloud logs are sent to the `owncloud.log` file in the default ownCloud data directory.

If syslogging is desired, set this parameter to `syslog`. Setting this parameter to `errorlog` will use the PHP `error_log` function for logging.

```
'logfile' => '/var/log/owncloud.log',
```

Log file path for the ownCloud logging type.

Defaults to `[datadirectory]/owncloud.log`

```
'loglevel' => 2,
```

Loglevel to start logging at. Valid values are: 0 = Debug, 1 = Info, 2 = Warning, 3 = Error, and 4 = Fatal. The default value is Warning.

```
'syslog_tag' => 'ownCloud',
```

If you maintain different instances and aggregate the logs, you may want to distinguish between them. `syslog_tag` can be set per instance with a unique id. Only available if `log_type` is set to `syslog`.

The default value is `ownCloud`.

```
'log.conditions' => [
    [
        'shared_secret' => '57b58edb6637fe3059b3595cf9c41b9',
        'users' => ['user1'],
        'apps' => ['files_texteditor'],
        'logfile' => '/tmp/test.log'
    ],
    [
        'shared_secret' => '57b58edb6637fe3059b3595cf9c41b9',
        'users' => ['user1'],
        'apps' => ['gallery'],
        'logfile' => '/tmp/gallery.log'
    ],
],
```

Log condition for log level increase based on conditions. Once one of these conditions is met, the required log level is set to debug. This allows to debug specific requests, users or apps

Supported conditions:

- **shared_secret:** if a request parameter with the name `log_secret` is set to this value the condition is met
- **users:** if the current request is done by one of the specified users, this condition is met
- **apps:** if the log message is invoked by one of the specified apps, this condition is met
- **logfile:** the log message invoked by the specified apps get redirected to this logfile, this condition is met Note: Not applicable when using `syslog`.

Defaults to an empty array.

```
'logdateformat' => 'F d, Y H:i:s',
```

This uses PHP.date formatting; see <http://php.net/manual/en/function.date.php>

```
'logtimezone' => 'Europe/Berlin',
```

The default timezone for logfiles is UTC. You may change this; see <http://php.net/manual/en/timezones.php>

```
'cron_log' => true,
```

Log successful cron runs.

```
'log_rotate_size' => false,
```

Enables log rotation and limits the total size of the logfiles.

The default is 0 or false which disables log rotation. Specify a size in bytes, for example 104857600 (100 megabytes = 100 * 1024 * 1024 bytes). A new logfile is created with a new name when the old logfile reaches the defined limit. If a rotated log file is already present, it will be overwritten. If enabled, only the active log file and one rotated file are stored.

Alternate Code Locations

Some of the ownCloud code may be stored in alternate locations.

```
'customclient_desktop' =>
    'https://owncloud.org/install/#install-clients',
'customclient_android' =>
    'https://play.google.com/store/apps/details?id=com.owncloud.android',
'customclient_ios' =>
    'https://itunes.apple.com/us/app/owncloud/id543672169?mt=8',
```

This section is for configuring the download links for ownCloud clients, as seen in the first-run wizard and on Personal pages.

```
'apps_paths' =>
    array (
        0 =>
            array (
                'path' => OC::$SERVERROOT.'/apps',
                'url' => '/apps',
                'writable' => false,
            ),
        1 =>
            array (
                'path' => OC::$SERVERROOT.'/apps-external',
                'url' => '/apps-external',
                'writable' => true,
            ),
    ),
```

If you want to store apps in a custom directory instead of ownCloud's default `/app`, you need to modify the `apps_paths` key. There, you need to add a new associative array that contains three elements. These are:

- `path` The absolute file system path to the custom app folder.
- `url` The request path to that folder relative to the ownCloud web root, prefixed with `/`.
- **writable** Whether users can install apps in that folder. After the configuration is added, new apps will only install in a directory where `writable` is set to `true`.

The configuration example shows how to add a second directory, called `/apps-external`. Here, new apps and updates are only written to the `/apps-external` directory. This eases upgrade procedures of owncloud where shipped apps are delivered to `apps/` by default. `OC::$SERVERROOT` points to the web root of your instance. Please see the Apps Management description on how to move custom apps properly.

Previews

ownCloud supports previews of image files, the covers of MP3 files, and text files. These options control enabling and disabling previews, and thumbnail size.

```
'enable_previews' => true,
```

By default, ownCloud can generate previews for the following filetypes:

- Image files
- Covers of MP3 files
- Text documents

Valid values are `true`, to enable previews, or `false`, to disable previews

```
'preview_max_x' => 2048,
```

The maximum width, in pixels, of a preview. A value of `null` means there is no limit.

```
'preview_max_y' => 2048,
```

The maximum height, in pixels, of a preview. A value of `null` means there is no limit.

```
'preview_max_scale_factor' => 10,
```

If a lot of small pictures are stored on the ownCloud instance and the preview system generates blurry previews, you might want to consider setting a maximum scale factor. By default, pictures are upscaled to 10 times the original size. A value of `1` or `null` disables scaling.

```
'preview_max_filesize_image' => 50,
```

max file size for generating image previews with `imagegd` (default behaviour) If the image is bigger, it'll try other preview generators, but will most likely show the default mimetype icon

Value represents the maximum filesize in megabytes Default is 50 Set to -1 for no limit

```
'preview_libreoffice_path' => '/usr/bin/libreoffice',
```

custom path for LibreOffice/OpenOffice binary

```
'preview_office_cl_parameters' =>
    ' --headless --nologo --nofirststartwizard --invisible --norestore '.
    '--convert-to pdf --outdir ',
```

Use this if LibreOffice/OpenOffice requires additional arguments.

```
'enabledPreviewProviders' => array(
    'OC\Preview\PNG',
    'OC\Preview\JPEG',
    'OC\Preview\GIF',
    'OC\Preview\BMP',
    'OC\Preview\XBitmap',
    'OC\Preview\MP3',
    'OC\Preview\TXT',
    'OC\Preview\Markdown'
),
```

Only register providers that have been explicitly enabled

The following providers are enabled by default:

- OC\Preview\PNG
- OC\Preview\JPEG
- OC\Preview\GIF
- OC\Preview\BMP
- OC\Preview\XBitmap
- OC\Preview\Markdown
- OC\Preview\MP3
- OC\Preview\TXT

The following providers are disabled by default due to performance or privacy concerns:

- OC\Preview\Illustrator
- OC\Preview\Movie
- OC\Preview\MSOffice2003
- OC\Preview\MSOffice2007
- OC\Preview\MSOfficeDoc
- OC\Preview\OpenDocument
- OC\Preview\PDF
- OC\Preview\Photoshop
- OC\Preview\Postscript
- OC\Preview\StarOffice
- OC\Preview\SVG
- OC\Preview\TIFF
- OC\Preview\Font

Note: Troubleshooting steps for the MS Word previews are available at the [../configuration/files/collaborative_documents_configuration](#) section of the Administrators Manual.

The following providers are not available in Microsoft Windows:

- OC\Preview\Movie
- OC\Preview\MSOfficeDoc
- OC\Preview\MSOffice2003
- OC\Preview\MSOffice2007
- OC\Preview\OpenDocument
- OC\Preview\StarOffice

Comments

Global settings for the Comments infrastructure

```
'comments.managerFactory' => '\OC\Comments\ManagerFactory',
```

Replaces the default Comments Manager Factory. This can be utilized if an own or 3rdParty CommentsManager should be used that – for instance – uses the filesystem instead of the database to keep the comments.

```
'systemtags.managerFactory' => '\OC\SystemTag\ManagerFactory',
```

Replaces the default System Tags Manager Factory. This can be utilized if an own or 3rdParty SystemTagsManager should be used that – for instance – uses the filesystem instead of the database to keep the tags.

Maintenance

These options are for halting user activity when you are performing server maintenance.

```
'maintenance' => false,
```

Enable maintenance mode to disable ownCloud

If you want to prevent users from logging in to ownCloud before you start doing some maintenance work, you need to set the value of the maintenance parameter to true. Please keep in mind that users who are already logged-in are kicked out of ownCloud instantly.

```
'singleuser' => false,
```

When set to true, the ownCloud instance will be unavailable for all users who are not in the admin group.

SSL

```
'openssl' => array(
    'config' => '/absolute/location/of/openssl.cnf',
),
```

Extra SSL options to be used for configuration.

```
'enable_certificate_management' => false,
```

Allow the configuration of system wide trusted certificates

Memory caching backend configuration

Available cache backends:

- \OC\Memcache\APC Alternative PHP Cache backend
- \OC\Memcache\APCu APC user backend
- \OC\Memcache\ArrayCache In-memory array-based backend (not recommended)
- \OC\Memcache\Memcached Memcached backend
- \OC\Memcache\Redis Redis backend
- \OC\Memcache\XCache XCache backend

Advice on choosing between the various backends:

- APCu should be easiest to install. Almost all distributions have packages. Use this for single user environment for all caches.

- Use Redis or Memcached for distributed environments. For the local cache (you can configure two) take APCu.

```
'memcache.local' => '\OC\Memcache\APCu',
```

Memory caching backend for locally stored data

- Used for host-specific data, e.g. file paths

```
'memcache.distributed' => '\OC\Memcache\Memcached',
```

Memory caching backend for distributed data

- Used for installation-specific data, e.g. database caching
- If unset, defaults to the value of memcache.local

```
'redis' => [  
    'host' => 'localhost', // can also be a unix domain socket: '/tmp/redis.sock'  
    'port' => 6379,  
    'timeout' => 0.0,  
    'password' => '', // Optional, if not defined no password will be used.  
    'dbindex' => 0, // Optional, if undefined SELECT will not run and will use Redis Server's default db  
],
```

Connection details for redis to use for memory caching in a single server configuration.

For enhanced security it is recommended to configure Redis to require a password. See <http://redis.io/topics/security> for more information.

```
'redis.cluster' => [  
    'seeds' => [ // provide some/all of the cluster servers to bootstrap discovery, port required  
        'localhost:7000',  
        'localhost:7001'  
    ],  
    'timeout' => 0.0,  
    'read_timeout' => 0.0,  
    'failover_mode' => \RedisCluster::FAILOVER_DISTRIBUTE  
],
```

Connection details for a Redis Cluster

Only for use with Redis Clustering, for Sentinel-based setups use the single server configuration above, and perform HA on the hostname.

Redis Cluster support requires the php module `phpredis` in version 3.0.0 or higher.

Available failover modes:

- `\RedisCluster::FAILOVER_NONE` - only send commands to master nodes (default)
- `\RedisCluster::FAILOVER_ERROR` - failover to slaves for read commands if master is unavailable
- `\RedisCluster::FAILOVER_DISTRIBUTE` - randomly distribute read commands across master and slaves

```
'memcached_servers' => array(  
    // hostname, port and optional weight. Also see:  
    // http://www.php.net/manual/en/memcached.addservers.php  
    // http://www.php.net/manual/en/memcached.addserver.php  
    array('localhost', 11211),  
    //array('other.host.local', 11211),  
) ,
```

Server details for one or more memcached servers to use for memory caching.

```
'memcached_options' => array(
    // Set timeouts to 50ms
    \Memcached::OPT_CONNECT_TIMEOUT => 50,
    \Memcached::OPT_RETRY_TIMEOUT => 50,
    \Memcached::OPT_SEND_TIMEOUT => 50,
    \Memcached::OPT_RECV_TIMEOUT => 50,
    \Memcached::OPT_POLL_TIMEOUT => 50,

    // Enable compression
    \Memcached::OPT_COMPRESSION => true,

    // Turn on consistent hashing
    \Memcached::OPT_LIBKETAMA_COMPATIBLE => true,

    // Enable Binary Protocol
    \Memcached::OPT_BINARY_PROTOCOL => true,

    // Binary serializer will be enabled if the igbinary PECL module is available
    //\Memcached::OPT_SERIALIZER => \Memcached::SERIALIZER_IGBINARY,
),
```

Connection options for memcached, see <http://apprize.info/php/scaling/15.html>

```
'cache_path' => '',
```

Location of the cache folder, defaults to `data/$user/cache` where `$user` is the current user. When specified, the format will change to `$cache_path/$user` where `$cache_path` is the configured cache directory and `$user` is the user.

```
'cache_chunk_gc_ttl' => 86400, // 60*60*24 = 1 day
```

TTL of chunks located in the cache folder before they're removed by garbage collection (in seconds). Increase this value if users have issues uploading very large files via the ownCloud Client as upload isn't completed within one day.

```
'dav.chunk_base_dir' => '',
```

Location of the chunk folder, defaults to `data/$user/uploads` where `$user` is the current user. When specified, the format will change to `$dav.chunk_base_dir/$user` where `$dav.chunk_base_dir` is the configured cache directory and `$user` is the user.

Sharing

Global settings for Sharing

```
'sharing.managerFactory' => '\OC\Share20\ProviderFactory',
```

Replaces the default Share Provider Factory. This can be utilized if own or 3rdParty Share Providers are used that – for instance – use the filesystem instead of the database to keep the share information.

```
'sharing.federation.allowHttpFallback' => false,
```

When talking with federated sharing server, allow falling back to HTTP instead of hard forcing HTTPS

All other configuration options

```
'dbdriveroptions' => array(
    PDO::MYSQL_ATTR_SSL_CA => '/file/path/to/ca_cert.pem',
    PDO::MYSQL_ATTR_INIT_COMMAND => 'SET wait_timeout = 28800'
),
```

Additional driver options for the database connection, eg. to enable SSL encryption in MySQL or specify a custom wait timeout on a cheap hoster.

```
'sqlite.journal_mode' => 'DELETE',
```

sqlite3 journal mode can be specified using this configuration parameter - can be 'WAL' or 'DELETE' see for more details <https://www.sqlite.org/wal.html>

```
'mysql.utf8mb4' => false,
```

During setup, if requirements are met (see below), this setting is set to true and MySQL can handle 4 byte characters instead of 3 byte characters.

If you want to convert an existing 3-byte setup into a 4-byte setup please set the parameters in MySQL as mentioned below and run the migration command:

```
./occ db:convert-mysql-charset
```

The config setting will be set automatically after a successful run.

Consult the documentation for more details.

MySQL requires a special setup for longer indexes (> 767 bytes) which are needed:

```
[mysqld] innodb_large_prefix=ON innodb_file_format=Barracuda innodb_file_per_table=ON
```

Tables will be created with

- character set: utf8mb4
- collation: utf8mb4_bin
- row_format: compressed

See: <https://dev.mysql.com/doc/refman/5.7/en/charset-unicode-utf8mb4.html> https://dev.mysql.com/doc/refman/5.7/en/innodb-parameters.html#sysvar_innodb_large_prefix https://mariadb.com/kb/en/mariadb/xtradbinnodb-server-system-variables/#innodb_large_prefix <http://www.tocker.ca/2013/10/31/benchmarking-innodb-page-compression-performance.html> <http://mechanics.flite.com/blog/2014/07/29/using-innodb-large-prefix-to-avoid-error-1071/>

```
'supportedDatabases' => array(
    'sqlite',
    'mysql',
    'pgsql',
    'oci',
),
```

Database types that are supported for installation.

Available:

- sqlite (SQLite3 - Not in Enterprise Edition)
- mysql (MySQL)
- pgsql (PostgreSQL)
- oci (Oracle - Enterprise Edition Only)

```
'tempdirectory' => '/tmp/owncloudtemp',
```

Override where ownCloud stores temporary files. Useful in situations where the system temporary directory is on a limited space ramdisk or is otherwise restricted, or if external storages which do not support streaming are in use.

The Web server user must have write access to this directory.

```
'hashingCost' => 10,
```

The hashing cost used by hashes generated by ownCloud.

Using a higher value requires more time and CPU power to calculate the hashes. As this number grows, the amount of work (typically CPU time or memory) necessary to compute the hash increases exponentially.

```
'blacklisted_files' => array('.htaccess'),
```

Blacklist a specific file or files and disallow the upload of files with this name. `.htaccess` is blocked by default.

WARNING: USE THIS ONLY IF YOU KNOW WHAT YOU ARE DOING.

```
'excluded_directories' =>
    array (
        '.snapshot',
        '~snapshot',
    ),
```

Exclude specific directory names and disallow scanning, creating and renaming using these names. Case insensitive.

Excluded directory names are queried at any path part like at the beginning, in the middle or at the end and will not be further processed if found. Please see the documentation for details and examples. Use when the storage backend supports eg snapshot directories to be excluded. **WARNING: USE THIS ONLY IF YOU KNOW WHAT YOU ARE DOING.**

```
'integrity.excluded.files' =>
    array (
        '.DS_Store',
        'Thumbs.db',
        '.directory',
        '.webapp',
        '.htaccess',
        '.user.ini',
    ),
```

Exclude files from the integrity checker command

```
'integrity.ignore.missing.app.signature' =>
    array(
        'app-id of app-1',
        'app-id of theme-2',
    ),
```

The list of apps that are allowed to have no signature.json. Besides ownCloud apps, this is particularly useful when creating ownCloud themes, because themes are treated as apps. The app is identified with it's app-id.

The following example allows app-1 and theme-2 to have no signature.

```
'share_folder' => '/',
```

Define a default folder for shared files and folders other than root.

```
'theme' => '',
```

If you are applying a theme to ownCloud, enter the name of the theme here.

The default location for themes is `owncloud/themes/`.

```
'cipher' => 'AES-256-CFB',
```

The default cipher for encrypting files. Currently AES-128-CFB and AES-256-CFB are supported.

```
'minimum.supported.desktop.version' => '2.2.4',
```

The minimum ownCloud desktop client version that will be allowed to sync with this server instance. All connections made from earlier clients will be denied by the server. Defaults to the minimum officially supported ownCloud version at the time of release of this server version.

When changing this, note that older unsupported versions of the ownCloud desktop client may not function as expected, and could lead to permanent data loss for clients or other unexpected results.

```
'quota_include_external_storage' => false,
```

EXPERIMENTAL: option whether to include external storage in quota calculation, defaults to false.

```
'filesystem_check_changes' => 0,
```

Specifies how often the local filesystem (the ownCloud `data/` directory, and NFS mounts in `data/`) is checked for changes made outside ownCloud. This does not apply to external storages.

0 -> Never check the filesystem for outside changes, provides a performance increase when it's certain that no changes are made directly to the filesystem

1 -> Check each file or folder at most once per request, recommended for general use if outside changes might happen.

```
'part_file_in_storage' => true,
```

By default ownCloud will store the part files created during upload in the same storage as the upload target. Setting this to false will store the part files in the root of the users folder which might be required to work with certain external storage setups that have limited rename capabilities.

```
'mount_file' => '/var/www/owncloud/data/mount.json',
```

Where `mount.json` file should be stored, defaults to `data/mount.json` in the ownCloud directory.

```
'filesystem_cache_readonly' => false,
```

When `true`, prevent ownCloud from changing the cache due to changes in the filesystem for all storage.

```
'secret' => '',
```

Secret used by ownCloud for various purposes, e.g. to encrypt data. If you lose this string there will be data corruption.

```
'trusted_proxies' => array('203.0.113.45', '198.51.100.128'),
```

List of trusted proxy servers

If you configure these also consider setting `forwarded_for_headers` which otherwise defaults to `HTTP_X_FORWARDED_FOR` (the `X-Forwarded-For` header).

```
'forwarded_for_headers' => array('HTTP_X_FORWARDED', 'HTTP_FORWARDED_FOR'),
```

Headers that should be trusted as client IP address in combination with `trusted_proxies`. If the HTTP header looks like `'X-Forwarded-For'`, then use `'HTTP_X_FORWARDED_FOR'` here.

If set incorrectly, a client can spoof their IP address as visible to ownCloud, bypassing access controls and making logs useless!

Defaults to 'HTTP_X_FORWARDED_FOR' if unset

```
'max_filesize_animated_gifs_public_sharing' => 10,
```

max file size for animating gifs on public-sharing-site.

If the gif is bigger, it'll show a static preview

Value represents the maximum filesize in megabytes. Default is 10. Set to -1 for no limit.

```
'filelocking.enabled' => true,
```

Enables transactional file locking.

This is enabled by default.

Prevents concurrent processes from accessing the same files at the same time. Can help prevent side effects that would be caused by concurrent operations. Mainly relevant for very large installations with many users working with shared files.

```
'filelocking.ttl' => 3600,
```

Set the lock's time-to-live in seconds.

Any lock older than this will be automatically cleaned up.

If not set this defaults to either 1 hour or the php max_execution_time, whichever is higher.

```
'memcache.locking' => '\\OC\\Memcache\\Redis',
```

Memory caching backend for file locking

Because most memcache backends can clean values without warning using redis is highly recommended to *avoid data loss*.

```
'upgrade.disable-web' => false,
```

Disable the web based updater

```
'upgrade.automatic-app-update' => true,
```

Automatic update of market apps, set to "false" to disable.

```
'debug' => false,
```

Set this ownCloud instance to debugging mode

Only enable this for local development and not in production environments This will disable the minifier and outputs some additional debug information

Warning: Be warned that, if you set this to `true`, exceptions display stack traces on the web interface, *including passwords*, — **in plain text!**. We strongly encourage you never to use it in production.

```
'data-fingerprint' => '',
```

Sets the data-fingerprint of the current data served

This is a property used by the clients to find out if a backup has been restored on the server. Once a backup is restored run `./occ maintenance:data-fingerprint` To set this to a new value.

Updating/Deleting this value can make connected clients stall until the user has resolved conflicts.

```
'copied_sample_config' => true,
```

This entry is just here to show a warning in case somebody copied the sample configuration. **DO NOT ADD THIS SWITCH TO YOUR CONFIGURATION!**

If you, brave person, have read until here be aware that you should not modify *ANY* settings in this file without reading the documentation.

```
'files_external_allow_create_new_local' => false,
```

Set this property to true if you want to enable the files_external local mount Option.

Default: false

App config options

Retention for activities of the activity app:

```
'activity_expire_days' => 365,
```

Every day a cron job is ran, which deletes all activities for all users which are older then the number of days that is set for activity_expire_days

```
'smb.logging.enable' => true,
```

This enables debug logging for SMB access. Use this carefully as it can generate a huge amount of log data.

Overriding Existing Parameter Values Using Environment Variables

ownCloud supports the ability to override the *web UI*, *command line*, and *Cron* environment settings by using environment variables. By doing so, you avoid the need to store credentials and other sensitive data in code. What's more, by using environment variables, you do not have to manage configurations (e.g., database connections) for different server environments, because environment variables store this information for you.

To override an existing setting, you need to export an environment variable which has the same name as the one which you want to override, prefixed with `OC_`. For example, if you wanted to override the value of `dbname`, you would set the environment variable `OC_dbname`.

Below are examples of setting an environment variable in the Apache and Nginx web servers, and for when running command line scripts.

Apache Web Server

```
# Inside a virtual host configuration
SetEnv OC_dbname owncloud_database_name
```

Nginx Web Server (php-fpm)

```
location / {
    fastcgi_param OC_dbname owncloud_database_name
}
```

Command Line

```
# export the variable into the environment before launching the Cron script
export OC_dbname=owncloud_database_name php -d variables_order=EGPCS cron.php
```

6.5.10 Email Configuration

ownCloud is capable of sending emails for a range of reasons. These include:

- Password reset emails
- Notifying users of new file shares
- Changes in files
- Activity notifications

To make use of them, users need to configure which notifications they want to receive. They can do this on their Personal pages.

Note: To be able to send emails, a functioning mail server must be available, whether locally in your network, or remotely.

Configuring an SMTP Server

To configure ownCloud to interact with an SMTP server, you can either update `config/config.php` by hand, or use the graphical Email Configuration Wizard, which updates `config/config.php` for you.

The Graphical Email Configuration Wizard

The wizard supports three mail server types: *SMTP*, *PHP*, and *Sendmail*. Use SMTP for a remote email server, and either PHP or Sendmail when your mail server is on the same machine as ownCloud.

Note: The Sendmail option refers to the Sendmail SMTP server, and any drop-in Sendmail replacement such as Postfix, Exim, or Courier. All of these include a `sendmail` binary, and are freely-interchangeable.

You need the following information from your mail server administrator to connect ownCloud to a remote SMTP server:

- Encryption type: None, SSL/TLS or STARTTLS.
- The From address you want your outgoing ownCloud mails to use.
- Whether authentication is required.
- Authentication method: None, Login, Plain, or NT LAN Manager.
- The server's IP address or fully-qualified domain name (FQDN).
- Login credentials, if required.

Your changes are saved immediately, and you can click the *Send Email* button to test your configuration. This sends a test message to the email address you configured on your Personal page. The test message says:

Email Server

This is used for sending out notifications. Saving...

Send mode	<input type="text" value="smtp"/>	Encryption	<input type="text" value="TLS"/>
From address	<input type="text" value="owncloud"/>	@	<input type="text" value="alrac.net"/>
Authentication method	<input type="text" value="Login"/>	<input checked="" type="checkbox"/>	Authentication required
Server address	<input type="text" value="None"/>	:	<input type="text" value="Port"/>
Credentials	<input type="text" value="Login"/>	:	<input type="text" value=""/>
	<input type="text" value="Plain"/>		
	<input type="text" value="NT LAN Manager"/>		<input type="text" value="...."/>

Test email settings

If you received this email, the settings seem to be correct.

--

ownCloud
web services under your control

Configuring PHP and Sendmail Configuring PHP or Sendmail requires only that you select one of them, and then enter your desired return address.

Email Server

This is used for sending out notifications. Saving...

Send mode	<input type="text" value="sendmail"/>
From address	<input type="text" value="owncloud"/> @ <input type="text" value="alrac.net"/>

Test email settings

How do you decide which one to use? PHP mode uses your local `sendmail` binary. Use this if you want to use `php.ini` to control some of your mail server functions, such as setting *paths*, *headers*, or passing extra command options to the `sendmail` binary. These vary according to which server you are using, so consult your server's documentation to see what your options are.

In most cases the `smtp` option is best, because it removes the extra step of passing through PHP, and you can control all of your mail server options in one place, in your mail server configuration.

Setting Mail Server Parameters in config.php

If you prefer, you may set your mail server parameters in `config/config.php`. The following examples are for *SMTP*, *PHP*, *Sendmail*, and *Qmail*.

SMTP If you want to send email using a local or remote SMTP server it is necessary to enter the name or IP address of the server, optionally followed by a colon separated port number, e.g. `:425`. If this value is not given the default port `25/tcp` will be used unless you change that by modifying the `mail_smtpport` parameter. Multiple servers can be entered, separated by semicolons:

```
<?php
"mail_smtpmode"    => "smtp",
"mail_smtphost"   => "smtp-1.server.dom;smtp-2.server.dom:425",
"mail_smtpport"   => 25,
```

Or:

```
<?php
"mail_smtpmode"    => "smtp",
"mail_smtphost"   => "smtp.server.dom",
"mail_smtpport"   => 425,
```

If a malware or SPAM scanner is running on the SMTP server it might be necessary that you increase the SMTP timeout to e.g., 30s:

```
<?php
"mail_smtptimeout" => 30,
```

If the SMTP server accepts insecure connections, the default setting can be used:

```
<?php
"mail_smtppsecure" => '',
```

If the SMTP server only accepts secure connections you can choose between the following two variants:

SSL/TLS A secure connection will be initiated using SSL/TLS via SMTPS on the default port `465/tcp`:

```
<?php
"mail_smtphost"    => "smtp.server.dom:465",
"mail_smtppsecure" => 'ssl',
```

STARTTLS A secure connection will be initiated using STARTTLS via SMTP on the default port `25/tcp`:

```
<?php
"mail_smtphost"    => "smtp.server.dom",
"mail_smtppsecure" => 'tls',
```

An alternative is the port `587/tcp` (recommended):

```
<?php
```

```
"mail_smtphost"    => "smtp.server.dom:587",  
"mail_smtsecure"  => 'tls',
```

Authentication And finally it is necessary to configure if the SMTP server requires authentication, if not, the default values can be taken as is.

```
<?php
```

```
"mail_smtpauth"   => false,  
"mail_smtpname"   => "",  
"mail_smtppassword" => "",
```

If SMTP authentication is required you have to set the required username and password and can optionally choose between the authentication types **LOGIN** (default) or **PLAIN**.

```
<?php
```

```
"mail_smtpauth"   => true,  
"mail_smtpauthtype" => "LOGIN",  
"mail_smtpname"   => "username",  
"mail_smtppassword" => "password",
```

PHP Mail If you want to use PHP mail it is necessary to have an installed and working email system on your server. Which program in detail is used to send email is defined by the configuration settings in the **php.ini** file. On *nix systems this will most likely be Sendmail. ownCloud should be able to send email out of the box.

```
<?php
```

```
"mail_smtpmode"    => "php",  
"mail_smtphost"    => "127.0.0.1",  
"mail_smtpport"    => 25,  
"mail_smtptimeout" => 10,  
"mail_smtsecure"   => "",  
"mail_smtpauth"    => false,  
"mail_smtpauthtype" => "LOGIN",  
"mail_smtpname"    => "",  
"mail_smtppassword" => "",
```

Sendmail If you want to use the well known Sendmail program to send email, it is necessary to have an installed and working email system on your *nix server. The Sendmail binary (`/usr/sbin/sendmail`) is usually part of that system. ownCloud should be able to send email out of the box.

```
<?php
```

```
"mail_smtpmode"    => "sendmail",  
"mail_smtphost"    => "127.0.0.1",  
"mail_smtpport"    => 25,  
"mail_smtptimeout" => 10,  
"mail_smtsecure"   => "",  
"mail_smtpauth"    => false,  
"mail_smtpauthtype" => "LOGIN",  
"mail_smtpname"    => "",  
"mail_smtppassword" => "",
```

Qmail If you want to use the qmail program to send email, it is necessary to have an installed and working qmail email system on your server. The Sendmail binary (`/var/qmail/bin/sendmail`) will then be used to send email. ownCloud should be able to send email out of the box.

```
<?php

"mail_smtpmode"    => "qmail",
"mail_smtphost"    => "127.0.0.1",
"mail_smtpport"    => 25,
"mail_smtptimeout" => 10,
"mail_smtpsecure"  => "",
"mail_smtpauth"    => false,
"mail_smtpauthtype" => "LOGIN",
"mail_smtpname"    => "",
"mail_smtppassword" => "",
```

Send a Test Email

Regardless of how you have configured ownCloud to interact with an email server, to test your email configuration, save your email address in your personal settings and then use the **Send email** button in the *Email Server* section of the Admin settings page.

Using Self-Signed Certificates

When using self-signed certificates on the remote SMTP server the certificate must be imported into ownCloud. Please refer to *Importing System-wide and Personal SSL Certificates* for more information.

Troubleshooting

If you are unable to send email, try turning on debugging. Do this by enabling the `mail_smtpdebug` parameter in `config/config.php`.

```
<?php

"mail_smtpdebug" => true;
```

Note: Immediately after pressing the **Send email** button, as described before, several **SMTP -> get_lines(): ...** messages appear on the screen. This is expected behavior and can be ignored.

Why is my web domain different from my mail domain? The default domain name used for the sender address is the hostname where your ownCloud installation is served. If you have a different mail domain name you can override this behavior by setting the following configuration parameter:

```
<?php

"mail_domain" => "example.com",
```

This setting results in every email sent by ownCloud (for example, the password reset email) having the domain part of the sender address appear as follows

```
no-reply@example.com
```

How can I find out if an SMTP server is reachable? Use the ping command to check the server availability

```
ping smtp.server.dom
```

```
PING smtp.server.dom (ip-address) 56(84) bytes of data.  
64 bytes from your-server.local.lan (192.168.1.10): icmp_req=1 ttl=64  
time=3.64ms
```

How can I find out if the SMTP server is listening on a specific TCP port? The best way to get mail server information is to ask your mail server admin. If you are the mail server admin, or need information in a hurry, you can use the `netstat` command. This example shows all active servers on your system, and the ports they are listening on. The SMTP server is listening on localhost port 25.

```
# netstat -pant
```

```
Active Internet connections (servers and established)  
Proto Recv-Q Send-Q Local Address   Foreign Address State ID/Program name  
tcp    0      0 0.0.0.0:631     0.0.0.0:*       LISTEN 4418/cupsd  
tcp    0      0 127.0.0.1:25    0.0.0.0:*       LISTEN 2245/exim4  
tcp    0      0 127.0.0.1:3306 0.0.0.0:*       LISTEN 1524/mysqld
```

- 25/tcp is unencrypted smtp
- 110/tcp/udp is unencrypted pop3
- 143/tcp/udp is unencrypted imap4
- 465/tcp is encrypted smtps
- 993/tcp/udp is encrypted imaps
- 995/tcp/udp is encrypted pop3s

How can I determine if the SMTP server supports SMTPS? A good indication that the SMTP server supports SMTPS is that it is listening on port **465**.

How can I determine what authorization and encryption protocols the mail server supports? SMTP servers usually announce the availability of STARTTLS immediately after a connection has been established. You can easily check this using the `telnet` command.

Note: You must enter the marked lines to obtain the information displayed.

```
telnet smtp.domain.dom 25  
  
Trying 192.168.1.10...  
Connected to smtp.domain.dom.  
Escape character is '^]'.  
220 smtp.domain.dom ESMTP Exim 4.80.1 Tue, 22 Jan 2013 22:39:55 +0100  
EHLO your-server.local.lan # <<< enter this command  
250-smtp.domain.dom Hello your-server.local.lan [ip-address]  
250-SIZE 52428800  
250-8BITMIME  
250-PIPELINING  
250-AUTH PLAIN LOGIN CRAM-MD5 # <<< Supported auth protocols  
250-STARTTLS # <<< Encryption is supported  
250 HELP  
QUIT # <<< enter this command
```

```
221 smtp.domain.dom closing connection
Connection closed by foreign host.
```

Enabling Debug Mode

If you are unable to send email, it might be useful to activate further debug messages by enabling the `mail_smtpdebug` parameter:

```
<?php
"mail_smtpdebug" => true,
```

Note: Immediately after pressing the **Send email** button, as described before, several **SMTP -> get_lines(): ...** messages appear on the screen. This is expected behavior and can be ignored.

Using Email Templates

Most emails sent from ownCloud are based on editable email templates, which are a mixture of PHP and HTML. The currently available templates are:

Email	Format	Description	File Location
Activity notification mail	plain text	Notification of activities that users have enabled in the Notifications section of their Personal pages.	core/templates/mail.php
Lost password mail		Password reset email for users who lose their passwords.	core/templates/lostpassword/email.php
New user email	HTML plain text		settings/templates/email.new_user.php settings/templates/email.new_user_plain_text.php
Public link share email	HTML plain text	Notify users of new public link shares.	core/templates/mail.php core/templates/altmail.php
New file share email	HTML plain text	Notify users of new file shares.	core/templates/internalmail.php core/templates/internalaltmail.php

In addition to providing the email templates, this feature enables you to apply any pre-configured themes to the email. To modify an email template to users:

1. Access the Admin page.
2. Scroll to the Mail templates section.
3. Select a template from the drop-down menu.
4. Make any desired modifications to the template.

The templates are written in PHP and HTML, and are already loaded with the relevant variables such as *username*, *share links*, and *filenames*. You can, if you are careful, edit these — even without knowing PHP or HTML. Don't touch any of the code, but it's OK to edit the text portions of the messages.

For example, this the lost password mail template:

```
<?php
echo str_replace(
    '{link}',
    $_['link'],
    $l->t('Use the following link to reset your password: {link}')
);
```

You could change the text portion of the template, Use the following link to reset your password: to say something else, such as:

Click the following link to reset your password.
If you did not ask for a password reset, ignore this message.

Again, be very careful to change nothing but the message text, because the tiniest coding error will break the template.

Note: You can edit the templates directly in the template text box, or you can copy and paste them to a text editor for modification and then copy and paste them back to the template text box for use when you are done.

6.5.11 Excluding Directories and Blacklisting Files

Definitions of terms

Blacklisted Files that may harm the ownCloud environment like a foreign `.htaccess` file. Blacklisting prevents anyone from uploading blacklisted files to the ownCloud server.

Excluded Existing directories on your ownCloud server, including external storage mounts, that are excluded from being processed by ownCloud. In effect they are invisible to ownCloud.

Both types are defined in `config.php`. Blacklisted files and excluded directories are not scanned by ownCloud, not viewed, not synced, and cannot be created, renamed, deleted, or accessed via direct path input from a file explorer. Even when a filepath is entered manually via a file explorer, the path cannot be accessed.

For example configurations please see `owncloud/config/config.sample.php`.

Impact on System Performance

If you have a filesystem mounted with 200,000 files and directories and 15 snapshots in rotation, you would now scan and process 200,000 elements plus $200,000 \times 15 = 3,000,000$ elements additionally. These additional 3,000,000 elements, 15 times more than the original quantity, would also be available for viewing and synchronisation. Because this is a big and unnecessary overhead, most times confusing to clients, further processing can be eliminated by using excluded directories.

Blacklisted Files

By default, ownCloud blacklists the file `.htaccess` to secure the running instance, which is important when using Apache as webserver. A foreign `.htaccess` file could overwrite rules defined by ownCloud. There is no explicit need to enter the file name `.htaccess` as parameter to the `blacklisted_files` array in `config.php`, but you can add more blacklisted file names if necessary.

Excluded Directories

Reason for excluding directories:

1. Enterprise storage systems, or special filesystems like ZFS and BtrFS are capable of snapshots. These snapshots are directories and keep point-in-time views of the data.
2. Snapshot directories are read-only.
3. There is no common naming for these directories, and most likely will never be. NetApp uses `.snapshot` and `~snapshot`, EMC eg `.ckpt`, HDS eg `.latest` and `~latest`, the ZFS filesystem uses `.zfs` and so on.
4. Viewing and scanning of these directories does not make any sense as these directories are used to ease backup, restores, and cloning
5. Directories which are part of the mounted filesystem, but must not be accessible via ownCloud.

Example:

If you have a snapshot-capable storage or filesystem where snapshots are enabled and presented to clients, each directory will contain a “special” visible directory named e.g. `.snapshot`. Depending on the system, you may find underneath a list of snapshots taken and in the next lower level the complete set of files and directories which were present when the snapshot was created. In most systems, this mechanism is true in all directory levels:

```
/.snapshot
  /nightly.0
    /home
    /dat
    /pictures
    file_1
    file_2
  /nightly.1
    /home
    /dat
    /pictures
    file_1
    file_2
  /nightly.2
    /home
    /dat
    /pictures
    file_1
    file_2
  ...
/home
/dat
/pictures
file_1
file_2
...
```

Example `excluded_directories` entries in `config.php` look like this:

```
'excluded_directories' => [
    '.snapshot',
    '~snapshot',
    'dir1',
    'dir2',
],
```

Note that these are not pathnames, but directory names without any slashes. Excluding `dir1` excludes:

```
/home/dir1
/etc/stuff/dir1
```

But not:

```
/home/.dir1  
/etc/stuff/mydir1
```

Example `blacklisted_files` entries in `config.php` look like this:

```
'blacklisted_files' => [  
    'hosts',  
    'evil_script.sh',  
],
```

6.5.12 Linking External Sites

You can embed external Web sites inside your ownCloud pages with the External Sites app, as this screenshot shows.

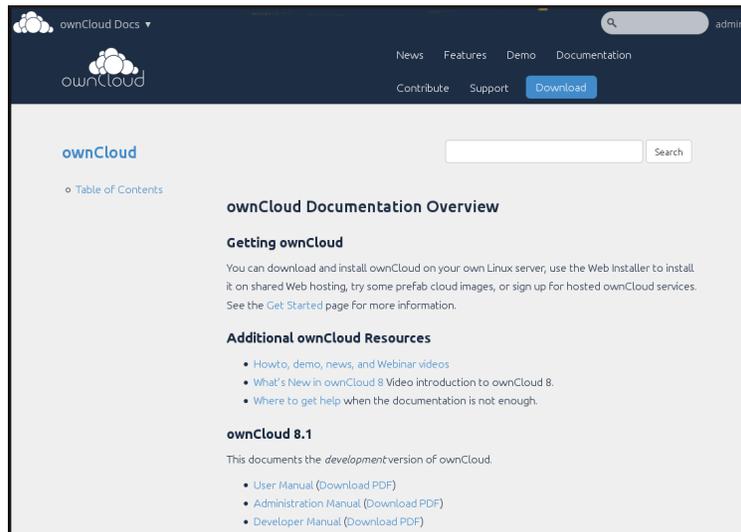


Figure 6.3: *Click to enlarge*

This is useful for quick access to important Web pages such as the ownCloud manuals and informational pages for your company, and for presenting external pages inside your custom ownCloud branding, if you use your own custom themes.

The External sites app is included in all versions of ownCloud. Go to **Apps > Not Enabled** to enable it. Then go to your ownCloud Admin page to create your links, which are saved automatically. There is a dropdown menu to select an icon, but there is only one default icon so you don't have to select one. Hover your cursor to the right of your links to make the trashcan icon appear when you want to remove them.

The links appear in the ownCloud dropdown menu on the top left after refreshing your page, and have globe icons.

Your links may or may not work correctly due to the various ways that Web browsers and Web sites handle HTTP and HTTPS URLs, and because the External Sites app embeds external links in IFrames. Modern Web browsers try very hard to protect Web surfers from dangerous links, and safety apps like [Privacy Badger](#) and ad-blockers may block embedded pages. It is strongly recommended to enforce HTTPS on your ownCloud server; do not weaken this, or any of your security tools, just to make embedded Web pages work. After all, you can freely access them outside of ownCloud.

Most Web sites that offer login functionalities use the `X-Frame-Options` or `Content-Security-Policy` HTTP header which instructs browsers to not allow their pages to be embedded for security reasons (e.g. "Clickjack-

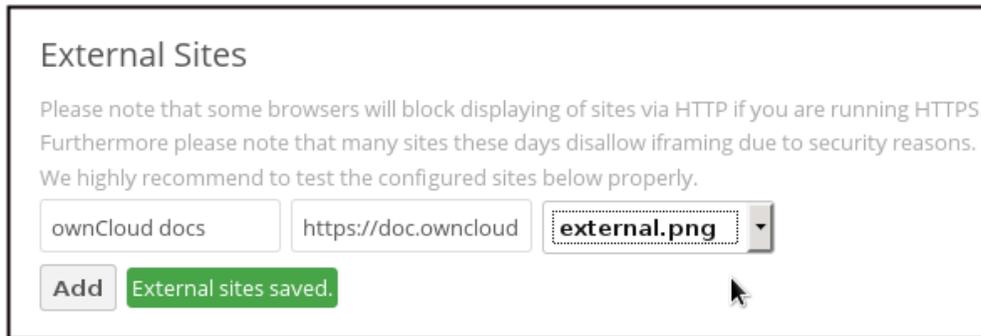
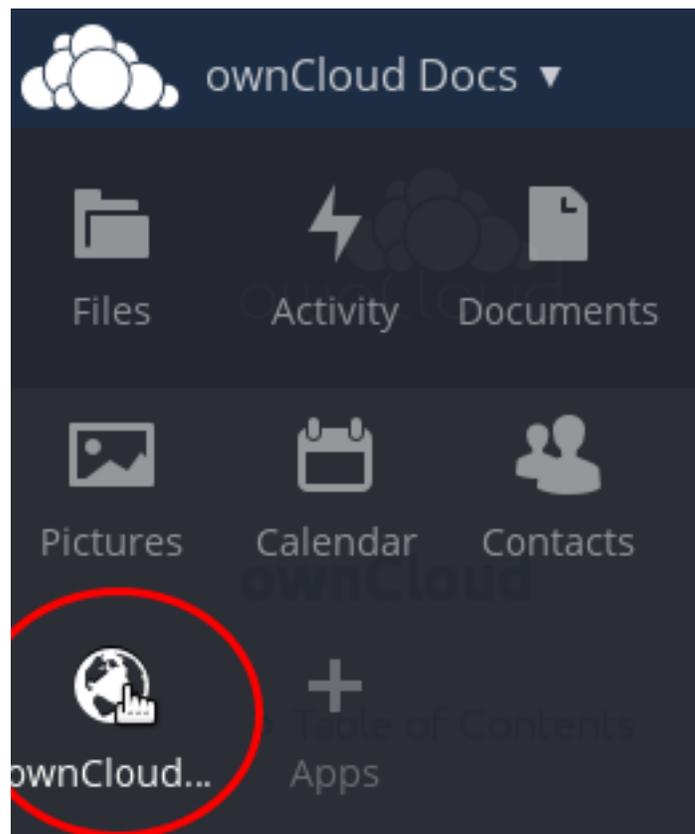
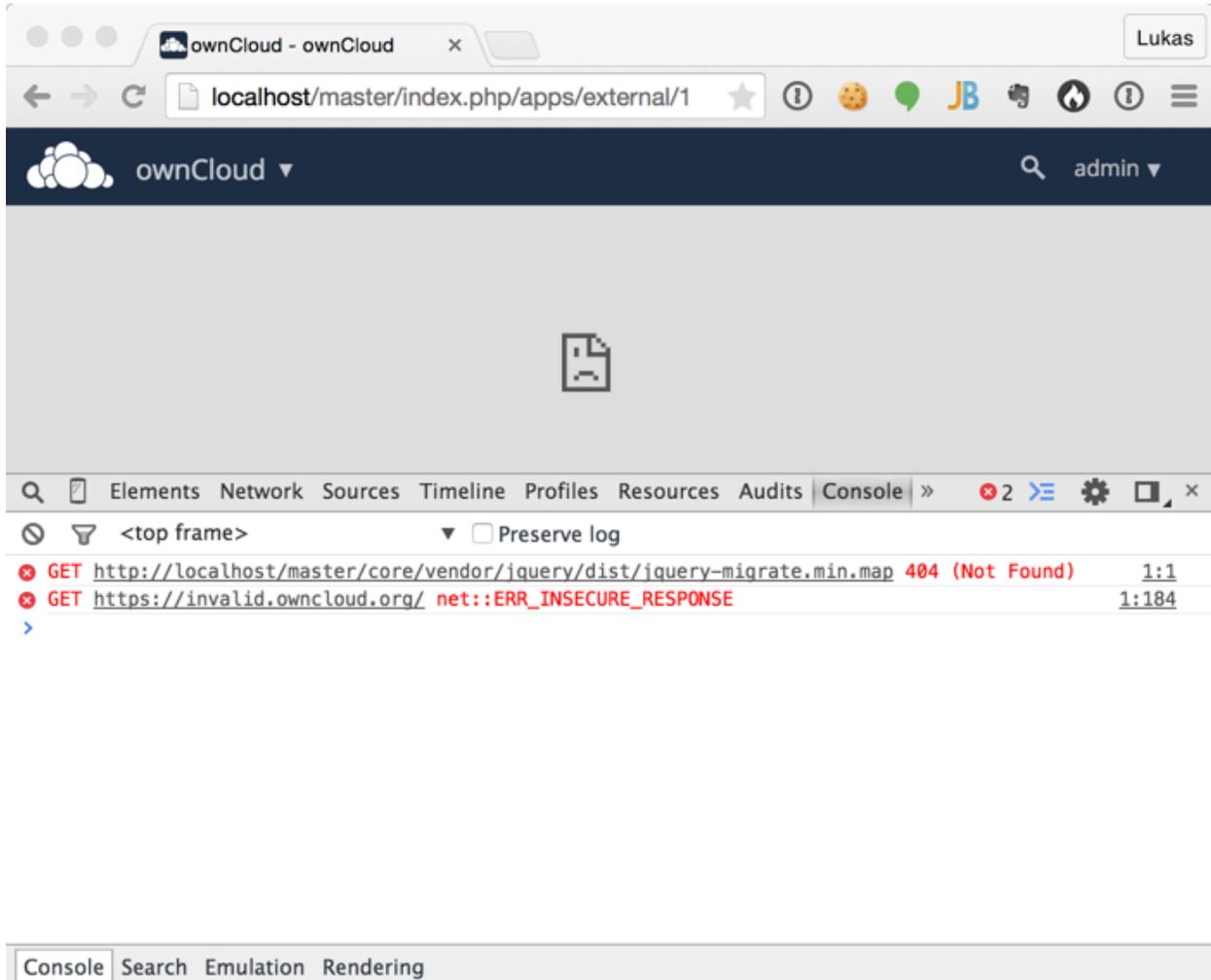


Figure 6.4: *Click to enlarge*



ing”). You can usually verify the reason why embedding the website is not possible by using your browser’s console tool. For example, this page has an invalid SSL certificate.



On this page, X-Frame-Options prevents the embedding.

There isn’t much you can do about these issues, but if you’re curious you can see what is happening.

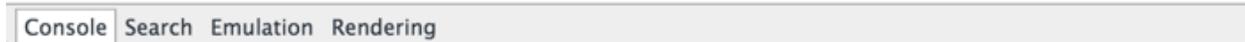
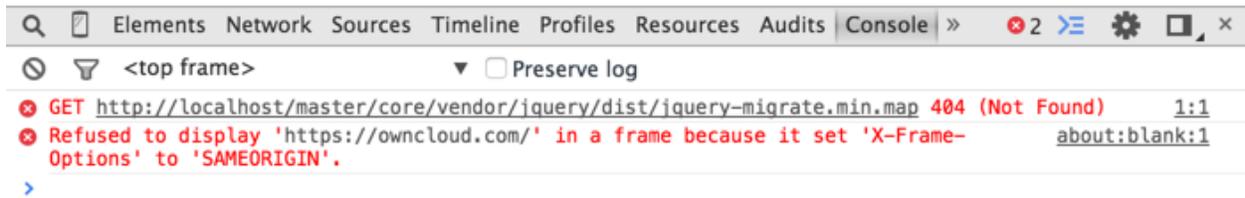
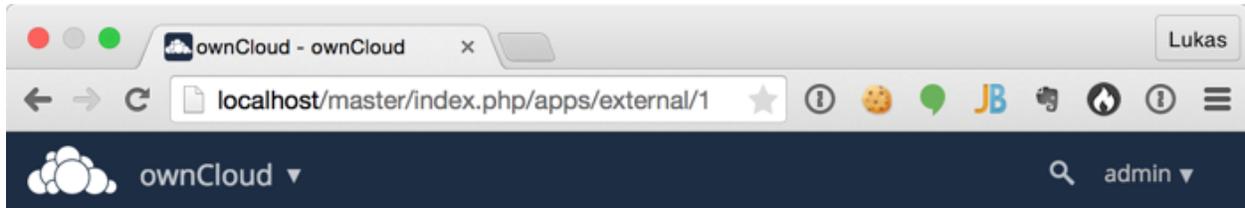
6.5.13 Custom Client Download Repositories

You may configure the URLs to your own download repositories for your ownCloud desktop clients and mobile apps in `config/config.php`. This example shows the default download locations:

```
<?php
"customclient_desktop" => "https://owncloud.org/sync-clients/",
"customclient_android" => "https://play.google.com/store/apps/details?id=com.owncloud.android",
"customclient_ios"     => "https://itunes.apple.com/us/app/owncloud/id543672169?mt=8",
```

Simply replace the URLs with the links to your own preferred download repos.

You may test alternate URLs without editing `config/config.php` by setting a test URL as an environment variable:



```
export OCC_UPDATE_URL=https://test.example.com
```

When you're finished testing you can disable the environment variable:

```
unset OCC_UPDATE_URL
```

6.5.14 Knowledge Base Configuration

The usage of ownCloud is more or less self explaining but nevertheless a user might run into a problem where he needs to consult the documentation or knowledge base. To ease access to the ownCloud documentation and knowledge base, a help menu item is shown in the settings menu by default.

Parameters

If you want to disable the ownCloud help menu item you can use the **knowledgebaseenabled** parameter inside the `config/config.php`.

```
<?php
    "knowledgebaseenabled" => true,
```

Note: Disabling the help menu item might increase the number of support requests you have to answer in the future

6.5.15 Language Configuration

In normal cases ownCloud will automatically detect the language of the Web-GUI. If this does not work properly or you want to make sure that ownCloud always starts with a given language, you can use the **default_language** parameter.

Please keep in mind, that this will not effect a users language preference, which has been configured under “personal -> language” once he has logged in.

Please check `settings/languageCodes.php` for the list of supported language codes.

Parameters

```
<?php
    "default_language" => "en",
```

This parameters can be set in the `config/config.php`

6.5.16 Legal Settings Configuration

Because of one or more legal frameworks around the world, some ownCloud instances may need to have links to Imprint and Privacy Policies on all pages; both in the WebUI and within email templates. Some of the more global legal frameworks prominent are:

- [The GDPR](#)
- [The Australian Privacy Act 1988](#)

- The Canadian Personal Information Protection and Electronic Data Act (PIPEDA)
- The California Online Privacy Protection Act (CalOPPA)
- The Children’s Online Privacy Protection Rule (COPPA)

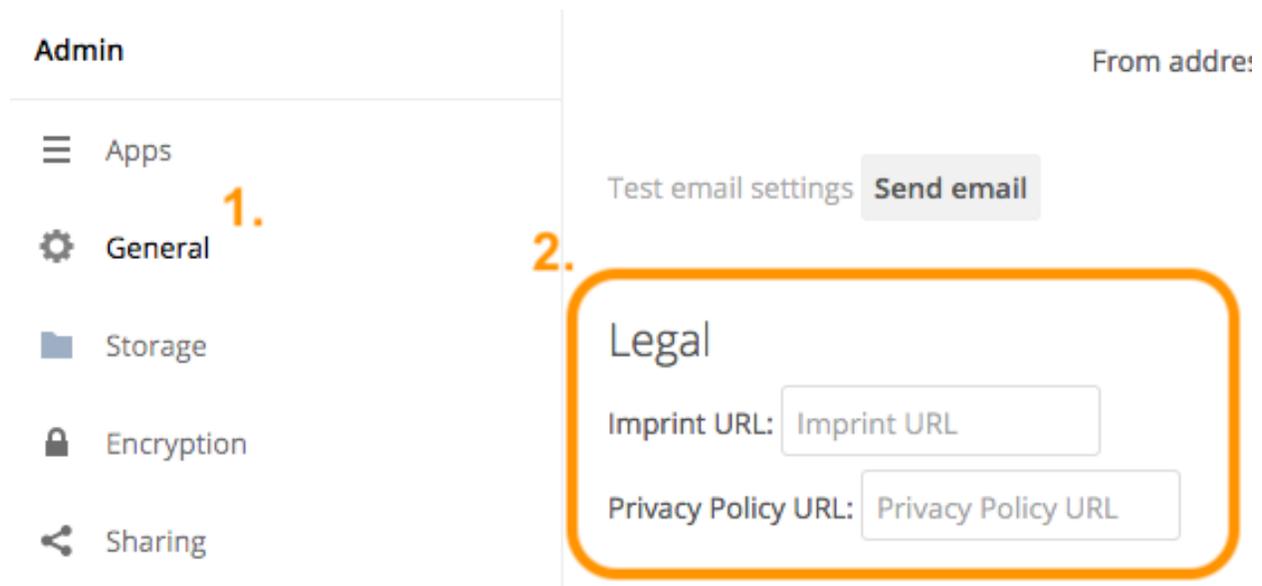
ownCloud Administrators may also be required to display a legal disclosure document, both in the WebUI and within email templates. A legal disclosure document is a legally mandated statement of the ownership and authorship of the ownCloud installation.

Note: You can also think of it as a rather fancy “*About Us*” page or an enhanced “*Terms and Conditions*” page. In Germany, this is known as an “*Impressum*”.

If you’re required to have one or more of these, you can specify the link to them in two ways.

Using the Web UI

In the Web UI, under “*Settings -> Admin -> General*”, under the heading “*Legal*”, you can provide a link to an Imprint and a Privacy Policy URL, as you can see in the screenshot below.



Note: The values entered will auto-save.

Using the Command Line

From the command line, you can use the `occ config:app:get` and `occ config:app:set` commands, as in the code sample below.

```
# Get the current values, if any, for the Imprint and Privacy Policy URLs
php occ config:app:get core legal.imprint_url
php occ config:app:get core legal.privacy_policy_url

# Set the Imprint and Privacy Policy URLs
php occ config:app:set core legal.imprint_url --value=new_value
php occ config:app:set core legal.privacy_policy_url --value=new_value
```

For more information about these commands, refer to *the config command reference in the occ commands documentation*.

6.5.17 Logging Configuration

Use your ownCloud log to review system status, or to help debug problems. You may adjust logging levels, and choose between using the ownCloud log or your syslog.

Parameters

Logging levels range from **DEBUG**, which logs all activity, to **FATAL**, which logs only fatal errors.

- **0**: **DEBUG**: Debug, informational, warning, and error messages, and fatal issues.
- **1**: **INFO**: Informational, warning, and error messages, and fatal issues.
- **2**: **WARN**: Warning, and error messages, and fatal issues.
- **3**: **ERROR**: Error messages and fatal issues.
- **4**: **FATAL**: Fatal issues only.

By default the log level is set to **2** (**WARN**). Use **DEBUG** when you have a problem to diagnose, and then reset your log level to a less-verbose level, as **DEBUG** outputs a lot of information, and can affect your server performance.

Logging level parameters are set in the `config/config.php` file, or on the Admin page of your ownCloud Web GUI.

ownCloud

All log information will be written to a separate log file which can be viewed using the log viewer on your Admin page. By default, a log file named **owncloud.log** will be created in the directory which has been configured by the **datadirectory** parameter in `config/config.php`.

The desired date format can optionally be defined using the **logdateformat** parameter in `config/config.php`. By default the **PHP date function** parameter “c” is used, and therefore the date/time is written in the format “2013-01-10T15:20:25+02:00”. By using the date format in the example below, the date/time format will be written in the format “January 10, 2013 15:20:25”.

```
'log_type' => 'owncloud',  
'logfile' => 'owncloud.log',  
'loglevel' => 2,  
'logdateformat' => 'F d, Y H:i:s',
```

Log rotation:

To rotate this log file, use the following key:

```
'log_rotate_size' => false,
```

The default is 0 or false which disables log rotation.

Specify a size in bytes, for example 104857600

(100 megabytes = 100 * 1024 * 1024 bytes).

A new logfile is created with a new name when the old logfile reaches your limit.

If a rotated log file is already present, it will be overwritten.

If enabled, only the active log file and one rotation file are present.

The file name of the rotated logfile is defined by the key `logfile` and a number as extension. Example:

```
owncloud.1
```

In case you want to implement more sophisticated log rotation, you can use the log rotation mechanism of your Linux operating system, see the following example. Please adopt or customize the configuration by your needs. The script assumes that the folder `/etc/logrotate.d/` is included in your Linux log rotate configuration. More information on Linux log rotation can be found in the [logrotate](#) documentation.

```
# Use an editor of your choice like vim

vim /etc/logrotate.d/owncloud

# Copy and paste the following into the file

/var/www/owncloud/data/owncloud.log {
size 10M                # Logfile Size Limit
rotate 12              # Amount of rotated logs to keeps
missingok              # If it's not there, no error will occur
compress               # after rotation, compress the copy of the log file
compresscmd /bin/gzip  # use this compression command
}
```

syslog

All log information will be sent to your default syslog daemon.

```
'log_type' => 'syslog',
'logfile' => '',
'loglevel' => 2,
```

The syslog format can be changed to remove or add information. In addition to the `%replacements%` below `%level%` can be used, but it is used as a dedicated parameter to the syslog logging facility anyway.

```
'log.syslog.format' => "[%reqId%][%remoteAddr%][%user%][%app%][%method%][%url%] %message%",
```

For the old syslog message format use:

```
'log.syslog.format' => '{%app%} %message%',
```

Conditional Logging Level Increase

You can configure the logging level to automatically increase to debug when the first condition inside a condition block is met. All conditions are optional !

- **shared_secret:** A unique token. If a http(s) request parameter named `log_secret` is added to the request and set to this token, the condition is met.
- **users:** If the current request is done by one of the specified users, this condition is met.
- **apps:** If the log message is invoked by one of the specified apps, this condition is met.
- **logfile:** The log message invoked gets redirected to this logfile when a condition above is met.

Notes regarding the logfile key:

1. If no logfile is defined, the standard logfile is used.
2. Not applicable when using syslog.

The following example demonstrates how all three conditions can look like.

The first one that matches triggers the condition block writing the log entry to the defined logfile.

```
'log.conditions' => [
  [
    'shared_secret' => '57b58edb6637fe3059b3595cf9c41b9',
    'users' => ['user1', 'user2'],
    'apps' => ['gallery'],
    'logfile' => '/tmp/test2.log'
  ]
],
```

Based on the conditional log settings above, following logs are written to the same logfile defined:

- Requests matching `log_secret` are debug logged.

```
curl -X PROPFIND -u sample-user:password \
  https://your_domain/remote.php/webdav/?log_secret=57b58edb6637fe3059b3595cf9c41b9
```

- `user1` and `user2` gets debug logged.
- Access to app `gallery` gets debug logged.

6.5.18 Hardening and Security Guidance

ownCloud aims to ship with secure defaults that do not need to get modified by administrators. However, in some cases some additional security hardening can be applied in scenarios where the administrator has complete control over the ownCloud instance. This page assumes that you run ownCloud Server on Apache2 in a Linux environment.

Note: ownCloud will warn you in the administration interface if some critical security-relevant options are missing. However, it is still up to the server administrator to review and maintain system security.

Limit on Password Length

ownCloud uses the `bcrypt` algorithm, and thus for security and performance reasons, e.g., denial of service as CPU demand increases exponentially, it only verifies the first 72 characters of passwords. This applies to all passwords that you use in ownCloud: user passwords, passwords on link shares, and passwords on external shares.

Operating system

Give PHP read access to `/dev/urandom`

ownCloud uses a [RFC 4086](#) (“Randomness Requirements for Security”) compliant mixer to generate cryptographically secure pseudo-random numbers. This means that when generating a random number ownCloud will request multiple random numbers from different sources and derive from these the final random number.

The random number generation also tries to request random numbers from `/dev/urandom`, thus it is highly recommended to configure your setup in such a way that PHP is able to read random data from it.

Note: When having an `open_basedir` configured within your `php.ini` file, make sure to include `/dev/urandom`.

Enable hardening modules such as SELinux

It is highly recommended to enable hardening modules such as SELinux where possible. See *SELinux Configuration* to learn more about SELinux.

Deployment

Place data directory outside of the web root

It is highly recommended to place your data directory outside of the Web root (i.e. outside of `/var/www`). It is easiest to do this on a new installation.

Disable preview image generation

ownCloud is able to generate preview images of common filetypes such as images or text files. By default the preview generation for some file types that we consider secure enough for deployment is enabled by default. However, administrators should be aware that these previews are generated using PHP libraries written in C which might be vulnerable to attack vectors.

For high security deployments we recommend disabling the preview generation by setting the `enable_previews` switch to `false` in `config.php`. As an administrator you are also able to manage which preview providers are enabled by modifying the `enabledPreviewProviders` option switch.

Use HTTPS

Using ownCloud without using an encrypted HTTPS connection opens up your server to a man-in-the-middle (MITM) attack, and risks the interception of user data and passwords. It is a best practice, and highly recommended, to always use HTTPS on production servers, and to never allow unencrypted HTTP.

How to setup HTTPS on your Web server depends on your setup; please consult the documentation for your HTTP server. The following examples are for Apache.

Redirect all unencrypted traffic to HTTPS

To redirect all HTTP traffic to HTTPS administrators are encouraged to issue a permanent redirect using the 301 status code. When using Apache this can be achieved by adding a setting such as the following in the Apache VirtualHosts configuration containing the `<VirtualHost *:80>` entry:

```
Redirect permanent / https://example.com/
```

Enable HTTP Strict Transport Security

While redirecting all traffic to HTTPS is good, it may not completely prevent man-in-the-middle attacks. Thus administrators are encouraged to set the HTTP Strict Transport Security header, which instructs browsers to not allow

any connection to the ownCloud instance using HTTP, and it attempts to prevent site visitors from bypassing invalid certificate warnings.

This can be achieved by setting the following settings within the Apache VirtualHost file containing the `<VirtualHost *:443>` entry:

```
<IfModule mod_headers.c>
  Header always set Strict-Transport-Security "max-age=15552000; includeSubDomains"
</IfModule>
```

If you don't have access to your Apache configuration it is also possible to add this to the main `.htaccess` file shipped with ownCloud. Make sure you're adding it below the line:

```
#### DO NOT CHANGE ANYTHING ABOVE THIS LINE ####
```

This example configuration will make all subdomains only accessible via HTTPS. If you have subdomains not accessible via HTTPS, remove `includeSubDomains`.

Note: This requires the `mod_headers` extension in Apache.

Proper SSL configuration

Default SSL configurations by Web servers are often not state-of-the-art, and require fine-tuning for an optimal performance and security experience. The available SSL ciphers and options depend completely on your environment and thus giving a generic recommendation is not really possible.

We recommend using the [Mozilla SSL Configuration Generator](#) to generate a suitable configuration suited for your environment, and the free [Qualys SSL Labs Tests](#) gives good guidance on whether your SSL server is correctly configured.

Also ensure that HTTP compression is disabled to mitigate the BREACH attack.

Use a dedicated domain for ownCloud

Administrators are encouraged to install ownCloud on a dedicated domain such as `cloud.domain.tld` instead of `domain.tld` to gain all the benefits offered by the Same-Origin-Policy.

Ensure that your ownCloud instance is installed in a DMZ

As ownCloud supports features such as Federated File Sharing we do not consider Server Side Request Forgery (SSRF) part of our threat model. In fact, given all our external storage adapters this can be considered a feature and not a vulnerability.

This means that a user on your ownCloud instance could probe whether other hosts are accessible from the ownCloud network. If you do not want this you need to ensure that your ownCloud is properly installed in a segregated network and proper firewall rules are in place.

Serve security related Headers by the Web server

Basic security headers are served by ownCloud already in a default environment. These include:

- **X-Content-Type-Options: nosniff**
 - Instructs some browsers to not sniff the mimetype of files. This is used for example to prevent browsers from interpreting text files as JavaScript.

- **X-XSS-Protection: 1; mode=block**
 - Instructs browsers to enable their browser side Cross-Site-Scripting filter.
- **X-Robots-Tag: none**
 - Instructs search machines to not index these pages.
- **X-Frame-Options: SAMEORIGIN**
 - Prevents embedding of the ownCloud instance within an iframe from other domains to prevent Click-jacking and other similar attacks.

These headers are hard-coded into the ownCloud server, and need no intervention by the server administrator.

For optimal security, administrators are encouraged to serve these basic HTTP headers by the Web server to enforce them on response. To do this Apache has to be configured to use the `.htaccess` file and the following Apache modules need to be enabled:

- `mod_headers`
- `mod_env`

Administrators can verify whether this security change is active by accessing a static resource served by the Web server and verify that the above mentioned security headers are shipped.

Use Fail2ban

Another approach to hardening the server(s) on which your ownCloud installation rest is using an intrusion detection system. An excellent one is [Fail2ban](#). Fail2ban is designed to protect servers from brute force attacks. It works by monitoring log files (such as those for *ssh*, *web*, *mail*, and *log* servers) for certain patterns, specific to each server, and taking actions should those patterns be found.

Actions include banning the IP from which the detected actions are being made from. This serves to both make the process more difficult as well as to prevent DDOS-style attacks. However, after a predefined time period, the banned IP is normally un-banned again.

This helps if the login attempts were genuine, so the user doesn't lock themselves out permanently. An example of such an action is users attempting to brute force login to a server via *ssh*. In this case, Fail2ban would look for something similar to the following in `/var/log/auth.log`.

```
Mar 15 11:17:37 yourhost sshd[10912]: input_userauth_request: invalid user audra [preauth]
Mar 15 11:17:37 yourhost sshd[10912]: pam_unix(sshd:auth): check pass; user unknown
Mar 15 11:14:51 yourhost sshd[10835]: PAM 2 more authentication failures; logname= uid=0 euid=0 tty=
Mar 15 11:14:57 yourhost sshd[10837]: pam_unix(sshd:auth): authentication failure; logname= uid=0 eu
Mar 15 11:14:59 yourhost sshd[10837]: Failed password for root from 221.194.44.231 port 46838 ssh2
Mar 15 11:15:04 yourhost sshd[10837]: message repeated 2 times: [ Failed password for root from 221.
Mar 15 11:15:04 yourhost sshd[10837]: Received disconnect from 221.194.44.231: 11: [preauth]
```

Note: If you're not familiar with what's going on, this snippet highlights a number of failed login attempts being made.

Using Fail2ban to secure an ownCloud login

On Ubuntu, you can install Fail2ban using the following commands:

```
apt update && apt upgrade
apt install fail2ban
```

Fail2ban installs several default filters for *Apache*, *NGINX*, and various other services, but none for ownCloud. Given that, we have to define our own filter. To do so, you first need to make sure that ownCloud uses your local timezone for writing log entries; otherwise, fail2ban cannot react appropriately to attacks. To do this, edit your `config.php` file and add the following line:

```
'logtimezone' => 'Europe/Berlin',
```

Note: Adjust the timezone to the one that your server is located in, based on [PHP's list of supported timezones](#).

This change takes effect as soon as you save `config.php`. You can test the change by:

1. Entering false credentials at your ownCloud login screen
2. Checking the timestamp of the resulting entry in ownCloud's log file.

Next, define a new Fail2ban filter rule for ownCloud. To do so, create a new file called `/etc/fail2ban/filter.d/owncloud.conf`, and insert the following configuration:

```
[Definition]
failregex={.*Login failed: \'.*\' \(Remote IP: \'<HOST>\'\)"}
ignoreregex =
```

This filter needs to be loaded when Fail2ban starts, so a further configuration entry is required to be added in `/etc/fail2ban/jail.d/defaults-debian.conf`, which you can see below:

```
[owncloud]
enabled = true
port = 80,443
protocol = tcp
filter = owncloud
maxretry = 3
bantime = 10800
logpath = /var/owncloud_data/owncloud.log
```

This configuration:

1. Enables the filter rules for TCP requests on ports 80 and 443.
2. Bans IPs for 10800 seconds (3 hours).
3. Sets the path to the log file to analyze for malicious logins

Note: The most important part of the configuration is the `logpath` parameter. If this does not point to the correct log file, Fail2ban will either not work properly or refuse to start.

After saving the file, restart Fail2ban by running the following command:

```
service fail2ban restart
```

To test that the new ownCloud configuration has been loaded, use the following command:

```
fail2ban-client status
```

If “owncloud” is listed in the console output, the filter is both loaded and active. If you want to test the filter, run the following command, adjusting the path to your `owncloud.log`, if necessary:

```
fail2ban-regex /var/owncloud_data/owncloud.log /etc/fail2ban/filter.d/owncloud.conf
```

The output will look similar to the following, if you had one failed login attempt:

```
fail2ban-regex /var/www/owncloud_data/owncloud.log /etc/fail2ban/filter.d/owncloud.conf
```

```
Running tests
```

```
=====
```

```
Use failregex file : /etc/fail2ban/filter.d/owncloud.conf
Use log file : /var/www/owncloud_data/owncloud.log
```

```
Results
```

```
=====
```

```
Failregex: 1 total
|- #) [# of hits] regular expression
| 1) [1] {.*Login failed: \'.*\' \(Remote IP: \'<HOST>\'\)"}
\`_
```

```
Ignoreregex: 0 total
```

```
Date template hits:
|- [# of hits] date format
| [40252] ISO 8601
\`_
```

```
Lines: 40252 lines, 0 ignored, 1 matched, 40251 missed
```

The Failregex counter increments by 1 for every failed login attempt. To un-ban an IP, which was locked either during testing or unintentionally, use the following command:

```
fail2ban-client set owncloud unbanip <IP>
```

You can check the status of your ownCloud filter with the following command:

```
fail2ban-client status owncloud
```

This will produce an output similar to this:

```
Status for the jail: owncloud
|- filter
| |- File list: /var/www/owncloud_data/owncloud.log
| |- Currently failed: 1
| `-- Total failed: 7
`-- action
    |- Currently banned: 0
    | `-- IP list:
    `-- Total banned: 1
```

6.5.19 Password Policy

From the 2.0.0 release of the [Password Policy app](#), ownCloud administrators (both enterprise **and** community edition) have the option of installing and enabling the application. The Password Policy application enables administrators to define password requirements for user passwords and public links.

Some of policy rules apply to both user passwords and public links, and some apply to just one or the other. The table below shows where each option can be used.

Password and public link expiration policies

Minimum password requirements for user accounts and public links:

- different than last passwords
- minimum characters
- lowercase letters
- uppercase letters
- numbers
- special characters
- Define special characters:

User password policies:

- days until user password expires
- days before password expires, users will receive a reminder notification
- Force users to change their password on first login

Public link expiration policies:

- days until link expires if password is set
- days until link expires if password is not set

Save

Setting	User Passwords	Public Links
Specify valid password requirements	•	•
Disallow usage of a number of previous passwords	•	
Specify a password expiration period	•	
Forced password change on first login	•	
Disallowing passwords that match a configurable . number of previous passwords (defaults to the previous 3)	•	
Users can be notified a configurable number of days before their password expires	•	
Users will be notified when their password has expired.	•	
Specify expiration dates for public link shares		•
Specify the number of days until link expires if a password is set		•
Specify the number of days until link expires if a password is <i>not</i> set		•

Note: Active user sessions will **not** end when passwords expire. However, a password change will be forced when the user session expires (e.g., on logout). OAuth2 tokens for app or client authentication, and App passwords are not affected.

Note: Installing and enabling the application also extends the `occ` command to support *the `user:expire-password` command*.

Caution: After enabling the “*days until user password expires*” policy setting in the web UI, administrators need to run the `occ user:expire-password` command to set an initial password change date for all existing users.

The Security App

Caution: Do not configure password policies using the Security and Password Policy apps simultaneously. Please use either one or the other. However, the brute-force protection part of the Security app can and should be used in parallel with the Password Policy app.

You can, *alternatively*, use [the Security app](#). It supports configuring a basic password policy, which includes:

1. Setting a password length
2. Whether to enforce at least one upper and lower case character, a numerical character, and a special character.

Tip: In the next release, the Security app’s feature-set will be reduced to provide only brute-force protection capabilities and be renamed “*Brute-Force Protection*”.

Password Policy

Determine minimum password length

- Enforce at least one upper and one lower case character on passwords
- Enforce at least one numerical characters on passwords
- Enforce at least one special characters on passwords

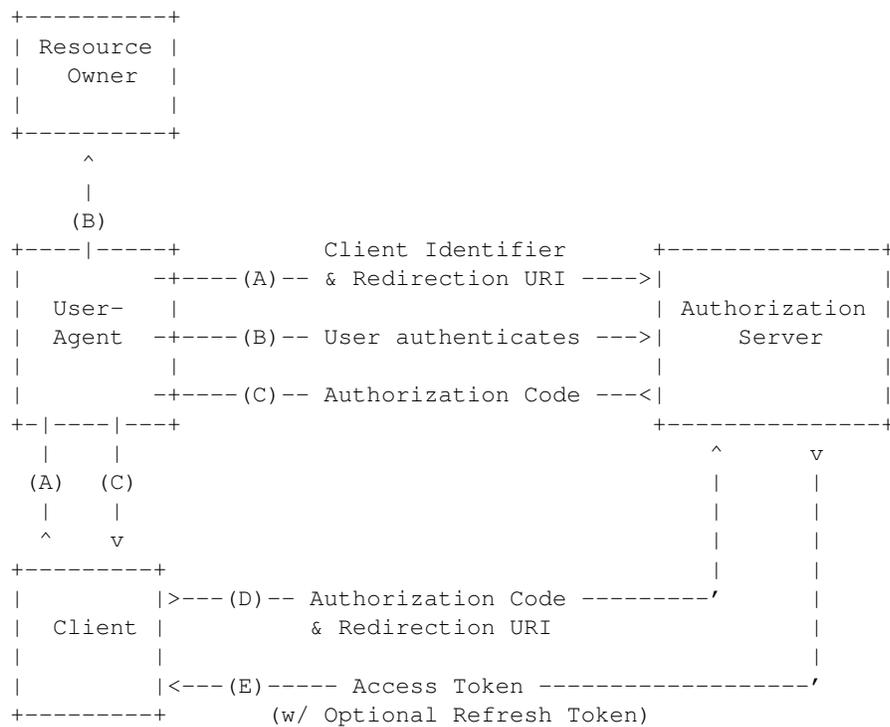
6.5.20 OAuth2

What is it?

OAuth2 is summarized in [RFC 6749](#) as follows:

The OAuth 2.0 authorization framework enables a third-party application to obtain limited access to an HTTP service, either on behalf of a resource owner by orchestrating an approval interaction between the resource owner and the HTTP service, or by allowing the third-party application to obtain access on its own behalf.

Here is an overview of how the process works:



The OAuth2 App

OAuth2 support is available in ownCloud via an [OAuth2 application](#) which is available from the ownCloud Marketplace. The app aims to:

1. Connect ownCloud clients (both desktop and mobile) in a standardized and secure way.
2. Make 3rd party software integrations easier by providing an unified authorization interface.

Endpoints

Description	URI
Authorization URL	/index.php/apps/oauth2/authorize
Access Token URL	/index.php/apps/oauth2/api/v1/token

Protocol Flow

Client Registration The clients first have to be registered in the admin settings: </settings/admin?sectionid=authentication>. You need to specify a name for the client (the name is unrelated to the OAuth 2.0 protocol and is just used to recognize it later) and the redirection URI. A client identifier and client secret are generated when adding a new client, which both consist of 64 characters. For further information about client registration, please refer to [the official client registration RFC from the IETF](#).

Authorization Request For every registered client an authorization request can be made. The client redirects the resource owner to the authorization URL and requests authorization. The following URL parameters have to be specified:

Parameter	Required	Description
<code>response_type</code>	yes	Needs to be <i>code</i> because at this time only the authorization code flow is implemented.
<code>client_id</code>	yes	The client identifier obtained when registering the client.
<code>redirect_uri</code>	yes	The redirection URI specified when registering the client.
<code>state</code>	no	Can be set by the client “to maintain state between the request and callback”. See RFC 6749 for more information.

For further information about client registration, please refer to [the official authorization request RFC from the IETF](#).

Authorization Response After the resource owner’s authorization, the app redirects to the `redirect_uri` specified in the authorization request and adds the authorization code as URL parameter *code*. An authorization code is valid for 10 minutes. For further information about client registration, please refer to [the official authorization response RFC from the IETF](#).

Access Token Request With the authorization code, the client can request an access token using the access token URL. [Client authentication](#) is done using basic authentication with the client identifier as username and the client secret as a password. The following URL parameters have to be specified:

Parameter	Required	Description
<code>grant_type</code>		Either <code>authorization_code</code> or <code>refresh_token</code> .
<code>code</code>	if the grant type <code>authorization_code</code> is used.	
<code>redirect_uri</code>	if the grant type <code>authorization_code</code> is used.	
<code>refresh_token</code>	if the grant type <code>refresh_token</code> is used.	

For further information about client registration, please refer to [the official access token request RFC from the IETF](#).

Access Token Response The app responds to a valid access token request with a JSON response like the following. An access token is valid for 1 hour and can be refreshed with a refresh token.

```
{
  "access_token" : "1vtnuo1NkIsbndAjVnh17y0wJha59JyaAiFIVQDvcBY2uvKmj5EPBEhss0pauzdQ",
  "token_type" : "Bearer",
  "expires_in" : 3600,
  "refresh_token" : "7y0wJuvKmj5E1vjVnh1PBEhha59JyaAiFIVQDvcBY2ss0pauzdQtnuo1NkIsbndA",
  "user_id" : "admin",
  "message_url" : "https://www.example.org/owncloud/index.php/apps/oauth2/authorization-successful"
}
```

For further information about client registration, please refer to [the official access token response RFC from the IETF](#).

Note: For a succinct explanation of the differences between access tokens and authorization codes, check out [this answer on StackOverflow](#).

Installation

To install the application, place the content of the OAuth2 app inside your installation's `app` directory, or use the Market application.

Requirements

If you are hosting your ownCloud installation from the Apache web server, then both the `mod_rewrite` and `mod_headers` modules are required to be installed and enabled.

Basic Configuration

To enable token-only based app or client logins in `config/config.php` set `token_auth_enforced` to `true`.

Restricting Usage

- Enterprise installations can limit the access of authorized clients, preventing unwanted clients from connecting.

Limitations

- Since the app handles no user passwords, only master key encryption works (similar to [the Shibboleth app](#)).
- Clients cannot migrate accounts from Basic Authorization to OAuth2, if they are currently using the `~user_ldap~` backend.

Connecting Clients via OAuth2

Revoking Sessions

6.5.21 Reverse Proxy Configuration

ownCloud can be run through a reverse proxy, which can cache static assets such as images, CSS, or Javascript files, move the load of handling HTTPS to a different server or load balance between multiple servers.

Defining Trusted Proxies

For security, you must explicitly define the proxy servers that ownCloud is to trust. Connections from trusted proxies will be specially treated to get the real client information, for use in access control and logging. Parameters are configured in `config/config.php`

Set the **trusted_proxies** parameter as an array of IP address to define the servers ownCloud should trust as proxies. This parameter provides protection against client spoofing, and you should secure those servers as you would your ownCloud server.

A reverse proxy can define HTTP headers with the original client IP address, and ownCloud can use those headers to retrieve that IP address. ownCloud uses the de-facto standard header 'X-Forwarded-For' by default, but this can be configured with the **forwarded_for_headers** parameter. This parameter is an array of PHP lookup strings, for example 'X-Forwarded-For' becomes 'HTTP_X_FORWARDED_FOR'. Incorrectly setting this parameter may allow clients to spoof their IP address as visible to ownCloud, even when going through the trusted proxy! The correct value for this parameter is dependent on your proxy software.

Overwrite Parameters

The automatic hostname, protocol or webroot detection of ownCloud can fail in certain reverse proxy situations. This configuration allows the automatic detection to be manually overridden.

If ownCloud fails to automatically detect the hostname, protocol or webroot you can use the **overwrite** parameters inside the `config/config.php`. The **overwritehost** parameter is used to set the hostname of the proxy. You can also specify a port. The **overwriteprotocol** parameter is used to set the protocol of the proxy. You can choose between the two options **http** and **https**. The **overwritewebroot** parameter is used to set the absolute web path of the proxy to the ownCloud folder. When you want to keep the automatic detection of one of the three parameters you can leave the value empty or don't set it. The **overwritecondaddr** parameter is used to overwrite the values dependent on the remote address. The value must be a **regular expression** of the IP addresses of the proxy. This is useful when you use a reverse SSL proxy only for https access and you want to use the automatic detection for http access.

Example

Multiple Domains Reverse SSL Proxy

If you want to access your ownCloud installation **http://domain.tld/owncloud** via a multiple domains reverse SSL proxy **https://ssl-proxy.tld/domain.tld/owncloud** with the IP address **10.0.0.1** you can set the following parameters inside the `config/config.php`.

```
<?php
$CONFIG = [
    "trusted_proxies" => ['10.0.0.1'],
    "overwritehost"   => "ssl-proxy.tld",
```

```
"overwriteprotocol" => "https",  
"overwritewebroot"  => "/domain.tld/owncloud",  
"overwritecondaddr" => "^10\.0\.0\.1$",  
];
```

With an Apache as reverse proxy (ssl-proxy.tld) you can use this configuration:

```
ProxyPass "/domain.tld/owncloud" "http://domain.tld/owncloud"  
ProxyPassReverse "/domain.tld/owncloud" "http://domain.tld/owncloud"
```

Note: If you want to use the SSL proxy during installation you have to create the `config/config.php` otherwise you have to extend the existing `$CONFIG` array.

6.5.22 Using Third Party PHP Components

ownCloud uses some third party PHP components to provide some of its functionality. These components are part of the software package and are contained in the `/3rdparty` folder.

Managing Third Party Parameters

When using third party components, keep the following parameters in mind:

- **3rdpartyroot** – Specifies the location of the 3rd-party folder. To change the default location of this folder, you can use this parameter to define the absolute file system path to the folder location.
- **3rdpartyurl** – Specifies the http web path to the 3rdpartyroot folder, starting at the ownCloud web root.

An example of what these parameters might look like is as follows:

```
<?php  
  
"3rdpartyroot" => OC::$SERVERROOT."/3rdparty",  
"3rdpartyurl"  => "/3rdparty",
```

6.5.23 Automatic Configuration Setup

If you need to install ownCloud on multiple servers, you normally do not want to set up each instance separately as described in *Database Configuration*. For this reason, ownCloud provides an automatic configuration feature.

To take advantage of this feature, you must create a configuration file, called `../owncloud/config/autoconfig.php`, and set the file parameters as required. You can specify any number of parameters in this file. Any unspecified parameters appear on the “Finish setup” screen when you first launch ownCloud.

The `../owncloud/config/autoconfig.php` is automatically removed after the initial configuration has been applied.

Parameters

When configuring parameters, you must understand that two parameters are named differently in this configuration file when compared to the standard `config.php` file.

autoconfig.php	config.php
directory	datadirectory
dbpass	dbpassword

Automatic Configurations Examples

The following sections provide sample automatic configuration examples and what information is requested at the end of the configuration.

Data Directory

Using the following parameter settings, the “Finish setup” screen requests database and admin credentials settings.

```
<?php
$AUTOCONFIG = array(
    "directory"    => "/www/htdocs/owncloud/data",
);
```

SQLite Database

Using the following parameter settings, the “Finish setup” screen requests data directory and admin credentials settings.

```
<?php
$AUTOCONFIG = array(
    "dbtype"       => "sqlite",
    "dbname"       => "owncloud",
    "dbtableprefix" => "",
);
```

MySQL Database

Using the following parameter settings, the “Finish setup” screen requests data directory and admin credentials settings.

```
<?php
$AUTOCONFIG = array(
    "dbtype"       => "mysql",
    "dbname"       => "owncloud",
    "dbuser"       => "username",
    "dbpass"       => "password",
    "dbhost"       => "localhost",
    "dbtableprefix" => "",
);
```

Note: Keep in mind that the automatic configuration does not eliminate the need for creating the database user and database in advance, as described in [Database Configuration](#).

PostgreSQL Database

Using the following parameter settings, the “Finish setup” screen requests data directory and admin credentials settings.

```
<?php
$AUTOCONFIG = array(
    "dbtype"      => "pgsql",
    "dbname"      => "owncloud",
    "dbuser"      => "username",
    "dbpass"      => "password",
    "dbhost"      => "localhost",
    "dbtableprefix" => "",
);
```

Note: Keep in mind that the automatic configuration does not eliminate the need for creating the database user and database in advance, as described in *Database Configuration*.

All Parameters

Using the following parameter settings, because all parameters are already configured in the file, the ownCloud installation skips the “Finish setup” screen.

```
<?php
$AUTOCONFIG = array(
    "dbtype"      => "mysql",
    "dbname"      => "owncloud",
    "dbuser"      => "username",
    "dbpass"      => "password",
    "dbhost"      => "localhost",
    "dbtableprefix" => "",
    "adminlogin"  => "root",
    "adminpass"   => "root-password",
    "directory"   => "/www/htdocs/owncloud/data",
);
```

Note: Keep in mind that the automatic configuration does not eliminate the need for creating the database user and database in advance, as described in *Database Configuration*.

6.5.24 ownCloud Server Tuning

Using Cron to Perform Background Jobs

See *Background Jobs* for a description and the benefits.

Enable Memory Caching

Caching improves performance by storing data, code, and other objects in memory. Memory cache configuration for ownCloud is no longer automatically available from ownCloud 8.1 but must be installed and configured separately. ownCloud supports [Redis](#), [APCu](#), and [Memcached](#) as memory caching backends. See *Memory Caching*, for further details.

Use Redis-based Transactional File Locking

File locking is enabled by default, using the database locking backend. However, this places a significant load on your database. See the section *Transactional File Locking* for how to configure ownCloud to use Redis-based Transactional File Locking.

Redis Tuning

Redis tuning improves both file locking (if used) and memory caching (when using Redis). Here is a brief guide for tuning Redis to improve the performance of your ownCloud installation, when working with sizeable instances.

TCP-Backlog

If you raised the TCP-backlog setting, the following warning appears in the Redis logs:

```
WARNING: The TCP backlog setting of 20480 cannot be enforced because /proc/sys/net/core/somaxconn is
```

If so, please consider that newer versions of Redis have their own TCP-backlog value set to 511, and that you have to increase it if you have many connections. In high requests-per-second environments, you need a significant backlog to avoid slow clients connection issues.

Note: The Linux kernel will silently truncate the TCP-backlog setting to the value of `/proc/sys/net/core/somaxconn`. So make sure to raise both the value of `somaxconn` and `tcp_max_syn_backlog`, to get the desired effect.

To fix this warning, set the value of `net.core.somaxconn` to 65535 in `/etc/rc.local`, so that it persists upon reboot, by running the following command.

```
sudo echo sysctl -w net.core.somaxconn=65535 >> /etc/rc.local
```

After the next reboot, 65535 connections will be allowed, instead of the default value.

Transparent Huge Pages (THP)

If you are experiencing latency problems with Redis, the following warning may appear in your Redis logs:

```
WARNING you have Transparent Huge Pages (THP) support enabled in your kernel. This creates both later
```

If so, unfortunately, when a Linux kernel has [Transparent Huge Pages](#) enabled, Redis incurs a significant latency penalty after the fork call is used, to persist information to disk. Transparent Huge Pages are the cause of the following issue:

1. A fork call is made, resulting in two processes with shared huge pages being created.
2. In a busy instance, a few event loops cause commands to target a few thousand pages, causing the copy-on-write of almost the entire process memory.
3. Big latency and memory usage result.

As a result, make sure to disable Transparent Huge Pages using the following command:

```
echo never > /sys/kernel/mm/transparent_hugepage/enabled
```

Redis Latency Problems

If you are having issues with Redis latency, please refer to [the official Redis guide](#) on how to handle them.

Database Tuning

Using MariaDB/MySQL Instead of SQLite

MySQL or MariaDB are preferred because of the [performance limitations of SQLite with highly concurrent applications](#), like ownCloud.

See the section [Database Configuration](#) for how to configure ownCloud for MySQL or MariaDB. If your installation is already running on SQLite then it is possible to convert to MySQL or MariaDB using the steps provided in [Converting Database Type](#).

Tune MariaDB/MySQL

A comprehensive guide to tuning MySQL and MariaDB is outside the scope of the ownCloud documentation. However, here are three links that can help you find further information:

- [MySQLTuner](#).
- [Percona Tools for MySQL](#)
- [Optimizing and Tuning MariaDB](#).

Tune PostgreSQL

A comprehensive guide to tuning PostgreSQL is outside the scope of the ownCloud documentation. However, here are three links that can help you find further information:

- [Five Steps to PostgreSQL Performance](#)
- [Tuning the autovacuum proceff for tables with huge update workloads \(oc_filecache\)](#)

SSL / Encryption App

SSL (HTTPS) and file encryption/decryption can be offloaded to a processor's AES-NI extension. This can both speed up these operations while lowering processing overhead. This requires a processor with the [AES-NI instruction set](#).

Here are some examples how to check if your CPU / environment supports the AES-NI extension:

- For each CPU core present: `grep flags /proc/cpuinfo` or as a summary for all cores: `grep -m 1 ^flags /proc/cpuinfo` If the result contains any `aes`, the extension is present.
- Search eg. on the Intel web if the processor used supports the extension [Intel Processor Feature Filter](#) You may set a filter by "AES New Instructions" to get a reduced result set.
- For versions of openssl \geq 1.0.1, AES-NI does not work via an engine and will not show up in the `openssl engine` command. It is active by default on the supported hardware. You can check the openssl version via `openssl version -a`
- If your processor supports AES-NI but it does not show up eg via `grep` or `coreinfo`, it is maybe disabled in the BIOS.
- If your environment runs virtualized, check the virtualization vendor for support.

Webserver Tuning

Tune Apache

Enable HTTP/2 Support If you want to improve the speed of an ownCloud installation, while at the same time increasing its security, you can [enable HTTP/2 support for Apache](#). Please be aware that [most browsers require HTTP/2 to be used with SSL enabled](#).

Apache Processes An Apache process uses around 12MB of RAM. Apache should be configured so that the maximum number of HTTPD processes times 12MB is lower than the amount of RAM. Otherwise the system begins to swap and the performance goes down.

Use KeepAlive The [KeepAlive](#) directive enables persistent HTTP connections, allowing multiple requests to be sent over the same TCP connection. Enabling it reduces latency by as much as 50%. In combination with the periodic checks of the sync client the following settings are recommended:

```
KeepAlive On
KeepAliveTimeout 100
MaxKeepAliveRequests 200
```

Hostname Lookups

```
# cat /etc/httpd/conf/httpd.conf
...
HostnameLookups off
```

Log files Log files should be switched off for maximum performance. To do that, comment out the [CustomLog](#) directive. However, keep [ErrorLog](#) set, so errors can be tracked down.

6.5.25 Enable index.php-less URLs

Since ownCloud 9.0.3 you need to explicitly configure and enable `index.php-less` URLs (e.g. <https://example.com/apps/files/> instead of <https://example.com/index.php/apps/files/>). The following documentation provides the needed steps to configure this for the Apache Web server.

Prerequisites

Before being able to use `index.php-less` URLs you need to enable the `mod_rewrite` and `mod_env` Apache modules. Furthermore a configured `AllowOverride All` directive within the `vhost` of your Web server is needed. Please have a look at the [Apache manual](#) for how to enable and configure these.

Furthermore these instructions are only working when using Apache together with the `mod_php` Apache module for PHP. Other modules like `php-fpm` or `mod_fastcgi` are unsupported.

Finally the user running your Web server (e.g. `www-data`) needs to be able to write into the `.htaccess` file shipped within the ownCloud root directory (e.g. `/var/www/owncloud/.htaccess`). If you have applied [Set Strong Directory Permissions](#) the user might be unable to write into this file and the needed update will fail. You need to revert this strong permissions temporarily by following the steps described in [Setting Permissions for Updating](#).

Configuration steps

The first step is to configure the `overwrite.cli.url` and `htaccess.RewriteBase` `config.php` options (See *Core Config.php Parameters*). If you're accessing your ownCloud instance via `https://example.com/` the following two options need to be added / configured:

```
'overwrite.cli.url' => 'https://example.com',  
'htaccess.RewriteBase' => '/',
```

If the instance is accessed via `https://example.com/owncloud` the following configuration is needed:

```
'overwrite.cli.url' => 'https://example.com/owncloud',  
'htaccess.RewriteBase' => '/owncloud',
```

As a second step ownCloud needs to enable `index.php-less` URLs. This is done:

- during the next update of your ownCloud instance
- by manually running the `occ` command `occ maintenance:update:htaccess` (See *Using occ core commands*)

Afterwards your instance should have `index.php-less` URLs enabled.

Troubleshooting

If accessing your ownCloud installation fails after following these instructions and you see messages like this in your ownCloud log:

```
The requested uri(\\/login) cannot be processed by the script '\\owncloud\\index.php'
```

make sure that you have configured the two `config.php` options listed above correctly.

6.6 User Management

6.6.1 User Management

On the User management page of your ownCloud Web UI you can:

- Create new users
- View all of your users in a single scrolling window
- Filter users by group
- See what groups they belong to
- Edit their full names and passwords
- See their data storage locations
- View and set quotas
- Create and edit their email addresses
- Send an automatic email notification to new users
- Delete them with a single click

Username		Password		Groups	Create	Search Users	
Username	Full Name	Password	Groups	Group Admin for	Quota		
 admin	admin	●●●●●●●●	admin ▼	no group ▼	Default ▼		
 layla	layla	●●●●●●●●	users, artists ▼	artists ▼	10 GB ▼		
 molly	molly	●●●●●●●●	users ▼	no group ▼	Default ▼		
 ritasue	ritasue	●●●●●●●●	artists ▼	users ▼	10 GB ▼		
 stashcat	stashcat	●●●●●●●●	users, admin ▼	no group ▼	5 GB ▼		

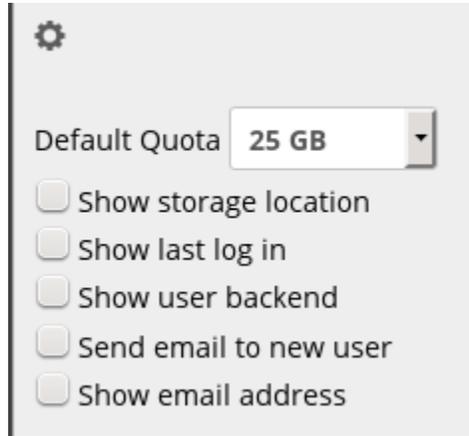
+ Add Group

Everyone	5
Admins	2
users	3
artists	2

The default view displays basic information about your users.

The Group filters on the left sidebar lets you quickly filter users by their group memberships, and create new groups.

Click the gear icon on the lower left sidebar to set a default storage quota, and to display additional fields: **Show storage location**, **Show last log in**, **Show user backend**, **Send email to new users**, and **Show email address**.



User accounts have the following properties:

Login Name (Username) The unique ID of an ownCloud user, and it cannot be changed.

Full Name The user's display name that appears on file shares, the ownCloud Web interface, and emails. Admins and users may change the Full Name anytime. If the Full Name is not set it defaults to the login name.

Password The admin sets the new user's first password. Both the user and the admin can change the user's password at anytime.

Groups You may create groups, and assign group memberships to users. By default new users are not assigned to any groups.

Group Admin Group admins are granted administrative privileges on specific groups, and can add and remove users from their groups.

Quota The maximum disk space assigned to each user. Any user that exceeds the quota cannot upload or sync data. You have the option to include external storage in user quotas.

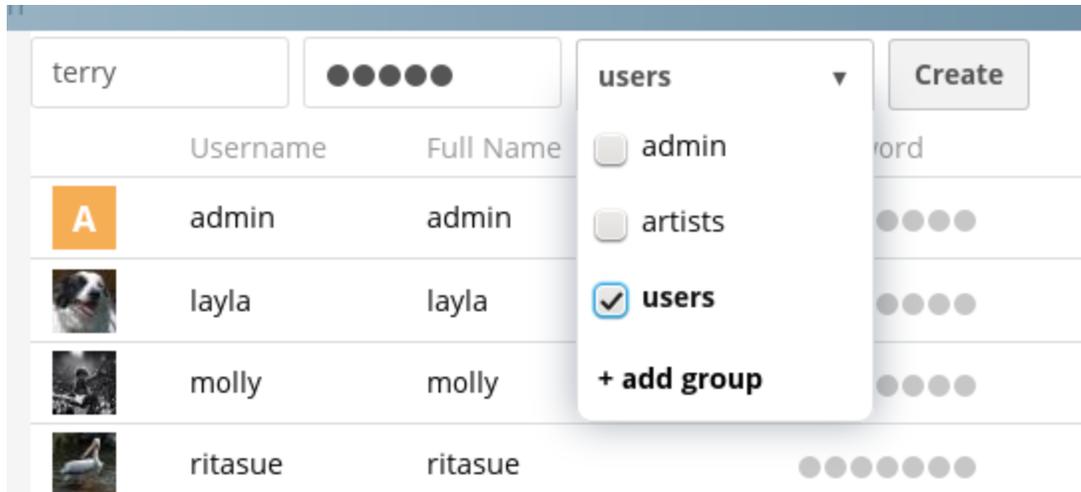
Creating a New User

To create a user account:

- Enter the new user's **Login Name** and their initial **Password**
- Optionally, assign **Groups** memberships
- Click the **Create** button

Login names may contain letters (a-z, A-Z), numbers (0-9), dashes (-), underscores (_), periods (.) and at signs (@). After creating the user, you may fill in their **Full Name** if it is different than the login name, or leave it for the user to complete.

If you have checked **Send email to new user** in the control panel on the lower left sidebar, you may also enter the new user's email address, and ownCloud will automatically send them a notification with their new login information. You may edit this email using the email template editor on your Admin page (see [Email Configuration](#)).



Reset a User's Password

You cannot recover a user's password, but you can set a new one:

- Hover your cursor over the user's **Password** field
- Click on the **pencil icon**
- Enter the user's new password in the password field, and remember to provide the user with their password

If you have encryption enabled, there are special considerations for user password resets. Please see [Encryption Configuration](#).

Renaming a User

Each ownCloud user has two names: a unique **Login Name** used for authentication, and a **Full Name**, which is their display name. You can edit the display name of a user, but you cannot change the login name of any user.

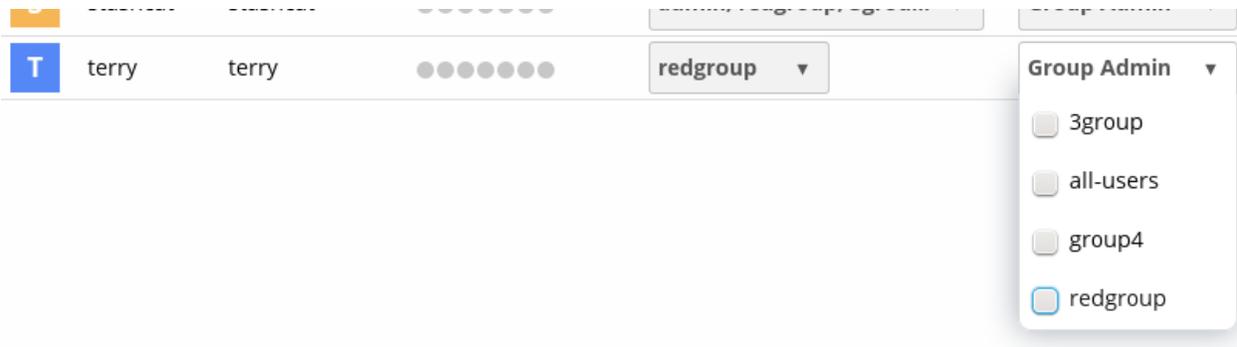
To set or change a user's display name:

- Hover your cursor over the user's **Full Name** field
- Click on the **Pencil icon**
- Enter the user's new display name

Granting Administrator Privileges to a User

ownCloud has two types of administrators: **Super Administrators** and **Group Administrators**. Group administrators have the rights to create, edit and delete users in their assigned groups. Group administrators cannot access system settings, or add or modify users in the groups that they are not **Group Administrators** for. Use the dropdown menus in the **Group Admin** column to assign group admin privileges.

Super Administrators have full rights on your ownCloud server, and can access and modify all settings. To assign the **Super Administrators** role to a user, simply add them to the `admin` group.



Managing Groups

You can assign new users to groups when you create them, and create new groups when you create new users. You may also use the **Add Group** button at the top of the left pane to create new groups. New group members will immediately have access to file shares that belong to their new groups.

Setting Storage Quotas

There are 4 Types of Quota Settings in ownCloud when dealing with LDAP users.

Quota Field

Found in “*User Authentication -> the Advanced Tab -> Special Attributes*”, this setting overwrites the rest. If set, this is what will be set for an LDAP user’s quota in ownCloud.

Quota Default

Found in “*User Authentication -> the Advanced Tab -> Special Attributes*”, this is the fallback option if no quota field is defined.

User Quota

This is what you set in the web UI drop down menu, and is how you set user quota.

Default Quota

This will be set if no quota is set, and is found in “*Users Tab -> Gear Wheel, Default Quota*”. If Quota Field is not set, but Quota Default is, and a systems administrator tries to set a quota for an LDAP user with User Quota, it will not work, since it is overridden by Quota Default.

Click the gear on the lower left pane to set a default storage quota. This is automatically applied to new users. You may assign a different quota to any user by selecting from the **Quota** dropdown, selecting either a preset value or entering a custom value. When you create custom quotas, use the normal abbreviations for your storage values such as 500 MB, 5 GB, 5 TB, and so on.

You now have a configurable option in `config.php` that controls whether external storage is counted against user’s quotas. This is still experimental, and may not work as expected. The default is to not count external storage as part of user storage quotas. If you prefer to include it, then change the default `false` to `true`:

```
'quota_include_external_storage' => false,
```

Metadata (such as thumbnails, temporary files, and encryption keys) takes up about 10% of disk space, but is not counted against user quotas. Users can check their used and available space on their Personal pages. Only files that originate with users count against their quotas, and not files shared with them that originate from other users. For example, if you upload files to a different user's share, those files count against your quota. If you re-share a file that another user shared with you, that file does not count against your quota, but the originating user's.

Encrypted files are a little larger than unencrypted files; the unencrypted size is calculated against the user's quota.

Deleted files that are still in the trash bin do not count against quotas. The trash bin is set at 50% of quota. Deleted file aging is set at 30 days. When deleted files exceed 50% of quota then the oldest files are removed until the total is below 50%.

When version control is enabled, the older file versions are not counted against quotas.

When a user creates a public share via URL, and allows uploads, any uploaded files count against that user's quota.

Deleting users

Deleting a user is easy: hover your cursor over their name on the **Users** page until a trashcan icon appears at the far right. Click the trashcan, and they're gone. You'll see an undo button at the top of the page, which remains until you refresh the page. When the undo button is gone you cannot recover the deleted user.

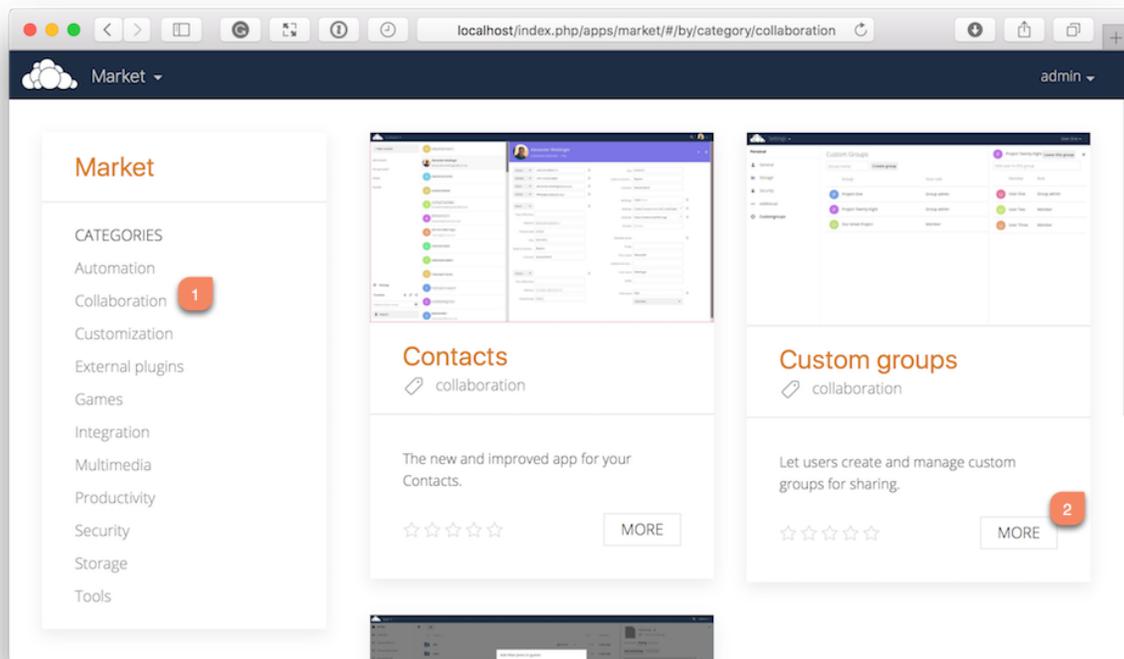
All of the files owned by the user are deleted as well, including all files they have shared. If you need to preserve the user's files and shares, you must first download them from your ownCloud Files page, which compresses them into a zip file, or use a sync client to copy them to your local computer. See *File Sharing* to learn how to create persistent file shares that survive user deletions.

Enabling Custom Groups

In previous versions of ownCloud, files and folders could only be shared with individual users or groups created by administrators. This wasn't the most efficient way to work. From ownCloud 10.0, users can create groups on-the-fly, through a feature called "Custom Groups", enabling them to share content in a more flexible way.

To enable Custom Groups:

1. From the ownCloud Market, which you can find in version 10.0 under the Apps menu, click "**Market**".
2. Click "**Collaboration**" (1), to filter the list of available options and click the "**Custom groups**" application (2).



3. Click **“INSTALL”** in the bottom right-hand corner of the Custom Groups application.

Settings User One ▾

Personal

- General
- Storage
- Security
- Additional
- Customgroups

Custom Groups

Group name Create group

Group	Your role
P Project One	Group admin
P Project Twenty-Eight	Group admin
O Our Great Project	Member

P Project Twenty-Eight Leave this group ✕

Add user to this group

Member	Role
U User One	Group admin
U User Two	Member
U User Three	Member

Let users create and manage custom groups for sharing.

VERSION	DATE	LICENSE
0.2	April 24, 2017	GNU Affero General Public License

UPDATE INSTALL

With this done, Custom Group functionality will be available in your ownCloud installation.

Custom Groups Settings

Sharing

i Help & Tips

⋮ Additional

Extra field to display in autocomplete results

None ▾

Federation

ownCloud Federation allows you to connect with other trusted ownClouds to exchange

Add server automatically once a federated share was created successfully

Trusted ownCloud Servers

+ Add ownCloud server

Federated Cloud Sharing *i*

Allow users on this server to send shares to other servers

Allow users on this server to receive shares from other servers

Custom Groups

Only group admins are allowed to create custom groups

Allow creating multiple groups with the same name

As an ownCloud admin, you can enable/disable these 2 options for custom groups.

- The first one limits the creation of custom groups to group admins.
- The second option allows the creation of custom groups with the same name.

ownCloud admins can see all custom groups of an instance and have group admin privileges for those.

6.6.2 Resetting a Lost Admin Password

The normal ways to recover a lost password are:

1. Click the password reset link on the login screen; this appears after a failed login attempt. This works only if you have entered your email address on your Personal page in the ownCloud Web interface, so that the ownCloud server can email a reset link to you.
2. Ask another ownCloud server admin to reset it for you.

If neither of these is an option, then you have a third option, and that is using the `occ` command. `occ` is in the `owncloud` directory, for example `/var/www/owncloud/occ`. `occ` has a command for resetting all user passwords, `user:resetpassword`. It is best to run `occ` as the `HTTP` user, as in this example on Ubuntu Linux:

```
$ sudo -u www-data php /var/www/owncloud/occ user:resetpassword admin
Enter a new password:
Confirm the new password:
Successfully reset password for admin
```

If your ownCloud username is not `admin`, then substitute your ownCloud username.

You can find your HTTP user in your HTTP configuration file. These are the default Apache HTTP user:group on Linux distros:

- Centos, Red Hat, Fedora: apache:apache
- Debian, Ubuntu, Linux Mint: www-data:www-data
- openSUSE: wwwrun:www

See *Using occ core commands* to learn more about using the `occ` command.

6.6.3 Resetting a User Password

The ownCloud login screen displays a **Wrong password. Reset it?** message after a user enters an incorrect password, and then ownCloud automatically resets their password. However, if you are using a read-only authentication backend such as LDAP or Active Directory, this will not work. In this case you may specify a custom URL in your `config.php` file to direct your user to a server than can handle an automatic reset:

```
'lost_password_link' => 'https://example.org/link/to/password/reset',
```

6.6.4 User Authentication with IMAP, SMB, and FTP

You may configure additional user backends in ownCloud's configuration file (`config/config.php`) using the following syntax:

```
<?php
"user_backends" => [
    0 => [
        "class"      => ...,
        "arguments" => [
            0 => ...
        ],
    ],
],
```

Note: A non-blocking or correctly configured SELinux setup is needed for these backends to work, if SELinux is enabled on your server.. Please refer to *the SELinux documentation* for further details.

Currently the `External user support app` (`user_external`), *which is not enabled by default*, provides three backends. These are:

- IMAP
- SMB
- FTP

See *Installing and Managing Apps* for more information.

IMAP

Provides authentication against IMAP servers.

Option	Value/Description
Class	OC_User_IMAP.
Arguments	A mailbox string as defined in the PHP documentation.
Dependency	PHP's IMAP extension. See <i>Manual Installation on Linux</i> for instructions on how to install it.

Example

```
<?php
"user_backends" => [
    0 => [
        "class"      => "OC_User_IMAP",
        "arguments" => [
            // The IMAP server to authenticate against
            '{imap.gmail.com:993/imap/ssl}',
            // The domain to send email from
            'example.com'
        ],
    ],
],
```

Warning: The second `arguments` parameter ensures that only users from that domain are allowed to login. When set, after a successful login, the domain will be stripped from the email address and the rest used as an ownCloud username. For example, if the email address is `guest.user@example.com`, then `guest.user` will be the username used by ownCloud.

SMB

Provides authentication against Samba servers.

Option	Value/Description
Class	OC_User_SMB.
Arguments	The samba server to authenticate against.
Dependency	PECL's <code>smbclient</code> extension or <code>smbclient</code> .

Example

```
<?php
"user_backends" => [
    0 => [
        "class"      => "OC_User_SMB",
        "arguments" => [
            0 => 'localhost'
        ],
    ],
],
```

FTP

Provides authentication against FTP servers.

Option	Value/Description
Class	OC_User_FTP.
Arguments	The FTP server to authenticate against.
Dependency	PHP's FTP extension. See <i>Manual Installation on Linux</i> for instructions on how to install it.

Example

```
<?php
"user_backends" => [
    0 => [
        "class"      => "OC_User_FTP",
        "arguments" => [
            0 => 'localhost'
        ],
    ],
],
```

6.6.5 User Authentication with LDAP

Warning: Please check both the advanced and expert configurations carefully before using in production

ownCloud ships with an LDAP application which allows LDAP users (including Active Directory) to appear in your ownCloud user listings. These users will authenticate to ownCloud with their LDAP credentials, so you don't have to create separate ownCloud user accounts for them. You will manage their ownCloud group memberships, quotas, and sharing permissions just like any other ownCloud user.

Note: The PHP LDAP module is required. It is supplied by php7.1-ldap on Debian/Ubuntu and php-ldap on CentOS/Red Hat/Fedora. Please check for the correct version, based on your installation of PHP.

The LDAP application supports:

- LDAP group support
- File sharing with ownCloud users and groups
- Access via WebDAV and ownCloud Desktop Client
- Versioning, external Storage and all other ownCloud features
- Seamless connectivity to Active Directory, with no extra configuration required
- Support for primary groups in Active Directory
- Auto-detection of LDAP attributes such as base DN, email, and the LDAP server port number
- Only read access to your LDAP (edit or delete of users on your LDAP is not supported)

Warning: The LDAP app is not compatible with the User backend using remote HTTP servers app. You cannot use both of them at the same time.

Note: A non-blocking or correctly configured SELinux setup is needed for the LDAP backend to work. Please refer to the *SELinux Configuration*.

Configuration

First, enable the LDAP user and group backend app on the Apps page in ownCloud. Then, go to your Admin page to configure it. The LDAP configuration panel has four tabs. A correctly completed first tab (“Server”) is mandatory to access the other tabs. A green indicator lights when the configuration is correct. Hover your cursor over the fields to see some pop-up tooltips.

Server Tab

Start with the Server tab. You may configure multiple servers if you have them. At a minimum you must supply the LDAP server’s hostname. If your server requires authentication, enter your credentials on this tab. ownCloud will then attempt to auto-detect the server’s port and base DN. The base DN and port are mandatory, so if ownCloud cannot detect them you must enter them manually.

LDAP

The screenshot displays the LDAP configuration panel. At the top, there are tabs for 'Server', 'Users', 'Login Attributes', 'Groups', 'Advanced', and 'Expert'. The 'Server' tab is selected, showing a list of servers with '1. Server' as the first entry. Below the list, there are input fields for 'Host', 'Port', 'User DN', and 'Password'. There are also buttons for 'Detect Port', 'Detect Base DN', and 'Test Base DN'. A checkbox for 'Manually enter LDAP filters (recommended for large directories)' is present. At the bottom, there is a 'Configuration incomplete' message and 'Continue' and 'Help' buttons.

Server configuration: Configure one or more LDAP servers. Click the “**Delete Configuration**” button to remove the active configuration.

Host: The host name or IP address of the LDAP server. It can also be an **ldaps://** URI. If you enter the port number, it speeds up server detection.

Examples:

- `directory.my-company.com`
- `ldaps://directory.my-company.com`
- `directory.my-company.com:9876`

Port: The port on which to connect to the LDAP server. The field is disabled in the beginning of a new configuration. If the LDAP server is running on a standard port, the port will be detected automatically. If you are using a non-standard port, ownCloud will attempt to detect it. If this fails you must enter the port number manually.

Example:

- `389`

User DN: The name as DN of a user who has permissions to do searches in the LDAP directory. Leave it empty for anonymous access. We recommend that you have a special LDAP system user for this.

Example:

- `uid=owncloudsystemuser,cn=sysusers,dc=my-company,dc=com`

Password: The password for the user given above. Empty for anonymous access.

Base DN: The base DN of LDAP, from where all users and groups can be reached. You may enter multiple base DN's, one per line. Base DN's for users and groups can be set in the Advanced tab. This field is mandatory. ownCloud attempts to determine the Base DN according to the provided User DN or the provided Host, and you must enter it manually if ownCloud does not detect it.

Example:

- `dc=my-company,dc=com`

User Filter

Use this to control which LDAP users are listed as ownCloud users on your ownCloud server. In order to control which LDAP users can login to your ownCloud server use the Login filter. Those LDAP users who have access but are not listed as users (if there are any) will be hidden users. You may bypass the form fields and enter a raw LDAP filter if you prefer.

Limit ownCloud access to users meeting these criteria:

Only these object classes:

The most common object classes for users are organizationalPerson, person, user, and inetOrgPerson. If you are not sure which object class to select, please consult your directory admin.

Only from these groups:

[Edit LDAP Query](#)

Configuration incomplete [Help](#)

Only those object classes: ownCloud will determine the object classes that are typically available for user objects in your LDAP. ownCloud will automatically select the object class that returns the highest amount of users. You may select multiple object classes.

Only from those groups: If your LDAP server supports the `memberof-overlay` in LDAP filters, you can define that only users from one or more certain groups are allowed to appear in user listings in ownCloud. By default, no value will be selected. You may select multiple groups.

Note: Group membership is configured by adding `memberUid`, `uniqueMember` or `member` attributes to an ldap group (see *Group Member association*) below. In order to efficiently look up the groups a user who is a member of the LDAP server must support a `memberof-overlay`. It allows using the virtual `memberOf` or `isMemberOf` attributes of an LDAP user in the user filter. If your LDAP server does not support the `memberof-overlay` in LDAP filters, the input field is disabled. Please contact your LDAP administrator.

- Active Directory uses `memberOf` and is enabled by default.
- OpenLDAP uses `memberOf`. [Reverse Group Membership Maintenance](#) needs to be enabled.
- Oracle uses `isMemberOf` and is enabled by default.

Edit raw filter instead: Clicking on this text toggles the filter mode and you can enter the raw LDAP filter directly.

Example

```
(&(objectClass=inetOrgPerson)(memberOf=cn=owncloudusers,ou=groups,dc=example,dc=com))
```

x users found: This is an indicator that tells you approximately how many users will be listed in ownCloud. The number updates automatically after any changes.

Active Directory offers “Recursive retrieval of all AD group memberships of a user”. This means essentially that you would be able to search the group you enter and all the other child groups from this groups for users.

Enter this filter to access this feature for a single group:

```
(&(objectClass=user)(memberOf:1.2.840.113556.1.4.1941:=CN=<groupname>,DC=example,DC=com))
```

Enter your group name instead of the “<groupname>” placeholder.

If you want to search multiple groups with this feature, adjust your filter like this:

```
(&
  (objectClass=user)
  (
    (memberOf:1.2.840.113556.1.4.1941:=CN=<groupname1>,CN=Users,DC=example,DC=com)
    (memberOf:1.2.840.113556.1.4.1941:=CN=<groupname2>,CN=Users,DC=example,DC=com)
  )
)
```

You can add as many groups to recurse by using the format: `(| (m1) (m2) (m3))`

Description from Microsoft:

The string `1.2.840.113556.1.4.1941` specifies `LDAP_MATCHING_RULE_IN_CHAIN`. This applies only to DN attributes. This is an extended match operator that walks the chain of ancestry in objects all the way to the root until it finds a match. **This reveals group nesting.** It is available only on domain controllers with Windows Server 2003 SP2 or Windows Server 2008 (or above).

For more information, see the following from Technet:

- <http://social.technet.microsoft.com/wiki/contents/articles/5392.active-directory-ldap-syntax-filters.aspx>
- <http://blogs.technet.com/b/heyscriptingguy/archive/2014/11/25/active-directory-week-explore-group-membership-with-powershell.aspx>

Login Filter

The settings in the Login Filter tab determine which LDAP users can log in to your ownCloud system and which attribute or attributes the provided login name is matched against (e.g., LDAP/AD username, email address). You may select multiple user details. You may bypass the form fields and enter a raw LDAP filter if you prefer. You may override your User Filter settings on the User Filter tab by using a raw LDAP filter.

LDAP Username: If this value is checked, the login value will be compared to the username in the LDAP directory. The corresponding attribute, usually `uid` or `samaccountname` will be detected automatically by ownCloud.

LDAP Email Address: If this value is checked, the login value will be compared to an email address in the LDAP directory; specifically, the `mailPrimaryAddress` and `mail` attributes.

Other Attributes: This multi-select box allows you to select other attributes for the comparison. The list is generated automatically from the user object attributes in your LDAP server.

Edit raw filter instead: Clicking on this text toggles the filter mode and you can enter the raw LDAP filter directly. The `%uid` placeholder is replaced with the login name entered by the user upon login.

Examples:

- only username:

```
(& (objectClass=inetOrgPerson) (memberOf=cn=owncloudusers,ou=groups,dc=example,dc=com) (uid=%uid))
```

- username or email address:

```
((& (objectClass=inetOrgPerson) (memberOf=cn=owncloudusers,ou=groups,dc=example,dc=com) (| (uid=
```

Group Filter

By default, no LDAP groups will be available in ownCloud. The settings in the group filter tab determine which groups will be available in ownCloud. You may also elect to enter a raw LDAP filter instead.

Only those object classes: ownCloud will determine the object classes that are typically available for group objects in your LDAP server. ownCloud will only list object classes that return at least one group object. You can select multiple object classes. A typical object class is `group`, or `posixGroup`.

Only from those groups: ownCloud will generate a list of available groups found in your LDAP server. From these groups, you can select the group or groups that get access to your ownCloud server.

Edit raw filter instead: Clicking on this text toggles the filter mode and you can enter the raw LDAP filter directly.

Example:

- `objectClass=group`
- `objectClass=posixGroup`

y groups found: This tells you approximately how many groups will be available in ownCloud. The number updates automatically after any change.

Advanced Settings

The LDAP Advanced Setting section contains options that are not needed for a working connection. This provides controls to disable the current configuration, configure replica hosts, and various performance-enhancing options. The Advanced Settings are structured into three parts:

- Connection Settings
- Directory Settings
- Special Attributes

Connection Settings

Configuration Active: Enables or Disables the current configuration. By default, it is turned off. When ownCloud makes a successful test connection it is automatically turned on.

LDAP

Server	Users	Login Attributes	Groups	Advanced	Expert
▼ Connection Settings					
Configuration					
Active <input checked="" type="checkbox"/>					
Backup (Replica) Host <input type="text"/>					
Backup (Replica) Port <input type="text"/>					
Disable Main Server <input type="checkbox"/>					
Turn off SSL certificate validation. <input type="checkbox"/>					
Cache Time-To-Live <input type="text" value="600"/>					
▶ Directory Settings					
▶ Special Attributes					
Test Configuration <i>i</i> Help					

Backup (Replica) Host: If you have a backup LDAP server, enter the connection settings here. ownCloud will then automatically connect to the backup when the main server cannot be reached. The backup server must be a replica of the main server so that the object UUIDs match.

Example:

- `directory2.my-company.com`

Backup (Replica) Port: The connection port of the backup LDAP server. If no port is given, but only a host, then the main port (as specified above) will be used.

Example:

- `389`

Disable Main Server: You can manually override the main server and make ownCloud only connect to the **backup server**. This is useful for planned downtimes for example **Upgrades or Updates of the Main Server**. **Backup Server Handling** When ownCloud is not able to contact the main LDAP server, ownCloud assumes it is offline and will not try to connect again for the time specified in” **Cache Time-To-Live**”.

Turn off SSL certificate validation: Turns off SSL certificate checking. Use it for testing only!

Cache Time-To-Live: A cache is introduced to avoid unnecessary LDAP traffic, for example caching usernames so they don’t have to be looked up for every page, and speeding up loading of the Users page. Saving the configuration empties the cache. The time is given in seconds.

Note that almost every PHP request requires a new connection to the LDAP server. If you require fresh PHP requests we recommend defining a minimum lifetime of 15s or so, rather than completely eliminating the cache.

Examples:

- Ten minutes: `600`
- One hour: `3600`

See the Caching section below for detailed information on how the cache operates.

Directory Settings

User Display Name Field: The attribute that should be used as display name in ownCloud.

Examples:

- `displayName`
- `givenName`
- `sn`

2nd User Display Name Field: An optional second attribute displayed in brackets after the display name, for example using the `mail` attribute displays as `Molly Foo (molly@example.com)`.

Examples:

- `mail`
- `userPrincipalName`
- `sAMAccountName`

Base User Tree: The base DN of LDAP, from where all users can be reached. This must be a complete DN, regardless of what you have entered for your Base DN in the Basic setting. You can specify multiple base trees, one on each line.

Examples:

Server	Users	Login Attributes	Groups	Advanced	Expert
<p>▸ Connection Settings</p> <p>▾ Directory Settings</p> <p>User Display Name Field <input type="text" value="displayname"/></p> <p>2nd User Display Name Field <input type="text"/></p> <p>Base User Tree <input type="text" value="dc=example,dc=com"/> Base User Tree</p> <p>User Search Attributes <input type="text" value="Optional; one attribute per line"/></p> <p>Group Display Name Field <input type="text" value="cn"/></p> <p>Base Group Tree <input type="text"/></p> <p>Group Search Attributes <input type="text" value="Optional; one attribute per line"/></p> <p>Group-Member association <input type="text" value="uniqueMember"/></p> <p>Dynamic Group Member URL <input type="text"/></p> <p>Nested Groups <input type="checkbox"/></p> <p>Paging chunksize <input type="text" value="500"/></p> <p>▸ Special Attributes</p> <p>Test Configuration i Help</p>					

- `cn=programmers,dc=my-company,dc=com`
- `cn=designers,dc=my-company,dc=com`

User Search Attributes: These attributes are used when searches for users are performed, for example in the share dialogue. The user display name attribute is the default. You may list multiple attributes, one per line.

If an attribute is not available on a user object, the user will not be listed, and will be unable to login. This also affects the display name attribute. If you override the default you must specify the display name attribute here.

Examples:

- `displayName`
- `mail`

Group Display Name Field: The attribute that should be used as ownCloud group name. ownCloud allows a limited set of characters (`a-zA-Z0-9.-_@`). Once a group name is assigned it cannot be changed.

Examples:

- `cn`

Base Group Tree: The base DN of LDAP, from where all groups can be reached. This must be a complete DN, regardless of what you have entered for your Base DN in the Basic setting. You can specify multiple base trees, one in each line.

Examples:

- `cn=barcelona,dc=my-company,dc=com`
- `cn=madrid,dc=my-company,dc=com`

Group Search Attributes: These attributes are used when a search for groups is done, for example in the share dialogue. By default the group display name attribute as specified above is used. Multiple attributes can be given, one in each line.

If you override the default, the group display name attribute will not be taken into account, unless you specify it as well.

Examples:

- `cn`
- `description`

Group Member association: The attribute that is used to indicate group memberships, i.e., the attribute used by LDAP groups to refer to their users. ownCloud detects the value automatically. You should only change it if you have a very valid reason and know what you are doing.

Examples:

- `member` with FDN for objectclass `groupOfNames` groups
- `memberUid` with RDN for objectclass `posixGroup` groups
- `uniqueMember` with FDN for objectclass `groupOfUniqueNames` groups

Note: The Group Member association is used to efficiently query users of a certain group, eg., on the `userManagement` page or when resolving all members of a group share.

Dynamic Group Member URL The LDAP attribute that on group objects contains an LDAP search URL that determines what objects belong to the group. An empty setting disables dynamic group membership functionality. See [Configuring Dynamic Groups](#) for more details.

Nested Groups: This makes the LDAP connector aware that groups could be stored inside existing group records. By default a group will only contain users, so enabling this option isn't necessary. However, if groups are contained inside groups, and this option is not enabled, any groups contained within other groups will be ignored and not returned in search results.

Paging Chunk Size: This sets the maximum number of records able to be returned in a response when ownCloud requests data from LDAP. If this value is greater than the limit of the underlying LDAP server (such as 3000 for Microsoft Active Directory) the LDAP server will reject the request and the search request will fail. Given that, it is important to set the requested chunk size to a value no larger than that which the underlying LDAP server supports.

Special Attributes

The screenshot shows the 'Special Attributes' configuration page. It features a navigation bar with tabs: Server, Users, Login Attributes, Groups, Advanced, and Expert. The 'Groups' tab is selected. Below the navigation bar, there are three expandable sections: 'Connection Settings', 'Directory Settings', and 'Special Attributes'. The 'Special Attributes' section is expanded, revealing four input fields: 'Quota Field', 'Quota Default', 'Email Field', and 'User Home Folder Naming Rule'. At the bottom of the page, there are two buttons: 'Test Configuration' and 'Help'.

Quota Field: The name of the LDAP attribute to retrieve the user quota limit from, e.g., `ownCloudQuota`. *Note:* any quota set in LDAP overrides quotas set in ownCloud's user management page.

Quota Default: Override ownCloud's default quota *for LDAP users* who do not have a quota set in the Quota Field, e.g., 15 GB.

Please bear in mind the following, when using these fields to assign user quota limits. It should help to alleviate any, potential, confusion.

1. After installation ownCloud uses an unlimited quota by default.
2. Administrators can modify this value, at any time, in the user management page.
3. However, when an LDAP quota is set it will override any values set in ownCloud.
4. If an LDAP per/attribute quota is set, it will override the LDAP Quota Default value.

Note:

Administrators are not allowed to modify the user quota limit in the user management page when steps 3 or 4 are in effect. At this point, updates are only possible via LDAP.

See the [LDAP Schema for OwnCloud Quota](#)

Email Field: Set the user’s email from an LDAP attribute, e.g., `mail`. Leave it empty for default behavior.

User Home Folder Naming Rule: By default, the ownCloud server creates the user directory in your ownCloud data directory and gives it the ownCloud username, e.g., `/var/www/owncloud/data/5a9df029-322d-4676-9c80-9fc8892c4e4b`, if your data directory is set to `/var/www/owncloud/data`.

It is possible to override this setting and name it after an LDAP attribute value, e.g., `attr:cn`. The attribute can return either an absolute path, e.g., `/mnt/storage43/alice`, or a relative path which must not begin with a `/`, e.g., `CloudUsers/CookieMonster`. This relative path is then created inside the data directory (e.g., `/var/www/owncloud/data/CloudUsers/CookieMonster`).

Since ownCloud 8.0.10 and up the home folder rule is enforced. This means that once you set a home folder naming rule (get a home folder from an LDAP attribute), it must be available for all users. If it isn’t available for a user, then that user will not be able to login. Also, the filesystem will not be set up for that user, so their file shares will not be available to other users. For older versions you may enforce the home folder rule with the `occ` command, like this example on Ubuntu:

```
sudo -u www-data php occ config:app:set user_ldap enforce_home_folder_naming_rule --value=1
```

Since ownCloud 10.0 the home folder naming rule is only applied when first provisioning the user. This prevents data loss due to re-provisioning the users home folder in case of unintentional changes in LDAP.

Expert Settings

Warning: In the Expert Settings fundamental behavior can be adjusted to your needs. The configuration should be well-tested before starting production use.

Internal Username: The internal username is the identifier in ownCloud for LDAP users. By default it will be created from the UUID attribute. The UUID attribute ensures that the username is unique, and that characters do not need to be converted. Only these characters are allowed: `[\a-\zA-\z0-\9_.\@-]`. Other characters are replaced with their ASCII equivalents, or are simply omitted.

The LDAP backend ensures that there are no duplicate internal usernames in ownCloud, i.e., that it is checking all other activated user backends (including local ownCloud users). On collisions a random number (between 1000 and 9999) will be attached to the retrieved value. For example, if “alice” exists, the next username may be “alice_1337”.

The internal username is the default name for the user home folder in ownCloud. It is also a part of remote URLs, for instance for all *DAV services.

You can override all of this with the Internal Username setting. Leave it empty for default behavior. Changes will affect only newly mapped LDAP users.

Examples:

- `uid`

Override UUID detection By default, ownCloud auto-detects the UUID attribute. The UUID attribute is used to uniquely identify LDAP users and groups. The internal username will be created based on the UUID, if not specified otherwise.

You can override the setting and pass an attribute of your choice. You must make sure that the attribute of your choice can be fetched for both users and groups and it is unique. Leave it empty for default behavior. Changes will have effect only on newly mapped LDAP users and groups.

Server	Users	Login Attributes	Groups	Advanced	Expert
--------	-------	------------------	--------	----------	--------

Internal Username

By default the internal username will be created from the UUID attribute. It makes sure that the username is unique and characters do not need to be converted. The internal username has the restriction that only these characters are allowed: [a-zA-Z0-9_@-]. Other characters are replaced with their ASCII correspondence or simply omitted. On collisions a number will be added/increased. The internal username is used to identify a user internally. It is also the default name for the user home folder. It is also a part of remote URLs, for instance for all *DAV services. With this setting, the default behavior can be overridden. To achieve a similar behavior as before ownCloud 5 enter the user display name attribute in the following field. Leave it empty for default behavior. Changes will have effect only on newly mapped (added) LDAP users.

Internal Username

Attribute:

Override UUID detection

By default, the UUID attribute is automatically detected. The UUID attribute is used to doubtlessly identify LDAP users and groups. Also, the internal username will be created based on the UUID, if not specified otherwise above. You can override the setting and pass an attribute of your choice. You must make sure that the attribute of your choice can be fetched for both users and groups and it is unique. Leave it empty for default behavior. Changes will have effect only on newly mapped (added) LDAP users and groups.

UUID Attribute for

Users:

UUID Attribute for

Groups:

Username-LDAP User Mapping

Use names are used to store and assign (meta) data. In order to precisely identify and recognize users, each LDAP user will have an internal username. This requires a mapping from username to LDAP user. The created username is mapped to the UUID of the LDAP user. Additionally the DN is cached as well to reduce LDAP interaction, but it is not used for identification. If the DN changes, the changes will be found. The internal username is used all over. Clearing the mappings will have leftovers everywhere. Clearing the mappings is not configuration sensitive, it affects all LDAP configurations! Never clear the mappings in a production environment, only in a testing or experimental stage.

It also will have effect when a user's or group's DN changes and an old UUID was cached, which will result in a new user. Because of this, the setting should be applied before putting ownCloud in production use and clearing the bindings (see the [User and Group Mapping](#) section below).

Examples:

- `cn`

Username-LDAP User Mapping ownCloud uses usernames as keys to store and assign data. In order to precisely identify and recognize users, each LDAP user will have a internal username in ownCloud. This requires a mapping from ownCloud username to LDAP user. The created username is mapped to the UUID of the LDAP user. Additionally the DN is cached as well to reduce LDAP interaction, but it is not used for identification. If the DN changes, the change will be detected by ownCloud by checking the UUID value.

The same is valid for groups. The internal ownCloud name is used all over in ownCloud. Clearing the Mappings will have leftovers everywhere. Never clear the mappings in a production environment, but only in a testing or experimental server.

Clearing the mappings is not configuration sensitive, it affects all LDAP configurations!

Testing the configuration

The “**Test Configuration**” button checks the values as currently given in the input fields. You do not need to save before testing. By clicking on the button, ownCloud will try to bind to the ownCloud server using the settings currently given in the input fields. If the binding fails you'll see a yellow banner with the error message:

“The configuration is invalid. Please have a look at the logs for further details.”

When the configuration test reports success, save your settings and check if the users and groups are fetched correctly on the [Users](#) page.

Syncing Users

While users who match the login and user filters can log in, only synced users will be found in the sharing dialog. Whenever users log in their display name, email, quota, avatar and search attributes will be synced to ownCloud. If you want to keep the metadata up to date you can set up a cron job, using *the `occ` command*. Versions of ownCloud before 10.0 imported all users when the users page was loaded, but this is no longer the case.

We recommend *creating a Cron job*, to automate regularly syncing LDAP users with your ownCloud database.

How Often Should the Job Run?

This depends on the amount of users and speed of the update, but we recommend *at least* once per day. You can run it more frequently, but doing so may generate too much load on the server.

ownCloud Avatar integration

ownCloud supports user profile pictures, which are also called avatars. If a user has a photo stored in the `jpegPhoto` or `thumbnailPhoto` attribute on your LDAP server, it will be used as their avatar. In this case the user cannot alter their avatar (on their [Personal](#) page) as it must be changed in LDAP. `jpegPhoto` is preferred over `thumbnailPhoto`.

If the `jpegPhoto` or `thumbnailPhoto` attribute is not set or empty, then users can upload and manage their avatars on their ownCloud [Personal](#) pages. Avatars managed in ownCloud are not stored in LDAP.

Profile picture



Your avatar is provided by your original account.

The `jpegPhoto` or `thumbnailPhoto` attribute is fetched once a day to make sure the current photo from LDAP is used in ownCloud. LDAP avatars override ownCloud avatars, and when an LDAP avatar is deleted then the most recent ownCloud avatar replaces it.

Photos served from LDAP are automatically cropped and resized in ownCloud. This affects only the presentation, and the original image is not changed.

Troubleshooting, Tips and Tricks

SSL Certificate Verification (LDAPS, TLS)

A common mistake with SSL certificates is that they may not be known to PHP. If you have trouble with certificate validation make sure that

- You have the certificate of the server installed on the ownCloud server
- The certificate is announced in the system's LDAP configuration file, usually `/etc/ldap/ldap.conf`.
- Using LDAPS, also make sure that the port is correctly configured (by default 636)
- If you get the error "Lost connection to LDAP server" or "**No connection to LDAP server**" double check the connection parameters and try connecting to LDAP with tools like `ldapsearch`. If using ldaps or TLS make sure the certificate is readable by the user that is used to serve ownCloud.

Microsoft Active Directory

Compared to earlier ownCloud versions, no further tweaks need to be done to make ownCloud work with Active Directory. ownCloud will automatically find the correct configuration in the set-up process.

memberOf / Read MemberOf permissions

If you want to use `memberOf` within your filter you might need to give your querying user the permissions to use it. For Microsoft Active Directory this is described [here](#).

Duplicating Server Configurations

In case you have a working configuration and want to create a similar one or "snapshot" configurations before modifying them you can do the following:

1. Go to the “**Server**” tab
2. On “**Server Configuration**” choose “**Add Server Configuration**”
3. Answer the question “**Take over settings from recent server configuration?**” with “**yes**”.
4. (optional) Switch to “**Advanced**” tab and uncheck “**Configuration Active**” in the “**Connection Settings**”, so the new configuration is not used on Save
5. Click on “**Save**”

Now you can modify and enable the configuration.

Performance tips

Caching

Using caching to speed up lookups. See *Memory Caching*. The ownCloud cache is populated on demand, and remains populated until the “**Cache Time-To-Live**” for each unique request expires. User logins are not cached, so if you need to improve login times set up a slave LDAP server to share the load.

You can adjust the “**Cache Time-To-Live**” value to balance performance and freshness of LDAP data. All LDAP requests will be cached for 10 minutes by default, and you can alter this with the “**Cache Time-To-Live**” setting. The cache answers each request that is identical to a previous request, within the time-to-live of the original request, rather than hitting the LDAP server.

The “**Cache Time-To-Live**” is related to each single request. After a cache entry expires there is no automatic trigger for re-populating the information, as the cache is populated only by new requests, for example by opening the User administration page, or searching in a sharing dialog.

There is one trigger which is automatically triggered by a certain background job which keeps the `user-group-mappings` up-to-date, and always in cache.

Under normal circumstances, all users are never loaded at the same time. Typically the loading of users happens while page results are generated, in steps of 30 until the limit is reached or no results are left. For this to work on an oC-Server and LDAP-Server, “**Paged Results**” must be supported, which assumes PHP ≥ 5.6 .

ownCloud remembers which user belongs to which LDAP-configuration. That means each request will always be directed to the right server unless a user is defunct, for example due to a server migration or unreachable server. In this case the other servers will also receive the request.

LDAP indexing

Turn on indexing. Deciding which attributes to index depends on your configuration and which LDAP server you are using. See *The openLDAP tuning guide* for openLDAP, and *How to Index an Attribute in Active Directory* for Active Directory.

Use precise base DN's

The more precise your base DN, the faster LDAP can search because it has fewer branches to search.

Use precise filters

Use good filters to further define the scope of LDAP searches, and to intelligently direct your server where to search, rather than forcing it to perform needlessly-general searches.

ownCloud LDAP Internals

Some parts of how the LDAP backend works are described here.

User and Group Mapping

In ownCloud the user or group name is used to have all relevant information in the database assigned. To work reliably a permanent internal user name and group name is created and mapped to the LDAP DN and UUID. If the DN changes in LDAP it will be detected, and there will be no conflicts.

Those mappings are done in the database table `ldap_user_mapping` and `ldap_group_mapping`. The user name is also used for the user's folder (except if something else is specified in *User Home Folder Naming Rule*), which contains files and meta data.

As of ownCloud 5 the internal user name and a visible display name are separated. This is not the case for group names, yet, i.e., a group name cannot be altered.

That means that your LDAP configuration should be good and ready before putting it into production. The mapping tables are filled early, but as long as you are testing, you can empty the tables any time. Do not do this in production.

Handling with Backup Server

When ownCloud is not able to contact the main LDAP server, ownCloud assumes it is offline and will not try to connect again for the time specified in "Cache Time-To-Live". If you have a backup server configured ownCloud will connect to it instead. When you have scheduled downtime, check "Disable Main Server" to avoid unnecessary connection attempts.

6.6.6 User Provisioning API

The Provisioning API application enables a set of APIs that external systems can use to:

- Create, edit, delete and query user attributes
- Query, set and remove groups
- Set quota and query total storage used in ownCloud
- Group admin users can also query ownCloud and perform the same functions as an admin for groups they manage.
- Query for active ownCloud applications, application info, and to enable or disable an app.

HTTP requests can be used via a [Basic Auth header](#) to perform any of the functions listed above. The Provisioning API app is enabled by default. The base URL for all calls to the share API is `owncloud_base_url/ocs/v1.php/cloud`.

Instruction Set For Users

Add User

Create a new user on the ownCloud server. Authentication is done by sending a basic HTTP authentication header.

Syntax	Request Path	Method	Content Type
	ocs/v1.php/cloud/users	POST	text/plain

Argument	Type	Description
userid	string	The required username for the new user
password	string	The required password for the new user
groups	array	Groups to add the user to [optional]

Status Codes

- 100 - successful
- 101 - invalid input data
- 102 - username already exists
- 103 - unknown error occurred whilst adding the user
- 104 - group does not exist

Example

```
# Creates the user ``Frank`` with password ``frankspassword``
curl -X POST http://admin:secret@example.com/ocs/v1.php/cloud/users \
  -d userid="Frank" \
  -d password="frankspassword"
```

```
# Creates the user ``Frank`` with password ``frankspassword`` and adds him to the ``finance`` and ``r
curl -X POST http://admin:secret@example.com/ocs/v1.php/cloud/users \
  -d userid="Frank" \
  -d password="frankspassword" \
  -d groups[]="finance" -d groups[]="management"
```

XML Output

```
<?xml version="1.0"?>
<ocs>
  <meta>
    <status>ok</status>
    <statuscode>100</statuscode>
    <message/>
  </meta>
  <data/>
</ocs>
```

Get Users

Retrieves a list of users from the ownCloud server. Authentication is done by sending a Basic HTTP Authorization header.

Request Path	Method	Content Type
ocs/v1.php/cloud/users	GET	text/plain

Argument	Type	Description
search	string	optional search string
limit	int	optional limit value
offset	int	optional offset value

Status Codes

- 100 - successful

Example

```
# Returns list of users matching the search string.
curl http://admin:secret@example.com/ocs/v1.php/cloud/users?search=Frank
```

XML Output

```
<?xml version="1.0"?>
<ocs>
  <meta>
    <statusCode>100</statusCode>
    <status>ok</status>
  </meta>
  <data>
    <users>
      <element>Frank</element>
    </users>
  </data>
</ocs>
```

Get User

Retrieves information about a single user. Authentication is done by sending a Basic HTTP Authorization header.

Request Path	Method	Content Type
Syntax: ocs/v1.php/cloud/users/{userid}	GET	text/plain

Argument	Type	Description
userid	int	Id of the user to retrieve

Status Codes

- 100 - successful

Example

```
# Returns information on the user ``Frank``
curl http://admin:secret@example.com/ocs/v1.php/cloud/users/Frank
```

XML Output

```
<?xml version="1.0"?>
<ocs>
  <meta>
    <status>ok</status>
    <statusCode>100</statusCode>
    <message/>
  </meta>
  <data>
    <enabled>true</enabled>
    <quota>
      <free>81919008768</free>
    </quota>
  </data>
</ocs>
```

```
<used>5809166</used>
<total>81924817934</total>
<relative>0.01</relative>
</quota>
<email>user@example.com</email>
<displayname>Frank</displayname>
<home>/mnt/data/files/Frank</home>
<two_factor_auth_enabled>>false</two_factor_auth_enabled>
</data>
</ocs>
```

Edit User

Edits attributes related to a user. Users are able to edit *email*, *displayname* and *password*; admins can also edit the quota value. Authentication is done by sending a Basic HTTP Authorization header.

Request Path	Method	Content Type
ocs/v1.php/cloud/users/{userid}	PUT	text/plain

Argument	Type	Description
key	string	the field to edit (email, quota, display, password)
value	mixed	the new value for the field

Status Codes

- 100 - successful
- 101 - user not found
- 102 - invalid input data

Examples

```
Updates the email address for the user ``Frank``
curl -X PUT http://admin:secret@example.com/ocs/v1.php/cloud/users/Frank \
  -d key="email" \
  -d value="franksnewemail@example.org"
```

```
Updates the quota for the user ``Frank``
curl -X PUT http://admin:secret@example.com/ocs/v1.php/cloud/users/Frank \
  -d key="quota" \
  -d value="100MB"
```

XML Output

```
<?xml version="1.0"?>
<ocs>
  <meta>
    <statuscode>100</statuscode>
    <status>ok</status>
  </meta>
</data/>
</ocs>
```

Enable User

Enables a user on the ownCloud server. Authentication is done by sending a Basic HTTP Authorization header.

Request Path	Method	Content Type
ocs/v1.php/cloud/users/{userid}/enable	PUT	text/plain

Argument	Type	Description
userid	string	The id of the user to enable

Status Codes

- 100 - successful
- 101 - failure

Example

```
# Enable the user ``Frank``
curl -X PUT http://admin:secret@example.com/ocs/v1.php/cloud/users/Frank/enable
```

XML Output

```
<?xml version="1.0"?>
<ocs>
  <meta>
    <status>ok</status>
    <statuscode>100</statuscode>
    <message/>
  </meta>
  <data/>
</ocs>
```

Disable User

Disables a user on the ownCloud server. Authentication is done by sending a Basic HTTP Authorization header.

Request Path	Method	Content Type
ocs/v1.php/cloud/users/{userid}/disable	PUT	text/plain

Argument	Type	Description
userid	string	The id of the user to disable

Status Codes

- 100 - successful
- 101 - failure

Example

```
# Disable the user ``Frank``
curl -X PUT http://admin:secret@example.com/ocs/v1.php/cloud/users/Frank/disable
```

XML Output

```
<?xml version="1.0"?>
<ocs>
  <meta>
    <status>ok</status>
    <statusCode>100</statusCode>
    <message/>
  </meta>
  <data/>
</ocs>
```

Delete User

Deletes a user from the ownCloud server. Authentication is done by sending a Basic HTTP Authorization header.

Request Path	Method	Content Type
ocs/v1.php/cloud/users/{userid}	DELETE	text/plain

Argument	Type	Description
userid	string	The id of the user to delete

Status Codes

- 100 - successful
- 101 - failure

Example

```
# Deletes the user ``Frank``
curl -X DELETE http://admin:secret@example.com/ocs/v1.php/cloud/users/Frank
```

XML Output

```
<?xml version="1.0"?>
<ocs>
  <meta>
    <statusCode>100</statusCode>
    <status>ok</status>
  </meta>
  <data/>
</ocs>
```

Get Groups

Retrieves a list of groups the specified user is a member of. Authentication is done by sending a Basic HTTP Authorization header.

Request Path	Method	Content Type
ocs/v1.php/cloud/users/{userid}/groups	GET	text/plain

Argument	Type	Description
userid	string	The id of the user to retrieve groups for

Status Codes

- 100 - successful

Example

```
# Retrieves a list of groups of which ``Frank`` is a member
curl http://admin:secret@example.com/ocs/v1.php/cloud/users/Frank/groups
```

XML Output

```
<?xml version="1.0"?>
<ocs>
  <meta>
    <statuscode>100</statuscode>
    <status>ok</status>
  </meta>
  <data>
    <groups>
      <element>admin</element>
      <element>group1</element>
    </groups>
  </data>
</ocs>
```

Add To Group

Adds the specified user to the specified group. Authentication is done by sending a Basic HTTP Authorization header.

Request Path	Method	Content Type
ocs/v1.php/cloud/users/{userid}/groups	POST	text/plain

Argument	Type	Description
userid	string	The id of the user to retrieve groups for
groupid	string	The group to add the user to

Status Codes

- 100 - successful
- 101 - no group specified
- 102 - group does not exist
- 103 - user does not exist
- 104 - insufficient privileges
- 105 - failed to add user to group

Example

```
# Adds the user ``Frank`` to the group ``newgroup``
curl -X POST http://admin:secret@example.com/ocs/v1.php/cloud/users/Frank/groups -d groupid="newgroup"
```

XML Output

```
<?xml version="1.0"?>
<ocs>
  <meta>
    <statusCode>100</statusCode>
    <status>ok</status>
  </meta>
  <data/>
</ocs>
```

Remove From Group

Removes the specified user from the specified group. Authentication is done by sending a Basic HTTP Authorization header.

Request Path	Method	Content Type
ocs/v1.php/cloud/users/{userid}/groups	DELETE	text/plain

Argument	Type	Description
userid	string	The id of the user to retrieve groups for
groupid	string	The group to remove the user from

Status Codes

- 100 - successful
- 101 - no group specified
- 102 - group does not exist
- 103 - user does not exist
- 104 - insufficient privileges
- 105 - failed to remove user from group

Example

```
# Removes the user ``Frank`` from the group ``newgroup``
curl -X DELETE http://admin:secret@example.com/ocs/v1.php/cloud/users/Frank/groups -d groupid="newgroup"
```

XML Output

```
<?xml version="1.0"?>
<ocs>
  <meta>
    <statusCode>100</statusCode>
    <status>ok</status>
  </meta>
  <data/>
</ocs>
```

Create Sub-admin

Makes a user the sub-admin of a group. Authentication is done by sending a Basic HTTP Authorization header.

Request Path	Method	Content Type
ocs/v1.php/cloud/users/{userid}/subadmins	POST	text/plain

Argument	Type	Description
userid	string	The id of the user to be made a sub-admin
groupid	string	the group of which to make the user a sub-admin

Status Codes

- 100 - successful
- 101 - user does not exist
- 102 - group does not exist
- 103 - unknown failure

Example

```
# Makes the user ``Frank`` a sub-admin of the ``group`` group
curl -X POST https://admin:secret@example.com/ocs/v1.php/cloud/users/Frank/subadmins -d groupid="group"
```

XML Output

```
<?xml version="1.0"?>
<ocs>
  <meta>
    <statusCode>100</statusCode>
    <status>ok</status>
  </meta>
  <data/>
</ocs>
```

Remove Sub-admin

Removes the sub-admin rights for the user specified from the group specified. Authentication is done by sending a Basic HTTP Authorization header.

Request Path	Method	Content Type
ocs/v1.php/cloud/users/{userid}/subadmins	DELETE	text/plain

Argument	Type	Description
userid	string	the id of the user to retrieve groups for
groupid	string	the group from which to remove the user's sub-admin rights

Status Codes

- 100 - successful
- 101 - user does not exist
- 102 - user is not a sub-admin of the group / group does not exist
- 103 - unknown failure

Example

```
# Removes ``Frank's`` sub-admin rights from the ``oldgroup`` group
curl -X DELETE https://admin:secret@example.com/ocs/v1.php/cloud/users/Frank/subadmins --d groupid="o
```

XML Output

```
<?xml version="1.0"?>
<ocs>
  <meta>
    <statusCode>100</statusCode>
    <status>ok</status>
  </meta>
  <data/>
</ocs>
```

Get Sub-admin Groups

Returns the groups in which the user is a sub-admin. Authentication is done by sending a Basic HTTP Authorization header.

Request Path	Method	Content Type
ocs/v1.php/cloud/users/{userid}/subadmins	GET	text/plain

Argument	Type	Description
userid	string	The id of the user to retrieve sub-admin groups for

Status Codes

- 100 - successful
- 101 - user does not exist
- 102 - unknown failure

Example

```
# Returns the groups of which ``Frank`` is a sub-admin
curl -X GET https://admin:secret@example.com/ocs/v1.php/cloud/users/Frank/subadmins
```

XML Output

```
<?xml version="1.0"?>
<ocs>
  <meta>
    <status>ok</status>
    <statusCode>100</statusCode>
    <message/>
  </meta>
  <data>
    <element>testgroup</element>
  </data>
</ocs>
```

Instruction Set For Groups

Get Groups

Retrieves a list of groups from the ownCloud server. Authentication is done by sending a Basic HTTP Authorization header.

Request Path	Method	Content Type
ocs/v1.php/cloud/groups	GET	text/plain

Argument	Type	Description
search	string	optional search string
limit	int	optional limit value
offset	int	optional offset value

Status Codes

- 100 - successful

Example

```
# Returns list of groups matching the search string.
curl http://admin:secret@example.com/ocs/v1.php/cloud/groups?search=admin
```

XML Output

```
<?xml version="1.0"?>
<ocs>
  <meta>
    <statusCode>100</statusCode>
    <status>ok</status>
  </meta>
  <data>
    <groups>
      <element>admin</element>
    </groups>
  </data>
</ocs>
```

Add Group

Adds a new group. Authentication is done by sending a Basic HTTP Authorization header.

Request Path	Method	Content Type
ocs/v1.php/cloud/groups	POST	text/plain

Argument	Type	Description
groupid	string	the new group's name

Status Codes

- 100 - successful
- 101 - invalid input data
- 102 - group already exists

- 103 - failed to add the group

Example

```
# Adds a new group called ``newgroup``
curl -X POST http://admin:secret@example.com/ocs/v1.php/cloud/groups -d groupid="newgroup"
```

XML Output

```
<?xml version="1.0"?>
<ocs>
  <meta>
    <statuscode>100</statuscode>
    <status>ok</status>
  </meta>
  <data/>
</ocs>
```

Get Group

Retrieves a list of group members. Authentication is done by sending a Basic HTTP Authorization header.

Request Path	Method	Content Type
ocs/v1.php/cloud/groups/{groupid}	GET	text/plain

Argument	Type	Description
groupid	string	The group id to return members from

Status Codes

- 100 - successful

Example

```
# Returns a list of users in the ``admin`` group
curl http://admin:secret@example.com/ocs/v1.php/cloud/groups/admin
```

XML Output

```
<?xml version="1.0"?>
<ocs>
  <meta>
    <statuscode>100</statuscode>
    <status>ok</status>
  </meta>
  <data>
    <users>
      <element>Frank</element>
    </users>
  </data>
</ocs>
```

Get Sub-admins

Returns sub-admins of the group. Authentication is done by sending a Basic HTTP Authorization header.

Request Path	Method	Content Type
ocs/v1.php/cloud/groups/{groupid}/subadmins	GET	text/plain

Argument	Type	Description
groupid	string	The group id to get sub-admins for

Status Codes

- 100 - successful
- 101 - group does not exist
- 102 - unknown failure

Example

```
# Return the sub-admins of the group: ``mygroup``
curl https://admin:secret@example.com/ocs/v1.php/cloud/groups/mygroup/subadmins
```

XML Output

```
<?xml version="1.0"?>
<ocs>
  <meta>
    <status>ok</status>
    <statuscode>100</statuscode>
    <message/>
  </meta>
  <data>
    <element>Tom</element>
  </data>
</ocs>
```

Delete Group

Removes a group. Authentication is done by sending a Basic HTTP Authorization header.

Request Path	Method	Content Type
ocs/v1.php/cloud/groups/{groupid}	DELETE	text/plain

Argument	Type	Description
groupid	string	the group to delete

Status Codes

- 100 - successful
- 101 - group does not exist
- 102 - failed to delete group

Example

```
# Delete the group ``mygroup``  
curl -X DELETE http://admin:secret@example.com/ocs/v1.php/cloud/groups/mygroup
```

XML Output

```
<?xml version="1.0"?>  
<ocs>  
  <meta>  
    <statusCode>100</statusCode>  
    <status>ok</status>  
  </meta>  
  <data/>  
</ocs>
```

Instruction Set For Apps

Get Apps

Returns a list of apps installed on the ownCloud server. Authentication is done by sending a Basic HTTP Authorization header.

Request Path	Method	Content Type
ocs/v1.php/cloud/apps/	GET	text/plain

Argument	Type	Description
filter	string	Whether to retrieve enabled or disable apps. Available values are enabled and disabled.

Status Codes

- 100 - successful
- 101 - invalid input data

Example

```
# Gets enabled apps  
curl http://admin:secret@example.com/ocs/v1.php/cloud/apps?filter=enabled
```

XML Output

```
<?xml version="1.0"?>  
<ocs>  
  <meta>  
    <statusCode>100</statusCode>  
    <status>ok</status>  
  </meta>  
  <data>  
    <apps>  
      <element>files</element>  
      <element>provisioning_api</element>  
    </apps>  
  </data>  
</ocs>
```

Get App Info

Provides information on a specific application. Authentication is done by sending a Basic HTTP Authorization header.

Request Path	Method	Content Type
ocs/v1.php/cloud/apps/{appid}	GET	text/plain

Argument	Type	Description
appid	string	The app to retrieve information for

Status Codes

- 100 - successful

Example

```
# Get app info for the ``files`` app
curl http://admin:secret@example.com/ocs/v1.php/cloud/apps/files
```

XML Output

```
<?xml version="1.0"?>
<ocs>
  <meta>
    <statusCode>100</statusCode>
    <status>ok</status>
  </meta>
  <data>
    <info/>
    <remote>
      <files>appinfo/remote.php</files>
      <webdav>appinfo/remote.php</webdav>
      <filesync>appinfo/filesync.php</filesync>
    </remote>
    <public/>
    <id>files</id>
    <name>Files</name>
    <description>File Management</description>
    <licence>AGPL</licence>
    <author>Robin Appelman</author>
    <require>4.9</require>
    <shipped>>true</shipped>
    <standalone></standalone>
    <default_enable></default_enable>
    <types>
      <element>filesystem</element>
    </types>
  </data>
</ocs>
```

Enable

Enable an app. Authentication is done by sending a Basic HTTP Authorization header.

Request Path	Method	Content Type
ocs/v1.php/cloud/apps/{appid}	POST	text/plain

Argument	Type	Description
appid	string	The id of the app to enable

Status Codes

- 100 - successful

Example

```
# Enable the ``files_texteditor`` app
curl -X POST http://admin:secret@example.com/ocs/v1.php/cloud/apps/files_texteditor
```

XML Output

```
<?xml version="1.0"?>
<ocs>
  <meta>
    <statuscode>100</statuscode>
    <status>ok</status>
  </meta>
</ocs>
```

Disable

Disables the specified app. Authentication is done by sending a Basic HTTP Authorization header.

Request Path	Method	Content Type
ocs/v1.php/cloud/apps/{appid}	DELETE	text/plain

Argument	Type	Description
appid	string	The id of the app to disable

Status Codes

- 100 - successful

Example

```
Disable the ``files_texteditor`` app
curl -X DELETE http://admin:secret@example.com/ocs/v1.php/cloud/apps/files_texteditor
```

XML Output

```
<?xml version="1.0"?>
<ocs>
  <meta>
    <statuscode>100</statuscode>
    <status>ok</status>
  </meta>
</ocs>
```

6.6.7 ownCloud Roles

ownCloud supports eight user roles. These are:

- Anonymous
- Guest
- Standard User
- Federated User
- ownCloud Group Administrator
- ownCloud Administrator
- System Administrator
- Auditor

The following information is not an in-depth guide, but more of a high-level overview of each type.

Anonymous

- Is not a regular user.
- Has access to specific content made available via public links. - Can be password-protected (optional, enforced, policy-enforced). - Can have an expiration date (optional, enforced, enforced dependent on password).
- Has no personal space
- Has no file ownership (ownership of uploaded/created files is directed to sharer).
- Has no use of clients.
- Quota is that of the sharer.
- Permissions are those granted by the sharer for specific content, e.g., *view-only*, *edit*, and *File Drop*.
- Can only use file and viewer apps, such as [PDF Viewer](#) and [Collabora Online](#).

Guest

- Is a regular user with restricted permissions, identified via e-mail address.
- Has no personal space.
- Has no file ownership (ownership of uploaded/created files is directed to sharer).
- Has access to shared space. The permissions are granted by the sharer.
- Is not bound to the inviting user.
 - Can log in as long as shares are available.
 - Becomes deactivated when no shares are left; this is *the shared with guests filter*.
 - Reactivated when a share is received.
 - Administrators will be able to automate user cleanup (“**disabled for x days**”).
- Can use all clients.
- Fully auditable in the enterprise edition.
- Can be promoted to group administrator or administrator, but will still have no personal space.

- Apps are specified by the admin (whitelist).

Note: The Shared with Guests Filter

This filter makes it easy for sharers to view and remove their shares with a guest, which also removes their responsibility for guests. When all of a guest's shares are removed, the guest is then disabled and can no longer login.

Standard User

- Is a regular user (from LDAP, ownCloud user backend, or another backend).
- Has personal space. Permissions are granted by the administrator.
- Shared space: Permissions as granted by sharer.
- Apps: All enabled, might be restricted by group membership.

Federated User

- Is not an internal user.
- Can trust *a federated system*.
- Has access to shared space through users on the considered ownCloud system.
- Can share data with the considered system (accept-/rejectable).

ownCloud Group Administrator

- Is a regular user, such as from LDAP, an ownCloud user backend, or another backend.
- Can manage users in their groups, such as adding and removing them, and changing quota of users in the group.
- Can add new users to their groups and can manage guests.
- Can enable and disable users.
- Can impersonate users in their groups.
- Custom group creation may be restricted to group admins.

ownCloud Administrator

- Is a regular user (from LDAP, ownCloud user backend, or another backend).
- Can configure ownCloud features via the UI, such as sharing settings, app-specific configurations, and external storages for users.
- Can manage users, such as adding and removing, enabling and disabling, quota and group management.
- Can restrict app usage to groups, where applicable.
- Configurable access to log files.
- Mounting of external shares and local shares (of external file systems) is disabled by default.

System Administrator

- Is not an ownCloud user.
- Has access to ownCloud code (e.g., `config.php` and apps folders) and command-line tool (*occ*).
- Configures and maintains the ownCloud environment (*PHP*, *Webserver*, *DB*, *Storage*, *Redis*, *Firewall*, *Cron*, and *LDAP*, etc.).
- Maintains ownCloud, such as updates, backups, and installs extensions.
- Can manage users and groups, such as via *occ*.
- Has access to the master key when storage encryption is used.
- **Storage admin:** Encryption at rest, which prevents the storage administrator from having access to data stored in ownCloud.
- **DB admin:** Calendar/Contacts etc. DB entries not encrypted.

Auditor

- Is not an ownCloud user.
- Conducts usage and compliance audits in enterprise scenarios.
- App logs (especially [Auditlog](#)) can be separated from ownCloud log. This separates the Auditor and Sysadmin roles. An `audit.log` file can be enabled, which the Sysadmin can't access.
- **Best practice:** parse separated log to an external analyzing tool.

MAINTENANCE

7.1 Maintenance Mode Configuration

You must put your ownCloud server into maintenance mode before performing upgrades, and for performing troubleshooting and maintenance. Please see *Using occ core commands* to learn how to put your server into the various maintenance modes (`maintenance:mode`, `maintenance:singleuser`, and `maintenance:repair`) with the `occ` command.

`maintenance:mode` locks the sessions of logged-in users and prevents new logins. This is the mode to use for upgrades. You must run `occ` as the HTTP user, like this example on Ubuntu Linux:

```
$ sudo -u www-data php occ maintenance:mode --on
```

You may also put your server into this mode by editing `config/config.php`. Change `"maintenance" => false` to `"maintenance" => true`:

```
<?php
```

```
    "maintenance" => true,
```

Then change it back to `false` when you are finished.

7.2 Backing up ownCloud

When you backup your ownCloud server, there are four things that you need to copy:

1. Your `config/` directory.
2. Your `data/` directory.
3. Your ownCloud database.
4. Your custom theme files, if you have any. (See [Theming ownCloud](#))

When you install your ownCloud server from our [Open Build Service](#) packages (or from distro packages, which we do not recommend) **do not backup your ownCloud server files**, which are the other files in your `owncloud/` directory such as `core/`, `3rdparty/`, `apps/`, `lib/`, and all the rest of the ownCloud files. If you restore these files from backup they may not be in sync with the current package versions, and will fail the code integrity check. This may also cause other errors, such as white pages.

When you install ownCloud from the source tarballs this will not be an issue, and you can safely backup your entire ownCloud installation, with the exception of your ownCloud database. Databases cannot be copied, but you must use the database tools to make a correct database dump.

To restore your ownCloud installation from backup, see [Restoring ownCloud](#) .

7.2.1 Backing Up the config/ and data/ Directories

Simply copy your `config/` and `data/` folder to a place outside of your ownCloud environment. This example uses `rsync` to copy the two directories to `/oc-backupdir/`:

```
rsync -Aax config data /oc-backupdir/
```

There are many ways to backup normal files, and you may use whatever method you are accustomed to.

7.2.2 Backup Database

You can't just copy a database, but must use the database tools to make a correct database dump.

MySQL/MariaDB

MySQL or MariaDB, which is a drop-in MySQL replacement, is the recommended database engine. To backup MySQL/MariaDB:

```
mysqldump --single-transaction -h [server] -u [username] -p [password] [db_name] > owncloud-dbbbackup_
```

Example:

```
mysqldump --single-transaction -h localhost -u username -p password owncloud > owncloud-dbbbackup_`date`
```

SQLite

```
sqlite3 data/owncloud.db .dump > owncloud-dbbbackup_`date` +%Y%m%d`.bak
```

PostgreSQL

```
PGPASSWORD="password" pg_dump [db_name] -h [server] -U [username] -f owncloud-dbbbackup_`date` +%Y%m%
```

7.2.3 Restoring Files From Backup When Encryption Is Enabled

If you need to restore files from backup, which were backed up when encryption was enabled, here's how to do it.

Note: This is effective from at least version v8.2.7 of ownCloud onwards. Also, this is **not officially supported**. ownCloud officially supports either restoring the full backup or restoring nothing — not restoring individual parts of it.

1. Restore the file from backup.
 2. Restore the file's encryption keys from your backup.
 3. Run `occ files:scan`; this makes the scanner find it.
-

Note: In the DB it will:

- Have the “size” set to the encrypted size, which is wrong (and bigger);
 - The “encrypted” flag will be set to 0
-

4. Retrieve the encrypted flag value.
5. Update the encrypted flag.

Note: There's no need to update the encrypted flag for files in either "files_versions" or "files_trashbin", because these aren't scanned or found by `occ files:scan`.

6. Download the file once as the user; the file's size will be corrected automatically.

This process might not be suitable across all environments. If it's not suitable for yours, you might need to run an OCC command that does the scanning. But, that will require the user's password or recovery key.

Retrieve the Encrypted Flag Value

1. In the backup database, retrieve the `numeric_id` value for the storage where the file was located from the `oc_storages` table and store the value for later reference.

For example, if you have the following in your `oc_storages` table, then `numeric_id` you should use is 3, if you need to restore a file for `user1`.

id	numeric_id	available	last_checked
home::admin	1	1	NULL
local::/var/www/owncloud/data/	2	1	NULL
home::user1	3	1	NULL

2. In the live database instance, find the `fileid` of the file to restore by running the query below, substituting the placeholders for the retrieved values, and store the value for later reference.

```
SELECT fileid
FROM oc_filecache
WHERE path = 'path/to/the/file/to/restore'
      AND storage = <numeric_id>
```

3. Retrieve the backup, which includes the data folder and database.
4. Retrieve the required file from your backup and copy it to the real instance.
5. In the backup database, retrieve the file's `encrypted` value, by running the query below and store the value for later reference.

```
SELECT encrypted
FROM oc_filecache
WHERE path = 'path/to/the/file/to/restore'
      AND storage = <numeric_id>
```

This assumes the storage was the same and the file was in the same location. If not, you will need to track down where the file was before.

6. Update the live database instance with retrieved information, by running the following query, substituting the placeholders for the retrieved values:

```
UPDATE oc_filecache
SET encrypted = <encrypted>
WHERE fileid = <fileid>.
```

7.3 How to Upgrade Your ownCloud Server

We recommend that you keep your ownCloud server up to date. When an update is available for your ownCloud server, you will see a notification at the top of your ownCloud Web interface. When you click the notification, it will bring you here.

Before beginning an upgrade, please keep the following points in mind:

- Review *the release notes* for important information about the needed migration steps during that upgrade to help ensure a smooth upgrade process.
- Skipping major releases is not supported. However *you can* migrate from 9.0.9 straight to 10.0.
- Downgrading is not supported.
- Upgrading is disruptive, as your ownCloud server will be put into *maintenance mode*.
- Large installations may take several hours to complete the upgrade.
- Downgrading **is not supported** as it risks corrupting your data. If you want to revert to an older ownCloud version, make a new, fresh installation and then restore your data from backup. Before doing this, file a support ticket (if you have paid support) or ask for help in the ownCloud forums to resolve your issue without downgrading.

7.3.1 Prerequisites

We strongly recommend that you always maintain *regular backups* as well as make a fresh backup before every upgrade. We also recommend that you review any installed third-party apps for compatibility with the new ownCloud release. Ensure that they are all disabled before beginning the upgrade. After the upgrade is complete re-enable any which are compatible with the new release.

Warning: Install unsupported apps at your own risk.

7.3.2 Upgrade Options

There are three ways to upgrade your ownCloud server:

1. **(Recommended)** Perform a *manual upgrade*, using the latest ownCloud release.
2. Use your distribution's *package manager*, in conjunction with our official ownCloud repositories. **Note:** This approach should not be used unattended nor in clustered setups.
3. Use the *Updater App*. This is needed in scenarios where the admin does not have access to the command line. It is recommended for shared hosting environments and for users who want an easy way to track different release channels.

Note: Enterprise customers will use their Enterprise software repositories to maintain their ownCloud servers, rather than the Open Build Service. Please see *Installing & Upgrading ownCloud Enterprise Edition* for more information.

7.4 Upgrade ownCloud From Packages

7.4.1 Upgrade Quickstart

The best method for keeping ownCloud current on Linux servers is by configuring your system to use ownCloud's [Open Build Service](#) repository. Then stay current by using your Linux package manager to install fresh ownCloud packages. After installing upgraded packages you must run a few more steps to complete the upgrade. These are the basic steps to upgrading ownCloud:

Warning: Make sure that you don't skip a major release when upgrading via repositories. For example you can't upgrade from 8.1.x to 9.0.x directly as you would skip the 8.2.x major release. See [Upgrading Across Skipped Releases](#) for more information.

- *Disable* all third-party apps.
- Make a *fresh backup*.
- Upgrade your ownCloud packages.
- Run *occ upgrade* (The optional parameter to skip migration tests was removed from oC 9.2. See [Test the Upgrade](#) for background information).
- *Apply strong permissions* to your ownCloud directories.
- Take your ownCloud server out of *maintenance mode*.
- Re-enable third-party apps.

Warning: When upgrading from oC 9.0 to 9.1 with existing Calendars or Addressbooks please have a look at the [9.0 release notes](#) for important information about the needed migration steps during that upgrade.

7.4.2 Upgrade Tips

Upgrading ownCloud from our [Open Build Service](#) repository is just like any normal Linux upgrade. For example, on Debian or Ubuntu Linux this is the standard system upgrade command:

```
apt-get update && apt-get upgrade
```

Or you can upgrade just ownCloud with this command:

```
apt-get update && apt-get install owncloud-files
```

On Fedora, CentOS, and Red Hat Linux use yum to see all available updates:

```
yum check-update
```

You can apply all available updates with this command:

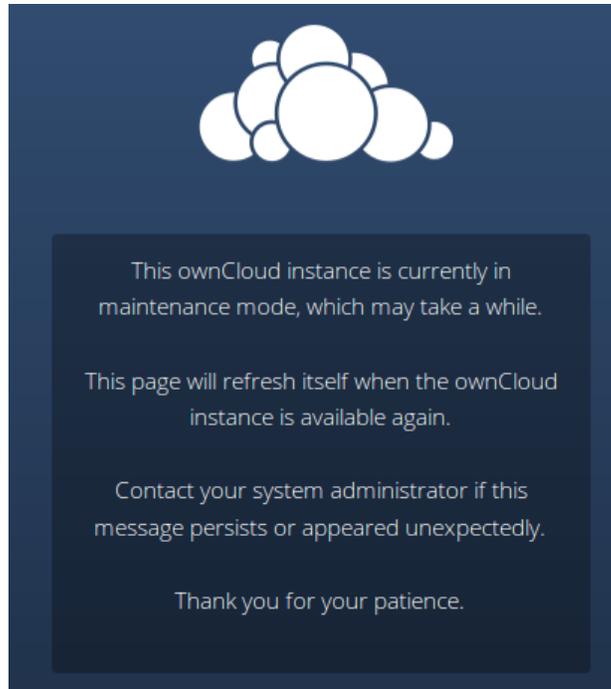
```
yum update
```

Or update only ownCloud:

```
yum update owncloud-files
```

Your Linux package manager only downloads the current ownCloud packages. Then your ownCloud server is immediately put into maintenance mode. You may not see this until you refresh your ownCloud page.

Then use `occ` to complete the upgrade. You must run `occ` as your HTTP user. This example is for Debian/Ubuntu:



```
sudo -u www-data php occ upgrade
```

This example is for CentOS/RHEL/Fedora:

```
sudo -u apache php occ upgrade
```

The optional parameter to skip migration tests during this step was removed in oC 9.2. See *Test the Upgrade* for background information.

See *Using occ core commands* to learn more.

7.4.3 Setting Strong Directory Permissions

After upgrading, verify that your ownCloud directory permissions are set according to *Set Strong Directory Permissions*.

7.4.4 Upgrading Across Skipped Releases

It is best to update your ownCloud installation with every new point release (e.g. 8.1.10), and to never skip any major release (e.g. don't skip 8.2.x between 8.1.x and 9.0.x). If you have skipped any major release you can bring your ownCloud current with these steps:

1. Add the repository of your current version (e.g. 8.1.x)
2. Upgrade your current version to the latest point release (e.g. 8.1.10) via your package manager
3. Run the `occ upgrade` routine (see Upgrade Quickstart above)
4. Add the repository of the next major release (e.g. 8.2.x)
5. Upgrade your current version to the next major release (e.g. 8.2.8) via your package manager
6. Run the `occ upgrade` routine (see Upgrade Quickstart above)

7. Repeat from step 4 until you reach the last available major release (e.g. 9.1.x)

You'll find repositories of previous ownCloud major releases in the [ownCloud Server Changelog](#).

7.5 Upgrading ownCloud with the Updater App

The Updater app automates many of the steps of upgrading an ownCloud installation. It is useful for installations that do not have root access, such as shared hosting, for installations with a smaller number of users and data, and it automates updating *manual installations*.

Warning: When upgrading from oC 9.0 to 9.1 with existing Calendars or Addressbooks please have a look at the [Release Notes](#) of oC 9.0 for important info about this migration.

New in 9.0, the Updater app has *command-line options*.

Note: The Updater app is **not enabled and not supported** in ownCloud Enterprise edition.

The Updater app is **not included** in the [Linux packages on our Open Build Service](#), but only in the [tar and zip archives](#). When you install ownCloud from packages you should keep it updated with your package manager.

Downgrading is not supported and risks corrupting your data! If you want to revert to an older ownCloud version, install it from scratch and then restore your data from backup. Before doing this, file a support ticket (if you have paid support) or ask for help in the ownCloud forums to see if your issue can be resolved without downgrading.

You should maintain regular backups (see [Backing up ownCloud](#)), and make a backup before every update. The Updater app does not backup your database or data directory.

The Updater app performs these operations:

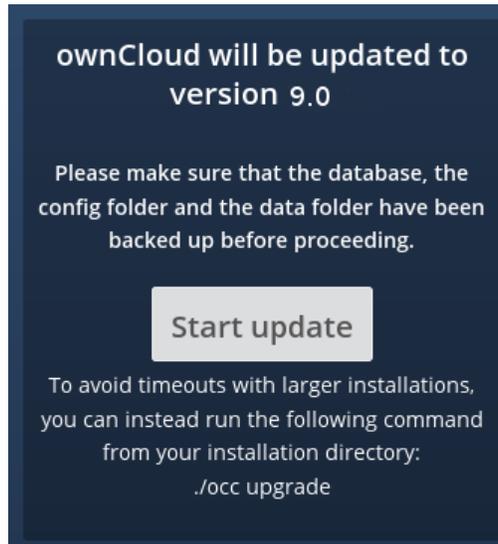
- Creates an `updater_backup` directory under your ownCloud data directory
- Downloads and extracts updated package content into the `updater_backup/packageVersion` directory
- Makes a copy of your current ownCloud instance, except for your data directory, to `updater_backup/currentVersion-randomstring`
- Moves all directories except `data` and `config` from the current instance to `updater_backup/tmp`
- Moves all directories from `updater_backup/packageVersion` to the current version
- Copies your old `config.php` to the new `config/` directory

Note: Backups created by the updater app can use up significant disc space, if kept across multiple updates. We recommend that you save storage space by only keeping the ones that are crucial to your instance and removing any others.

Using the Updater app to update your ownCloud installation is just a few steps:

1. You should see a notification at the top of any ownCloud page when there is a new update available.
2. Even though the Updater app backs up important directories, you should always have your own current backups (See [Backing up ownCloud](#) for details.)
3. Verify that the HTTP user on your system can write to your whole ownCloud directory; see the [Setting Permissions for Updating](#) section below.
4. Navigate to your Admin page and click the **Update Center** button under Updater. This takes you to the Updater control panel.

5. Click Update, and carefully read the messages. If there are any problems it will tell you. The most common issue is directory permissions; your HTTP user needs write permissions to your whole ownCloud directory. (See *Set Strong Directory Permissions*.) Another common issue is SELinux rules (see *SELinux Configuration*.) Otherwise you will see messages about checking your installation and making backups.
6. Click Proceed, and then it performs the remaining steps, which takes a few minutes.
7. If your directory permissions are correct, a backup was made, and downloading the new ownCloud archive succeeded you will see the following screen. Click the Start Update button to complete your update:



Note: If you have a large ownCloud installation and have shell access, you should use the `occ upgrade` command, running it as your HTTP user, instead of clicking the Start Update button, in order to avoid PHP timeouts.

This example is for Ubuntu Linux:

```
$ sudo -u www-data php occ upgrade
```

The optional parameter to skip migration tests during this step was removed in oC 9.2. See *Test the Upgrade* for more information.

8. It runs for a few minutes, and when it is finished displays a success message, which disappears after a short time.

Refresh your Admin page to verify your new version number. In the Updater section of your Admin page you can see the current status and backups. These are backups of your old and new ownCloud installations, and do not contain your data files. If your update works and there are no problems you can delete the backups from this screen.

If the update fails, then you must update manually. (See *Manually upgrading*.)

7.5.1 Setting Permissions for Updating

For hardened security, we highly recommend setting the permissions on your ownCloud directory as strictly as possible, immediately after the initial installation. However, these strict permissions will prevent the Updater app from working, as it needs your whole ownCloud directory to be owned by the HTTP user.

So to set the appropriate permissions for updating, run the code below. Replace the `ocpath` variable with the path to your ownCloud directory, and replace the `htuser` and `htgroup` variables with your HTTP user and group.

```
#!/bin/bash
# Sets permissions of the owncloud instance for updating

ocpath='/var/www/owncloud'
htuser='www-data'
htgroup='www-data'

chown -R ${htuser}:${htgroup} ${ocpath}
```

You can find your HTTP user in your HTTP server configuration files. Or you can use *PHP Version and Information* (Look for the **User/Group** line).

- The HTTP user and group in Debian/Ubuntu is `www-data`.
- The HTTP user and group in Fedora/CentOS is `apache`.
- The HTTP user and group in Arch Linux is `http`.
- The HTTP user in openSUSE is `wwwrun`, and the HTTP group is `www`.

After the update is completed, re-apply *the strong directory permissions* immediately.

7.5.2 Command Line Options

The Updater app includes command-line options to automate updates, to create checkpoints and to roll back to older checkpoints. You must run it as your HTTP user. This example on Ubuntu Linux displays command options:

```
sudo -u www-data php updater/application.php list
```

See usage for commands, like this example for the `upgrade:checkpoint` command:

```
sudo -u www-data php updater/application.php upgrade:checkpoint -h
```

You can display a help summary:

```
sudo -u www-data php updater/application.php --help
```

When you run it without options it runs a system check:

```
sudo -u www-data php owncloud/updater/application.php
ownCloud updater 1.0 - CLI based ownCloud server upgrades
Checking system health.
- file permissions are ok.
Current version is 9.0.0.12
No updates found online.
Done
```

Create a checkpoint:

```
sudo -u www-data php updater/application.php upgrade:checkpoint --create
Created checkpoint 9.0.0.12-56d5e4e004964
```

List checkpoints:

```
sudo -u www-data php updater/application.php upgrade:checkpoint --list
```

Restore an earlier checkpoint:

```
sudo -u www-data php owncloud/updater/application.php upgrade:checkpoint
--restore=9.0.0.12-56d5e4e004964
```

Add a line like this to your crontab to automatically create daily checkpoints:

```
2 15 * * * sudo -u www-data php /path/to/owncloud/updater/application.php
upgrade:checkpoint --create > /dev/null 2>&1
```

7.5.3 updater.secret value in config.php

When running the updater, you will be prompted to add a hashed secret into your config.php file. On the updater web interface, you then need to enter the unhashed secret into the web form.

In case you forgot your password/secret, you can re-create it by changing config.php. You can run this on your shell:

```
php -r 'echo password_hash("Enter a random password here", PASSWORD_DEFAULT)."\n";'
```

Please replace `Enter a random password here` with your own. Then add this into your config.php:

```
'updater.secret' => 'The value you got from the above hash command',
```

7.6 Manual ownCloud Upgrade

Note: If you're not comfortable performing a manual upgrade, you can also use your Linux distribution's *package manager*, or use *the Updater App*.

7.6.1 Backup Your Existing Installation

First, *backup* the following items:

- The ownCloud server data directory
- The config.php file
- All 3rd party apps
- The ownCloud server database

```
# This example assumes Ubuntu Linux and MariaDB
cp -rv /var/www/owncloud /opt/backup/owncloud && mysqldump <db_name> > /opt/backup/backup-file.sql
```

7.6.2 Review Third-Party Apps

Review any installed third-party apps for compatibility with the new ownCloud release. Ensure that they are all disabled before beginning the upgrade. After the upgrade is complete re-enable any which are compatible with the new release.

Warning: Install unsupported apps at your own risk.

7.6.3 Check ownCloud's Mandatory Requirements

ownCloud's mandatory requirements (such as PHP versions and extensions) can change from one version to the next. Ensure that you review them and update your server(s), if required, before upgrading ownCloud.

7.6.4 Enable Maintenance Mode

Put your server in *maintenance mode* and disable *Cron jobs*.

Doing so prevents new logins, locks the sessions of logged-in users, and displays a status screen so that users know what is happening.

There are two ways to enable maintenance mode. The preferred method is to use the *occ command* — which you must run as your webserver user. The other way is by entering your `config.php` file and changing `'maintenance' => false`, to `'maintenance' => true`,.

```
# Enable maintenance mode using the occ command.
sudo -u www-data php occ maintenance:mode --on
```

```
# Disable Cron jobs
sudo service cron stop
```

7.6.5 Stop the Webserver

With those steps completed, stop your webserver.

```
sudo service apache2 stop
```

7.6.6 Download the Latest Installation

Download the latest ownCloud server release from owncloud.org/install/ into an empty directory **outside** of your current installation.

Note: Enterprise users must download their new ownCloud archives from their accounts on <https://customer.owncloud.com/owncloud/>.

7.6.7 Setup the New Installation

Not all installations are the same, so we encourage you to take one of two paths to upgrade your ownCloud installation. These are the [standard upgrade](#) and the [power user upgrade](#).

If you're reasonably new to ownCloud, or not too familiar with upgrading an ownCloud installation, please follow the standard upgrade. Otherwise, take the approach that you're most comfortable with, likely the power user upgrade.

Note: Regardless of which approach that you take, they will both assume that your existing ownCloud installation is located in the default location: `/var/www/owncloud`.

The Standard Upgrade

Delete all files and folders in your existing ownCloud directory (`/var/www/owncloud`) — **except** `data` and `config`.

Attention: Don't keep the `apps` directory.

With those files and folders deleted, extract the archive of the latest ownCloud server, over the top of your existing installation.

```
# Extract the .tar.bz2 archive
tar -jxf owncloud-10.0.3.tar.bz2 -C /var/www/

# Extract the zip archive
unzip -q owncloud-10.0.3.zip -d /var/www/
```

The Power User Upgrade

Rename your current ownCloud directory, for example, from `owncloud` to `owncloud-old`. Extract the unpacked ownCloud server directory and its contents to the location of your original ownCloud installation.

```
# Assumes that the new release was unpacked into /tmp/
mv /tmp/owncloud /var/www/
```

With the new source files now in place of the old ones, next copy the `config.php` file from your old ownCloud directory to your new ownCloud directory.

```
cp /var/www/owncloud-old/config/config.php /var/www/owncloud/config/config.php
```

If you keep your `data/` directory *inside* your `owncloud/` directory, copy it from your old version of ownCloud to your new version. If you keep it *outside* of your `owncloud/` directory, then you don't have to do anything with it, because its location is configured in your original `config.php`, and none of the upgrade steps touch it.

7.6.8 Market and Marketplace App Upgrades

Before getting too far into the upgrade process, please be aware of how the Market app and its configuration options affect the upgrade process.

- The Market app is not upgraded if it is either disabled (because `appstoreenabled` is set to `false`) or it is not available.
- If `upgrade.automatic-app-update` is set to `false` apps installed from the Marketplace are not automatically upgraded.

In addition to these two points, if there are installed apps (whether compatible or incompatible with the next version, or missing source code) and the Market app is enabled, but there is no available internet connection, then these apps will need to be manually updated once the upgrade is finished.

7.6.9 Start the Upgrade

With the apps disabled and the webserver started, launch the upgrade process from the command line.

```
# Here is an example on CentOS Linux
sudo -u www-data php occ upgrade
```

Note: The optional parameter to skip migration tests during this step was removed in oC 10.0. See [Test the Upgrade](#) for background information. See [Using occ core commands](#) to learn more about the `occ` command.

The upgrade operation can take anywhere from a few minutes to a few hours, depending on the size of your installation. When it is finished you will see either a success message, or an error message which indicates why the process did not complete successfully.

7.6.10 Copy Old Apps

If you are using 3rd party applications, look in your new `/var/www/owncloud/apps/` directory to see if they are there. If not, copy them from your old `apps/` directory to your new one, and make sure that the directory permissions are the same as for the other ones.

7.6.11 Disable Maintenance Mode

Assuming your upgrade succeeded, next disable maintenance mode. The simplest way is by using `occ` from the command line.

```
sudo -u www-data php occ maintenance:mode --off
```

7.6.12 Restart the Webserver

With all that done, restart your web server.

```
sudo service apache2 start
```

7.6.13 Finalize the Installation

With maintenance mode disabled, login and:

- Check that the version number reflects the new installation. It's visible at the bottom of your Admin page.
- Check that your other settings are correct.
- Go to the Apps page and review the core apps to make sure the right ones are enabled.
- Re-enable your third-party apps.
- *Apply strong permissions* to your ownCloud directories.

7.6.14 Test the Upgrade

Previous versions of ownCloud included a migration test. ownCloud first ran a migration simulation by copying the ownCloud database and performing the upgrade on the copy, to ensure that the migration would succeed.

Then the copied tables were deleted after the upgrade was completed. This doubled the upgrade time, so admins could skip this test (by risking a failed upgrade) with `php occ upgrade --skip-migration-test`.

The migration test has been removed from ownCloud 9.2. ownCloud server admins should have current backups before migration, and rely on backups to correct any problems from the migration.

7.6.15 Reverse Upgrade

If you need to reverse your upgrade, see *Restoring ownCloud*.

7.6.16 Troubleshooting

When upgrading ownCloud and you are running MySQL or MariaDB with binary logging enabled, your upgrade may fail with these errors in your MySQL/MariaDB log:

```
An unhandled exception has been thrown:
exception 'PDOException' with the message 'SQLSTATE[HY000]: General error: 1665
Cannot execute statement: impossible to write to binary log since
BINLOG_FORMAT = STATEMENT and at least one table uses a storage engine limited to row-based logging.
```

Please refer to *MySQL / MariaDB with Binary Logging Enabled* on how to correctly configure your environment.

Occasionally, *files do not show up after an upgrade*. A rescan of the files can help:

```
sudo -u www-data php console.php files:scan --all
```

See the [owncloud.org support page](https://owncloud.org/support) for further resources for both home and enterprise users.

Sometimes, ownCloud can get *stuck in a upgrade*. This is usually due to the process taking too long and encountering a PHP time-out. Stop the upgrade process this way:

```
sudo -u www-data php occ maintenance:mode --off
```

Then start the manual process:

```
sudo -u www-data php occ upgrade
```

If this does not work properly, try the repair function:

```
sudo -u www-data php occ maintenance:repair
```

7.7 Restoring ownCloud

When you install ownCloud from packages, follow these steps to restore your ownCloud installation. Start with a fresh ownCloud package installation in a new, empty directory. Then restore these items from your backup (see *Backing up ownCloud*):

1. Your `config/` directory.
2. Your `data/` directory.
3. Your ownCloud database.
4. Your custom theme files, if you have any. (See *Theming ownCloud*)

When you install ownCloud from the source tarballs you may safely restore your entire ownCloud installation from backup, with the exception of your ownCloud database. Databases cannot be copied, but you must use the database tools to make a correct restoration.

When you have completed your restoration, see *Setting Strong Permissions*.

7.7.1 Restore Directories

Simply copy your configuration and data folder to your ownCloud environment. You could use this command, which restores the backup example in *Backing up ownCloud*:

```
rsync -Aax config data /var/www/owncloud/
```

There are many ways to restore normal files from backups, and you may use whatever method you are accustomed to.

7.7.2 Restore Database

Note: This guide assumes that your previous backup is called “owncloud-dbbbackup.bak”

MySQL

MySQL is the recommended database engine. To restore MySQL:

```
occ maintenance:mode --on
mysql -h [server] -u [username] -p[password] [db_name] < owncloud-dbbbackup.bak
occ maintenance:data-fingerprint
occ maintenance:mode --off
```

SQLite

```
rm data/owncloud.db
sqlite3 data/owncloud.db < owncloud-dbbbackup.bak
```

PostgreSQL

```
PGPASSWORD="password" pg_restore -c -d owncloud -h [server] -U [username]
owncloud-dbbbackup.bak
```

7.8 Migrating to a Different Server

If the need arises, ownCloud can be migrated to a different server. A typical use case would be a hardware change or a migration from *the Enterprise appliance* to a physical server. All migrations have to be performed with ownCloud in maintenance mode. Online migration is supported by ownCloud only when implementing industry-standard clustering and high-availability solutions **before** ownCloud is installed for the first time.

To start, let’s work through a potential use case. A configured ownCloud instance runs reliably on one machine, but for some reason the instance needs to be moved to a new machine. Depending on the size of the ownCloud instance the migration might take several hours.

For the purpose of this use case, it is assumed that:

1. The end users reach the ownCloud instance via a virtual hostname (such as a DNS CNAME record) which can be pointed at the new location.
2. The authentication method (e.g., LDAP) remains the same after the migration.

Warning: During the migration, do not make any changes to the original system, except for putting it into maintenance mode. This ensures, should anything unforeseen happen, that you can go back to your existing installation and resume availability of your ownCloud installation while debugging the problem.

7.8.1 How to Migrate

Firstly, set up the new machine with your desired Linux distribution. At this point you can either *install ownCloud manually* via the compressed archive, or *with your Linux package manager*.

Then, on the original machine turn on maintenance mode and then stop ownCloud. After waiting for 6 - 7 minutes for all sync clients to register that the server is in maintenance mode, ref:*stop the web server <maintenance_commands_label>* that is serving ownCloud.

After that, *create a database dump from the database*, copy it to the new machine, and *import it into the new database*.

Then, copy only your data, configuration, and database files from your original ownCloud instance to the new machine (See *Backing up ownCloud* and *Restore Directories*).

Warning: You must keep the `data/` directory's original file path during the migration. However, *you can change it* before you begin the migration, or after the migration's completed.

The data files should keep their original timestamp otherwise the clients will re-download all the files after the migration. This step might take several hours, depending on your installation. This can be done on a number of sync clients, such as by using `rsync` with `-t` option

With ownCloud still in maintenance mode and before changing the DNS CNAME record, start up the database and web server on the new machine. Then point your web browser to the migrated ownCloud instance and confirm that:

1. You see the maintenance mode notice
2. That a log file entry is written by both the web server and ownCloud
3. That no error messages occur.

If all of these things occur, then take ownCloud out of maintenance mode and repeat. After doing this, log in as an admin and confirm that ownCloud functions as normal.

At this point, change the DNS CNAME entry to point your users to the new location. And with the CNAME entry updated, you now need to update the trusted domains.

7.8.2 Managing Trusted Domains

All URLs used to access your ownCloud server must be whitelisted in your `config.php` file, under the `trusted_domains` setting. Users are allowed to log into ownCloud only when they point their browsers to a URL that is listed in the `trusted_domains` setting.

Note: This setting is important when changing or moving to a new domain name. You may use IP addresses and domain names.

A typical configuration looks like this:

```
'trusted_domains' => [  
    0 => 'localhost',  
    1 => 'server1.example.com',  
    2 => '192.168.1.50',  
],
```

The loopback address, `127.0.0.1`, is automatically whitelisted, so as long as you have access to the physical server you can always log in. In the event that a load-balancer is in place, there will be no issues as long as it sends the correct `X-Forwarded-Host` header.

7.8.3 Example Migration

Now, let's step through an example migration. For this example to work, you will need the following on both the servers that you will use for the migration:

- Ubuntu 16.04
- SSH with `PermitRootLogin` set to `yes`

Preparation

Before you can perform a migration, you have to prepare. To do this, first make sure SSH is installed:

```
apt install ssh -y
```

Next, edit `ssh-config` and enable root ssh login.

```
nano /etc/ssh/sshd_config
PermitRootLogin yes
```

And then restart SSH.

```
service ssh restart
```

Lastly, install ownCloud on the new server.

Migration

Enable Maintenance Mode

The first step is to enable maintenance mode. To do that, use the following commands:

```
cd /var/www/owncloud/
sudo -u www-data php occ maintenance:mode --on
```

After that's done, wait for 6-7 minutes and stop Apache:

```
service apache2 stop
```

Transfer the Database

Now, you have to transfer the database from the old server to the new one. To do that, first backup the database.

```
cd /var/www/owncloud/
mysqldump --single-transaction -h localhost -u admin -ppassword owncloud > owncloud-dbbbackup.bak
```

Then, export the database to the new server.

```
rsync -Aaxt owncloud-dbbbackup.bak root@new_server_address:/var/www/owncloud
```

With that completed, import the database on new server.

```
mysql -h localhost -u admin -ppassword owncloud < owncloud-dbbbackup.bak
```

Note: You can find the values for the `mysqldump` command in your `config.php`, in your owncloud root directory. `[server]=dbhost`, `[username]=dbuser`, `[password]=dbpassword`, and `[db_name]=dbname`.

Note: For InnoDB tables only The `--single-transaction` flag will start a transaction before running. Rather than lock the entire database, this will let `mysqldump` read the database in the current state at the time of the transaction, making for a consistent data dump.

Note: For Mixed MyISAM/ InnoDB tables Either dumping your MyISAM tables separately from InnoDB tables or use `--lock-tables` instead of `--single-transaction` to guarantee the database is in a consistent state when using `mysqldump`.

Transfer Data and Configure the New Server

```
rsync -Aavxt config data root@new_server_address:/var/www/owncloud
```

Warning: If you want to move your data directory to another location on the target server, it is advised to do this as a second step. Please see the data directory migration document [How To Manually Move a Data Directory](#) for more details.

Finish the Migration

Now it's time to finish the migration. To do that, on the new server, first verify that ownCloud is in maintenance mode.

```
sudo -u www-data php occ maintenance:mode
```

Next, start up the database and web server on the new machine.

```
service mysql start
service apache2 start
```

With that done, point your web browser to the migrated ownCloud instance, and confirm that you see the maintenance mode notice, and that no error messages occur. If both of these occur, take ownCloud out of maintenance mode.

```
sudo -u www-data php occ maintenance:mode --off
```

And finally, log in as admin and confirm normal function of ownCloud. If you have a domain name, and you want an SSL certificate, we recommend [certbot](#).

Reverse the Changes to ssh-config

Now you need to reverse the change to `ssh-config`. Specifically, set `PermitRootLogin` to `no` and restart `ssh`. To do that, run the following command:

```
service ssh restart
```

Update DNS and Trusted Domains

Finally, update the DNS' `CNAME` entry to point to your new server. If you have not only migrated physically from server to server but have also changed your ownCloud server's domain name, you also need to update the domain in *the Trusted Domain setting* in `config.php`, on the target server.

7.9 How To Manually Move a Data Directory

If you need to move your ownCloud data directory from its current location to somewhere else, here is a manual process that you can take to make it happen.

Note: This example assumes that:

- The current folder is: `/var/www/owncloud/data`
 - The new folder is: `/mnt/owncloud`
 - You're using Apache as your webserver
-

1. Stop Apache
2. Use rsync to sync the files from the current folder to the new one
3. Create a symbolic link from the new directory to the old one
4. Double-check the [directory permissions](#) on the new directory
5. Restart Apache

To save time, here's the commands which you can copy and use:

```
apachectl -k stop
rsync -avz /var/www/owncloud/data /mnt/owncloud
ln -s /mnt/owncloud /var/www/owncloud/data
apachectl -k graceful
```

Note: If you're on CentOS/Fedora, try `systemctl restart httpd`. If you're on Debian/Ubuntu try `sudo systemctl restart apache2` To learn more about the `systemctl` command, please refer to [the systemd essentials guide](#)

7.9.1 Fix Hardcoded Database Path Variables

Update the `oc_storages` table

If you want to manually change the location of the data folder in the database, run the SQL below:

```
UPDATE oc_storages SET id='local::/mnt/owncloud'
WHERE id='local::/var/www/owncloud/data/';
```

Update the `oc_accounts` table

You next need to update the `home` column in the `oc_accounts` table. This column contains the absolute path for user folders, e.g., `/mnt/data/files/admin`. Assuming that the new home directory is `/mnt/data/files/super-admin`, and that the user's `id` is 1, you could change it using the following SQL statement:

```
UPDATE oc_accounts SET home='/mnt/data/files/super-admin'
WHERE id=1;
```

Note: Please don't copy and paste this example verbatim — nor any of the others. It, and the others, are provided only as guides to what you should or could do.

Update the `oc_jobs` table

The next area to check is the `oc_jobs` table. The `logrotate` process may have hard-coded a non-standard (or old) value for the data path. To check it, run the SQL below and see if any results are returned:

```
SELECT * FROM oc_jobs
WHERE class = 'OC\Log\Rotate';
```

If any are, run the SQL below to update them, changing the value as appropriate.

```
UPDATE oc_jobs SET argument = '/your/new/data/path'
WHERE id = <id of the incorrect record>;
```

7.9.2 Fix Application Settings

One thing worth noting is that individual apps may reference the data directory separate from the core system configuration. If so, then you will need to find which applications do this, and change them as needed.

For example, if you listed the application configuration by running `occ config:list`, then you might see output similar to that below:

```
{
  "apps": {
    "fictitious": {
      "enabled": "yes",
      "installed_version": "2.3.2",
      "types": "filesystem",
      "datadir": "var/www/owncloud/data"
    }
  }
}
```

Here, the “fictitious” application references the data directory as being set to `var/www/owncloud/data`. So you would have to change the value by using the `config:app:set` option. Here’s an example of how you would update the setting:

```
occ config:app:set --value /mnt/owncloud fictitious datadir
```

ISSUES AND TROUBLESHOOTING

8.1 General Troubleshooting

If you have trouble installing, configuring or maintaining ownCloud, please refer to our community support channels:

- [The ownCloud Forums](#)

Note: The ownCloud forums have a [FAQ category](#) where each topic corresponds to typical mistakes or frequently occurring issues

- [The ownCloud User mailing list](#)
- The ownCloud IRC chat channel `irc://#owncloud@freenode.net` on [freenode.net](#), also accessible via [webchat](#)

Please understand that all these channels essentially consist of users like you helping each other out. Consider helping others out where you can, to contribute back for the help you get. This is the only way to keep a community like ownCloud healthy and sustainable!

If you are using ownCloud in a business or otherwise large scale deployment, note that ownCloud Inc. offers the [Enterprise Edition](#) with commercial support options.

8.1.1 Bugs

If you think you have found a bug in ownCloud, please:

- Search for a solution (see the options above)
- Double-check your configuration

If you can't find a solution, please use our [bugtracker](#). You can generate a configuration report with the `occ config command`, with passwords automatically obscured.

8.1.2 General Troubleshooting

Check the ownCloud [System Requirements](#), especially supported browser versions.

When you see warnings about `code integrity`, refer to [Code Signing](#).

Disable 3rdparty / non-shipped apps

It might be possible that 3rd party / non-shipped apps are causing various different issues. Always disable 3rd party apps before upgrades, and for troubleshooting. Please refer to the *Commands managing Apps* on how to disable an app from command line.

ownCloud Logfiles

In a standard ownCloud installation the log level is set to `Normal`. To find any issues you need to raise the log level to `All` in your `config.php` file, or to **Everything** on your ownCloud Admin page. Please see *Logging Configuration* for more information on these log levels.

Some logging - for example JavaScript console logging - needs debugging enabled. Edit `config/config.php` and change `'debug' => false`, to `'debug' => true`, Be sure to change it back when you are finished.

For JavaScript issues you will also need to view the javascript console. All major browsers have developer tools for viewing the console, and you usually access them by pressing F12. For Firefox we recommend to installing the [Firebug extension](#).

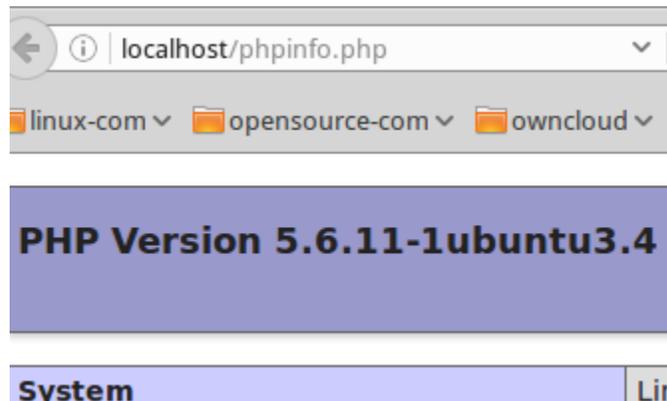
Note: The logfile of ownCloud is located in the data directory `owncloud/data/owncloud.log`.

PHP Version and Information

You will need to know your PHP version and configurations. To do this, create a plain-text file named **phpinfo.php** and place it in your Web root, for example `/var/www/html/phpinfo.php`. (Your Web root may be in a different location; your Linux distribution documentation will tell you where.) This file contains just this line:

```
<?php phpinfo(); ?>
```

Open this file in a Web browser by pointing your browser to `localhost/phpinfo.php`:



Your PHP version is at the top, and the rest of the page contains abundant system information such as active modules, active `.ini` files, and much more. When you are finished reviewing your information you must delete `phpinfo.php`, or move it outside of your Web directory, because it is a security risk to expose such sensitive data.

Debugging Sync Issues

Warning: The data directory on the server is exclusive to ownCloud and must not be modified manually.

Disregarding this can lead to unwanted behaviours like:

- Problems with sync clients
- Undetected changes due to caching in the database

If you need to directly upload files from the same server please use a WebDAV command line client like `cadaver` to upload files to the WebDAV interface at:

```
https://example.com/owncloud/remote.php/dav
```

Common problems / error messages

Some common problems / error messages found in your logfiles as described above:

- `SQLSTATE[HY000] [1040] Too many connections -> You need to increase the connection limit of your database, please refer to the manual of your database for more information.`
- `SQLSTATE[HY000]: General error: 5 database is locked -> You're using SQLite which can't handle a lot of parallel requests. Please consider converting to another database like described in Converting Database Type.`
- `SQLSTATE[HY000]: General error: 2006 MySQL server has gone away -> Please refer to Troubleshooting for more information.`
- `SQLSTATE[HY000] [2002] No such file or directory -> There is a problem accessing your SQLite database file in your data directory (data/owncloud.db). Please check the permissions of this folder/file or if it exists at all. If you're using MySQL please start your database.`
- `Connection closed / Operation cancelled or expected filesize 4734206 got 458752 -> This could be caused by wrong KeepAlive settings within your Apache config. Make sure that KeepAlive is set to On and also try to raise the limits of KeepAliveTimeout and MaxKeepAliveRequests. On Apache with mod_php using a different Multi-Processing Module \(MPM\) then prefork could be another reason. Further information is available in the forums.`
- `No basic authentication headers were found -> This error is shown in your data/owncloud.log file. Some Apache modules like mod_fastcgi, mod_fcgid or mod_proxy_fcgi are not passing the needed authentication headers to PHP and so the login to ownCloud via WebDAV, CalDAV and CardDAV clients is failing. More information on how to correctly configure your environment can be found at the forums.`

8.1.3 OAuth2

ownCloud clients cannot connect to the ownCloud server

If ownCloud clients cannot connect to your ownCloud server, check to see if `PROPFIND` requests receive HTTP/1.1 401 Unauthorized responses. If this is happening, more than likely your webserver configuration is stripping out the bearer authorization header.

If you're using the Apache web server, add the following `SetEnvIf` directive to your Apache configuration, whether in the general Apache config, in a configuration include file, or in ownCloud's `.htaccess` file.

```
SetEnvIf Authorization "(.*)" HTTP_AUTHORIZATION=$1
```

Alternatively, if you're using NGINX, add the following configuration to your NGINX setup:

```
# Adding this allows the variable to be accessed with $_SERVER['Authorization']
fastcgi_param Authorization $http_authorization;
```

8.1.4 Missing Data Directory

During the normal course of operations, the ownCloud data directory may be temporarily unavailable for a variety of reasons. These can include network timeouts on mounted network disks, unintentional unmounting of the partition on which the directory sits, or a corruption of the RAID setup. If you have experienced this, here's how ownCloud works and what you can expect.

During normal operation, ownCloud's data directory contains a hidden file, named `.ocdata`. The purpose of this file is for setups where the data folder is mounted (such as via NFS) and for some reason the mount disappeared. If the directory isn't available, the data folder would, in effect, be completely empty and the `".ocdata"` would be missing. When this happens, ownCloud will return a `503 Service not available` error, to prevent clients believing that the files are gone.

8.1.5 Troubleshooting Web server and PHP problems

Logfiles

When having issues the first step is to check the logfiles provided by PHP, the Web server and ownCloud itself.

Note: In the following the paths to the logfiles of a default Debian installation running Apache2 with `mod_php` is assumed. On other Web servers, Linux distros or operating systems they can differ.

- The logfile of Apache2 is located in `/var/log/apache2/error.log`.
- The logfile of PHP can be configured in your `/etc/php5/apache2/php.ini`. You need to set the directive `log_errors` to `On` and choose the path to store the logfile in the `error_log` directive. After those changes you need to restart your Web server.
- The logfile of ownCloud is located in the data directory `/var/www/owncloud/data/owncloud.log`.

Web Server and PHP Modules

Note: `Lighttpd` is not supported with ownCloud, and some ownCloud features may not work at all on `Lighttpd`.

There are some Web server or PHP modules which are known to cause various problems like broken up-/downloads. The following shows a draft overview of these modules:

1. Apache
 - `libapache2-mod-php5filter` (use `libapache2-mod-php5` instead)
 - `mod_dav`
 - `mod_deflate`
 - `mod_evasive`
 - `mod_pagespeed`
 - `mod_proxy_html` (can cause broken PDF downloads)
 - `mod_reqtimeout`
 - `mod_security`
 - `mod_spdy` together with `libapache2-mod-php5 / mod_php` (use `fcgi` or `php-fpm` instead)
 - `mod_xsendfile / X-Sendfile` (causing broken downloads if not configured correctly)

2. NGINX

- ngx_pagespeed
- HttpDavModule
- X-Sendfile (causing broken downloads if not configured correctly)

3. PHP

- eAccelerator

8.1.6 Troubleshooting WebDAV

General troubleshooting

ownCloud uses SabreDAV, and the SabreDAV documentation is comprehensive and helpful.

See:

- [SabreDAV FAQ](#)
- [Web servers](#) (Lists lighttpd as not recommended)
- [Working with large files](#) (Shows a PHP bug in older SabreDAV versions and information for mod_security problems)
- [0 byte files](#) (Reasons for empty files on the server)
- [Clients](#) (A comprehensive list of WebDAV clients, and possible problems with each one)
- [Finder, OS X's built-in WebDAV client](#) (Describes problems with Finder on various Web servers)

There is also a well maintained FAQ thread available at the [ownCloud Forums](#) which contains various additional information about WebDAV problems.

Error 0x80070043 “The network name cannot be found.” while adding a network drive

The windows native WebDAV client might fail with the following error message:

```
Error 0x80070043 "The network name cannot be found." while adding a network drive
```

A known workaround for this issue is to update your web server configuration.

Apache

You need to add the following rule set to your main web server or virtual host configuration, or the `.htaccess` file in your document root.

```
# Fixes Windows WebDav client error 0x80070043 "The network name cannot be found."
RewriteEngine On
RewriteCond %{HTTP_USER_AGENT} ^ (DavClnt) $
RewriteCond %{REQUEST_METHOD} ^ (OPTIONS) $
RewriteRule .* - [R=401,L]
```

8.1.7 Troubleshooting Contacts & Calendar

Service discovery

Some clients - especially on iOS/Mac OS X - have problems finding the proper sync URL, even when explicitly configured to use it.

If you want to use CalDAV or CardDAV clients together with ownCloud it is important to have a correct working setup of the following URLs:

```
https://example.com/.well-known/carddav
https://example.com/.well-known/caldav
```

Those need to be redirecting your clients to the correct DAV endpoints. If running ownCloud at the document root of your Web server the correct URL is:

```
https://example.com/remote.php/dav
```

and if running in a subfolder like owncloud:

```
https://example.com/owncloud/remote.php/dav
```

For the first case the `.htaccess` file shipped with ownCloud should do this work for your when running Apache. You only need to make sure that your Web server is using this file.

If your ownCloud instance is installed in a subfolder called `owncloud` and you're running Apache create or edit the `.htaccess` file within the document root of your Web server and add the following lines:

```
Redirect 301 /.well-known/carddav /owncloud/remote.php/dav
Redirect 301 /.well-known/caldav /owncloud/remote.php/dav
```

Now change the URL in the client settings to just use:

```
https://example.com
```

instead of e.g.

```
https://example.com/owncloud/remote.php/dav/principals/username.
```

There are also several techniques to remedy this, which are described extensively at the [Sabre DAV website](#).

Unable to update Contacts or Events

If you get an error like:

```
PATCH https://example.com/remote.php/dav HTTP/1.0 501 Not Implemented
```

it is likely caused by one of the following reasons:

Using Pound reverse-proxy/load balancer As of writing this Pound doesn't support the HTTP/1.1 verb. Pound is easily [patched](#) to support HTTP/1.1.

Misconfigured Web server Your Web server is misconfigured and blocks the needed DAV methods. Please refer to [Troubleshooting WebDAV](#) above for troubleshooting steps.

8.1.8 Client Sync Stalls

One known reason is stray locks. These should expire automatically after an hour. If stray locks don't expire (identified by e.g. repeated `file.txt is locked` and/or `Exception\\\\\\FileLocked` messages in your `data/owncloud.log`), make sure that you are running system cron and not Ajax cron (See *Background Jobs*). See <https://github.com/owncloud/core/issues/22116> and <https://central.owncloud.org/t/file-is-locked-how-to-unlock/985> for some discussion and additional info of this issue.

8.1.9 Other issues

Some services like *Cloudflare* can cause issues by minimizing JavaScript and loading it only when needed. When having issues like a not working login button or creating new users make sure to disable such services first.

8.2 Code Signing

ownCloud supports code signing for the core releases, and for ownCloud applications. Code signing gives our users an additional layer of security by ensuring that nobody other than authorized persons can push updates.

It also ensures that all upgrades have been executed properly, so that no files are left behind, and all old files are properly replaced. In the past, invalid updates were a significant source of errors when updating ownCloud.

8.2.1 FAQ

Why Did ownCloud Add Code Signing?

By supporting Code Signing we add another layer of security by ensuring that nobody other than authorized persons can push updates for applications, and ensuring proper upgrades.

Do We Lock Down ownCloud?

The ownCloud project is open source and always will be. We do not want to make it more difficult for our users to run ownCloud. Any code signing errors on upgrades will not prevent ownCloud from running, but will display a warning on the Admin page. For applications that are not tagged “Official” the code signing process is optional.

Not Open Source Anymore?

The ownCloud project is open source and always will be. The code signing process is optional, though highly recommended. The code check for the core parts of ownCloud is enabled when the ownCloud release version branch has been set to stable.

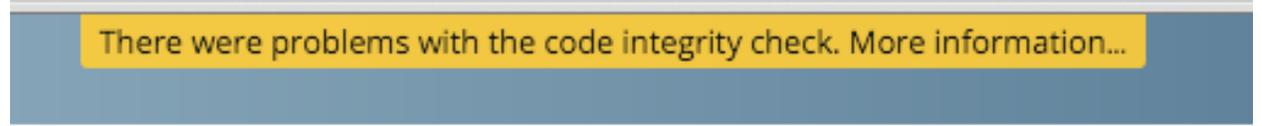
For custom distributions of ownCloud it is recommended to change the release version branch in `version.php` to something else than “stable”.

Is Code Signing Mandatory For Apps?

Code signing is optional for all third-party applications.

8.2.2 Fixing Invalid Code Integrity Messages

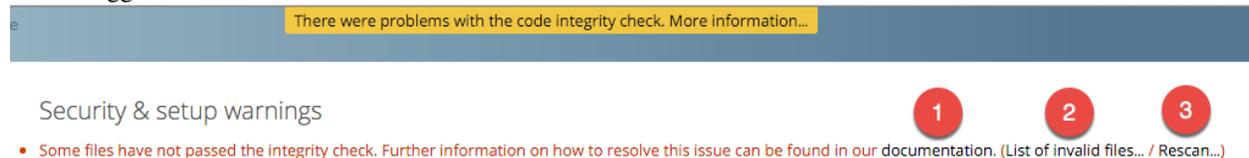
A code integrity error message (“There were problems with the code integrity check. More information...”) appears in a yellow banner at the top of your ownCloud Web interface:



Note: The yellow banner is only shown for admin users.

Clicking on this link will take you to your ownCloud admin page, which provides the following options:

1. Link to this documentation entry.
2. Show a list of invalid files.
3. Trigger a rescan.



To debug issues caused by the code integrity check click on “List of invalid files...”, and you will be shown a text document listing the different issues. The content of the file will look similar to the following example:

```
Technical information
=====
```

```
The following list covers which files have failed the integrity check. Please read
the previous linked documentation to learn more about the errors and how to fix
them.
```

```
Results
=====
```

```
- core
  - INVALID_HASH
    - /index.php
    - /version.php
  - EXTRA_FILE
    - /test.php
- calendar
  - EXCEPTION
    - OC\IntegrityCheck\Exceptions\InvalidSignatureException
    - Signature data not found.
- tasks
  - EXCEPTION
    - OC\IntegrityCheck\Exceptions\InvalidSignatureException
    - Certificate has been revoked.
```

```
Raw output
=====
```

```
Array
(
  [core] => Array
```

```

(
  [INVALID_HASH] => Array
    (
      [/index.php] => Array
        (
          [expected] =>
            f1c5e2630d784bc9cb02d5a28f55d6f24d06dae2a0fee685f3
            c2521b050955d9d452769f61454c9ddfa9c308146ade10546c
            fa829794448eaffbc9a04a29d216
          [current] =>
            ce08bf30bcbb879a18b49239a9bec6b8702f52452f88a9d321
            42cad8d2494d5735e6bfa0d8642b2762c62ca5be49f9bf4ec2
            31d4a230559d4f3e2c471d3ea094
        )

      [/version.php] => Array
        (
          [expected] =>
            c5a03bacae8dedf8b239997901ba1fffd2fe51271d13a00cc4
            b34b09cca5176397a89fc27381cbb1f72855fa18b69b6f87d7
            d5685c3b45aee373b09be54742ea
          [current] =>
            88a3a92c11db91de1ac3be0e1c87f862c95ba6ffaaaa3f2c3
            b8f682187c66f07af3a3b557a868342ef4a271218fe1c1e300
            c478e6c156c5955ed53c40d06585
        )
      )
    )

  [EXTRA_FILE] => Array
    (
      [/test.php] => Array
        (
          [expected] =>
          [current] =>
            09563164f9904a837f9ca0b5f626db56c838e5098e0ccc1d8b
            935f68fa03a25c5ec6f6b2d9e44a868e8b85764dafd1605522
            b4af8db0ae269d73432e9a01e63a
        )
      )
    )

)

[calendar] => Array
(
  [EXCEPTION] => Array
    (
      [class] => OC\IntegrityCheck\Exceptions\InvalidSignature
      Exception
      [message] => Signature data not found.
    )
  )

)

[tasks] => Array
(
  [EXCEPTION] => Array
    (

```

```
        [class] => OC\IntegrityCheck\Exceptions\InvalidSignatureException
        [message] => Certificate has been revoked.
    )
)
)
```

In above error output it can be seen that:

1. In the ownCloud core (that is, the ownCloud server itself) the files “index.php” and “version.php” do have the wrong version.
2. In the ownCloud core the unrequired extra file “/test.php” has been found.
3. It was not possible to verify the signature of the calendar application.
4. The certificate of the task application was revoked.

You have to do the following steps to solve this:

1. Upload the correct “index.php” and “version.php” files from e.g. the archive of your ownCloud version.
2. Delete the “test.php” file.
3. Contact the developer of the application. A new version of the app containing a valid signature file needs to be released.
4. Contact the developer of the application. A new version of the app signed with a valid signature needs to be released.

For other means on how to receive support please take a look at <https://owncloud.org/support/>. After fixing these problems verify by clicking “Rescan...”.

Note: When using a FTP client to upload those files make sure it is using the Binary transfer mode instead of the ASCII transfer mode.

8.2.3 Rescans

Rescans are triggered at installation, and by updates. You may run scans manually with the `occ` command. The first command scans the ownCloud core files, and the second command scans the named app. There is not yet a command to manually scan all apps:

```
occ integrity:check-core
occ integrity:check-app $appid
```

See *Using occ core commands* to learn more about using `occ`.

8.2.4 Errors

Warning: Please don't modify the mentioned `signature.json` itself.

The following errors can be encountered when trying to verify a code signature.

- `INVALID_HASH`
 - The file has a different hash than specified within `signature.json`. This usually happens when the file has been modified after writing the signature data.

- MISSING_FILE
 - The file cannot be found but has been specified within `signature.json`. Either a required file has been left out, or `signature.json` needs to be edited.
- EXTRA_FILE
 - The file does not exist in `signature.json`. This usually happens when a file has been removed and `signature.json` has not been updated. It also happens if you have placed additional files in your ownCloud installation folder.
- EXCEPTION
 - Another exception has prevented the code verification. There are currently these following exceptions:
 - * Signature data not found.
 - The app has mandatory code signing enforced but no `signature.json` file has been found in its `appinfo` folder.
 - * Certificate is not valid.
 - The certificate has not been issued by the official ownCloud Code Signing Root Authority.
 - * Certificate is not valid for required scope. (Requested: %s, current: %s)
 - The certificate is not valid for the defined application. Certificates are only valid for the defined app identifier and cannot be used for others.
 - * Signature could not get verified.
 - There was a problem with verifying the signature of `signature.json`.
 - * Certificate has been revoked.
 - The certificate which was used to sign the application was revoked.

8.3 Impersonating Users

Sometimes you may need to use your ownCloud installation as another user, whether to help users debug an issue or to get a better understanding of what they see when they use their ownCloud account. The ability to do so is a feature delivered via an ownCloud app called [Impersonate](#).

Note: This functionality is available only to administrators.

8.3.1 Impersonating a User

When installed, you can then impersonate users; in effect, you will be logged in as said user. To do so, go to the Users list, where you will now see a new column available called “**Impersonate**”, as in the screenshot below.

Username	Password	Groups	Create	
Username	Impersonate	Full Name	Password	Groups
 admin		admin	admin
 matthew_setter_gmail_cor		matthew	guest_app
 settermjd		ettermjd	share1, share2, share3, sha.
 share1		hare1	no group
 share2		hare2	no group

Click the gray head icon next to the user that you want to impersonate. Doing so will log you in as that user, temporarily pausing your current session. You will see a notification at the top of the page that confirms you're now logged in as (or impersonating) that user.

Logged in as settermjd

> +

Name ▲


Documents

 share1


Photos



Anything that you see until you log out will be what that user would see.

8.3.2 Ending an Impersonation

When you're ready to stop impersonating the user, log out and you will return to your normal user session.

8.3.3 Restrict Impersonation to Groups & Group administrators

As a security measure, the application lets ownCloud administrators restrict the ability to impersonate users to administrators of specific groups. When enabled and configured, only a group's administrator can impersonate members of their group.

For example, if an ownCloud administrator restricts user impersonation only to the group: 'group1', then **only** 'group1's administrators can impersonate users belonging to 'group1'. No other users can impersonate other users.

Note: ownCloud administrators can always impersonate all users of an ownCloud instance when the application is installed.

To enable this option, in the administrator settings panel (administrator -> Settings -> Admin) in the “User Authentication” section, you’ll see a section titled: “**Impersonate Settings**”; which you can see below.

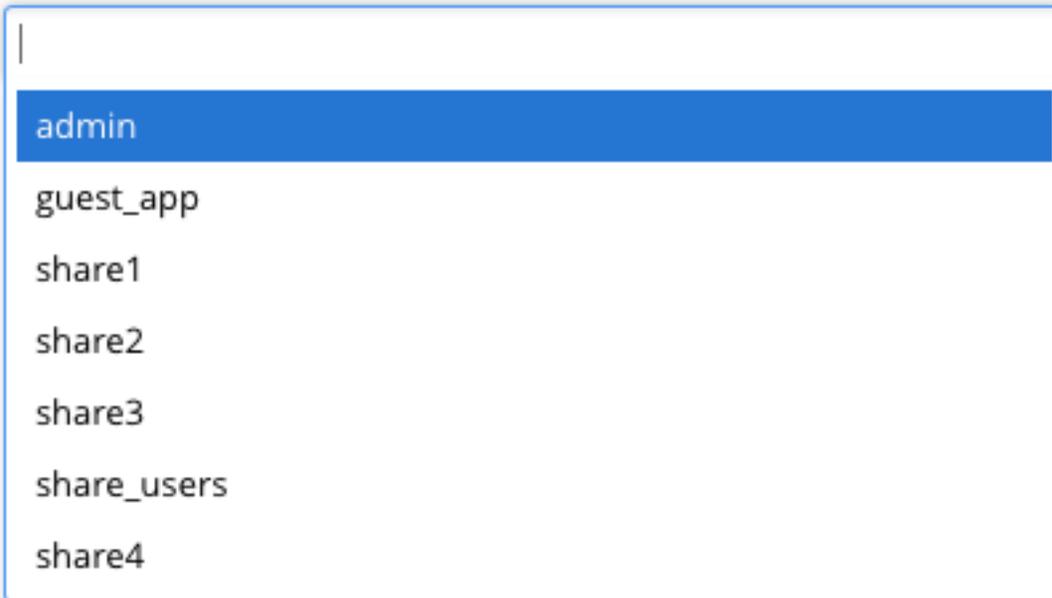
Impersonate Settings

Allow group admins to impersonate users from these groups

Check the checkbox under that, and a textbox will appear. If you click in the textbox, you will see a list of available groups on your ownCloud installation. As you type, the list will filter down to only ones that match the text entered, as you can see below.

Impersonate Settings

Allow group admins to impersonate users from these groups



A screenshot of the 'Impersonate Settings' section in the ownCloud administrator interface. The checkbox 'Allow group admins to impersonate users from these groups' is checked. Below it is a text input field with a dropdown menu open, showing a list of available groups. The groups listed are: admin, guest_app, share1, share2, share3, share_users, and share4. The 'admin' group is currently selected and highlighted in blue.

Choose one or more groups from the list, and they will be added to the textbox.

ENTERPRISE FEATURES

9.1 Installation

9.1.1 Installing & Upgrading ownCloud Enterprise Edition

The recommended method for installing and maintaining your ownCloud Enterprise edition is with your Linux package manager. Configure your package manager to use the ownCloud Enterprise repository, import the signing key, and then install and update ownCloud packages like any other software package.

Please refer to the `README - ownCloud Package Installation.txt` document in your account at [Customer.owncloud.com](https://customer.owncloud.com) account for instructions on setting up your Linux package manager.

After you have completed your initial installation of ownCloud as detailed in the README, follow the instructions in *The Installation Wizard* to finish setting up ownCloud.

To upgrade your Enterprise server, refer to *How to Upgrade Your ownCloud Server*.

Manual Installation

Download the ownCloud archive from your account at <https://customer.owncloud.com/owncloud>, then follow the instructions at *Manual Installation on Linux*.

SELinux

Linux distributions that use SELinux need to take some extra steps so that ownCloud will operate correctly under SELinux. Please see *SELinux Configuration* for some recommended configurations.

License Keys

Introduction

You'll need to install a license key to use ownCloud Enterprise Edition. There are two types of license keys: one is a free 30-day trial key. The other is a full license key for Enterprise customers.

You can [download and try ownCloud Enterprise for 30 days for free](#), which auto-generates a free 30-day key. When this key expires your ownCloud installation is not removed, so when you become an Enterprise customer you can enter your new key to regain access. See [How to Buy ownCloud](#) for sales and contact information.

Configuration

Once you get your Enterprise license key, it needs to be copied to your ownCloud configuration file, `config/config.php` file like this example:

```
'license-key' => 'test-20150101-XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX-YYYYYY',
```

Each running instance of ownCloud requires a license key. Keys will work across upgrades without issue, so new keys will not be required when you upgrade your ownCloud Enterprise to a new version.

Supported ownCloud Enterprise Edition Apps

See *Supported Apps in ownCloud* for a list of supported apps.

Note: 3rd party and unsupported apps must be disabled before performing a system upgrade. Then install the upgraded versions, and after the upgrade is complete re-enable them.

9.1.2 Oracle Database Setup

This document will cover the setup and preparation of the ownCloud server to support the use of Oracle as a backend database.

Outline of Steps

This document will cover the following steps:

- Setup of the ownCloud user in Oracle: This involves setting up a user space in Oracle for setting up the ownCloud database.
- Installing the Oracle Instant Client on the Web server (facilitating the connection to the Oracle Database).
- Compiling and installing the Oracle PHP Plugin `oci8` module
- Pointing ownCloud at the Oracle database in the initial setup process

The document assumes that you already have your Oracle instance running, and have provisioned the needed resources. It also assumes that you have installed ownCloud with all of the prerequisites.

Configuring Oracle

Setting up the User Space for ownCloud

Step one, if it has not already been completed by your DBA (DataBase Administrator), provision a user space on the Oracle instance for ownCloud. This can be done by logging in as a DBA and running the script below:

```
CREATE USER owncloud IDENTIFIED BY password;  
ALTER USER owncloud DEFAULT TABLESPACE users TEMPORARY TABLESPACE temp QUOTA unlimited ON users;  
GRANT create session, create table, create procedure, create sequence, create trigger, create view, o
```

Substitute an actual password for `password`. Items like *TableSpace*, *Quota* etc., will be determined by your DBA (database administrator).

Add OCI8 Client Packages

Installation of the OCI8 client is dependent on your distribution. Given that, please use the relevant section below to find the relevant instructions to install the client.

Ubuntu If you're using Ubuntu, we recommend that you use *this very thorough guide* from the Ubuntu Community Wiki to install the OCI8 extension.

Note: This *should* work for other Debian-based distributions, however your mileage may vary.

RedHat / Centos / Fedora To install *the OCI8 extension* on a RedHat-based distribution, you first need to download two Oracle Instant Client packages:

- Instant Client Package - Basic (oracle-instantclient12.2-basic-12.2.0.1.0-1.x86_64.rpm)
- Instant Client Package - SDK (oracle-instantclient12.2-devel-12.2.0.1.0-1.x86_64.rpm)

Then, to install them, use the following commands:

```
rpm --install oracle-instantclient12.2-basic-12.2.0.1.0-1.x86_64.rpm \
  oracle-instantclient12.2-devel-12.2.0.1.0-1.x86_64.rpm
```

Install the OCI8 PHP Extension

With the Oracle packages installed you're now ready to install PHP's OCI8 extension.

Note: Provide: `instantclient, /usr/lib/oracle/12.2/client64/lib` when requested, or let it auto-detect the location (if possible).

```
pecl install oci8
```

With the extension installed, you now need to configure it, by creating a configuration file for it. You can do so using the command below, substituting `FILE_PATH` with one from the list below the command.

```
cat << EOF > FILE_PATH
; Oracle Instant Client Shared Object extension
extension=oci8.so
EOF
```

Configuration File Paths

	PHP Version	Filename
Debian & Ubuntu	5.6	/etc/php/5.6/apache2/conf.d/20-oci.ini
	7.0	/etc/php/7.0/apache2/conf.d/20-oci.ini
	7.1	/etc/php/7.1/apache2/conf.d/20-oci.ini

	PHP Version	Filename
RedHat, Centos, & Fedora	5.6	/etc/opt/rh/rh-php56/php.d/20-oci8.ini
	7.0	/etc/opt/rh/rh-php70/php.d/20-oci8.ini

Validating the Extension

With all that done, confirm that it's been installed and available in your PHP distribution, run the following command:

```
php -m | grep -i oci8
```

When the process has completed, assuming that you don't encounter any errors, restart Apache and the extension is ready to use.

Configure ownCloud

The next step is to configure the ownCloud instance to point to the Oracle Database, again this document assumes that ownCloud has previously been installed.

Configuration Wizard

Create an admin account

👤	Username
⋮	Password 👁️

Advanced ▼

Data folder

/var/www/owncloud/data

Configure the database
Oracle will be used.

Database user
Database password
Database name
Database tablespace
localhost

Database user This is the user space created in step 2.1. In our Example this would be owncloud.

Database password Again this is defined in the script from section 2.1 above, or pre-configured and provided to you by your DBA.

Database Name Represents the database or the service that has been pre-configured on the TSN Listener on the Database Server. This should also be provided by the DBA. In this example, the default setup in the Oracle install was orcl (there is a TSN Listener entry for orcl on our database server).

This is not like setting up with MySQL or SQL Server, where a database based on the name you give is created. The oci8 code will call this specific service and it must be active on the TSN Listener on your Oracle Database server.

Database Table Space Provided by the DBA. In this example the users table space (as is seen in the user creation script above), was used.

Configuration File

Assuming all of the steps have been followed to completion, the first run wizard should complete successfully, and an operating instance of ownCloud should appear.

The configuration file should look something like this:

```
<?php
$CONFIG = [
    'instanceid' => 'abcdefgh',
    'passwordsalt' => '01234567890123456789',
    'datadirectory' => '/var/data',
    'dbtype' => 'oci',
    'version' => '8.2.x.y',
    'dbname' => 'orcl',
    'dbhost' => '192.168.1.57',
    'dbtableprefix' => 'oc_',
    'dbuser' => 'owncloud1',
    'dbpassword' => '*****',
    'installed' => true,
];
```

Useful SQL Commands

Is my Database Reachable?

On the machine where your Oracle database is installed, type:

```
sqlplus username
```

```
SQL> select * from v$version;
```

```
BANNER
```

```
-----
Oracle Database 11g Express Edition Release 11.2.0.2.0 - 64bit Production
PL/SQL Release 11.2.0.2.0 - Production
CORE 11.2.0.2.0 Production
TNS for Linux: Version 11.2.0.2.0 - Production
NLSRTL Version 11.2.0.2.0 - Production
```

```
SQL> exit
```

Show Database Users:

```
Oracle      : SELECT * FROM all_users;
```

Show available Databases:

```
Oracle      : SELECT name FROM v$databases; (requires DBA privileges)
```

Show ownCloud Tables in Database:

```
Oracle      : SELECT table_name FROM user_tables;
```

Quit Database:

```
Oracle      : quit
```

9.2 Firewall Configuration

9.2.1 File Firewall

The File Firewall GUI enables you to manage firewall rule sets. You can find it in your ownCloud admin page, under Admin -> Security. The File Firewall lets you control access and sharing in fine detail, by creating rules for allowing or denying access restrictions based on: *group, upload size, client devices, IP address, time of day*, as well as many more criteria. In addition to these restriction options, the File Firewall app also supports rules based on [regular expressions](#).

How the File Firewall Works

Each firewall rule set consists of one or more conditions. If a request matches all of the conditions, in at least one rule set, then the request is blocked by the firewall. Otherwise, the request is allowed by the firewall.

Note: The File Firewall app cannot lock out administrators from the web interface when rules are misconfigured.

Using the File Firewall

Figure 1 shows an empty firewall configuration panel. Set your logging level to **Blocked Requests Only** for debugging, and create a new rule set by clicking the **Add Group** button. After setting up your rules you must click the **Save Rules** button.

Figure 2 shows two rules. The first rule, **No Support outside office hours**, prevents members of the support group from logging into the ownCloud Web interface from 5pm-9am, and also blocks client syncing. The second rule prevents members of the “qa-team” group from accessing the Web UI from IP addresses that are outside of the local network.

All other users are not affected, and can log in anytime from anywhere.

Available Conditions

User Group The user (is/is not) a member of the selected group.

User Agent The User-Agent of the request (matches/does not match) the given string.

File Firewall

Requests are checked against all groups of rules that are defined below. A request is blocked when at least one group matches the request. A group matches a request when all rule conditions in the group evaluate to true.

The screenshot shows the File Firewall configuration interface. At the top, there is a text input field labeled 'Group Name'. Below it is a large container for rules, which currently contains a single rule represented by a dashed line in a dropdown menu and a 'Delete' button. At the bottom of this container are three buttons: '+ Add rule', '+ Add group', and 'x Delete'. Below the rule container is a 'Logging' section with a 'Save Rules' button and a dropdown menu currently set to 'Blocked Requests Only'.

Figure 9.1: Figure 1: Empty File Firewall configuration panel

User Device A shortcut for matching all known (android | ios | desktop) sync clients by their User Agent string.

Request Time The time of the request (has to must not) be in a single range from beginning time to end time.

Request URL The **full page URL** (has to must not) (match|contain|begin with|end) with a given string.

Request Type The request (is|is not) a (WebDAV|public share link|other) request.

Request IP Range (IPv4) and IP Range (IPv6) The request's REMOTE_ADDR header (is|is not) matching the given IP range.

File Size Upload When a file is uploaded the size has to be (less|less or equal|greater|greater or equal) to the given size.

File Mimetype Upload When a file is uploaded the mimetype (is|is not|begins with|does not begin with|ends with|does not end with) the given string.

System File Tag One of the parent folders or the file itself (is|is not) tagged with a System tag.

Regular Expression The File Firewall supports regular expressions, allowing you to create custom rules using the following conditions:

- IP Range (IPv4)
- IP Range (IPv6)
- User agent

File Firewall

Requests are checked against all groups of rules that are defined below. A request is blocked when at least one group matches the request. A group matches a request when all rule conditions in the group evaluate to true.

No support outside of:

User Group is support ✕ Delete

Request Time between 05:00 pm +0545 , 09:00 am +0545 ✕ Delete

+ Add rule + Add group ✕ Delete

No QA outside of the:

User Group is qa-team ✕ Delete

IP Range (IPv4) is not 192.168.1.0/24 ✕ Delete

+ Add rule + Add group ✕ Delete

Logging

Save Rules
Blocked Requests Only ▼

Figure 9.2: Figure 2: Two example rules that restrict logins per user group

- User group
- Request URL

You can combine multiple rules into one rule, e.g., if a rule applies to both the support and the qa-team you could write your rule like this:

```
Regular Expression > ^(support|qa-team)$ > is > User group
```

Warning: We do not recommend modifying the configuration values directly in your `config.php`. These use JSON encoding, so the values are difficult to read and a single typo will break all of your rules.

Controlling Access to Folders

The easiest way to block access to a folder, starting with ownCloud 9.0, is to use a system tag. A new rule type was added which allows you to block access to files and folders, where at least one of the parents has a given tag.

Now you just need to add the tag to the folder or file, and then block the tag with the File Firewall. This example blocks access to any folder with the tag “Confidential” from outside access.

Block by System Tag:

```
System file tag: is "Confidential"
IP Range (IPv4): is not "192.168.1.0/24"
```

File Firewall

Requests are checked against all groups of rules that are defined below. A request is blocked when at least one group matches the request. A group matches a request when all rule conditions in the group evaluate to true.

Block confidential file

System file tag is Confidential ✕ Delete

IP Range (IPv4) is not 192.168.1.0/24 ✕ Delete

+ Add rule + Add group ✕ Delete

Logging

Firewall logging can be set to **Off**, **Blocked Requests Only** or **All Requests**

Off The firewall blocks requests according to the defined rules but does not log any of its actions.

Blocked Requests Only The firewall logs blocked requests to the system log at **warning** level. To see these logs, the system log level must be set to a minimum level of **warning**.

All Requests The firewall logs blocked and successful requests to the system log at **warning** and **info** levels respectively. To see all these logs, the system log level must be set to a minimum level of **info**.

Note: Logging all requests can generate a large amount of log data. It is recommended to only select all requests for short-term checking of rule settings.

Custom Configuration for Branded Clients

If you are using *branded ownCloud clients*, you may define `firewall.branded_clients` in your `config.php` to identify your branded clients in the firewall “**User Device**” rule.

The configuration is a User-Agent => Device map. Device must be one of the following:

- android
- android_branded
- ios
- ios_branded
- desktop
- desktop_branded

The User-Agent is always compared all lowercase. By default the agent is compared with `equals`. When a trailing or leading asterisk, `*`, is found, the agent is compared with `starts with` or `ends with`. If the agent has both a leading and a trailing `*`, the string must appear anywhere. For technical reasons the User-Agent string must be at least 4 characters, including wildcards. When you build your branded client you have the option to create a custom User Agent.

In this example configuration you need to replace the example User Agent strings, for example `'android_branded'`, with your own User Agent strings:

```
// config.php

'firewall.branded_clients' => array(
    'my ownbrander android user agent string' => 'android_branded',
    'my ownbrander second android user agent string' => 'android_branded',
    'my ownbrander ios user agent string' => 'ios_branded',
    'my ownbrander second ios user agent string' => 'ios_branded',
    'my ownbrander desktop user agent string' => 'desktop_branded',
    'my ownbrander second desktop user agent string' => 'desktop_branded',
),
```

The Web UI dropdown then expands to the following options:

- Android Client - always visible
- iOS Client - always visible
- Desktop Client - always visible
- Android Client (Branded) - visible when at least one `android_branded` is defined
- iOS Client (Branded) - visible when at least one `ios_branded` is defined
- Desktop Client (Branded) - visible when at least one `desktop_branded` is defined
- All branded clients - visible when at least one of `android_branded`, `ios_branded` or `desktop_branded` is defined

- All non-branded clients - visible when at least one of `android_branded`, `ios_branded` or `desktop_branded` is defined
- Others (Browsers, etc.) - always visible

Then these options operate this way:

- The `* Client` options only match `android`, `ios` and `desktop` respectively.
- The `* Client (Branded)` options match the `*_branded` agents equivalent.
- All `branded clients` matches: `android_branded`, `ios_branded` and `desktop_branded`
- All `non-branded clients` matches: `android`, `ios` and `desktop`

9.3 Ransomware Protection

Ransomware is an [ever-present threat](#), both for large enterprises as well as for individuals. Once infected, a whole hard disk (or just parts of it) can become encrypted, leading to unrecoverable data loss.

Once this happens, attackers usually ask victims to pay a ransom, often via cryptocurrencies such as Bitcoin, in exchange for the decryption key required to decrypt their data.

While paying the ransom works in some cases, it is not recommended, as there is no guarantee that the attackers will supply the key after payment is made. To help mitigate such threats and ensure ongoing access to user data, ownCloud provides the Ransomware Protection app.

Important: It is essential to be aware that user data needs to be synchronized with you ownCloud Server using the ownCloud Desktop synchronization client. Data that is not synchronized and stored in ownCloud cannot be protected.

9.3.1 About Ransomware Protection

The app is tasked with *detecting*, *preventing*, and *reverting* anomalies. Anomalies are file operations (including *create*, *update*, *delete*, and *move*) not intentionally conducted by the user. It aims to do so in two ways: *prevention*, and *protection*.

9.3.2 Prevention: Blocking Common Ransomware File Extensions

Like other forms of cyberattack, ransomware has a range of diverse characteristics. On the one hand it makes them hard to detect and on the other it makes them even harder to prevent. Recent ransomware attacks either encrypt a user's files and add a specific file extension to them (e.g., ".crypt"), or they replace the original files with an encrypted copy and add a particular file extension.

File Extension Blacklist

The first line of defense against such threats is a blacklist that blocks write access to file extensions known to originate from ransomware.

Ransomware Protection ships with a [static extension list](#) of around 1,500 file extensions. As new extensions are regularly created, this list also needs to be regularly reviewed and updated. Future releases of Ransomware Protection will include an updated list and the ability to update the list via syncing with [FSRM's API](#) by using `occ`.

Important: Please check the provided ransomware blacklist! It is **strongly recommended** to check the provided

ransomware blacklist to ensure that it fits your needs. In some cases, the patterns might be too generic and result in false positives.

File Blocking

The second line of defense is file blocking. As files are uploaded, they are compared against the file extension blacklist. If a match is found, the upload is denied.

Note: File blocking is always enabled.

Account Locking

The third line of defense is account locking. If a client uploads a file matching a pattern in the ransomware blacklist, the account is locked (set as read-only) for client access (*create*, *change*, *move*, and *delete* operations). Doing this prevents further, malicious, changes.

Following this, clients receive an error (403 Access Forbidden) which notifies the user that the account is locked by Ransomware Protection.

Note: Write access (e.g., moving and deleting files) is still possible for users when they log in with their web browser.

When an account is locked, administrators can unlock the account using the `occ ransomguard:unlock` command. Administrators can also manually lock user accounts, using the `occ ransomguard:lock` command.

Note: When an account is locked, it will still be fully usable from the ownCloud web UI. However, ownCloud clients (as well as other WebDAV clients) will see the account as set to read-only mode.

Users will see a yellow notification banner in the ownCloud web UI directing them to “Personal Settings -> Security” (“*Ransomware detected: Your account is locked (read-only) for client access to protect your data. Click here to unlock.*”), where additional information is displayed and users can unlock their account when ransomware issues are resolved locally.

Note: Locking is enabled by default. If this is not desired, an administrator can disable it in the “Admin -> Security” panel.

9.3.3 Protection: Data Retention and Rollback

While Ransomware Prevention mitigates risks of a range of ransomware attacks, it is not a future-proof solution, because ransomware is becoming ever-more sophisticated. There are known attacks that change file extensions randomly or keep them unchanged which makes them harder to detect.

Ultimately there is a consensus that only one solution can provide future-proof protection from ransomware attacks: retaining data and providing the means to roll back to a particular point in time.

ownCloud Ransomware Protection will, therefore, record all changes on an ownCloud Server and allow administrators to rollback user data to a particular point in time, making use of ownCloud’s integrated Versioning and Trash bin features.

Doing so allows all user data that is synchronized with the server to be rolled back to its state before the attack occurred. A combination of Ransomware prevention and protection reduces risks to a minimum acceptable level.

9.3.4 Other Elements of Ransomware Protection

Name	Command (if applicable)	Description
Ransomware Prevention (Blocker)		First line of defense against ransomware attacks. Ransomware Protection uses a file name pattern blacklist to prevent uploading files that have file extensions associated with ransomware (e.g. ".crypt") thereby preserving the original files on the ownCloud Server.
Ransomguard Scanner	<code>occ ransomguard:scan <timestamp> <user></code>	A command to scan the ownCloud database for changes in order to discover anomalies in a user's account and their origin. It enables an administrator to determine the point in time where undesired actions happened as a prerequisite for restoration.
Ransomguard Restorer	<code>occ ransomguard:restore <timestamp> <user></code>	A command for administrators to revert all operations in a user account that occurred after a certain point in time.
Ransomguard Lock	<code>occ ransomguard:lock <user></code>	Set a user account as read-only for ownCloud and other WebDAV clients. This prevents any further changes to the account.
Ransomguard Unlock	<code>occ ransomguard:unlock <user></code>	Unlock a user account which was set to read-only.

Note: `<timestamp>` must be in the *Linux timestamp format*.

9.3.5 Requirements

Mandatory

1. **File Firewall rule (previous approach for ransomware protection).** If you have configured the File Firewall rule which was provided as a preliminary protection mechanism, please remove it. The functionality (Blocking) is covered by Ransomware Protection in an improved way.
2. **Ransomware Protection.** Ransomware protection needs to be in operation before an attack occurs, as it needs to record file operations to be able to revert them, in case of an attack.
3. **ownCloud Versions App.** Required to restore older file versions. The capabilities of Ransomware Protection depend on its configuration regarding version retention.
4. **ownCloud Trash Bin App.** Required to restore deleted files. The capabilities of Ransomware Protection depend on its configuration regarding trash bin retention.

Optional

1. **Activity app.** For viewing activity logs.

9.3.6 Limitations

- Ransomware Protection works with master-key based storage encryption. With credential-based storage encryption, only Ransomware Prevention (Blocking) works.
- Rollback is not based on snapshots:

- The `trash bin retention policy` may delete files, making them unrecoverable. To avoid this, set `trashbin_retention_obligation` to `disabled`, or choose a conservative policy for trash bin retention. However, please be aware that this may increase storage requirements.
- Trash bin items may be deleted by the user making them unrecoverable by Ransomware Protection => Users need to know this.
- Versions have a built-in “thin-out” policy which makes it possible that required file versions are unrecoverable by Ransomware Protection. To help avoid this, set `versions_retention_obligation` to `disabled` or choose a conservative policy for version retention. Please be aware that this might increase your storage needs.
- A specific version of a file that is needed for rollback might have been manually restored, making this version potentially unrecoverable by Ransomware Protection. Currently, after restoration the restored version *is not a version anymore*, e.g., the version is not present in versioning.
- Contents in secondary storages, such as *Windows network drives*, *Dropbox*, and *Google Drive*, are unrecoverable by Ransomware Protection, because they do not have versioning or trash bin enabled in ownCloud.
- Rolling files forward is not *currently* supported or tested. Therefore it is vital to:
 - Carefully decide the point in time to rollback to.
 - To have proper backups to be able to conduct the rollback again, if necessary.

9.4 File Management

9.4.1 Advanced File Tagging With the Workflow App

The Workflow App provides advanced management of file tagging. The app has three parts: Tag Manager, Automatic Tagging, and Retention.

The Workflow App should be enabled by default (Apps page), and the three configuration modules visible on your ownCloud Admin page.

See [Tagging Files](#) in the ownCloud User manual to learn how to apply and filter tags on files.

Tag Manager

The Tag Manager is for creating new tags, editing existing tags, and deleting tags. Tags may be marked as **Visible**, **Restricted**, or **Invisible**.

Visible means that all users may see, rename, and apply these tags to files and folders.

Restricted means tags are assignable and editable only to the user groups that you select. Other users can filter files by restricted tags, but cannot tag files with them or rename them. The tags are marked (restricted).

Invisible means visible only to ownCloud admins.

Use the **Collaborative tag management** module on your ownCloud admin page to edit and create tags.

This is what your tags look like in the **Tags** view on your files page. Non-admin users will not see invisible tags, but they will see visible and restricted tags.

Collaborative tag management

oldtag ▼

Edit tag

oldtag 

Restricted ▼

- × bluegroup
- × cranberrygroup
- darkgroup
- users

- mehtag
- newtag (invisible)
- oldtag (restricted)

Automatic Tagging

The Automatic Tagging module operates on newly-uploaded files. Create a set of conditions, and then when a file or folder matches those conditions it is automatically tagged. The tag must already have been created with the Tag Manager.

For example, you can assign the invisible tag **iOS Uploads** to all files uploaded from iOS devices. This tag is visible only to admins.

Automatic tagging

Automatically tag newly uploaded files, matching the conditions, with the following tags:

iOS files  

Conditions:

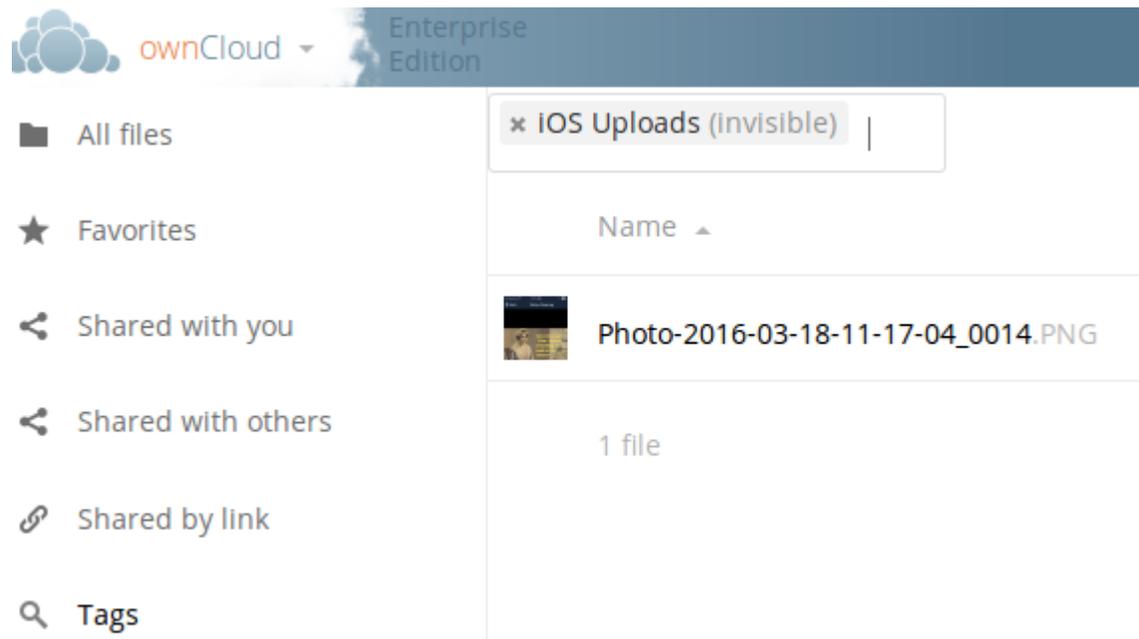
Device type is **iOS Client**

Add tags:

iOS Uploads (invisible)

[+ Add new rule](#)

When files with this tag are shared with you, you can view them with the Tags filter on the Files page.



The screenshot shows the ownCloud Enterprise Edition interface. On the left, a navigation menu includes 'All files', 'Favorites', 'Shared with you', 'Shared with others', 'Shared by link', and 'Tags'. The 'Tags' option is selected. The main content area shows a filter for 'x iOS Uploads (invisible)'. Below the filter, there is a table with one file listed: 'Photo-2016-03-18-11-17-04_0014.PNG'. The table has a 'Name' column header and a '1 file' summary below the list.

Automatic Tagging is especially useful with the Retention module.

Retention

The Retention module is your housecleaning power tool, because it automatically deletes files after a time period that you specify. Select which tag to set a time limit on, and then set your time limit. File age is calculated from the file mtime (modification time).

Retention periods

Delete files tagged with the following tags after the given time:

IOS Uploads (invisible)

24

Days



+ Add new rule

For best performance, retention tags should be applied high in your file hierarchy. If subfolders have the same tags as their parent folders, their tags must also be processed, so it will take a little longer.

Retention Engines

There are two retention engines that further allow you to fine-tune your retention settings: **TagBasedRetention** and **UserBasedRetention**. **TagBasedRetention** is the default.

TagBasedRetention: This checks files that have a particular tag assigned. Then it checks (depth-first) the children of the tagged item, before continuing with the other tagged items. Children that have already been checked will not be checked a second time.

This is optimised for processing smaller numbers of files that have multiple retention tags.

UserBasedRetention: Examines files per user. It first iterates over all files and folders (siblings first), then examines the tags for those items and checks their respective retention periods. This is optimised for many files with few retention tags.

To select UserBasedRetention, add this line to your ee.config.php:

```
'workflow.retention_engine' => userbased,
```

9.5 External Storage

9.5.1 Enterprise-Only Authentication Options

In ownCloud 9.0+, there are five authentication backends for external storage mounts:

- Username and password
- Log-in credentials, save in session
- Log-in credentials, save in database
- User entered, store in database
- Global credentials

The first two are common to all editions of ownCloud, and the last three are only in the Enterprise edition. These are available to:

- FTP
- ownCloud
- SFTP
- SMB/CIFS
- WebDAV
- Windows Network Drive

Username and password This is the default; a login entered by the admin when the external mount is created. The login is stored in the database, which allows sharing, and background jobs, such as file scanning, to operate.

Log-in credentials, save in session Credentials are only stored in the session and not captured in the database. Files cannot be shared, as credentials are not stored.

Log-in credentials, save in database Credentials are stored in the database, and files can be shared.

User entered, store in database Users provide their own login credentials, rather than using admin-supplied credentials. User credentials are stored in the database, and files can be shared.

Global credentials Re-usable credentials entered by the admin, files can be shared.

Global credentials are entered in a separate form.

External Storage

Global credentials for external storages

Use the dropdown selector to choose the authentication backend when you create a new external mount.

A screenshot of a dropdown menu with a light gray border. The menu is open, showing five options. The first option, "Username and password", is highlighted with a blue background. The other options are "Log-in credentials, save in session", "Log-in credentials, save in database", "User entered, store in database", and "Global Credentials". The text in the dropdown is black, and the background of the menu is white.

9.5.2 LDAP Home Connector

The LDAP Home Connector App enables you to configure your ownCloud server to display your users' Windows home directories on their Files pages, just like any other folder. Typically, Windows home directories are stored on a network server in a root folder, such as Users, which then contains individual folders for each user.

You must already have the LDAP app enabled and a working LDAP/Active Directory configuration in ownCloud.

Next, configure the root Windows home directory to be mounted on your ownCloud server. Then use the LDAP Home Connector and LDAP app to connect it to ownCloud.

Mount Home Directory

Create an entry in `/etc/fstab` for the remote Windows root home directory mount. Store the credentials to access the home directory in a separate file, for example `/etc/credentials`, with the username and password on separate lines, like this:

```
username=winhomeuser
password=winhomepassword
```

Then add a line like this to `/etc/fstab`, substituting your own server address and filenames:

```
//192.168.1.58/share /mnt/share cifs credentials=/etc/credentials,uid=33,gid=33
```

Configure the LDAP Home Connector

Enable the LDAP Home Connector app. Then go to the LDAP Home Connector form on your ownCloud admin page. In the **Display folder as:** field enter the name as you want it to appear on your users' File pages.

Then in the **Attribute name:** field enter the LDAP attribute name that will contain the home directory. Use any LDAP attribute that is not already in use, then save your changes.

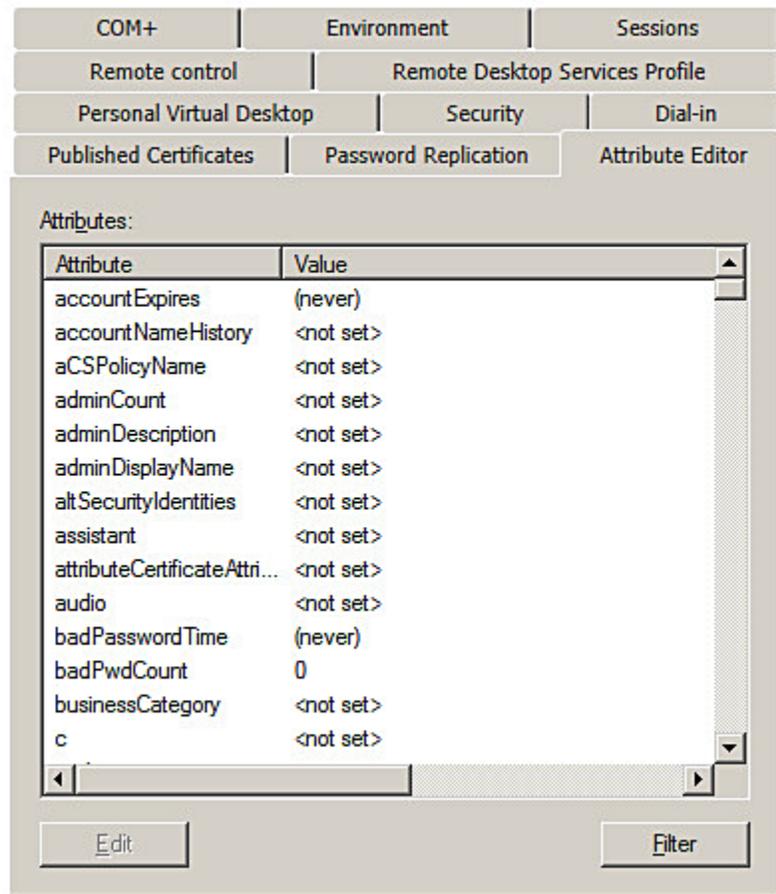
LDAP User Home

Display folder as:

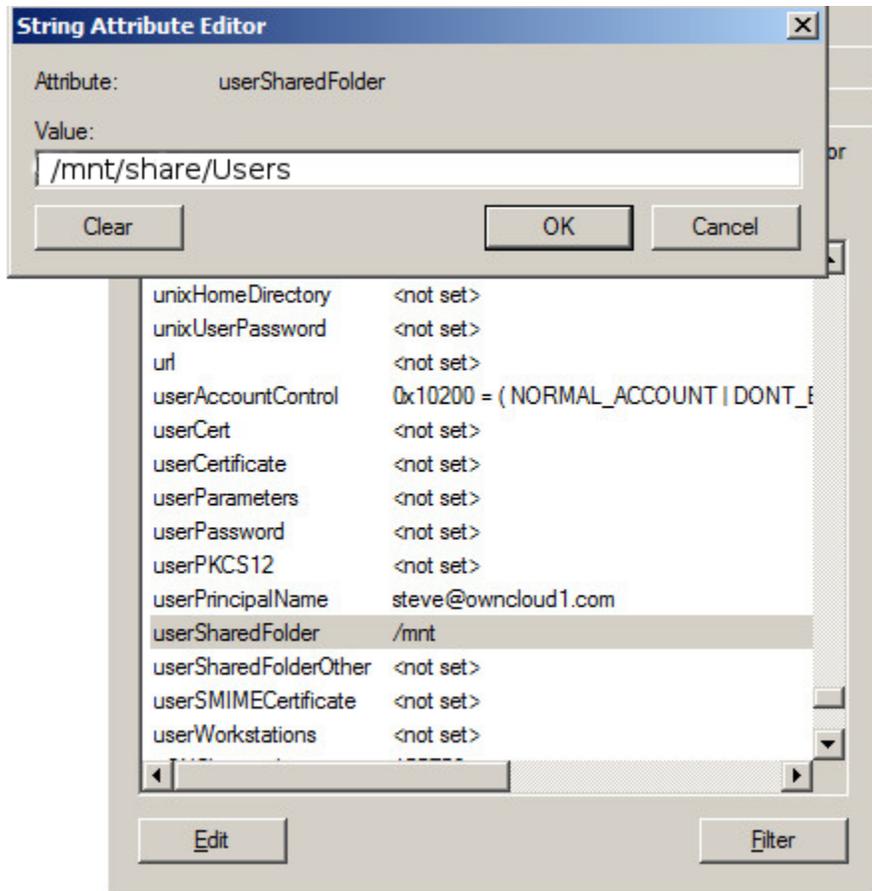
Attribute name:

Configure the LDAP Server

In Active Directory, open the user profile. Scroll to the **Extensions** section and open the **Attribute Editor** tab



Scroll to the attribute being used (UserSharedFolder in this instance), and click **Edit**. Enter the users home directory.



Save your changes, and you are finished.

9.5.3 Configuring SharePoint Integration

Native SharePoint support has been added to the ownCloud Enterprise edition as a secondary storage location for SharePoint 2007, 2010 and 2013. When this is enabled, users can access and sync all of their SharePoint content via ownCloud, whether in the desktop sync, mobile or Web interfaces. Updated files are bi-directionally synced automatically. SharePoint shares are created by the ownCloud admin, and optionally by any users who have SharePoint credentials.

The ownCloud SharePoint plugin uses SharePoint document lists as remote storage folders. ownCloud respects SharePoint access control lists (ACLs), so ownCloud sharing is intentionally disabled for SharePoint mountpoints. This is to preserve SharePoint ACLs and ensure content is properly accessed as per SharePoint rules.

The plugin uses the Simple Object Access Protocol (SOAP) and WebDAV for the uploads and downloads to talk to SharePoint servers. Your ownCloud server must have `php-soap` or `php5-soap` installed. Linux packages and ownCloud appliances will install `php5-soap` as a required dependency.

The supported authentication methods are:

- Basic Auth
- NTLM (Recommended)

Creating a SharePoint Mount

Enable the SharePoint app, and then enter the Admin panel to set up SharePoint connections in the SharePoint Drive Configuration section.

Enter your SharePoint Listing credentials. These credentials are not stored in the database, but are used only during plugin setup to list the Document Libraries available per SharePoint site.

SharePoint Configuration

Listing credentials. These fields are only used to list available SharePoint document list. They are not stored.

administrator

Global credentials. These fields can be used for each of the SharePoint mounts

administrator

Global credentials is optional. If you fill in these fields, these credentials will be used on on all SharePoint mounts where you select: **Use global credentials** as the authentication credentials.

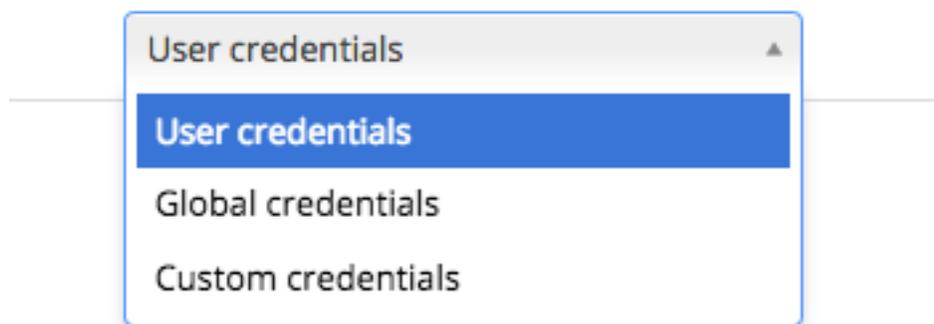
Local Folder Name	Available for	SharePoint Site Url	Document Library
sharepoint1	<input type="text" value="All users"/>	https://example.com	folder1
sharepoint2	<input type="text" value="All users"/>	https://example2.com	folder2

Enter your ownCloud mountpoint in the Local Folder Name column. This is the name of the folder that each user will see on the ownCloud filesystem. You may use an existing folder, or enter a name to create a new mount point

Select who will have access to this mountpoint, by default **All users**, or a user or a group.

Enter your SharePoint server URL, then click the little refresh icon to the left of the Document Library field. If your credentials and URL are correct you'll get a dropdown list of available SharePoint libraries. Select the document library you want to mount.

Authentication credentials



Select which kind of Authentication credentials you want to use for this mountpoint. If you select **Custom credentials** you will have to enter the the credentials on this line. Otherwise, the global credentials or the user's own credentials will be used. Click Save, and you're done

Enabling Users

You may allow your users to create their own SharePoint mounts on their Personal pages, and allow sharing on these mounts.

- Allow users to mount their own SharePoint document libraries
- Allow users to share content in SharePoint mount points

Note

Speed up load times by disabling file previews in `config.php`, because the previews are generated by downloading the remote files to a temp file. This means ownCloud will spend a lot of time creating previews for all of your SharePoint content. To disable file previews, add the following line to the ownCloud config file found in `/owncloud/config/config.php`:

```
'enable_previews' => false,
```

Troubleshooting

Unsharing

SharePoint unsharing is handled in the background via Cron. If you remove the sharing option from a SharePoint mount, it will take a little time for the share to be removed, until the Cron job runs.

Logging

Turn on SharePoint app logging by modifying `config/config.php`, setting `sharepoint.logging.enable` to `true`, as in the example below.

```
'sharepoint.logging.enable' => true,
```

Mount Points

Global mount points can't be accessed: You have to fill out your SharePoint credentials as User on the personal settings page, or in the popup menu. These credentials are used to mount all global mount points.

Personal mount points can't be accessed: You have to fill your SharePoint credentials as User on the personal settings page in case your personal mount point doesn't have its own credentials.

A user can't update the credentials: Verify that the correct credentials are configured, and the correct type, either global or custom.

9.5.4 Installing and Configuring the External Storage: Windows Network Drives App

The [External Storage: Windows Network Drives](#) app creates a control panel in your Admin page for seamlessly integrating Windows and Samba/CIFS shared network drives as external storages.

Any Windows file share and Samba servers on Linux and other Unix-type operating systems use the SMB/CIFS file-sharing protocol. The files and directories on the SMB/CIFS server will be visible on your Files page just like your other ownCloud files and folders.

They are labeled with a little four-pane Windows-style icon, and the left pane of your Files page includes a Windows Network Drive filter. Figure 1 shows a new Windows Network Drive share marked with red warnings.

These indicate that ownCloud cannot connect to the share because it requires the user to login, it is not available, or there is an error in the configuration.

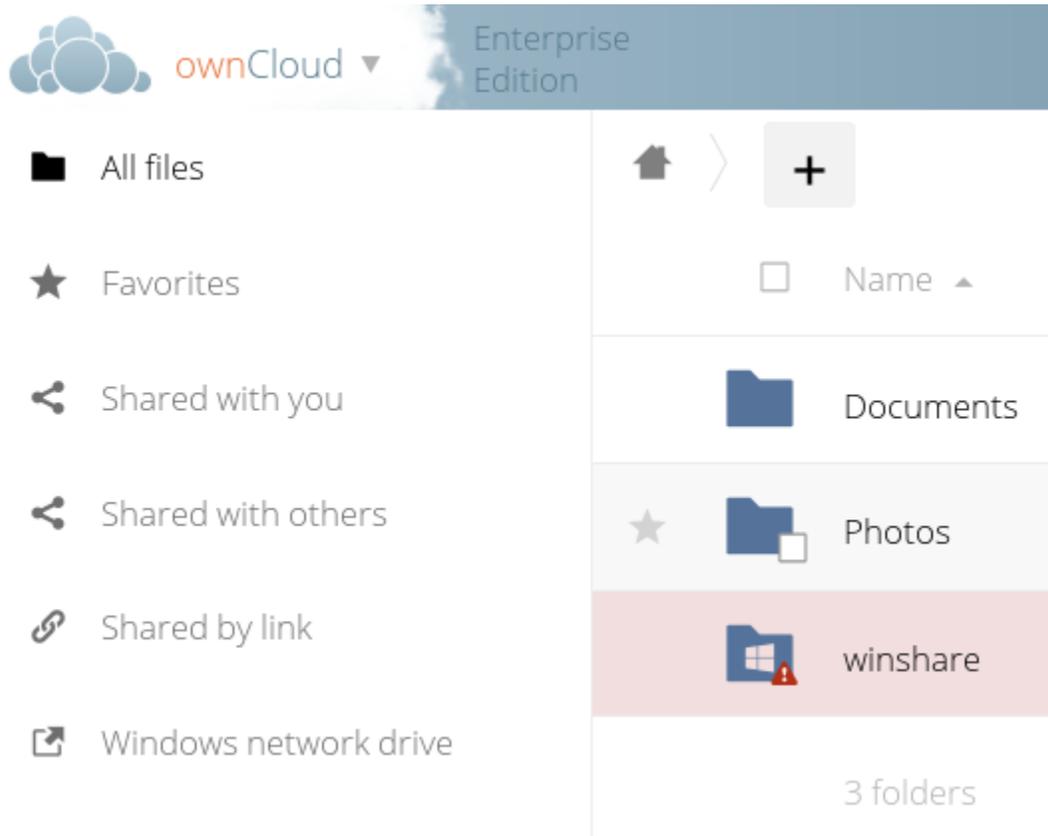


Figure 9.3: Figure 1: Windows Network Drive share on your Files page.

Files are synchronized bi-directionally, and you can create, upload, and delete files and folders. ownCloud server admins can create Windows Network Drive mounts and optionally allow users to set up their own personal Windows Network Drive mounts.

Depending on the authentication method, passwords for each mount are encrypted and stored in the ownCloud database, using a long random secret key stored in `config.php`, which allows ownCloud to access the shares when the users who own the mounts are not logged in. Or, passwords are not stored and available only for the current session, which adds security.

Installation

Install the [External Storage: Windows Network Drives](#) app from the ownCloud Market App or ownCloud Marketplace. For it to work, there are a few dependencies to install.

- A Samba client. This is included in all Linux distributions. On Debian, Ubuntu, and other Debian derivatives it is called `smbclient`. On SUSE, Red Hat, CentOS, and other Red Hat derivatives it is `samba-client`.

- `php-smbclient` (version 0.8.0+). It should be included in most Linux distributions. You can use [eduardok/lib smbclient-php](#), if your distribution does not provide it.
- `which` and `stdbuf`. These should be included in most Linux distributions.

Example

Assuming that your ownCloud installation is on Ubuntu, then the following commands will install the required dependencies:

```
# Install core packages
sudo apt-get update -y
sudo apt-get install -y smbclient php-smbclient coreutils
```

Other method using PECL is:

```
# Install php-smbclient using PECL
pecl install smbclient

# Install it from source
git clone git://github.com/eduardok/lib smbclient-php.git
cd lib smbclient-php ; phpize
./configure
make
sudo make install
```

Note: Regardless of the method you use, remember to check if an `smbclient.ini` file exists in `/etc/php/<your php version>/mods-available` and contains the following line:

```
extension="smbclient.so"
```

If so, then make it available via by running the following command:

```
sudo phpenmod -v ALL smbclient
```

Creating a New Share

When you create a new WND share you need three things:

- The login credentials for the share
- The server address, the share name; and
- The folder you want to connect to

Note: **Treat all the parameters as being case-sensitive.** Although some parts of the app might work properly, regardless of case, other parts might have problems if case isn't respected.

1. Enter the ownCloud mount point for your new WND share. This must not be an existing folder.
2. Then select your authentication method; See [Enterprise-Only Authentication Options](#) for complete information on the five available authentication methods.
3. Enter the address of the server that contains the WND share.
4. The Windows share name.

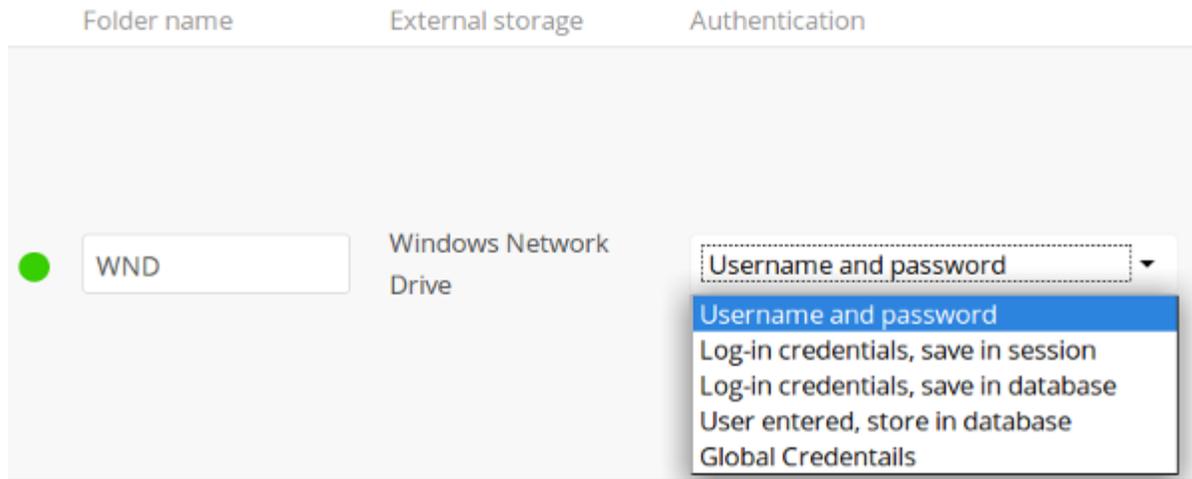


Figure 9.4: Figure 2: WND mountpoint and authorization credentials.

5. The root folder of the share. This is the folder name, or the `$user` variable for user's home directories. Note that the LDAP `Internal Username Attribute` must be set to the `samaccountname` for either the share or the root to work, and the user's home directory needs to match the `samaccountname`. (See *User Authentication with LDAP*.)
6. Login credentials.
7. Select users or groups with access to the share. The default is all users.
8. Click the gear icon for additional mount options. Note that previews are enabled by default, while sharing is not (see figure 2). Sharing is not available for all authorization methods; see *Enterprise-Only Authentication Options*. For large storages with many files, you may want to disable previews, because this can significantly increase performance.

Your changes are saved automatically.

Note: When you create a new mountpoint using Login credentials, you must log out of ownCloud and then log back in so you can access the share. You only have to do this the first time.

Personal WND Mounts

Users create their own WND mounts on their Personal pages. These are created the same way as Admin-created shares. Users have four options for login credentials:

- Username and password
- Log-in credentials, save in session
- Log-in credentials, save in database
- Global credentials

libsmbclient Issues

If your Linux distribution ships with `libsmbclient 3.x`, which is included in the Samba client, you may need to set up the `HOME` variable in Apache to prevent a segmentation fault. If you have `libsmbclient 4.1.6` and

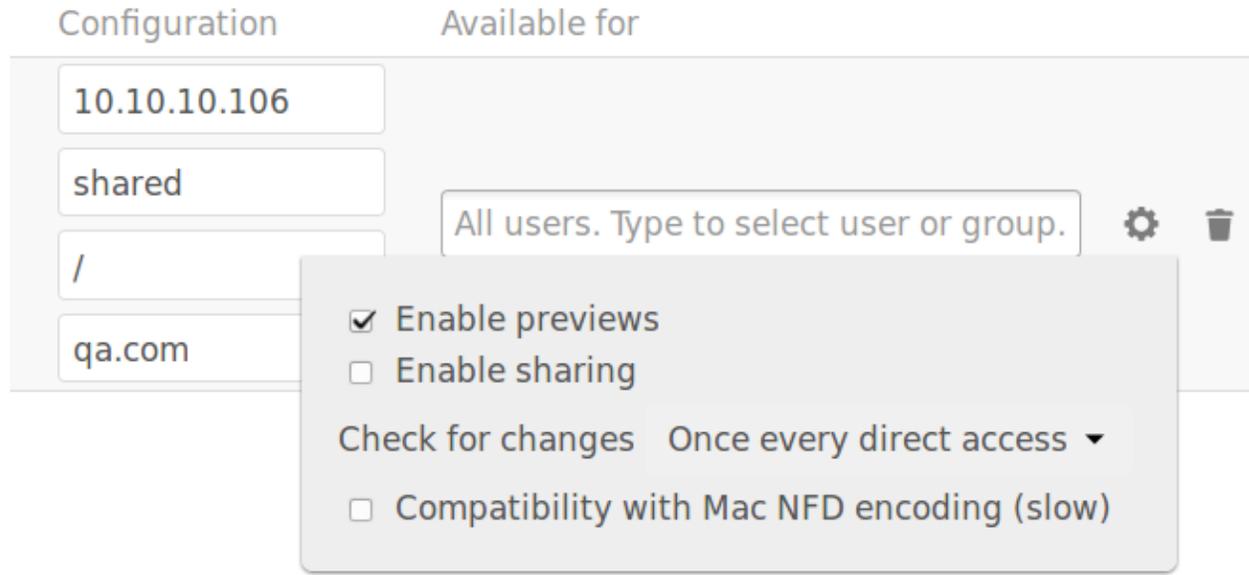


Figure 9.5: Figure 3: WND server, credentials, and additional mount options.

higher it doesn't seem to be an issue, so you won't have to change your HOME variable. To set up the HOME variable on Ubuntu, modify the `/etc/apache2/envvars` file:

```
unset HOME
export HOME=/var/www
```

In Red Hat/CentOS, modify the `/etc/sysconfig/httpd` file and add the following line to set the HOME variable in Apache:

```
export HOME=/usr/share/httpd
```

By default, CentOS has activated SELinux, and the `httpd` process can not make outgoing network connections. This will cause problems with the `curl`, `ldap` and `samba` libraries. You'll need to get around this to make this work. First, check the status:

```
getsebool -a | grep httpd
httpd_can_network_connect --> off
```

Then enable support for network connections:

```
setsebool -P httpd_can_network_connect 1
```

In openSUSE, modify the `/usr/sbin/start_apache2` file:

```
export HOME=/var/lib/apache2
```

Restart Apache, open your ownCloud Admin page and start creating SMB/CIFS mounts.

9.5.5 Windows Network Drive Listener

The SMB protocol supports registering for notifications of file changes on remote Windows SMB storage servers. Notifications are more efficient than polling for changes, as polling requires scanning the whole SMB storage. ownCloud

supports SMB notifications with an `occ` command, `occ wnd:listen`.

Note: The notifier only works with remote storage on Windows servers. It does not work reliably with Linux servers due to technical limitations.

Your `smbclient` version needs to be 4.x, as older versions do not support notifications. The ownCloud server needs to know about changes to files on integrated storage so that the changed files will be synced to the ownCloud server, and to desktop sync clients.

Files changed through the ownCloud Web Interface, or sync clients are automatically updated in the ownCloud file cache, but this is not possible when files are changed directly on remote SMB storage mounts.

To create a new SMB notification, start a listener on your ownCloud server with `occ wnd:listen`. The listener marks changed files, and a background job updates the file metadata.

Windows network drive connections and setup of `occ wnd:listen` often does not always work the first time. If you encounter issues using it, then try the following troubleshooting steps:

1. Check the connection with `smbclient` on the command line of the ownCloud server

Take the example of attempting to connect to the share named *MyData* using `occ wnd:listen`. Running the following command would work:

```
sudo -u www-data ./occ wnd:listen MyHost MyData svc_owncloud password
```

However, running this command would not:

```
sudo -u www-data ./occ wnd:listen MyHost mydata svc_owncloud password
```

Setting Up the WND Listener

The WND listener for ownCloud 10 includes two different commands that need to be executed:

- `wnd:listen`
- `wnd:process-queue`

wnd:listen

This command listens and stores notifications in the database coming from one specific host and share. It is intended to be run as a service. The command requires the host and share, which the listener will listen to, and the Windows/Samba account that will listen. The command does not produce any output by default, unless errors happen.

Note: You can increase the command's verbosity by using `-vvv`. Doing so displays what the listener is doing, including a timestamp and the notifications received.

Note: Although the exact permissions required for the Windows account are unknown, read-only should be enough.

The simplest way to start the `wnd:listen` process manually, perhaps for initial testing, is as follows

```
sudo -u www-data ./occ wnd:listen <host> <share> <username>
```

The password is an optional parameter and you'll be asked for it if you didn't provide it, as in the example above. In order to start the `wnd:listen` without any user interaction, provide the password as the user's 4th parameter, as in the following example:

```
sudo -u www-data ./occ wnd:listen <host> <share> <username> <password>
```

For additional options to provide the password, check *Password Options*

Note that in any case there won't be any processing of the password by default. This means that spaces or newline chars won't be removed unless explicitly told. Use the `--password-trim` option in those cases.

You should be able to run any of those commands, and/or wrap them into a systemd service or any other startup service, so that the `wnd:listen` command is automatically started during boot, if you need it.

wnd:process-queue

This command processes the stored notifications for a given host and share. This process is intended to be run periodically as a Cron job, or via a similar mechanism. The command will process the notifications stored by the `wnd:listen` process, showing only errors by default. If you need more information, increase the verbosity by calling `wnd:process-queue -vvv`.

As a simple example, you can check the following:

```
sudo -u www-data ./occ wnd:process-queue <host> <share>
```

You can run that command, even if there are no notifications to be processed.

As said, you can wrap that command in a Cron job so it's run every 5 minutes for example.

Basic Setup for One ownCloud Server

First, go to the admin settings and set up the required WND mounts. Be aware though, that there are some limitations. These are:

- We need access to the Windows account password for the mounts to update the file cache properly. This means that “*login credentials, saved in session*” won't work with the listener. “*login credentials, saved in DB*” should work and could be the best replacement.
- The `$user` placeholder in the share, such as `//host/$user/path/to/root`, for providing a share which is accessible `per/user` won't work with the listener. This is because the listener won't scale, as you'll need to setup one listener `per/share`. As a result, you'll end up with too many listeners. An alternative is to provide a common share for the users and use the `$user` placeholder in the root, such as `//host/share/$user/folder`.

Second, start the `wnd:listen` process if it's not already started, ideally running it as a service. If it isn't running, no notification are stored. The listener stores the notifications. Any change in the mount point configuration, such as adding or removing new mounts, and logins by new users, won't affect the behavior, so there is no need to restart the listener in those cases.

In case you have several mount point configurations, note that each listener attaches to one host and share. If there are several mount configurations targeting different shares, you'll need to spawn one listener for each. For example, if you have one configuration with `10.0.0.2/share1` and another with `10.0.0.2/share2`, you'll need to spawn 2 listeners, one for the first configuration and another for the second.

Third, run the `wnd:process-queue` periodically, usually via a *Cron job*. The command processes all the stored notifications for a specific host and share. If you have several, you could set up several Cron jobs, one for each host and share with different intervals, depending on the load or update urgency. As a simple example, you could run the command every 2 minutes for one server and every 5 minutes for another.

As said, the command processes all the stored notifications, squeeze them and scan the resulting folders. The process might crash if there are too many notifications, or if it has too many storages to update. The `--chunk-size` option will help by making the command process all the notifications in buckets of that size.

On the one hand the memory usage is reduced, on the other hand there is more network activity. We recommend using the option with a value high enough to process a large number of notifications, but not so large to crash the process. Between 200 and 500 should be fine, and we'll likely process all the notifications in one go.

Password Options

There are several ways to supply a password:

1. Interactively in response to a password prompt.

```
sudo -u www-data ./occ wnd:listen <host> <share> <username>
```

2. Sent as a parameter to the command.

```
sudo -u www-data ./occ wnd:listen <host> <share> <username> <password>
```

3. Read from a file, using the `--password-file` switch to specify the file to read from. Note that the password must be in plain text inside the file, and neither spaces nor newline characters will be removed from the file by default, unless the `--password-trim` option is added. The password file must be readable by the apache user (or www-data)

```
sudo -u www-data ./occ wnd:listen <host> <share> <username> \  
--password-file=/my/secret/password/file
```

```
sudo -u www-data ./occ wnd:listen <host> <share> <username> \  
--password-file=/my/secret/password/file --password-trim
```

Note: If you use the `--password-file` switch, the entire contents of the file will be used for the password, so please be careful with newlines.

Warning: If using `--password-file` make sure that the file is only readable by the apache / www-data user and inaccessible from the web. This prevents tampering or leaking of the information. The password won't be leaked to any other user using `ps`.

4. Using 3rd party software to store and fetch the password. When using this option, the 3rd party app needs to show the password as plaintext on standard output.

3rd Party Software Examples

```
cat /tmp/plainpass | sudo -u www-data ./occ wnd:listen <host> <share> <username> --password-file=-
```

This provides a bit more security because the `/tmp/plainpass` password should be owned by root and only root should be able to read the file (0400 permissions); Apache, particularly, shouldn't be able to read it. It's expected that root will be the one to run this command.

```
base64 -d /tmp/encodedpass | sudo -u www-data ./occ wnd:listen <host> <share> <username> \  
--password-file=-
```

Similar to the previous example, but this time the contents are encoded in [Base64 format](#) (there's not much security, but it has additional obfuscation).

Third party password managers can also be integrated. The only requirement is that they have to provide the password in plain text somehow. If not, additional operations might be required to get the password as plain text and inject it in the listener.

As an example:

You can use “pass” as a password manager. You can go through <http://xmodulo.com/manage-passwords-command-line-linux.html> to setup the keyring for whoever will fetch the password (probably root) and then use something like the following

```
pass the-password-name | sudo -u www-data ./occ wnd:listen <host> <share> <username> --password-file-
```

Password Option Precedence

If both the argument and the option are passed, e.g., `occ wnd:listen <host> <share> <username> <password> --password-file=/tmp/pass`, then the `--password-file` option will take precedence.

Optimizing wnd:process-queue

Note: Do not use this option if the process-queue is fast enough. The option has some drawbacks, specifically regarding password changes in the backend.

`wnd:process-queue` creates all the storages that need to be updated from scratch. To do so, we need to fetch all the users from all the backends (currently only the ones that have logged in at least once because the others won't have the storages that we'll need updates).

To optimize this, `wnd:process-queue` make use of two switches: “`--serializer-type`” and “`--serializer-params`”. These serialize storages for later use, so that future executions don't need to fetch the users, saving precious time — especially for large organizations.

Switch	Allowed Values
<code>--serializer-type</code>	Other valid values may be added in the future, as more implementations are requested.
<code>--serializer-params</code>	Depends on <code>--serializer-type</code> , because those will be the parameters that the chosen serializer will use. For the <code>file</code> serializer, you need to provide a file location in the host FS where the storages will be serialized. You can use <code>--serializer-params file=/tmp/file</code> as an example.

While the specific behavior will depend on the serializer implementation, the overall behavior can be simplified as follows:

If the serializer's data source (such as *a file*, *a database table*, or some *Redis keys*) has storage data, it uses that data to create the storages; otherwise, it creates the storages from scratch.

After the storages are created, notifications are processed for the storages. If the storages have been created from scratch, those storages are written in the data source so that they can be read on the next run.

Note: It's imperative to periodically clean up the data source to fetch fresh data, such as for new storages and updated passwords. There isn't a generic command to do this from ownCloud, because it depends on the specific serializer type. Though this option could be provided at some point if requested.

The File Serializer

The file serializer is a serializer implementation that can be used with the `wnd:process-queue` command. It requires an additional parameter where you can specify the location of the file containing the serialized storages.

There are several things you should know about this serializer:

- The generated file contains the encrypted passwords for accessing the backend. This is necessary in order to avoid re-fetching the user information, when next accessing the storages.

- The generated file is intended to be readable and writable **only** for the web server user. Other users shouldn't have access to this file. Do not manually edit the file. You can remove the file if it contains obsolete information.

Usage Recommendations

Number of Serializers Only one file serializer should be used per server and share, as the serialized file has to be per server and share. Consider the following usage scenario:

- If you have three shares: `10.0.2.2/share1`, `10.0.2.2/share2`, and `10.0.10.20/share2`, then you should use three different calls to `wnd:process-queue`, changing the target file for the serializer for each one.

Since the serialized file has to be per server and share, the serialized file has some checks to prevent misuse. Specifically, if we detect you're trying to read the storages for another server and share from the file, the contents of the file won't be read and will fallback to creating the storage from scratch. At this point, we'll then update the contents of that file with the new storage.

Doing so, though, creates unneeded competition, where several `process-queue` will compete for the serializer file. For example, let's say that you have two `process-queues` targeting the same serializer file. After the first process creates the file the second process will notice that the file is no longer available. As a result, it will recreate the file with new content.

At this point the first process runs again and notices that the file isn't available and recreate the file again. When this happens, the serializer file's purpose isn't fulfilled. As a result, we recommend the use of a different file per server and share.

File Clean Up The file will need to be cleaned up from time to time. The easiest way to do this is to remove the file when it is no longer needed. The file will be regenerated with fresh data the next execution if the serializer option is set.

Interaction Between Listener, Serializer, and Windows Password Lockout

Windows supports [password lockout policies](#). If one is enabled on the server where an ownCloud share is located, and a user fails to enter their password correctly several times, they may be locked out and unable to access the share.

This is a [known issue](#) that prevents these two inter-operating correctly. Currently, the only viable solution is to ignore that feature and use the `wnd:listen` and `wnd:process-queue`, without the serializer options.

There is also an additional issue to take into account though, which is that parallel runs of `wnd:process-queue` might lead to a user lockout. The reason for this is that several `wnd:process-queue` might use the same wrong password because it hasn't been updated by the time they fetch it.

As a result, it's recommended to force the execution serialization of that command to prevent this issue. You might want to use [Anacron](#), which seems to have an option for this scenario, or wrap the command with [flock](#).

If you need to serialize the execution of the `wnd:process-queue`, check the following example with [flock](#)

```
flock -n /my/lock/file sudo -u www-data ./occ wnd:process-queue <host> <share>
```

In that case, [flock](#) will try get the lock of that file and won't run the command if it isn't possible. For our case, and considering that file isn't being used by any other process, it will run only one `wnd:process-queue` at a time. If someone tries to run the same command a second time while the previous one is running, the second will fail and won't be executed. Check [flock's documentation](#) for details and other options.

Multiple Server Setup

Setups with several servers might have some difficulties in some scenarios:

- The `wnd:listen` component *might* be duplicated among several servers. This shouldn't cause a problem, depending on the limitations of the underlying database engine. The supported database engines should be able to handle concurrent access and de-duplication.
- The `wnd:process-queue` *should* also be able to run from any server, however limitations for concurrent executions still apply. As a result, you might need to serialized command execution of the `wnd:process-queue` among the servers (to avoid for the password lockout), which might not be possible or difficult to achieve. You might want to execute the command from just one specific server in this case.
- `wnd:process-queue + serializer`. First, check the above section to know the interactions with the password lockout. Right now, the only option you have to set it up is to store the target file in a common location for all the server. We might need to provide a specific serializer for this scenario (based on Redis or DB)

Basic Command Execution Examples

```
sudo -u www-data ./occ ``wnd:listen`` host share username password
```

```
sudo -u www-data ./occ ``wnd:process-queue`` host share
```

```
sudo -u www-data ./occ ``wnd:process-queue`` host share -c 500
```

```
sudo -u www-data ./occ ``wnd:process-queue`` host share -c 500 \  
--serializer-type file \  
--serializer-params file=/opt/oc/store
```

```
sudo -u www-data ./occ ``wnd:process-queue`` host2 share2 -c 500 \  
--serializer-type File \  
--serializer-params file=/opt/oc/store2
```

To set it up, make sure the listener is running as a system service:

```
sudo -u www-data ./occ ``wnd:listen`` host share username password
```

Setup a Cron job or similar with something like the following two commands:

```
sudo -u www-data ./occ wnd:process-queue host share -c 500 \  
--serializer-type file \  
--serializer-params file=/opt/oc/store1
```

```
rm -f /opt/oc/store1 # With a different schedule
```

The first run will create the `/opt/oc/store1` with the serialized storages, the rest of the executions will use that file. The second Cron job, the one removing the file, will force the `wnd:process-queue` to refresh the data.

It's intended to be run in a different schedule, so there are several executions of the `wnd:process-queue` fetching the data from the file. Note that the file can be removed manually at any time if it's needed (for example, the admin has reset some passwords, or has been notified about password changing).

9.5.6 Configuring S3 as Primary Storage

Administrators can configure Amazon S3 objects as the primary ownCloud storage location. Doing this replaces the default ownCloud `owncloud/data` directory. However, if you use S3 objects as the primary storage, you *need* to keep the `owncloud/data` directory for the following reasons:

- The ownCloud log file is saved in the data directory.
- Legacy apps may not support using anything but the `owncloud/data` directory.

Note: Even if the ownCloud log file is stored in an alternate location (by changing the location in `config.php`) `owncloud/data` may still be required for backward compatibility with some apps.

That said, the [Object Storage Support app](#) (`objectstore`) is still available, but the [S3 Object Storage app](#) (`files_primary_s3`) is the preferred way to provide S3 storage support. However, OpenStack Swift has been deprecated.

When using `files_primary_s3`, the Amazon S3 bucket needs to be created manually according to the [developer documentation](#), and versioning needs to be enabled.

Note: ownCloud GmbH provides consulting for migrations from `objectstore` to `files_primary_s3`.

Important: Implications

1. Apply this configuration before the first login of any user – including the admin user; otherwise, ownCloud can no longer find the user’s files.
 2. ownCloud, in “object store” mode, expects exclusive access to the object store container, because it only stores the binary data for each file. While in this mode, ownCloud stores the metadata in the local database for performance reasons.
 3. The current implementation is incompatible with any app that uses direct file I/O (input/output) as it circumvents the ownCloud virtual filesystem. Two excellent examples are:
 - (a) **The Encryption app:** It fetches critical files in addition to any requested file, which results in significant overhead.
 - (b) **The Gallery app:** It stores thumbnails directly in the filesystem.
 4. When using S3 primary storage with multiple buckets it is not recommended to use the command to transfer file ownership between users (`occ files:transfer-ownership`) as shares on the files can get lost. The reason for this is that fileIDs are changed during such cross-storage move operations.
-

Configuration

Look in `config.sample.php` for example configurations. Copy the relevant part to your `config.php` file. Any object store needs to implement `\OCP\Files\ObjectStore\IObjectStore`, and can be passed parameters in the constructor with the `arguments` key, as in the following example:

```
$CONFIG = [  
    'objectstore' => [  
        'class' => 'Implementation\\Of\\OCP\\Files\\ObjectStore\\IObjectStore',  
        'arguments' => [  
            ...  
        ],  
    ],  
],
```

Amazon S3

The S3 backend mounts a bucket of the Amazon S3 object store into the virtual filesystem. The class to be used is `OCA\Files_Primary_S3\S3Storage`, as in the following example:

```
<?php
$CONFIG = [
    'objectstore' => [
        'class' => 'OCA\Files_Primary_S3\S3Storage',
        'arguments' => [
            // replace with your bucket
            'bucket' => 'owncloud',
            // uncomment to enable server side encryption
            //'serversideencryption' => 'AES256',
            'options' => [
                // version and region are required
                'version' => '2006-03-01',
                // change to your region
                'region' => 'eu-central-1',
                'credentials' => [
                    // replace key and secret with your credentials
                    'key' => 'EJ39ITYZEUH5BGWDRUFY',
                    'secret' => 'M5MrXTRjkyMaxXPe2FRXMTfTfbKEnZCu+7uRTVSj',
                ],
            ],
        ],
    ],
],
```

Ceph S3

The S3 backend can also be used to mount the bucket of a Ceph S3 object store via the Amazon S3 API into the virtual filesystem. The class to be used is `OCA\Files_Primary_S3\S3Storage`:

```
<?php
$CONFIG = [
    'objectstore' => [
        'class' => 'OCA\Files_Primary_S3\S3Storage',
        'arguments' => [
            // replace with your bucket
            'bucket' => 'OWNCLOUD',
            // uncomment to enable server side encryption
            //'serversideencryption' => 'AES256',
            'options' => [
                // version and region are required
                'version' => '2006-03-01',
                'region' => 'us-central-1',
                'credentials' => [
                    // replace key and secret with your credentials
                    'key' => 'owncloud123456',
                    'secret' => 'secret123456',
                ],
                'use_path_style_endpoint' => true,
                'endpoint' => 'http://ceph:80/',
            ],
        ],
    ],
];
```

Scality S3

The S3 backend can also be used to mount the bucket of a Scality S3 object store via the Amazon S3 API into the virtual filesystem. The class to be used is `OCA\Files_Primary_S3\S3Storage`:

`<?php`

```
$CONFIG = [
    'objectstore' => [
        'class' => 'OCA\Files_Primary_S3\S3Storage',
        'arguments' => [
            // replace with your bucket
            'bucket' => 'owncloud',
            // uncomment to enable server side encryption
            //'serversideencryption' => 'AES256',
            'options' => [
                // version and region are required
                'version' => '2006-03-01',
                'region' => 'us-east-1',
                'credentials' => [
                    // replace key and secret with your credentials
                    'key' => 'accessKey1',
                    'secret' => 'verySecretKey1',
                ],
                'use_path_style_endpoint' => true,
                'endpoint' => 'http://scality:8000/',
            ],
        ],
    ],
];
```

9.5.7 How to Create and Configure Microsoft OneDrive

To use Microsoft OneDrive as an external storage option in ownCloud, you need to do two things:

1. Create an application configuration
2. Configure a mount point in ownCloud

Create an Application Configuration

Microsoft Application Registration Portal Tools Docs Feedback

My applications [Learn More](#) [Add an app](#)

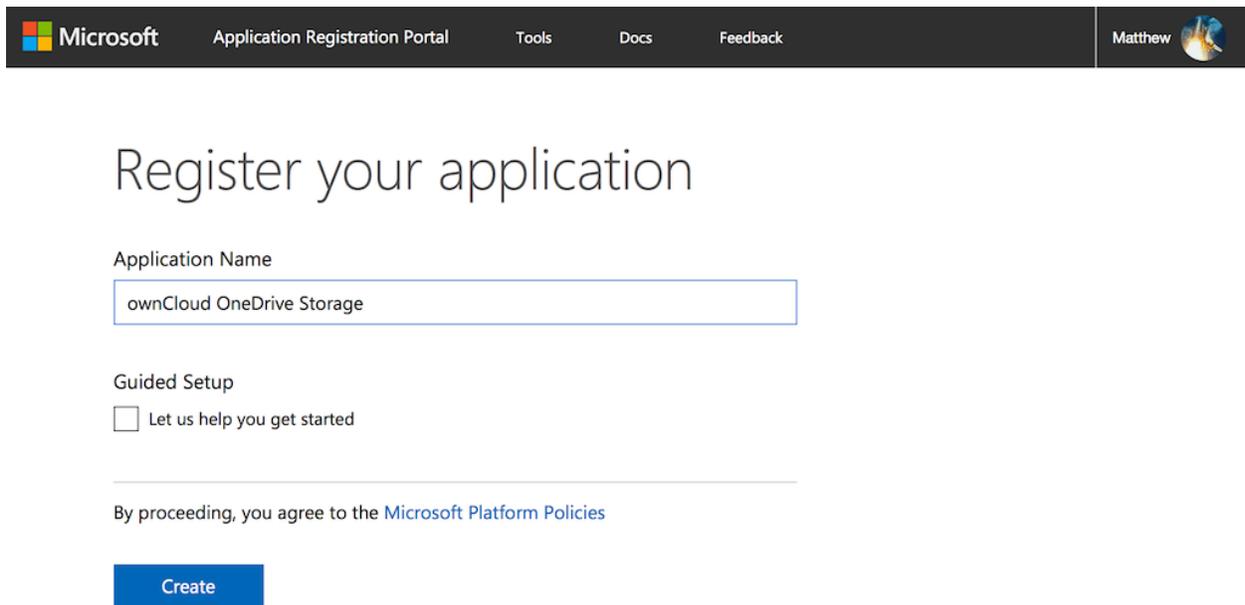
Name	App ID / Client Id
Press the "Add an App" button to create a new application	

To create a new application:

- Open <https://apps.dev.microsoft.com/> in your browser of choice and click “*Create App*”.
- Under “*Properties*”, set the application’s name.
- Click “*Create*”.

With the application created, you can then add a range of further settings. However, only a few of them are required for use with ownCloud.

Application Password



The screenshot shows the Microsoft Application Registration Portal interface. At the top, there is a navigation bar with the Microsoft logo, 'Application Registration Portal', 'Tools', 'Docs', 'Feedback', and a user profile for 'Matthew'. The main heading is 'Register your application'. Below this, there is a form with the following elements:

- A label 'Application Name' above a text input field containing 'ownCloud OneDrive Storage'.
- A label 'Guided Setup' above a checkbox labeled 'Let us help you get started', which is currently unchecked.
- A horizontal line below the checkbox.
- A text line: 'By proceeding, you agree to the [Microsoft Platform Policies](#)'.
- A blue 'Create' button.

Under “*Application Secrets*”, click “*Generate New Password*”, which generates a password and displays it in a popup window. It is required later during when configuring a mount point.

Note: Copy the password to your preferred password manager, as it is only displayed **once**.

Redirect URLs

Under “*Platforms*”, click “*Add Platform*” and choose “*Web*” in the popup window which appears. Only one redirect URL field is visible at first, so click “*Add URL*” to add another one.

With two fields available, add two redirect URLs; one for `settings/admin` and one for `settings/personal`, as you can see in the image below.

Application Permissions

Under “*Microsoft Graph Permissions*”, click “*Add*” next to “*Application Permissions*”. This opens a popup window where you can choose the required permissions. Add at least the following four:

- `Files.Read.All`

Platforms

[Add Platform](#)

Web [Delete](#)

Allow Implicit Flow

Redirect URLs ⓘ [Add URL](#)

Logout URL ⓘ

Microsoft Graph Permissions

The settings you set here may vary depending on whether you get a token from our V1 or V2 endpoint. [What's the difference?](#)

Delegated Permissions [Add](#) [About delegated permissions](#)

User.Read ×

Application Permissions [Add](#) [About application permissions](#)

- Files.ReadWrite.All
- IdentityRiskEvent.Read.All
- User.Read.All

With those settings added, click “Save”, located right at the bottom of the page.

Configure a Mount Point in ownCloud

You can add as many OneDrive mount points as you want. To do so:

1. Add a new storage, selecting “One Drive” for external storage.
2. Set the credentials of your OneDrive application, and then accept the permissions.
3. If everything is accepted, the mount points should appear, with a green status icon on the far left-hand side.

External Storage

Enable external storage

Global credentials for external storage

Username Password Save

Folder name	External storage	Authentication	Configuration	Available for
● OneDrive_old	One Drive	OneDrive OAuth2	386d9505-1e31-4948	Grant access All users. Type to select user or group.
● OneDrive	One Drive	OneDrive OAuth2	381584ee-7050-430c	Grant access All users. Type to select user or group.
● OneDrive_u2_app4	One Drive	OneDrive OAuth2	956c429b-25ac-4d29	Grant access All users. Type to select user or group.
● OneDrive1_u1_app3	One Drive	OneDrive OAuth2	48b47725-46d2-4636	Grant access All users. Type to select user or group.
● OneDrive1_u1_app6	One Drive	OneDrive OAuth2	386d9505-1e31-4948	Grant access All users. Type to select user or group.
● OneDrive_u2_app6	One Drive	OneDrive OAuth2	386d9505-1e31-4948	Grant access All users. Type to select user or group.

Folder name Add storage

To be able to use the `occ command files_onedrive:subscribe`, you need to have the variable `overwrite.cli.url` set in `config/config.php`, as in this example:

```
'overwrite.cli.url' => 'https://example.org:63984/index.php',
```

Note: The HTTPS prefix, port, and `/index.php` suffix are mandatory.

9.6 User Management

9.6.1 Shibboleth Integration

Introduction

The ownCloud Shibboleth user backend application integrates ownCloud with a Shibboleth Service Provider (SP) and allows operations in federated and single-sign-on (SSO) infrastructures. Setting up Shibboleth has two big steps:

1. Enable and configure the Apache Shibboleth module.
2. Enable and configure the ownCloud Shibboleth app.

The Apache Shibboleth module

Currently supported installations are based on the [native Apache integration](#). The individual configuration of the service provider is highly dependent on the operating system, as well as on the integration with the Identity Providers (IdP), and require case-by-case analysis and installation.

A good starting point for the service provider installation can be found in [the official Shibboleth Wiki](#).

A successful installation and configuration will populate Apache environment variables with at least a unique user id which is then used by the ownCloud Shibboleth app to login a user.

Apache Configuration

This is an example configuration as installed and operated on a Linux server running the Apache 2.4 Web server. These configurations are highly operating system specific and require a high degree of customization.

The ownCloud instance itself is installed in `/var/www/owncloud/`. The following aliases are defined in an Apache virtual host directive:

Further Shibboleth specific configuration as defined in `/etc/apache2/conf.d/shib.conf`:

```
# Load the Shibboleth module.
LoadModule mod_shib /usr/lib64/shibboleth/mod_shib_24.so

# Ensure handler will be accessible
<Location /Shibboleth.sso>
    AuthType None
    Require all granted
</Location>

# always fill env with shib variable for logout url
<Location />
    AuthType shibboleth
    ShibRequestSetting requireSession false
    Require shibboleth
</Location>

# authenticate only on the login page
<Location ~ "^(/index.php)?/login">
    # force internal users to use the IdP
    <If "-R '192.168.1.0/24'">
        AuthType shibboleth
        ShibRequestSetting requireSession true
        require valid-user
    </If>
    # allow basic auth for eg. guest accounts
    <Else>
        AuthType shibboleth
        ShibRequestSetting requireSession false
        require shibboleth
    </Else>
</Location>

# shib session for css, js and woff not needed
<Location ~ "/.*\.(css|js|woff)">
    AuthType None
    Require all granted
</Location>
```

To allow users to login via the IdP, add a login alternative with the `login.alternatives` option in `config.php`. Depending on the ownCloud Shibboleth app mode, you may need to revisit this configuration.

The ownCloud Shibboleth App

After enabling the Shibboleth app on your Apps page, you need to choose the app mode and map the necessary Shibboleth environment variables to ownCloud user attributes on your Admin page.

Choosing the App Mode

After enabling the app it will be in **Not active** mode, which ignores a Shibboleth session and allows you to login as an administrator and inspect the currently available Apache environment variables. Use this mode to set up the environment mapping for the other modes, and in case you locked yourself out of the system. You can also change the app mode and environment mappings by using the `occ` command, like this example on Ubuntu Linux:

```
$ sudo -u www-data php occ shibboleth:mode notactive
$ sudo -u www-data php occ shibboleth:mapping --uid login
```

In **Single sign-on only** mode the app checks if the environment variable for the Shibboleth session, by default **Shib-Session-Id**, is set. If that is the case it will take the value of the environment variable as the `uid`, by default `eppn`, and check if a user is known by that `uid`. In effect, this allows another user backend, e.g., the LDAP app, to provide the `displayname`, `email` and `avatar`.

Note: As an example the IdP can send the **userPrincipalName** which the Apache Shibboleth module writes to a custom Apache environment variable called `login`. The ownCloud Shibboleth app reads that `login` environment variable and tries to find an LDAP user with that `username`. For this to work **userPrincipalName** needs to be added to the **Additional Search Attributes** in the *LDAP directory settings on the advanced tab*. We recommend using a scoped login attribute like **userPrincipalName** or **mail** because otherwise the search might find multiple users and prevent login.

Note: In many scenarios Shibboleth is not intended to hide the user's password from the service provider, but only to implement SSO. If that is the case it is sufficient to protect the ownCloud base url with Shibboleth. This will send Web users to the IdP but allow desktop and mobile clients to continue using username and password, preventing popups due to an expired Shibboleth session lifetime.

In **Autoprovision Users** mode the app will not ask another user backend, but instead provision users on the fly by reading the two additional environment variables for display name and email address.

In ownCloud 8.1 the Shibboleth environment variable mapping was stored in `apps/user_shibboleth/config.php`. This file was overwritten on upgrades, preventing a seamless upgrade procedure. In ownCloud 8.2+ the variables are stored in the ownCloud database, making Shibboleth automatically upgradeable.

Mapping ownCloud User IDs

From 3.1.2 you can now specify a mapper that is used on inbound ownCloud user IDs, to adjust them before usage in ownCloud. You can set the mapper using `occ`:

```
$ sudo -u www-data php occ config:app:set user_shibboleth uid_mapper --value="OCA\User_Shibboleth\Map
```

You may view the currently configured mapper using:

Shibboleth

App Mode

Environment

Use as Shibboleth session

Use as uid

Use as email

Use as display name

Server Environment:

htaccessWorking	true
HTTP_HOST	docker.oc.solidgear.es:53738
HTTP_USER_AGENT	Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:42.0) G
HTTP_ACCEPT	text/html,application/xhtml+xml,application/xml;
HTTP_ACCEPT_LANGUAGE	en-US,en;q=0.5
HTTP_ACCEPT_ENCODING	gzip, deflate
HTTP_DNT	1
HTTP_COOKIE	PHPSESSID=nlkrv949lmuo7dpkkgb91gbe13; ocy0:
HTTP_CONNECTION	keep-alive
PATH	/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/:
SERVER_SIGNATURE	<address>Apache/2.4.7 (Ubuntu) Server at docke
SERVER_SOFTWARE	Apache/2.4.7 (Ubuntu)
SERVER_NAME	docker.oc.solidgear.es
SERVER_ADDR	172.17.1.245
SERVER_PORT	53738
REMOTE_ADDR	166.176.185.154
DOCUMENT_ROOT	/opt/owncloud
REQUEST_SCHEME	http

Figure 9.6: *figure 1: Enabling Shibboleth on the ownCloud Admin page*

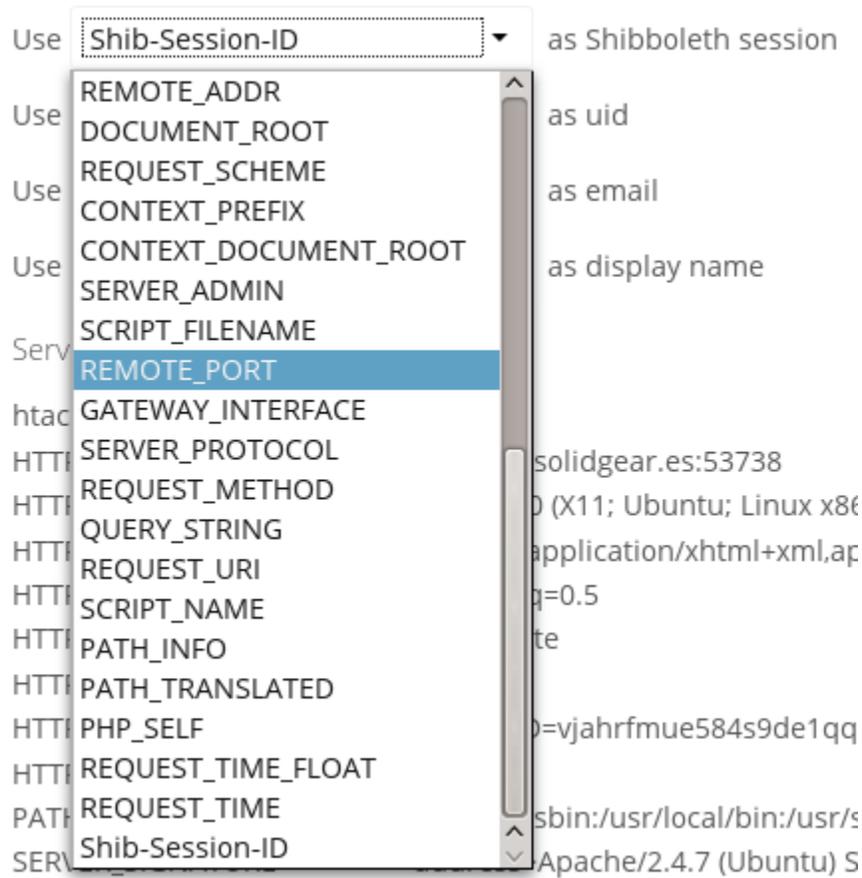


Figure 9.7: *figure 2: Mapping Shibboleth environment configuration variables to ownCloud user attributes*

```
$ sudo -u www-data php occ shibboleth:mapping
```

The following mappers are provided with the app:

- OCA\User_Shibboleth\Mapper\NoOpMapper - the default, does not alter the uid
- OCA\User_Shibboleth\Mapper\ADFSMapper - splits the uid around a ; character and takes the first piece
- OCA\User_Shibboleth\Mapper\GUIDInMemoryMapper - maps in binary GUIDs to strings

Shibboleth with Desktop and Mobile Clients

The ownCloud Desktop Client can interact with an ownCloud instance running inside a Shibboleth Service Provider by using OAuth2 tokens to authenticate.

The ownCloud Android and iOS mobile apps also work with OAuth2 tokens.

WebDAV Support

Users of standard WebDAV clients can generate an App Password on the Personal settings page. Use of App Passwords may be enforced with the `“token_auth_enforced“` option in `config.php`

Known Limitations

Encryption

File encryption can only be used together with Shibboleth when the *master key-based encryption* is used because the per-user encryption requires the user's password to unlock the private encryption key. Due to the nature of Shibboleth the user's password is not known to the service provider.

Other Login Mechanisms

You can allow other login mechanisms (e.g. LDAP or ownCloud native) by creating a second Apache virtual host configuration. This second location is not protected by Shibboleth, and you can use your other ownCloud login mechanisms.

Session Timeout

Session timeout on Shibboleth is controlled by the IdP. It is not possible to have a session length longer than the length controlled by the IdP. In extreme cases this could result in re-login on mobile clients and desktop clients every hour.

UID Considerations and Windows Network Drive compatibility

To log in LDAP users via SAML for Single Sign On the user in LDAP must be uniquely resolvable by searching for the username that was sent in the SAML token. For this to work the `ldap` attribute containing the username needs to be added to the **Additional Search Attributes** in the *LDAP directory settings on the advanced tab*. We recommend using a scoped login attribute like `userPrincipalName` or `mail` because otherwise the search might find multiple users and prevent login.

`user_shibboleth` will do the authentication, and `user_ldap` will provide user details such as `email` and `displayname`.

9.6.2 SAML 2.0 Based SSO with Active Directory Federation Services (ADFS) and mod_shib

Preparation

Before you can setup SAML 2.0 based with [Active Directory Federation Services \(ADFS\)](#) and `mod_shib`, ask your ADFS admin for the relevant server URLs. These are:

- The SAML 2.0 single sign-on service URL, e.g., `https://<ADFS server FQDN>/ADFS/ls`
- The IdP metadata URL, e.g., `https://<ADFS server FQDN>/FederationMetadata/2007-06/FederationMet`

Then, make sure that the web server is accessible with a trusted certificate:

```
$ sudo a2enmod ssl
$ sudo a2ensite default-ssl
$ sudo service apache2 restart
```

Installation

Firstly, install `mod_shib`. You can do this using the following command:

```
$ sudo apt-get install libapache2-mod_shib2
```

This will install packages needed for `mod_shib`, including `shibd`. Then, generate certificates for the `shibd` daemon by running the following command:

```
sudo shib-keygen
```

Download and Filter the ADFS Metadata

The metadata provided by ADFS cannot be automatically imported, and must be cleaned up before using it with the file based `MetadataProvider`. To do so, use `adfs2fed.php`, as in the following command:

```
php apps/user_shibboleth/tools/adfs2fed.php \
  https://<ADFS server FQDN>/FederationMetadata/2007-06/FederationMetadata.xml \
  <AD-Domain> > /etc/shibboleth/filtered-metadata.xml
```

Configure shibd

Next, you need to configure `shibd`. To do this, in `/etc/shibboleth/shibboleth2.xml`:

1. Use the URL of the ownCloud instance as the `entityID` in the `ApplicationDefaults`, e.g.,

```
<ApplicationDefaults entityID="https://<owncloud server FQDN>/login/saml" REMOTE_USER="eppn upn"
```

Note: `https://<owncloud server FQDN>/login/saml` is just an example. Adjust `<owncloud server FQDN>` to the full qualified domain name of your server.

2. Configure the SSO to use the `entityID` from the `filtered-metadata.xml`, e.g.,

```
<SSO entityID="https://<ADFS server FQDN>/<URI>/">
  SAML2
</SSO>
```

Note: Grab <ADFS server FQDN>/<URI>/ from the filtered-metadata.xml.

3. Configure an XML MetadataProvider with the local filtered-metadata.xml file:

```
<MetadataProvider type="XML" file="/etc/shibboleth/filtered-metadata.xml"/>
```

Metadata Available

Under `https://<owncloud server FQDN>/Shibboleth.sso/Metadata` shibd exposes the Metadata that is needed by ADFS to add the SP as a Relying party.

ADFS

This part needs to be done by an ADFS administrator. Let him do his job while you continue with the Apache configuration below.

Add a Relying Party Using Metadata

See [AD FS 2.0 Step-by-Step Guide](#) step 2.

Configure ADFS to send the userPrincipalName in the SAML token

If you have control over ADFS make it send the UPN and Group by adding the following LDAP claim rule:

- Map User Principal Name to UPN
- Map Token Groups - Unqualified Names and map it to Group

Change shibd attribute-map.xml to

```
<Attributes xmlns="urn:mace:shibboleth:2.0:attribute-map" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  <Attribute name="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/upn" id="upn"/>
</Attributes>
```

That will make the userPrincipalName available as the environment variable upn.

Apache2

To protect ownCloud with shibboleth you need to protect the URL with a mod_shib based auth. Currently, we recommend protecting only the login page.

user_shibboleth

When the app is enabled and ownCloud is protected by mod_shib, due to the Apache 2 configuration, you should be forced to authenticate against an ADFS. After a successful authentication you will be redirected to the ownCloud login page, where you can login as the administrator. Double check you have a valid SAML session by browsing to `https://<owncloud server FQDN>/Shibboleth.sso/Session`.

In the “User Authentication” settings for Shibboleth the upn environment variables will be filled with the authenticated user’s userPrincipalName in the “Server Environment” section.

Use upn as uid and set the app mode to ‘SSO Only’ by running: `.. code-block:: console`

```
occ shibboleth:mode ssoonly occ shibboleth:mapping -u upn
```

displayName and email are only relevant for autoprovisioning mode. Add Claims in ADFS and map them in the attribute-map.xml if needed.

Testing

- Close the browser tab to kill the session.
- Then visit `https://<owncloud server FQDN>` again.
- You should be logged in automatically.
- Close the tab or delete the cookies to log out.
- To make the logout work see the Logout section in this document.

Configuring SSO

- **On the ADFS Server:**

- Add “Windows Authentication” to the “Service” -> “Authentication Methods” for “Intranet”
- Run the following Powershell script for Firefox:

```
# Save the list of currently supported browser user-agents to a variable
$browsers=Get-ADFSProperties | Select -ExpandProperty WIASupportedUseragents
```

```
# Add Mozilla/5.0 user-agent to the list
$browsers+="Mozilla/5.0"
```

```
# Apply the new list
Set-ADFSProperties -WIASupportedUseragents $browsers
```

```
# Turn off Extended Protection
#Set-ADFSProperties -ExtendedProtectionTokenCheck None
```

```
# Restart the AD FS service
Restart-Service ADFSsrv
```

- **On the Windows client:**

- For Internet Explorer, Edge, and Chrome
 - * In the “Internet Settings” -> “Security” -> “Local Intranet”
 - * Click on “Sites”
 - * Click on “Advanced”
 - * Add your ADFS machine with `https://<ADFS server FQDN>/` and click OK.
 - * Click on “customize level”
 - * Find “User Authentication”
 - * Check “Automatic login only for Intranet zone”
- For Firefox
 - * Open “about:config”
 - * Accept the warning

- * Search for `network.negotiate-auth.trusted-uris` and set it to the FQDN of your ADFS server
- * Search for `network.automatic-ntlm-auth.trusted-uris` and set it to the FQDN of your ADFS server

Now if you logged into the domain and open your ownCloud server in the browser of your choice you should get directly to your ownCloud files without a login.

Debugging

In `/etc/shibboleth/shibd.logger` set the overall behavior to debug:

```
# set overall behavior
log4j.rootCategory=DEBUG, shibd_log, warn_log
[...]
```

After a restart `/var/log/shibboleth/shibd.log` will show the parsed SAML requests and also which claims / attributes were found and mapped, or why not.

Browsers

- For Chrome there is a [SAML Chrome Panel](#) that allows checking the SAML messages in the developer tools reachable via F12.
- For Firefox there is [SAML tracer](#)
- In the Network tab of the developer extension make sure that “preserve logs” is enabled in order to see the redirects without wiping the existing network requests

Logout

In SAML scenarios the session is held on the SP as well as the IdP. Killing the SP session will redirect you to the IdP where you are still logged in, causing another redirect that creates a new SP session, making logout impossible. Killing only the IdP session will allow you to use the SP session until it expires.

There are multiple ways to deal with this:

1. By default ownCloud shows a popup telling the user to close the browser tab. That kills the SP session. If the whole browser is closed the IdP may still use a Kerberos-based authentication to provide SSO in effect making logout impossible.
2. Hide the logout action in the personal menu via CSS. This forces users to log out at the IdP.

OAuth2

In upcoming versions the clients will use OAuth2 to obtain a device specific token to prevent session expiry, making the old `/oc-shib/remote.php/nonshib-webdav` obsolete

Further Reading

- [ADFS 2.0 Step-by-Step Guide: Federation with Shibboleth 2 and the InCommon Federation](#)
- [ADFS: How to Invoke a WS-Federation Sign-Out](#)
- [Shibboleth Service Provider Integration with ADFS](#)

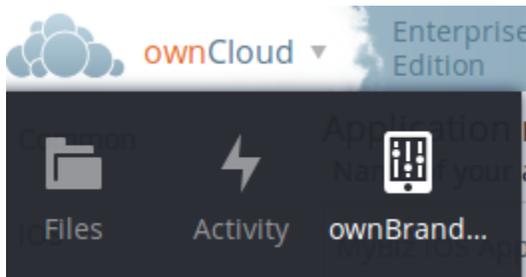
- <https://github.com/rohe/pysfemma/blob/master/tools/adfs2fed.py>
- [https://technet.microsoft.com/de-de/library/gg317734\(v=ws.10\).aspx#BKMK_EditClaimRulesforRelyingPartyTrust](https://technet.microsoft.com/de-de/library/gg317734(v=ws.10).aspx#BKMK_EditClaimRulesforRelyingPartyTrust)
- [https://wiki.shibboleth.net/confluence/display/SHIB2/NativeSPApplication#NativeSPApplication-BasicConfiguration\(Version2.4andAbove\)](https://wiki.shibboleth.net/confluence/display/SHIB2/NativeSPApplication#NativeSPApplication-BasicConfiguration(Version2.4andAbove))
- <https://wiki.shibboleth.net/confluence/display/SHIB2/NativeSPMetadataProvider#NativeSPMetadataProvider-XMLMetadataProvider>
- <https://wiki.shibboleth.net/confluence/display/SHIB2/NativeSPServiceSSO>

9.7 Creating Branded ownCloud Clients

9.7.1 Creating Branded Client Apps

Overview

ownBrander is an ownCloud build service that is exclusive to Enterprise customers for creating branded Android and iOS ownCloud sync apps, and branded ownCloud desktop sync clients. You build your apps with the ownBrander app on your [Customer.owncloud.com](https://www.owncloud.com/customer) account, and within 24-48 hours the completed, customized apps are loaded into your account. You must supply your own artwork, and you'll find all the specifications and required elements in ownBrander.



Building a Branded Desktop Sync Client

See [Building Branded ownCloud Clients](#) for instructions on building your own branded desktop sync client, and for setting up an automatic update service.

Your users may run both a branded and un-branded desktop sync client side-by-side. Both clients run independently of each other, and do not share account information or files.

Building a Branded iOS App

Building and distributing your branded iOS ownCloud app involves a large number of interdependent steps. The process is detailed in the [Building Branded ownCloud Clients](#) manual. Follow these instructions exactly and in order, and you will have a nice branded iOS app that you can distribute to your users.

Building an Android App

Building and distributing your branded Android ownCloud app is fairly simple, and the process is detailed in [Building Branded ownCloud Clients](#).

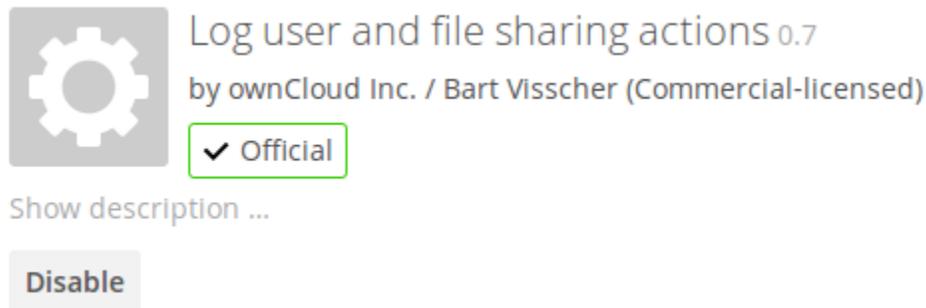
9.7.2 Custom Client Download Repositories

See *Custom Client Download Repositories* to learn how test and configure custom download repository URLs for your branded clients.

9.8 Logging Apps

9.8.1 Enterprise Logging Apps

The **Log user and file sharing actions** app (`apps/admin_audit`) records the file sharing activity of your users, file tagging, and user logins and logouts.



Your logging level must be set to at least **Info, warnings, errors, and fatal issues** on your ownCloud admin page, or `'loglevel' => 1` in `config.php`.

View your logfiles on your admin page. Click the **Download logfile** button to dump the plain text log, or open the logfile directly in a text editor. The default location is `owncloud/data/owncloud.log`.

See *Logging Configuration* and *Advanced File Tagging With the Workflow App* for more information on logging and tagging.

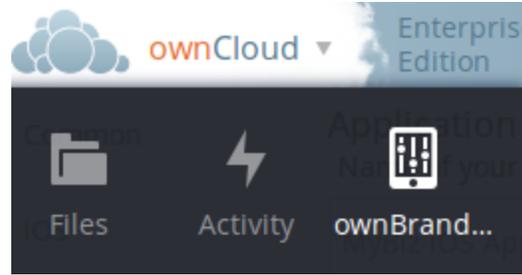
9.9 Server Branding

9.9.1 Custom Theming ownCloud

Overview

ownBrander is an ownCloud build service that is exclusive to Enterprise edition customers for creating branded ownCloud clients and servers. You may brand your ownCloud server using ownBrander to easily build a **custom theme**, using your own logo and artwork. ownCloud has always been theme-able, but it was a manual process that required editing CSS and PHP files. Now Enterprise customers can use ownBrander, which provides an easy graphical wizard.

You need an Enterprise subscription, an account on [Customer.owncloud.com](https://customer.owncloud.com), and the ownBrander app enabled on your account. When you complete the steps in the wizard the ownBrander service builds your new branded theme, and in 24-48 hours you'll see it in your account.



When you open the ownBrander app, go to the Web tab. You will see an introduction and the wizard, which starts with uploading your logo. You will need a number of images in specific sizes and formats, and the wizard tells you what you need. Example images are on the right, and you can click to enlarge them.

Note: If you see errors when you upload SVG files, such as “Incorrect extension.File type image/svg+xml is not correct”, “This SVG is invalid”, or “Error uploading file: Incorrect size”, try opening the file in [Inkscape](#) then save as “Plain SVG” and upload your SVG image again.

The wizard has two sections. The first section contains all the required elements: logos and other artwork, colors, naming, and your enterprise URL. The Suggested section contains optional items such as additional logo placements and custom URLs.

When you are finished, click the **Generate Web Server** button. If you want to change anything, go ahead and change it and click the **Generate Web Server** button. This will override your previous version, if it has not been created yet. In 24-48 hours you’ll find your new branded theme in the **Web** folder in your [Customer.owncloud.com](#) account.

Inside the **Web** folder you’ll find a **themes** folder. Copy this to your `owncloud/themes` directory. You may name your **themes** folder anything you want, for example `myBrandedTheme`. Then configure your ownCloud server to use your branded theme by entering it in your `config.php` file:

```
"theme" => "myBrandedTheme"
```

If anything goes wrong with your new theme, comment out this line to re-enable the default theme until you fix your branded theme. The branded theme follows the same file structure as the default theme, and you may further customize it by editing the source files. .. Note:: Always edit only your custom theme files. Never edit the default

theme files.

9.10 Document Classification and Policy Enforcement

When dealing with large amounts of data in an enterprise, it is essential to have mechanisms in place that allow you to stay in control of data flows. To implement such mechanisms the first step to take is to define guidelines that describe how the content of different security levels have to be treated.

Depending on the industry, such information security guidelines can originate from regulatory requirements, from recommendations of industry associations, or they can be self-imposed if there’s no external factor but internal risk management requirements that demand special treatment for specific information.

The leading information security standard [ISO 27001](#) defines guidelines for managing information security which can be certified. More specifically:

1. Information should enter an asset inventory (A.8.1.1)
2. Information should be classified (A.8.2.1)
3. Information should be labeled (A.8.2.2)

Login logo images



Login page logo

This is the image shown on the login page just above the Username and Password fields (svg format) (width: 252px height: 122px) *i*

Upload



Login page logo

This is the image shown on the login page just above the Username and Password fields. This image is used when the browser does not support svg, we recommend this to be the same as the previous one (Login page logo) (png format) (width: 252px height: 122px) *i*

Delete image

Upload



Logo icon



4. Information should be handled in a secure way (A.8.2.3)

As the leading international standard and certification for information security, ISO 27001 covers 75-80% of the GDPR. This makes it the ideal framework choice to support GDPR compliance requirements. Please see the [GDPR to ISO-27001 Mapping Guide](#) as an example to match the mentioned ISO Controls to the relevant *General Data Protection Regulation* (GDPR) articles.

Once the guidelines are set up, they need to be put into practice. First of all, highly sensitive data needs to be separated from less sensitive data. This is, usually, done by outlining the security levels present in the enterprise, and defining the criteria for information to qualify for each of these security levels.

Typically used security levels are *Public*, *Internal*, *Confidential*, and *Strictly Confidential*, but the requirements are usually determined individually. For example, if you are seeking GDPR compliance, then administrators can add additional ones, such as “*No PID (Personally Identifiable Information)*”, *PID*, and *Special PID*.

The actual separation of information can then be done by requiring users to classify documents according to the security levels before they leave their workstation, or by using other criteria to assign classification levels to data during further processing.

Based on the classification level, information can then be labeled and policies can be enforced to ensure that information is handled in a secure way - and in compliance with corporate guidelines.

ownCloud can boost productivity with unique collaboration features. Firstly, there's *Document Classification and Policy Enforcement*. This adds the capability to ensure that sensitive data is handled as required by information security guidelines.

Specifically, it enables ownCloud providers to:

- Comply with information security standards like ISO 27001/2 as recommended by the German Association of the Automotive Industry (VDA) and get certified to work securely within your value chain.
- Handle data in compliance with GDPR
- Manage risks effectively and cover potential data breaches.
- Separate information based on metadata.
- Display the data classification levels to raise user awareness.
- Prevent human mistakes when dealing with sensitive information.
- Fulfil corporate data protection requirements.

9.10.1 Overview

- **Classification**
 - *Tags for Classification*
 - *Automated Classification Based on Document Metadata*
 - *Automated Classification Based on File or User Properties*
 - *Manual Classification*
- **Policy Enforcement**
 - *Feature Policies*
 - *Access Policies*
- *Logging*
- *Limitations*

9.10.2 Classification

Employing document classification and respective policies in ownCloud generally involves three steps, which are outlined in detail below.

1. *Create tags for classification*
2. *Configure rules for classification (tagging)*
3. *Associate policies to the classification rules*

Tags for Classification

Document classification levels in ownCloud are represented via [Tagging Files](#). Different categories of tags can be used to achieve different behaviors for users; these are detailed in the table below.

Tag Name	Description
Visible	These tags are not available for classification based on metadata and feature policies because users can edit and delete them, which is undesirable in many cases
Restricted	These tags can be created by administrators using Tagging Files . This category is recommended as it enables users to recognize the classification level of files and to be able to filter accordingly. Additionally, certain groups of users can have the privilege to edit and assign or unassign these tags.
Invisible	These tags can be created by administrators using Tagging Files . This category is recommended when users should not be able to recognize the classification level of files or to be able to filter accordingly.

For setting up each classification rule, create a separate tag using [Tagging Files](#), which you can later assign to classification rules and/or policies.

Automated Classification Based on Document Metadata

Automated classification based on document metadata consists of two parts:

1. The actual classification metadata is embedded in documents using Office suite features
2. Document metadata is evaluated on file upload via the web interface and all ownCloud Clients. Automated classification in ownCloud therefore takes place on file upload. Existing files containing classification metadata currently can't be classified subsequently, except via manual user interaction.

Office Suite Features for Document Classification

Microsoft Office can be extended with the [NovaPath](#) addon, to provide classification capabilities. Currently Microsoft Office formats (*docx*, *dotx*, *xlsx*, *xltx*, *pptx*, *ppsx* and *potx*) are supported LibreOffice provides an integrated classification manager (TSCP).

To use automated classification based on document metadata, install and enable the [Document Classification](#) extension. The configuration depends on the tools and the classification framework in use.

Administrators can find examples and generalized configuration instructions, below.

Basic Examples for Classification and Policy Enforcement

Microsoft Office with the NovaPath Add-On Microsoft Office does *not* provide classification capabilities out-of-the-box. To extend it, we recommend the [NovaPath Add-On](#) by [M&H IT-Security GmbH](#). It comes with easy-to-use default classification categories, and provides the flexibility to set up custom classification schemes as desired.

Let's assume you want to use the default classification framework provided by NovaPath. In addition, let's assume that you take the classification level for documents classified as *Confidential* over to ownCloud to set up a policy that prevents said documents from being accessed by users in the group "Trainees".

This is how you set up an automated classification and the access policy in ownCloud:

- As an ownCloud administrator, navigate to the *Settings* section *Workflows & Tags*.
- In the *Tagging Files* panel, create a tag of type *Restricted* and call it `Class: Confidential`. Adding a group with special privileges for the tag is optional.
- Within "User Management", create the group *Trainees* and add some users.
- Set up the classification rule in the panel *Document Classification and Feature Policies* in the same section, and set the following two properties:
 - **Property XPath** = `//property[@name='Klassifizierung']/vt:lpwstr`
 - **Property Value** = `Confidential`

TIP: Take care, the property and value fields are case-sensitive!

- For *Tag*, choose `Class: Confidential`.
- Don't tick a policy checkbox as you don't want to set up a feature policy but an access policy.
- Hit *Save*.
- Set up the access policy in the *Settings* section *Security*.
- In the panel *File Firewall* enter a name for the group of rules, e.g., `Confidential` (optional). Hint: first click *Add group* if you already have other rules configured.
- From the drop-down menu, choose *System file tag*. In the tag picker, choose `Class: Confidential`. Now you should have `[System file tag] [is] [Class: Confidential]`.
- To add the group restriction, click *Add rule*, choose *User group* from the drop-down menu. In the group picker drop-down, choose *Trainees*. Now you should have `[User group] [is] [Trainees]`.
- Hit *Save Rules* to put the rules in place.
- To verify that the rule is in place, upload a classified file and check for the tag. Then share it with a member of the group "Trainees" (or with the whole group) and try to access it from a user account that is a member of said group.

LibreOffice LibreOffice implemented the open standards produced by TSCP (_Transglobal Secure Collaboration Participation, Inc.):

- The *Business Authentication Framework (BAF)* specifies how to describe the existing policy in a machine-readable format
- The *Business Authorization Identification and Labeling Scheme (BAILS)* defines how to refer to such a BAF policy in a document

There are three default BAF categories that come with different classification levels, which can be used out-of-the-box:

- Intellectual Property
- National Security
- Export Control

Assume you want to use the BAF category *Intellectual Property* and take the classification level for documents classified as *Confidential* over to ownCloud, to set up a policy that prevents said documents from being shared via a public link. This is how you set up an automated classification and the feature policy in ownCloud:

- As an ownCloud administrator, navigate to the *Settings* section *Workflows & Tags*.
- In the **Tagging Files** panel, create a tag of type *Restricted* and call it `Class: Confidential`. Adding a group with special privileges for the tag is optional.
- **Set up the classification rule and feature policy in the panel *Document Classification and Feature Policies* of the same section**
 - **Property XPath** = `//property[@name='urn:bails:IntellectualProperty:BusinessAuthorizat`
 - **Property Value** = `Confidential` (Take care, the property and value fields are case-sensitive!)
 - For *Tag* choose `Class: Confidential`.
 - Tick the checkbox *Prevent link sharing*.
 - Hit *Save*.
- To verify that the rule is in place, upload a classified file, check for the tag and try to create a public link share.

9.10.3 General Approach

Apart from the concrete examples above, a generalized method to employ document classification is available below.

Find the Metadata Properties and Values

- Classify a document in LibreOffice/MS Office and save it in an MS Office format.
- Rename the document's file extension to `.zip` and open it.
- Find the file `docProps/custom.xml` in the archive and open it with a text editor.
- Within `custom.xml`, find the property that contains the classification level value.
- Note down the classification property and value.
- Repeat the steps for all classification properties and values you want to set up classification rules for in ownCloud.

Set Up Classification Rules

- As an ownCloud administrator, navigate to the *Settings* section *Workflows & Tags*
- In the panel **“Document Classification and Feature Policies”** set up the rules:
 - **Property XPath: Enter the XPath that identifies the classification property.** Below you find a generalized example where `classification-property` is a placeholder for the property to evaluate.


```
//property[@name='classification-property']/vt:lpwstr
```
 - **Property Value:** Enter the value that triggers the classification rule when it matches with the metadata of an uploaded document, e.g., `Confidential`. Take care, the property and value fields are case-sensitive.
 - **Tag:** Choose the tag to apply to files when a match occurs.
- Repeat the steps to create classification rules for all desired properties and values

Automated Classification Based on File or User Properties

Apart from automated classification based on document metadata, uploaded files may also be classified according to criteria inherent to files or to the users uploading them, making use of [Tagging Files](#).

- Administrators may add rules for automated classification of files according to a file's size or file type.
- File uploads by specific users, devices, or source networks can be used as indicators for classification.
- Furthermore, administrators can define shared folders to automatically classify files uploaded to such folders, by tagging the respective folder and creating a *Workflow* rule based on the chosen *System file tag*.
- Additionally, the rules may be linked to achieving a more granular classification behavior (e.g., PDF files uploaded by a specific group of users should be classified as *Confidential*).

Assume you want to automatically classify all PDF documents uploaded by users that are members of the “**Management**” group. You can construct a workflow rule using the following steps:

- Within user management create the group *Management* and add some users.
- Navigate to the *Settings* section *Workflows & Tags*.
- In the [Tagging Files](#) panel, create a tag of type *Restricted* and call it `Class: Confidential`. Adding a group with special privileges for the tag is optional.
- In the panel *Workflow* you can now set up the classification rules. Hit *Add new workflow* and specify a useful name. Now configure the conditions that trigger the classification once they are met. For that choose *User group* from the drop-down menu, hit +, then choose *File mimetype* and hit + again. Then you have to provide the group *Management* and the MIME type for PDF (`application/pdf`) in the respective fields.
- Select the tag `Class: Confidential` to be added when the rules match.
- Hit *Add workflow* to save and enable it.

For more information, please check the options available for auto-tagging and consult the [Workflow extension Documentation](#).

For files classified with the *Workflow* extension, administrators can impose feature and access policies as described in the next section.

Manual Classification

As a further measure, it is possible to supply tags for users to autonomously classify all types of files in their own or shared spaces.

- As an ownCloud administrator, create a group within user management and add the users that should be able to classify files.
- Then navigate to the *Settings* section *Workflows & Tags*.
- In the [Tagging Files](#) panel, create a tag of type *Restricted* and give it a meaningful name. Then assign the group you created, in the beginning, to give it's users special privileges for the tag.
- Users that are not a member of the specified group(s) will only be able to see the respective tag but can't alter or assign/un-assign it.

For files that are classified manually, administrators can impose feature and access policies as described in the next section.

9.10.4 Policy Enforcement

ownCloud currently provides two types of policies that can be enforced based on classification, *Feature* and *Access* policies. These policies can be imposed independently of the classification mechanism. The following sections illustrate the available policies and explain how they can be applied to classified contents.

Feature Policies

Feature policies are restrictions that prevent users from using a feature or force them to use it in a certain way. They are provided by the [Document Classification](#) extension, which currently supports the following policies:

- *Prevent Upload*
- *Prevent Link Sharing*
- *Unprotected Links Expire After X Days*

Prevent Upload

To follow guidelines that prevent data of certain classification levels (e.g., *strictly confidential*) from being used in ownCloud at all, the *Prevent upload* policy is the right instrument to use. To impose such policies, tick the checkbox associated with the classification rule for the respective classification level.

When trying to upload documents caught by the policy, users will get the following error message:

```
A policy prohibits uploading files classified as '<tag>', where '<tag>' is the tag chosen for the cla
```

Note: Even though the server won't accept the uploaded files, in the end, it is mandatory to configure a tag for the classification rule to work.

Prevent Link Sharing

The prevent link sharing policy is tasked to ensure that classified data of certain confidentiality levels can't be shared publicly. This way, users can collaborate on the data internally, but it can't leave the company via ownCloud. To enable such policies, tick the checkbox associated with the classification rule for the respective classification level.

Documents with the associated classification level:

- Can't be shared via link (*public links on single files and folders containing classified files*); and
- Can't be moved to a publicly shared folder.

In all cases the user will see an error message containing the reasoning and the respective file(s): The file(s) "`**<file1>, <file2>**`" can't be shared via public link (classified as `<tag>`), where `<tag>` is the tag chosen for the classification rule.

Unprotected Links Expire After X Days

The policy *Unprotected links expire after X days* enables administrators to define public link expiration policies depending on the classification levels of the data that is shared via public links without password protection.

This makes it possible, for instance, to allow documents classified as *public* to be shared via public links for 30 days while documents classified as *internal* require public links to expire after seven days. To enable such policies, just define an expiration period associated with the classification rule for the respective classification level.

Note: The *Password Policy* extension also provides options to enforce public link expiration depending on whether the user sets a password or not.

The option *X days until link expires if password is not set* is mutually exclusive with this policy. When you enable the Password Policy option, it will always be dominant and effectively override the policy discussed in this section. In contrast, the Password Policy option *X days until link expires if password is set* can be used in parallel.

Note: The *Sharing settings option* provides the means to define a general public link expiration policy. This option currently is also mutually exclusive and will always override the policy discussed in this section.

Setting Up Policies Without Automated Classification Based on Document Metadata

All policies can also be enforced when using *Manual Classification* or *Automated Classification Based on File or User Properties*. For this, specify the tag that determines the files that the policy should apply to and leave the fields for *Property XPath* and *Property Value* empty. Then choose the desired policy and hit *Save*.

9.10.5 Access Policies

Access policies are restrictions that prevent users or groups of users from accessing specific resources even though they appear in their file list, e.g., via a share from another user. They are provided by the *File Firewall* <*firewall/file_firewall.adoc*> extension which currently supports policies to prevent access to classified documents.

To link access policies with classification levels, the bottom line of such policies is the associated classification tag ([System file tag] [is] [<tag>]). It can, for instance, be combined with the following conditions to realize exclusive ([is]) or inclusive ([is not]) policies:

Documents with the respective classification tag can't be accessed:

- *User group*: by users that are a member of the configured group (or can only be accessed by users that are a member of the configured group when using the [is not] operator).
- *User device*: from the configured device(s) (or only from the configured devices when using the [is not] operator)
- *Request time*: within the configured time frame (or only within the configured time frame when using the [is not] operator)
- *IP Range (Source network)*: from the configured IP range (or only from the configured IP range when using the [is not] operator)

9.10.6 Logging

When classified documents are uploaded, log entries will be written to ownCloud's log file, (*data/owncloud.log*). For this, it is possible to additionally specify another metadata property that will be used to add its value to the log entries in the form of a "**Document ID**".

With this, it is possible to filter the log according to a document identifier or to forward classification events for certain documents to external log analyzers. To set it up, add the desired property XPath to the *Document ID XPath* field of the respective rule as you did for the classification property.

Each uploaded file will generate three entries with different log levels. See some exemplary entries below:

```
INFO:  `\"Checking classified file 'confidential.xlsx' with document id '2'`\`  
INFO:  `\"Alice uploaded a classified file 'confidential.xlsx' with document class 'Confidential'`\`  
DEBUG:  `\"Assigning tag 'Class: Confidential' to 'confidential.xlsx'`\`
```

9.10.7 Limitations

Automated Classification Based on Document Metadata: Handling Classification Changes for Existing Files

- When a formerly classified document is replaced with a new version that does not contain classification metadata, the classification tag will remain assigned, and configured policies will still apply. In this case, it is recommended to either delete the original or upload the new version with a different name.
- When a formerly unclassified document is replaced with a new version that does contain classification metadata, the classification tag will be assigned. However, when the policy “**Prevent upload**” is set up in addition, the original file will be deleted, and the new version will be rejected due to the policy.

THE OWNCLOUD X APPLIANCE

10.1 What is the Appliance?

If you don't know a lot about Linux, only have a small IT staff, or are your IT staff — even if that's only in your spare time — the ownCloud X Appliance will let you get started using ownCloud quickly and easily.

The Appliance:

- Provides a pre-packaged, easy to deploy ownCloud, ready for you in most popular virtual machine formats, including *ESX*, *VirtualBox*, *KVM* and *VMware*.
- Contains the ownCloud 10 virtual image, and all the additional software you need to get up and running on ownCloud in minutes; this includes: *ownCloud X Server and Enterprise Apps*, *Apache 2*, *PHP*, and *MySQL*.
- Scales up to 500 users. Depending on the intensity and pattern of use, this can vary from 400 up to 600 users.

Note: Some configurations, such as SAML IDPs, or LDAP or AD instances, may need additional configuration to connect.

10.2 How to Install the Appliance

The install process is a little involved, but not too much. To keep it succinct, you need to:

- *Download* and *Install* the appliance
- Step through *the configuration wizard*
- *Activate* the configured appliance

Important: You need **Internet access** to use the appliance. The appliance has to be activated with a license that you will receive from Univenton via email. This license has to be imported in the appliance via the **web interface**. The appliance also needs access to a DHCP server so that it can receive an IP address and be accessible.

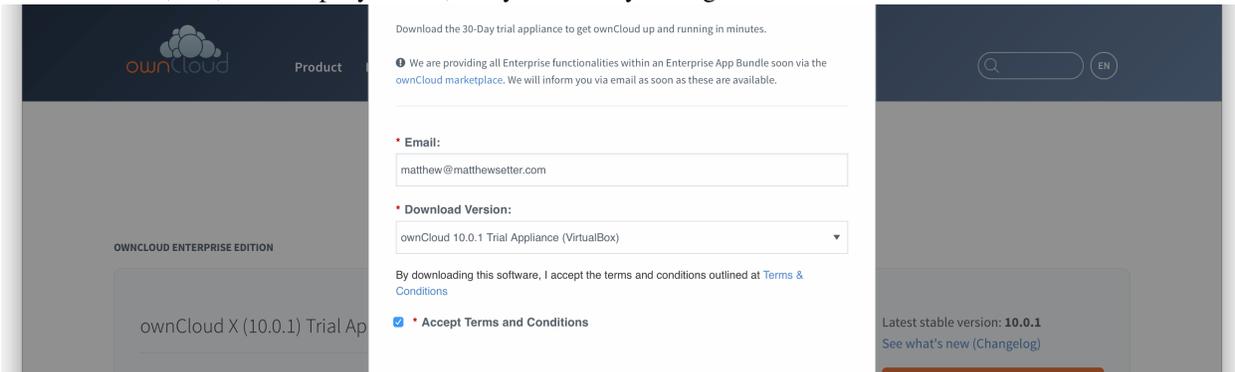
After that, you can access the running instance of ownCloud and *further configure it* to suit your needs.

10.2.1 Download the Appliance

First off, you need to download the ownCloud X Appliance from [the ownCloud download page](#) and click “DOWN-LOAD NOW”. This will display a form, which you can see a sample of below, which you'll need to fill out. It will ask you for the following details:

- Email address

- Download version (*ESXi, VirtualBox, VMware, KVM*)
- Your first, last, and company names, and your country of origin



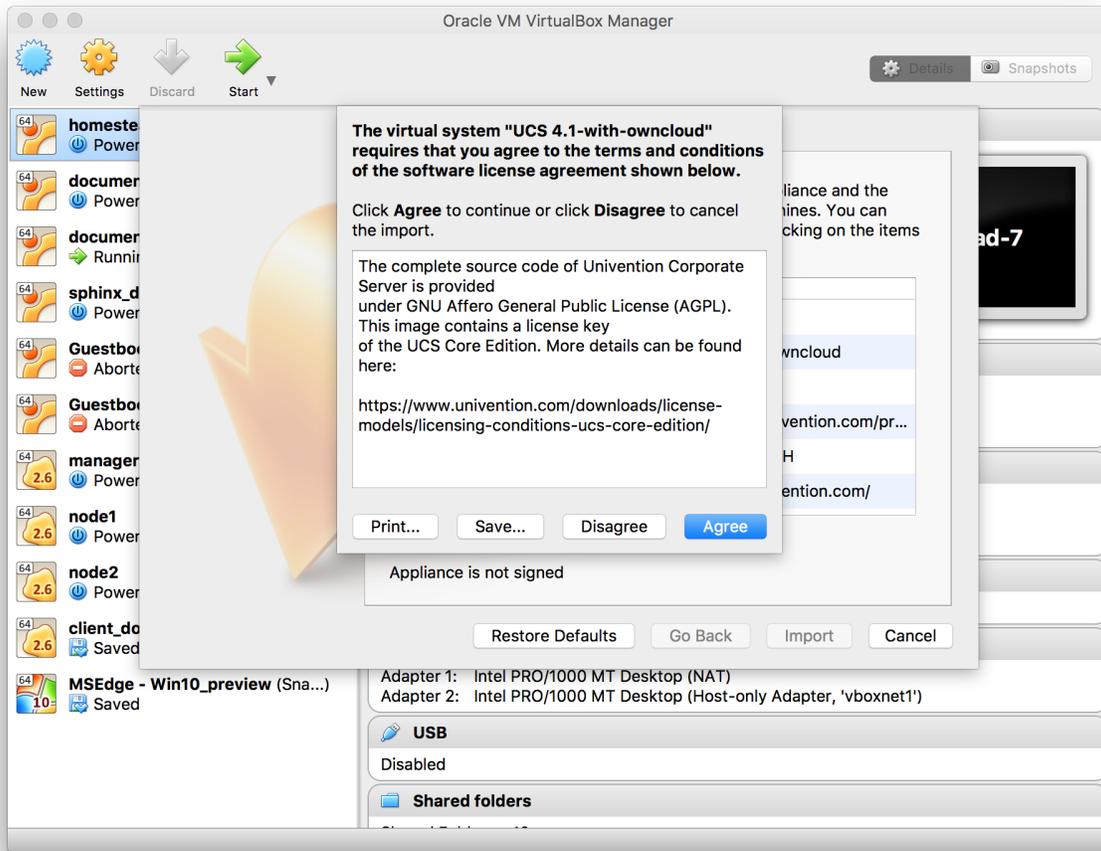
After you've filled out the form, click "**DOWNLOAD OWNCLOUD**" to begin the download of the virtual appliance.

Note: The virtual appliance files are around 1.4GB in size, so may take some time, depending on your network bandwidth.

Note: You can also download it from [the owncloud.org](https://owncloud.org) page.

10.2.2 Install the Appliance

Once you've downloaded the virtual appliance file, import it into your virtualization software, accept the T's & C's of the license agreement, and launch it. The example below shows this being done using VirtualBox.



Note: If you try to install an ownCloud appliance in your domain after removing an existing one, please remember to remove the original one from you DNS configuration.

Important: Don't Forget the **IP Address** and the **Administrator Password**. You will need them to use the Appliance.

10.2.3 Start the Appliance

Once imported, start the appliance. Doing so launches the installer wizard which helps you specify the core configuration. This includes:

Localization settings: Here, you can specify the language, timezone, and keyboard layout. Domain and network configuration: These settings can be either obtained automatically, via a DHCP lookup, or provided manually.

Domain setup: This lets you manage users and permissions directly within the ownCloud installation in the virtual appliance, or to make use of an existing Active Directory or UCS domain.

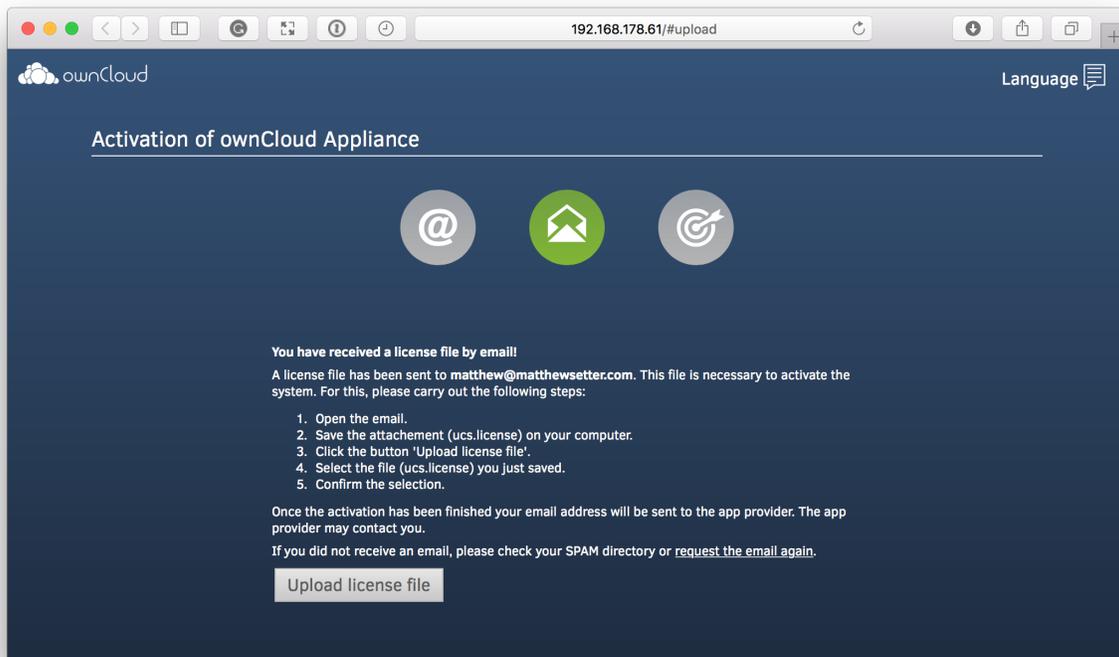
Account information: This lets you specify your organisation's name, the email address (used for receiving the license which you'll need to activate the appliance), and the administrator password. Note, this password is for the administrator (or root user) of the virtual machine, not for the ownCloud installation.

Host settings: This lets you specify the fully-qualified domain name of the virtual appliance, as well as an LDAP Base DN.

Once you've provided all of the required information, you can then finish the wizard, which will finish building the virtual appliance. Make sure that you double-check the information provided, so that you don't have to start over.

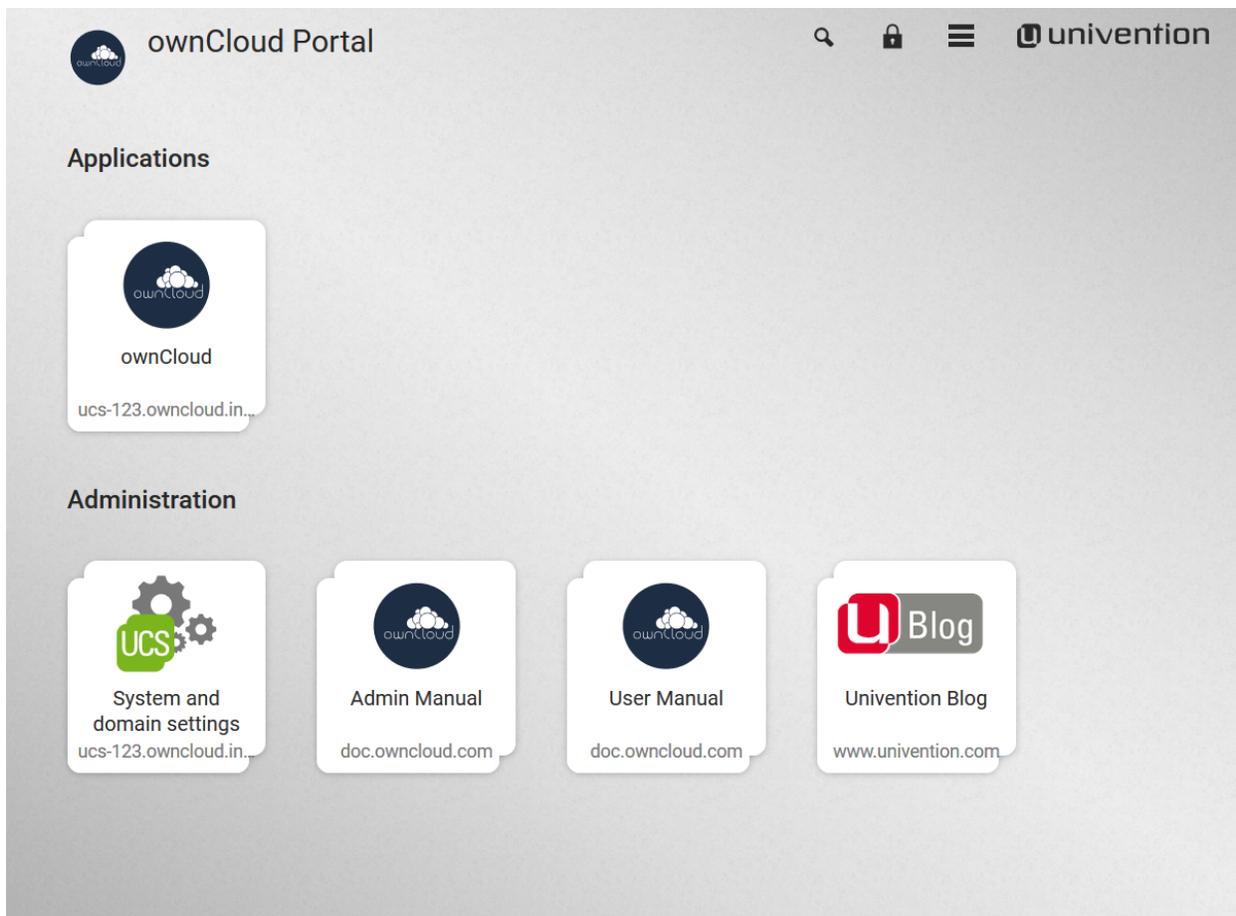
10.2.4 Activate the Appliance

When the wizard completes, the virtual machine will be almost ready to use. You then need only retrieve the license file from the email which was sent to you and upload it. The page to do that from can be found by opening your browser to the IP address of the virtual appliance, as you can see below. The installer may instruct you to use `https://` to access the activation page. If this gives an error in the browser, then remove the `https://`.

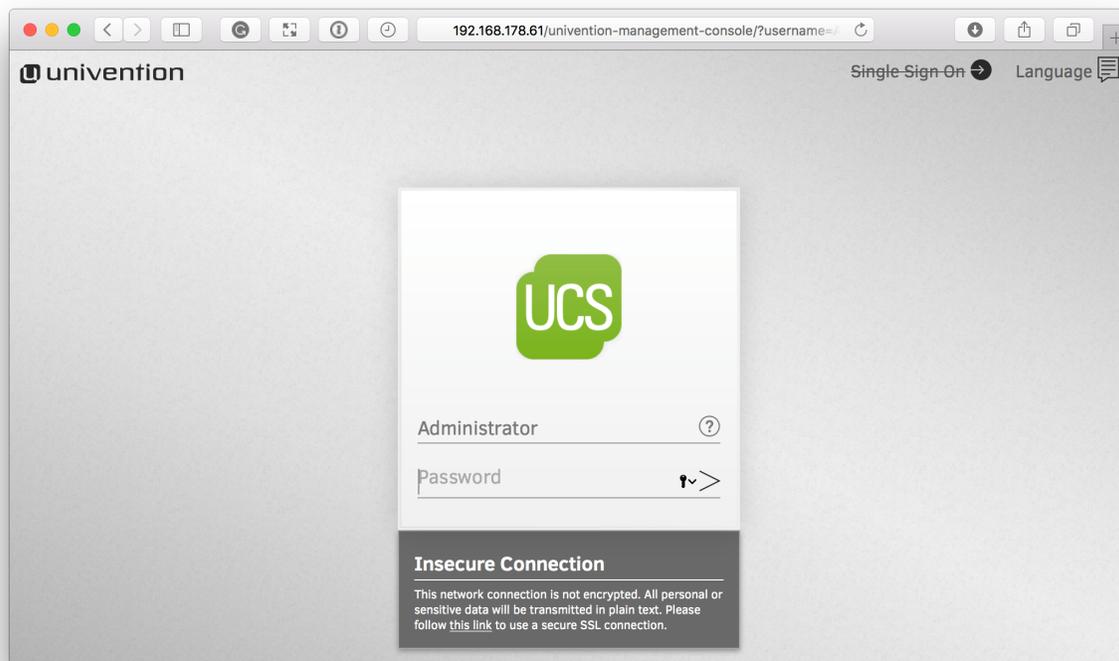


10.2.5 Administer the Appliance

Once activated, you should be redirected to the portal, which you can see below.

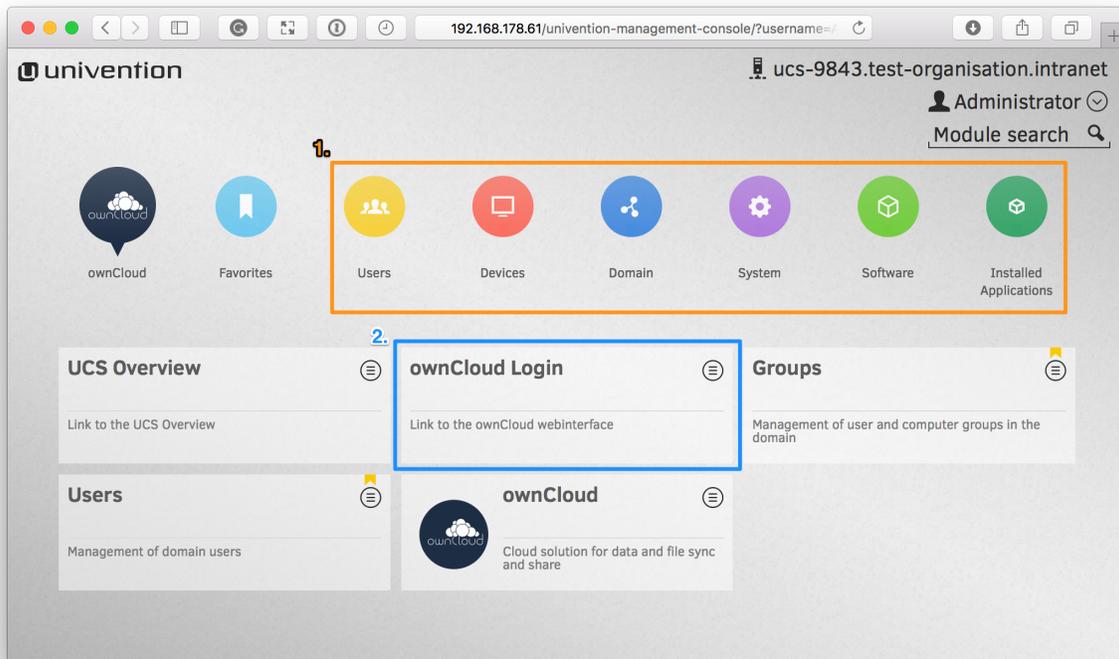


If you want to create new users and groups, or download apps from the Univention appcenter click on the “**System and domain settings**”. Login as the “**Administrator**” using the password that you supplied during the configuration wizard earlier.



Note: If you are not redirected to the appliance login page, you can open it using the following url: `https://<ip address of the virtual machine>/univention-management-console`.

After you've done so, you will now be at the Univention management console, which you can see below.



The management console allows you to manage the virtual appliance (1), covering such areas as: *users*, *devices*, *domains*, and *software*. You will also be able to access the ownCloud web interface (2).

Note: The default username for the ownCloud is: `owncloud` and so is the password. The password is **not** the password you supplied during the configuration wizard.

Note: For security reasons `rpcbind` should be disabled in the appliance. An open, from the internet accessible portmapper service like `rpcbind` can be used by an attacker to perform DDoS-Reflection-Attacks. Furthermore, the attacker can obtain information about your system, for example running `rpc-services`, or existing network shares. The german IT security agency “BSI” reported that systems with an open `rpcbind` service were used to perform DDoS-Reflection-Attacks against other systems. If you want to create NFS shares on the appliance and give someone permission to access them, then you can enable `rpcbind` again.

10.3 The ownCloud X Appliance Enterprise Trial

The appliance contains the community edition of ownCloud but can be easily upgraded to the enterprise edition. This upgrade gives you access to a free, 30-day trial of the enterprise edition and all its features. All you need is an email address to get started. Here are the necessary steps:

- Visit <https://marketplace.owncloud.com/enterprise-trial>
- Enter your email address and chose a password
- Click on Complete Process
- Check your email and activate your account
- Log in with your credentials at <https://marketplace.owncloud.com>

- Copy the API key

Now you have to go to your ownCloud installation and enable the Market app

- To enable enterprise features Select “Add API Key” and paste your key
- Start the Enterprise trial

Note

If you don't see the button to install the “Enterprise App Bundle” select “Clear cache” and refresh the page.

Now you have access to the full ownCloud enterprise experience.

10.4 ownCloud Appliance Login Information

Welcome to the ownCloud Appliance. Here are the login credentials.

```
username: owncloud
password: owncloud
```

Login to the Appliance via command line or SSH with the root account.

```
username: root
password: <Administrator password>
```

Login into the ownCloud docker container with this Univention command:

```
univention-app shell owncloud
```

ownCloud's data directory is under the following path:

```
/var/lib/univention-appcenter/apps/owncloud/data
```

ownCloud's config directory, containing config.php:

```
/var/lib/univention-appcenter/apps/owncloud/conf
```

10.5 How to Update ownCloud

There are two options to update an ownCloud installation hosted on an ownCloud X Appliance:

- Use the Univention Management Console
- Use the Command Line

Warning: Do not use the ownCloud built in web updater!

10.5.1 Use the Univention Management Console

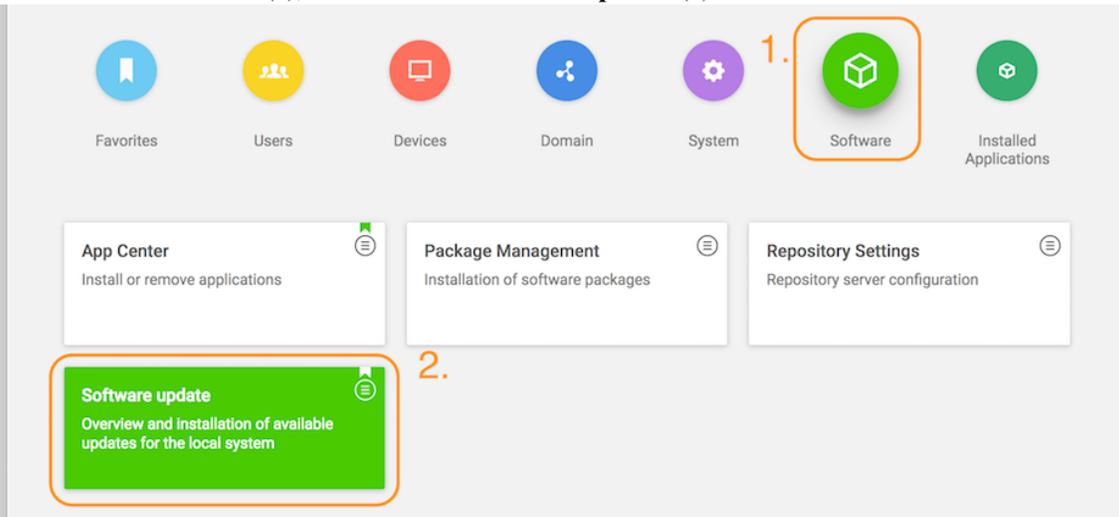
Using the Univention Management Console, there are two paths to upgrade an existing ownCloud installation:

- In-place Upgrade (for 10.0 users)
- Uninstall the Existing Version and Install the New Version (for 9.1 users)

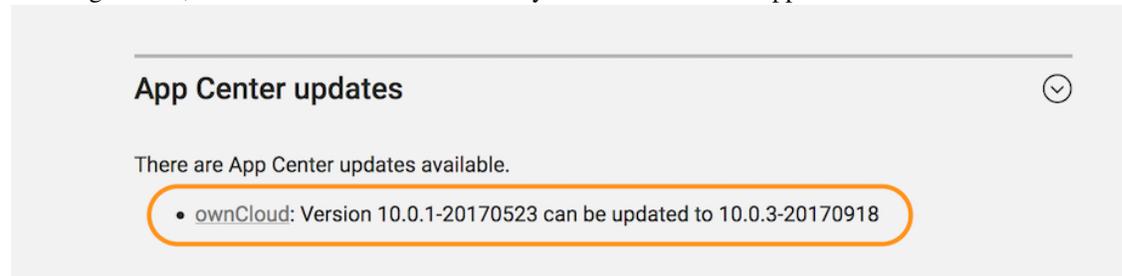
In-place Upgrade (for 10.0 users)

Note: Existing certificates and themes persist after an upgrade

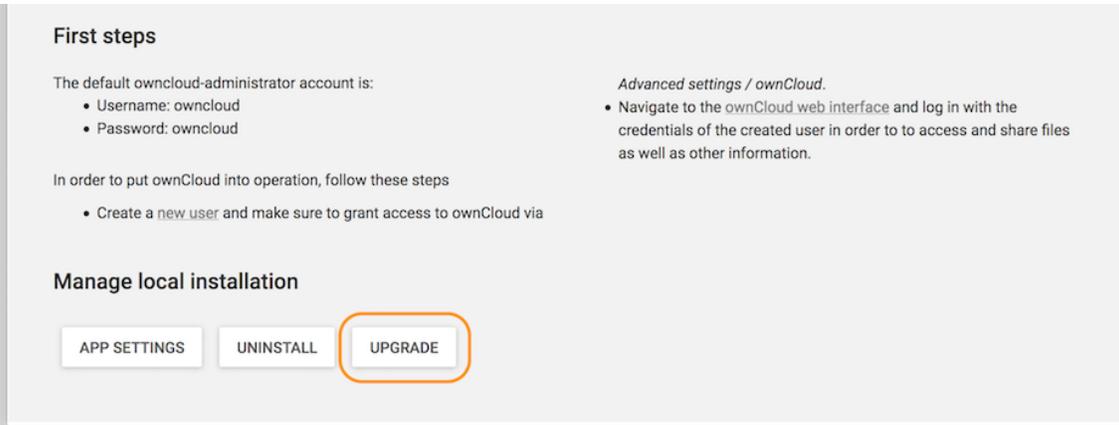
To perform an in-place upgrade, after logging in to the Univention server, under “**Administration**”, click the first option labeled “**System and domain settings**”. This takes you to the Univention Management Console. From there, click the “**Software**” shortcut (1), and then click “**Software update**” (2).



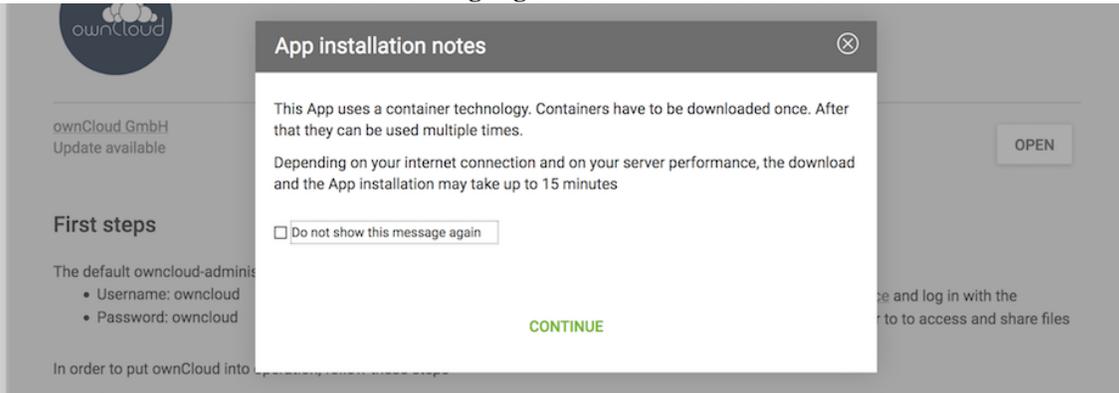
This will load the Software update management panel, after a short time scanning for available updates. If an update is available, under “**App Center updates**” you will see “**There are App Center updates available**”. If one is, as in the image below, click “**ownCloud**” which takes you to the ownCloud application.



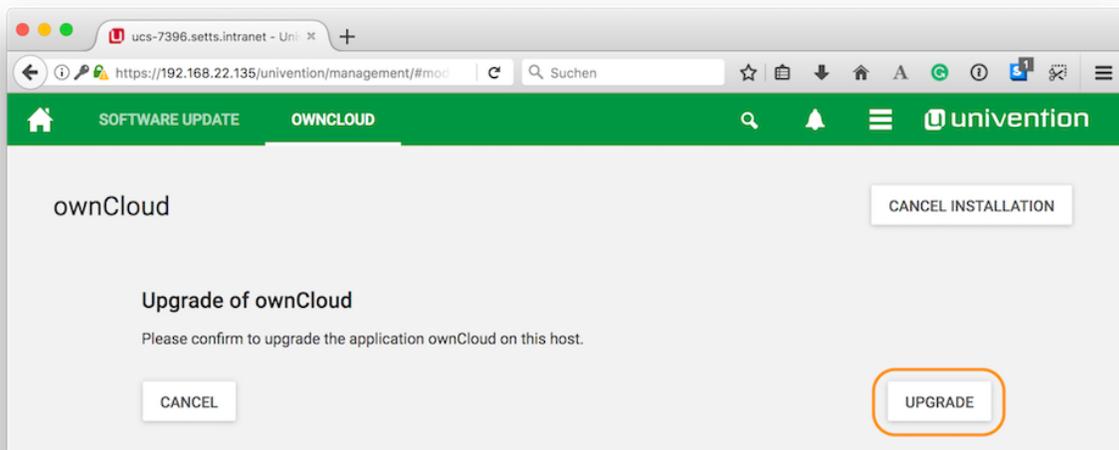
When there, part-way down the page you’ll see the “**Manage local installation**” section. Under there, click “**UPGRADE**”.



Before the upgrade starts, a prompt appears titled “App Installation notes”. This is nothing to be concerned about. So check the checkbox “Do not show this message again”. Then click “CONTINUE”.



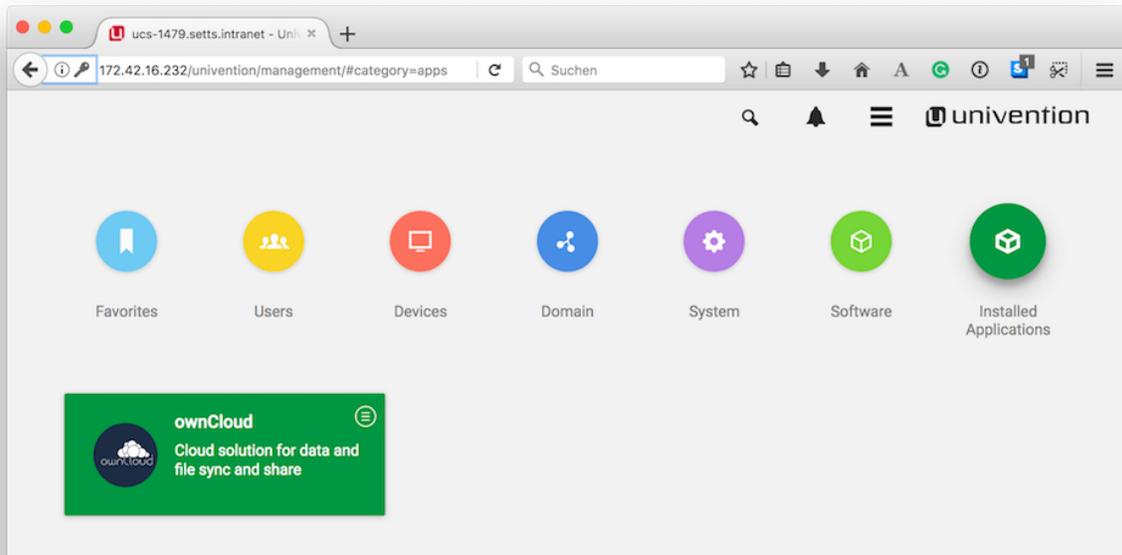
Next an upgrade confirmation page appears. To accept the confirmation, click “UPGRADE” on the far right-hand side of the confirmation page.



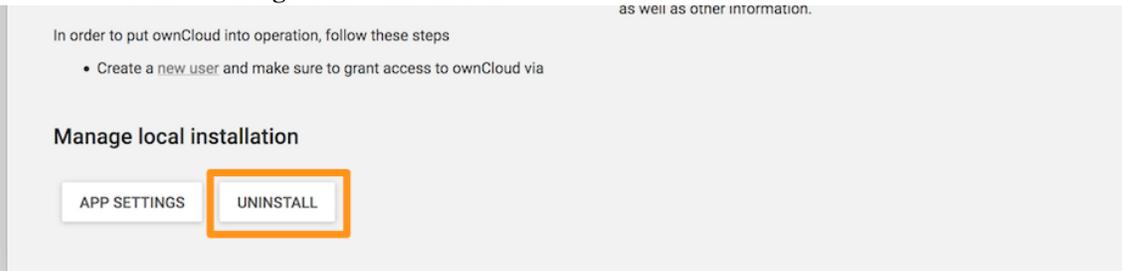
This launches the upgrade process, which requires no manual intervention. When the upgrade completes, the ownCloud app page will be visible again, but without the “UPGRADE” button. Now, login to ownCloud by clicking the “OPEN” button, on the far right-hand side of the page.

Uninstall the Existing Version and Install the New Version (for 9.1 users)

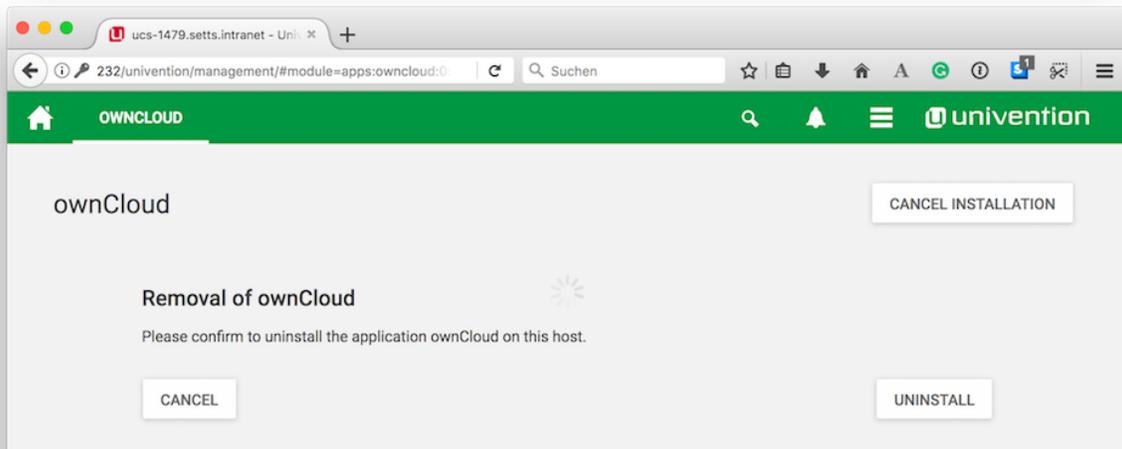
Open your ownCloud X Appliance and go to the “**System and Domain Settings**” dashboard. Then, after logging in, click “**Installed Applications**”, and then click ownCloud.



This takes you to the ownCloud app settings page. From there, begin uninstalling ownCloud by clicking “**UNINSTALL**” under “**Manage local installations**”

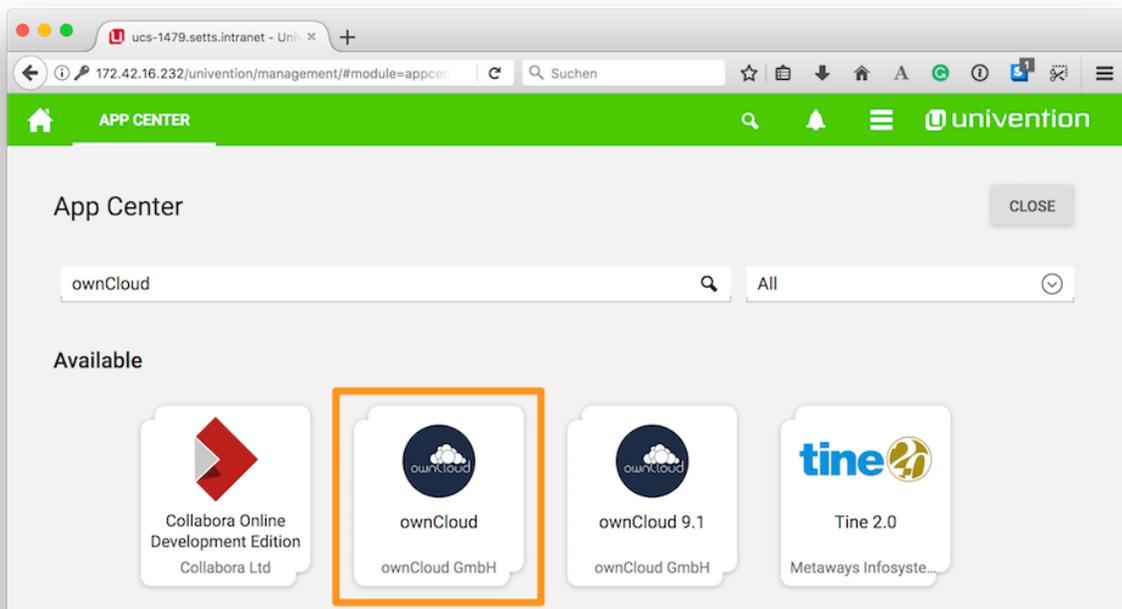


This takes you to an uninstall confirmation page. On that page, click UNINSTALL on the lower left-hand side of the page.



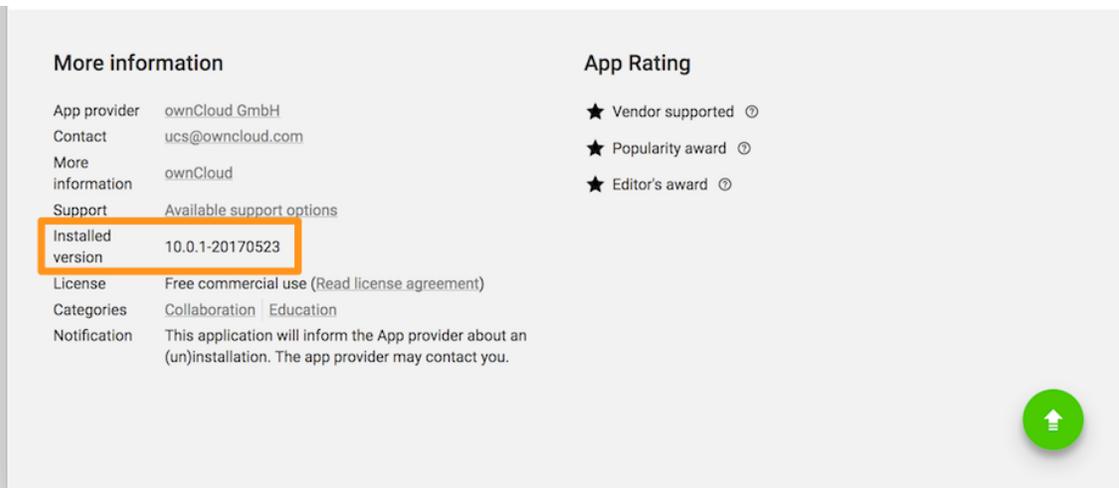
Follow the process until it's finished. Then, click on “Close” in the upper right corner.

Note: Your data and users will remain.

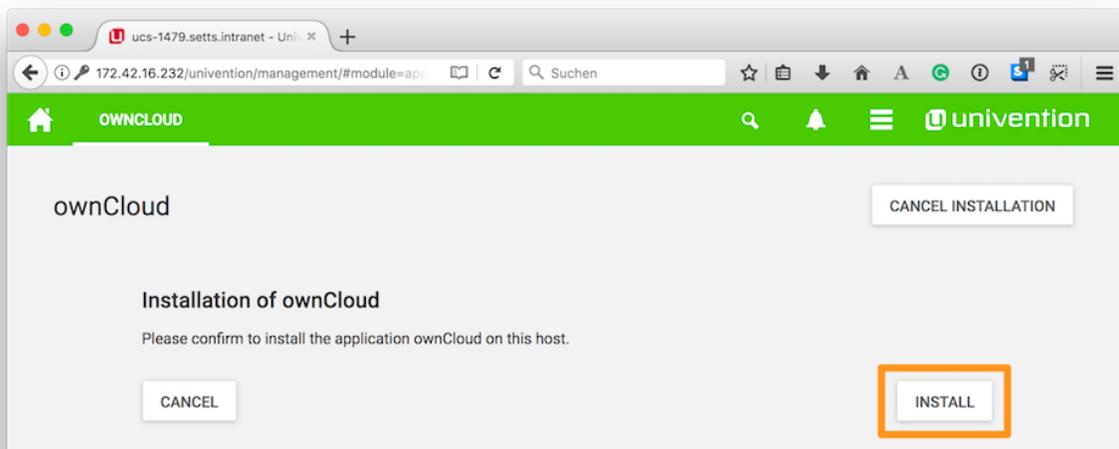


Following that, go to “Software - Appcenter”, and search for “ownCloud”. At the moment, two matching results will be returned. Pick the one that does not contain a version number.

To confirm the version number, scroll to the bottom of the page, and in the More information section, look for the version string, next to Installed version, as in the screenshot below.



If it is the right version, click **“INSTALL”**. Then the License Agreement is displayed. If you agree to it, click **“ACCEPT LICENSE”**. This will display an installation confirmation screen. To confirm the installation, click **“INSTALL”**.



The installation will then be carried out. When it is finished, you will have the latest version of ownCloud installed.

Note: Your data and users will persist.

10.5.2 Use the Command Line

As with the Univention Management Console, there are two paths to upgrade an existing ownCloud installation from the command line:

- [Upgrading From Version 10.0.1 to 10.0.3](#)
- [Upgrading From Versions Prior to 10.0](#)

Upgrading From Version 10.0.1 to 10.0.3

Upgrading from the command line is also available. To do so, login to your ownCloud X Appliance, either via ssh or directly on the server. Once logged in, check if there is an upgrade available.

You can use the command `univention-app info`. This command lists information about the current state of every installed App.

```
root@ucs-9446:~# univention-app info
UCS: 4.2-1 errata165
App Center compatibility: 4
Installed: 4.1/owncloud=10.0.1-20170523
Upgradable: owncloud
```

If an upgrade is available, you then need to run the `univention-app upgrade`, as in the example below.

```
univention-app upgrade owncloud
```

You will have to enter your Administrator password to start the upgrade. This command takes some time to complete, primarily based on the appliance's network connection speed. However, it should not take more than a few minutes.

After the upgrade has completed (if it was successful) as a sanity check, run `univention-app info`, to confirm the currently installed version of ownCloud. As in the example below, you should see that the installed version is now higher than before, and that ownCloud is no longer upgradable.

```
root@ucs-9446:~# univention-app info
UCS: 4.2-1 errata165
App Center compatibility: 4
Installed: 4.1/owncloud=10.0.3-20170918
Upgradable:
```

Upgrading From Versions Prior to 10.0

If you're running a version of ownCloud prior to 10.0, the above in-place upgrade doesn't work. This is because the earlier versions of ownCloud are installed with a different application to the 10.x version. More specifically, the versions of the ownCloud app, prior to 10, have a version suffix in the name. For example the ownCloud 8.2 app is named `owncloud82`.

For ownCloud 8.2 users: during the ownCloud App upgrade, user files will be moved to the new Docker data directory, `/var/lib/univention-appcenter/apps/owncloud/data/files`. Essentially, the following the command will be executed:

```
:: mv /var/lib/owncloud/* /var/lib/univention-appcenter/apps/owncloud/data/files
```

Please check your filesystems and mountpoints and make sure enough space is available for the operation.

Given that, you first have to uninstall the existing version and then install the 10.x version. To do so, run the following commands:

```
# Assumes that owncloud82 is the currently installed version
univention-app remove owncloud82
univention-app update
univention-app install owncloud
```

And after the upgrade and updates are completed, you can then login to ownCloud and verify the upgrade.

Username and Password remain the same as before the upgrade:

```
owncloudadmin
password
```

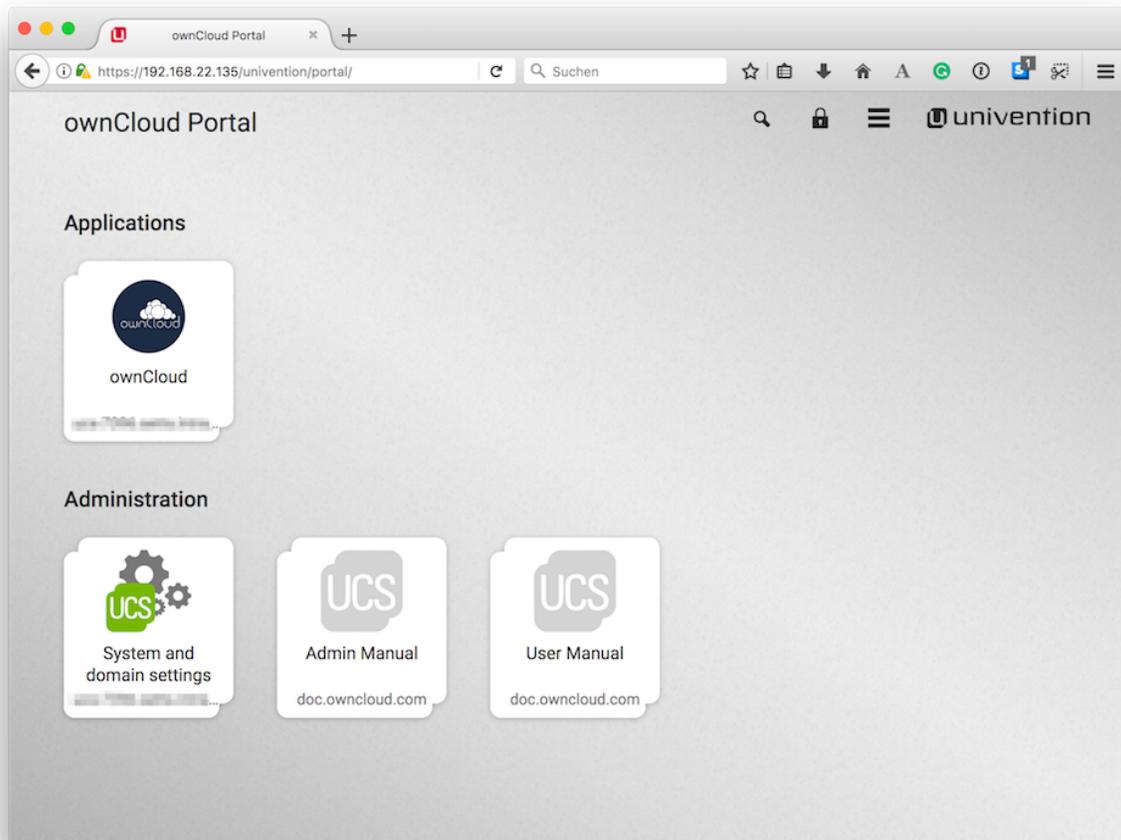
10.6 Managing UCS

10.6.1 Adding Users and Groups in UCS for ownCloud

If you want to add users and groups to your ownCloud installation via the UCS (Univention Corporate Server) UI, here's a concise guide showing how.

Login to the Univention Management Console

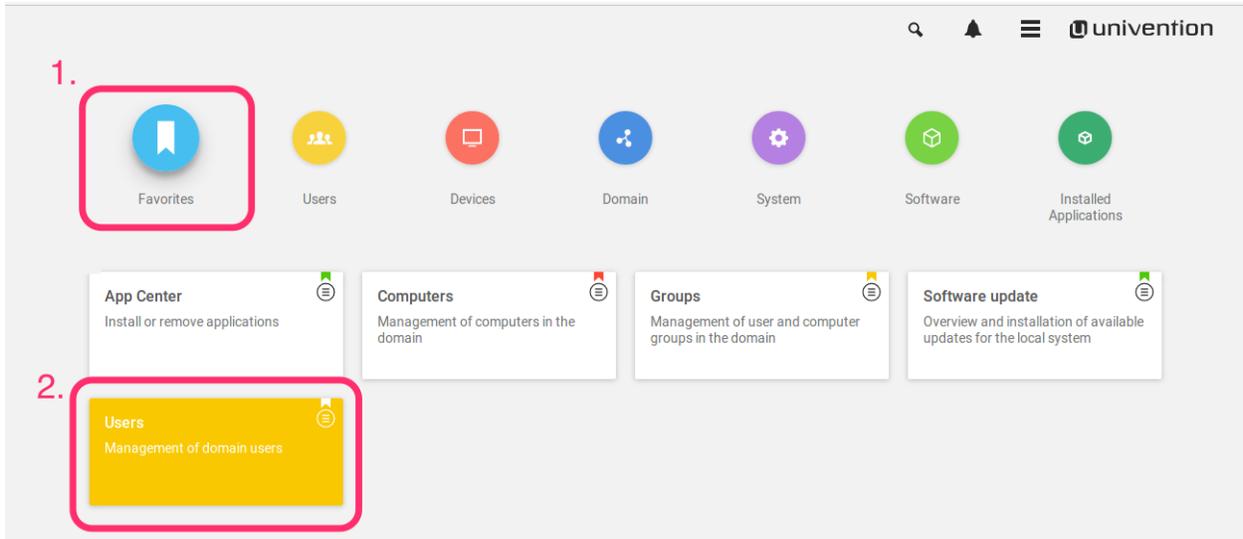
After logging in to the Univention server, under “**Administration**”, click the first option, labeled “**System and domain settings**”.



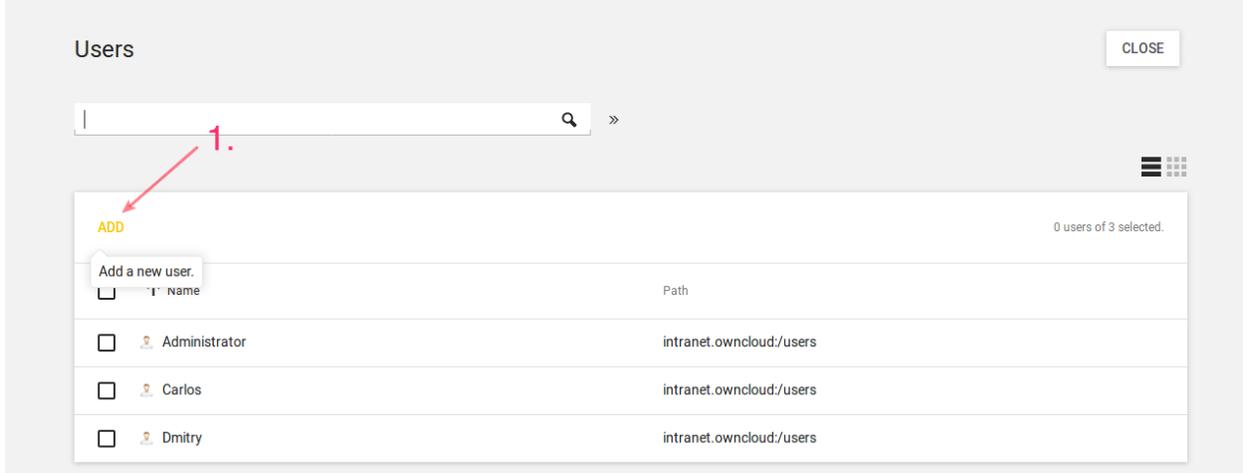
This takes you to the Univention Management Console.

Create the User

Once there, click “**Users**”.



In the screen that appears, add a new user by clicking “ADD” in the top left-hand corner of the users table.



This opens up a new user dialog, where you can supply the relevant details for the new user. Enter a username and optionally a first name, last name, and a title. Then click “NEXT”.

Add a new user.
✕

Title	First name	Last name *

User name *

CANCEL

2.

NEXT

In the next dialog that appears, enter and confirm the password. You can, optionally, choose some further options, if desired. Then click “**CREATE USER**”.

Add a new user.
✕

1.	2.
Password *	Password (retype) *

Change password on next login ?

Override password check

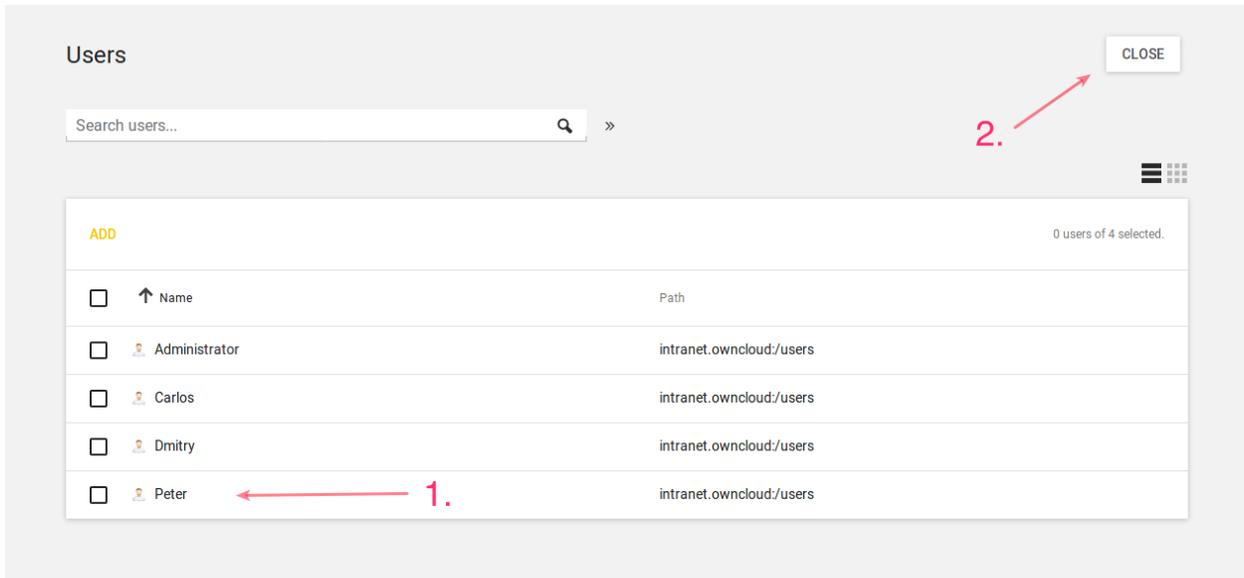
Account disabled

CANCEL

2.

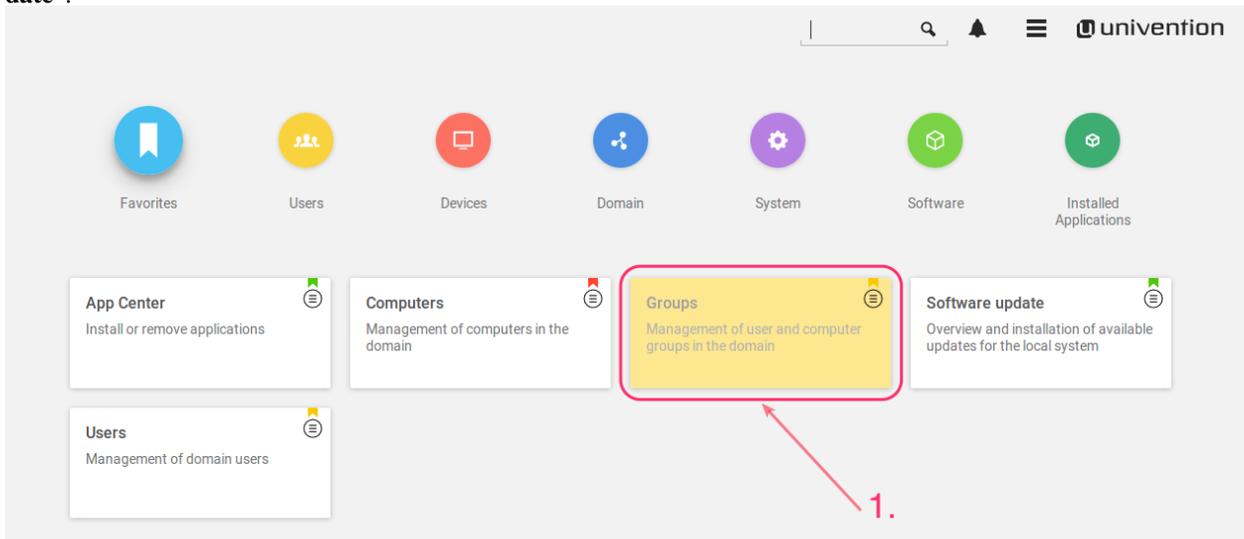
CREATE USER

The new user will have been created, so click the “**CLOSE**” button, in the top right-hand corner, to go back to “**Favorites**”.

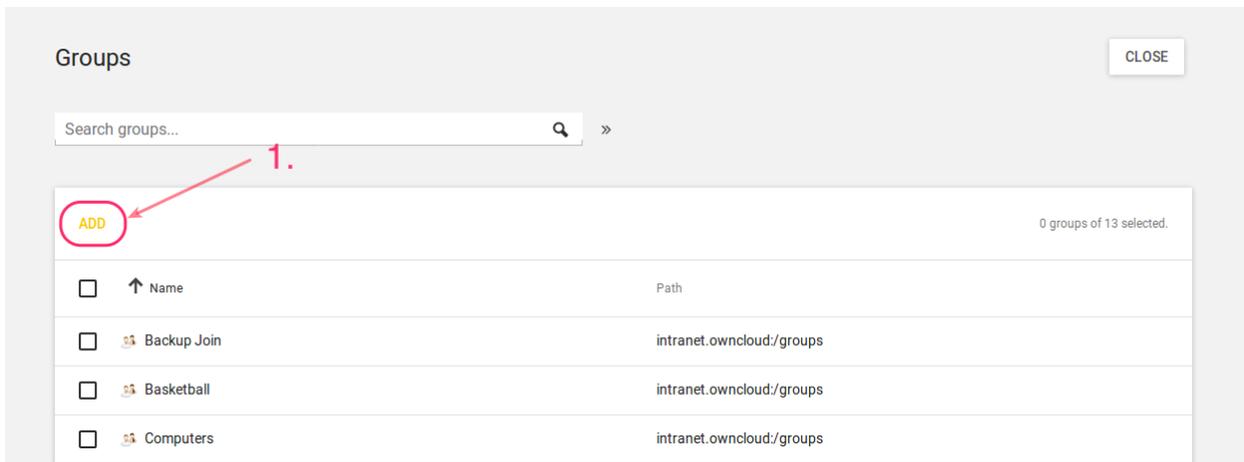


Create the Group

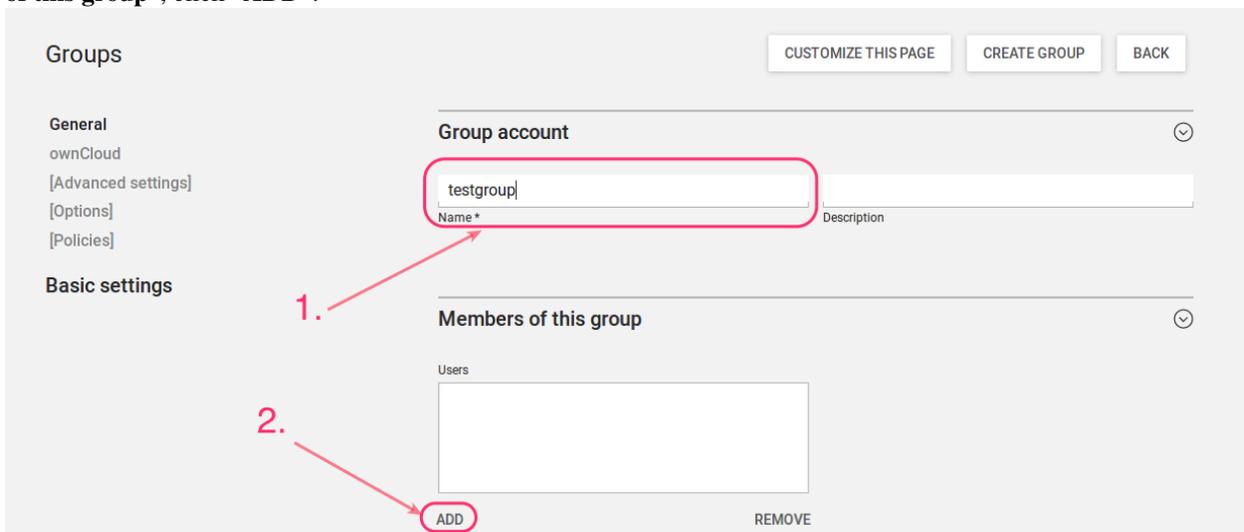
Now it's time to create a new group. Click **"Groups"**, which is located between **"Computers"** and **"Software Update"**.



From there, click **"ADD"**, located on the left-hand side of the groups table.



In the next dialog that appears, first enter the name of the group and optionally a description. Then, under “**Members of this group**”, click “**ADD**”.



This opens up an “**Add objects**” (or “Add new group”) dialog. Find the user, in the list at the bottom, that you want to add to the group, check the checkbox next to their name, and click “**ADD**”.

Add objects ⊗

Default properties ⌵

Object property

Default properties

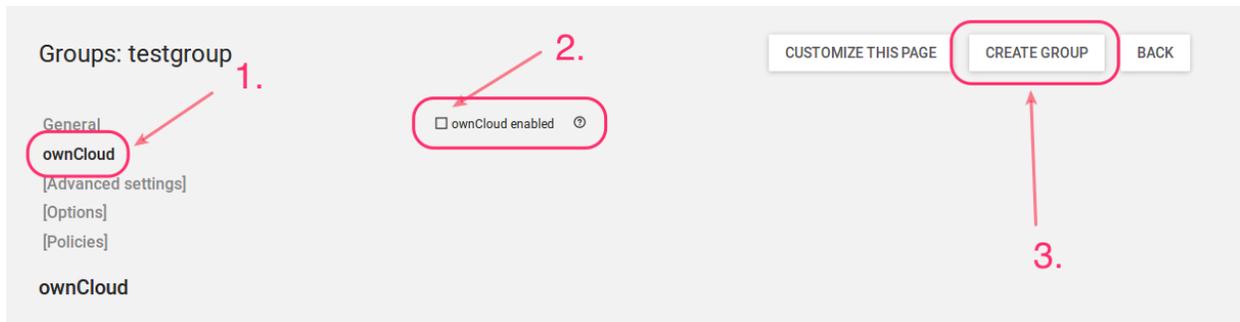
include hidden objects 🔍 1.

Search results:

<input type="checkbox"/>	Select all
<input type="checkbox"/>	Administrator
<input type="checkbox"/>	Carlos
<input type="checkbox"/>	Dmitry
<input checked="" type="checkbox"/>	Peter

→

After that, click on “ownCloud” in the left-hand side navigation, and check the option “ownCloud enabled”. And lastly, click “CREATE GROUP”.



With that done, the new user and group are now available in your ownCloud installation.

Note: Depending on your installation, you will either see these changes immediately or you will have to wait for the user sync to be done. This happens ever 10 minutes by default.

10.7 Install Antivirus Software in the ownCloud Appliance

This guide details how to enable a virus scanner in the ownCloud Appliance. It is composed of two parts:

1. [Install ClamAV and related components](#)
2. [Configure ownCloud to use ClamAV](#)

10.7.1 Install ClamAV and Related Components

First, start the appliance and go to “**System and domain settings**”.

When there, log in with the administrator account. After you have done that, click “**Software**” and open “**Package Management**”, as in the screenshot below.

From there, you first need to install ClamAV. To do this, in the third field, next to the one containing the text “**Package name**”, type in the phrase: “**clamav**” (1). Doing so filters the list of packages to only those matching that phrase. In the filtered list of packages, check the checkboxes next to “**clamav**” (2), “**clamav-freshclam**”, and “**clamav-daemon**”.

After doing that, click “**INSTALL**” (3) above the listed packages, next to “**SHOW DETAILS**”, to install them.

After you do so, a confirmation dialog appears, as in the screenshot below, asking for confirmation to install the packages. Confirm the choice by again clicking “**INSTALL**”.

The installation should only take a few minutes.

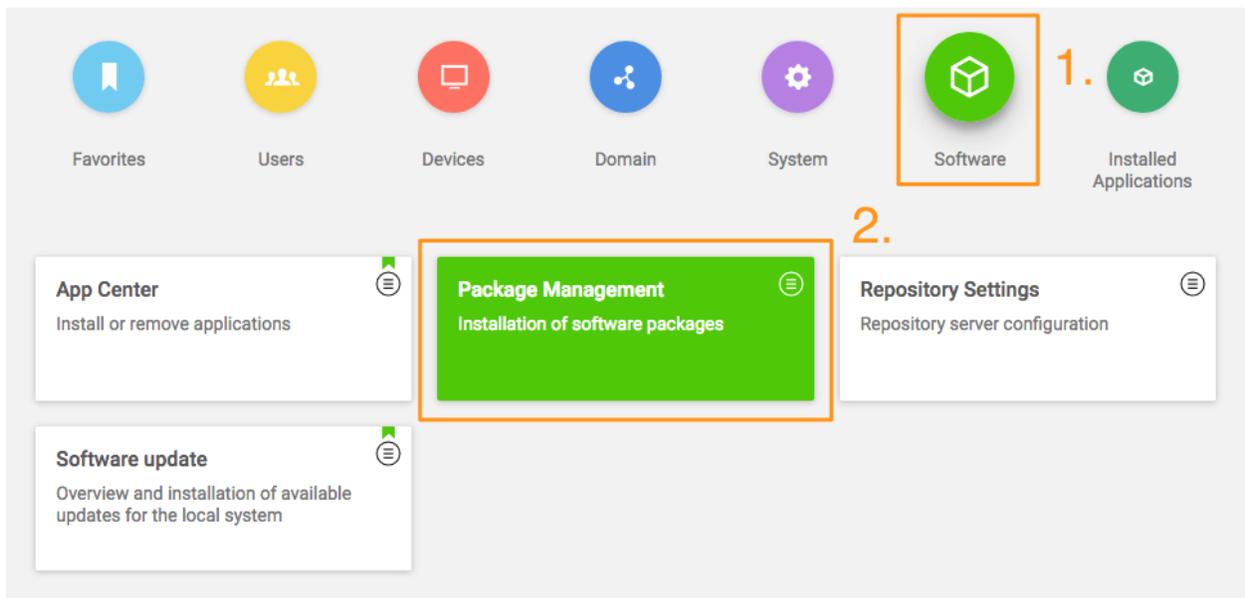
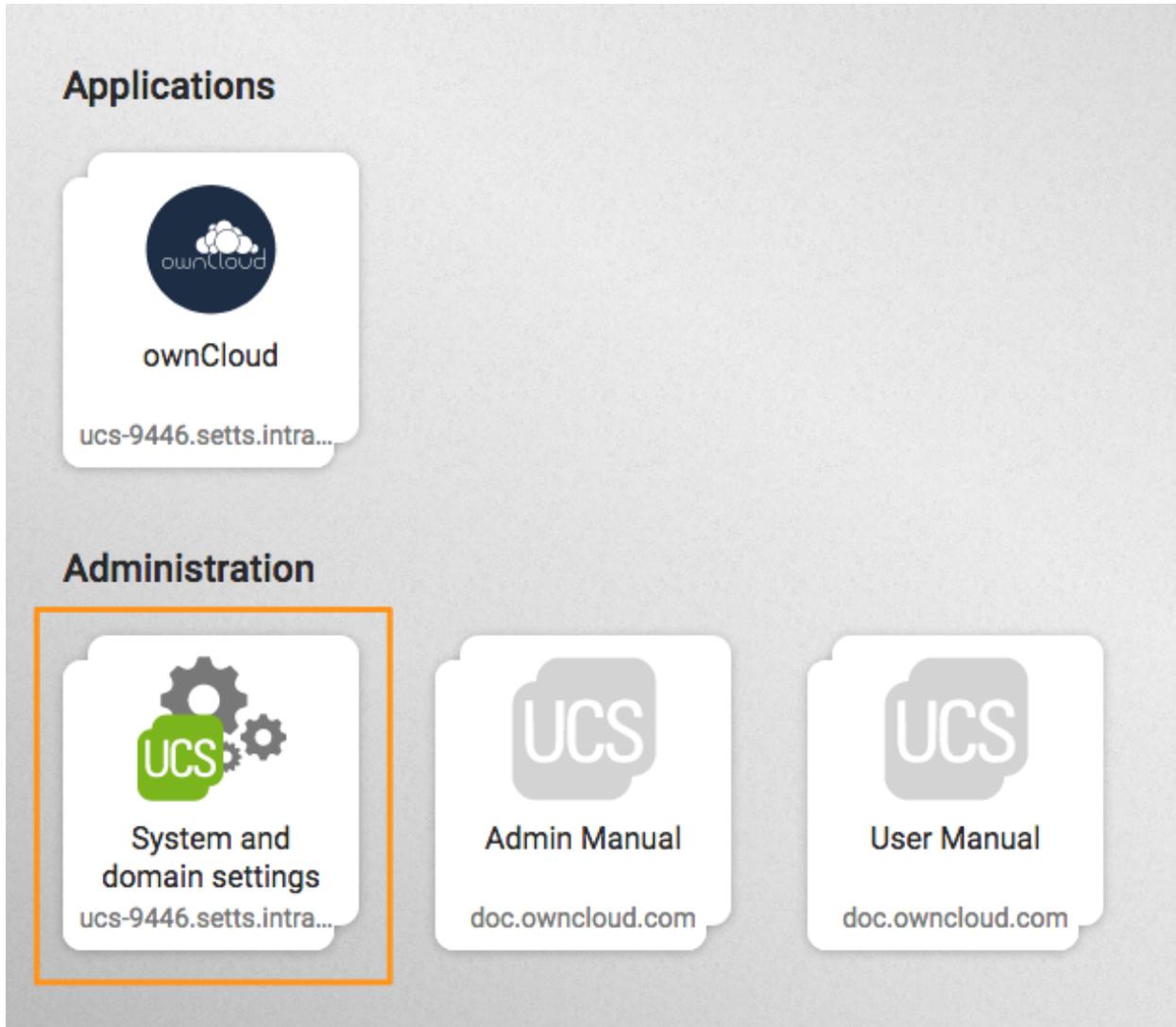
10.7.2 Configure ownCloud to Use ClamAV

You next need to configure ClamAV in your ownCloud instance. Please refer to [the ClamAV documentation](#) for instructions on how to do that.

If you try to update the ClamAV virus database manually, by entering `freshclam`, and see the error below, it means that `freshclam` is already updating the database.

```
ERROR: /var/log/clamav/freshclam.log is locked by another process
ERROR: Problem with internal logger (UpdateLogFile = /var/log/clamav/freshclam.log).
```

Updates are run based on the configured time interval in the applicable Cron job. In the example below, the update would run every 47 minutes:



PACKAGE MANAGEMENT

Package Management CLOSE

On this page, you see all software packages available on your system, and you can install, uninstall or update them.

Package categories: -- all -- Package name: clamav

2 entries of 11 selected

<input type="checkbox"/>	Package name	Package description	Installation status
<input checked="" type="checkbox"/>	clamav	anti-virus utility for Unix - command-line interface	not installed
<input type="checkbox"/>	clamav-base	anti-virus utility for Unix - base package	not installed
<input checked="" type="checkbox"/>	clamav-daemon	anti-virus utility for Unix - scanner daemon	not installed

Confirmation

Do you really want to install clamav, clamav-daemon?

The following packages will be installed or upgraded:

- clamav
- clamav-base
- clamav-daemon
- clamav-freshclam
- clamdscan
- libclamav7
- libmspack0

CANCEL

INSTALL

```
# m h dom mon dow command
47 * * * * * /usr/bin/freshclam --quiet
```

If there are errors running the freshclam process, check if a process is blocking the log file, by running the following command:

```
lsof /var/log/clamav/freshclam.log
```

If you want to refresh the ClamAV database manually, follow these steps:

```
# Gently end the freshclam process with this command:
sudo pkill -15 -x freshclam
```

```
# Start the refresh process again with this command:
sudo freshclam
```

..warning:

When the app is enabled -- but is not configured or has an incorrect configuration -- it will reject

10.8 How To Add Certificates

10.8.1 Let's Encrypt App

Univention offers an easy way to get secure certificates with their Let's Encrypt app. To install it:

- In the **Univention Appcenter**, click on **Software** and search for **Let's Encrypt**.
- Go to the **App Settings** and generate an certificate by entering your **domain name(s)**.
- After the certificate is generated, restart the web server (or the appliance).

10.8.2 Import your own certificates

If you want to use your own SSL certificates for the appliance, you have to follow these three steps:

1. Create the certificates and deposit them on your appliance.
2. Connect to your appliance either directly on the command line of your virtual machine or via ssh connection to your appliance.
3. Execute the following commands:

```
ucr set apache2/ssl/certificate="/etc/myssl/cert.pem"
ucr set apache2/ssl/key="/etc/myssl/private.key"
```

Note: Remember to adjust the path and filename to match your certificate.

Once you've completed these steps, restart Apache using the following command:

```
service apache2 restart
```

Now your certificates will be used to access your appliance.

If you want to limit the access to your server exclusively to HTTPS, use this command:

Let's Encrypt BACK TO OVERVIEW

UCS Let's Encrypt

Univention GmbH
Installed

First steps

1. Make sure your system is reachable from the Internet for validation.

```
host -t A service1.example.com  
service1.example.com has address 1.2.3.4
```
2. Open the App Settings below. Set your desired domain(s) and services and click "Save changes". You can check if the certificate has been obtained successfully by checking the "Status" field in the App Settings approx. 10 seconds afterwards.
3. Once the certificate has been configured, you need to restart the desired services via the "System services" module in the UMC. This is only required during setup. The automatic renewal mechanism restarts the services if needed.
If you want to change the hostname in the certificate later on, just change the configuration in the App Settings and save.

The app adds the Let's Encrypt certificate authority to the system's CA store. In order for all software to recognize the certificate as valid, the following command needs to be executed once. This can prevent problems with programs such as curl with a Let's Encrypt certificate configured. Web browsers and such recognize the certificate as valid without any issues nonetheless:

```
update-ca-certificates
```

If you encounter problems with the obtained certificate, please have a look at the status of the App via the App Settings page and the log file `/var/log/univention/letsencrypt.log`. All actions of the app are written to this log file. Also, refer to the "Troubleshooting" section in the original [article about Let's Encrypt](#) in the Univention Wiki.

To see if Let's Encrypt's systems are operational, check their [status page](#).

Manage local installation

APP SETTINGS UNINSTALL

Let's Encrypt

APPLY CHANGES CANCEL CONFIGURATION

Configure Let's Encrypt

Domains

Domain(s) to obtain a certificate for, separated by space

Services

Use certificate in Apache

Use certificate in Dovecot

Use certificate in Postfix

Use Let's Encrypt's staging environment

You can activate this option to use Let's Encrypt's staging environment. An invalid certificate will be issued. This certificate is not usable for production systems, because its CA is not present in browsers etc. and just suitable for testing purposes. As long as this option is active, no changes will be made to the configured services. More information: <https://letsencrypt.org/docs/rate-limits/>

```
ucr set apache2/force_https=yes
```

10.9 Active Directory Integration

In case you have tested the appliance with your Active Directory environment, removed the appliance and now want to include it again - you might run into some issues.

The solution is to clean up the previous DNS entries in your Domain Controller.

After that, you should be able to include the appliance again in your Active Directory environment.

10.10 Backup

If you remove the ownCloud app or update it - a backup is created automatically.

The backup remains on the host system and can be restored.

It is stored in

```
/var/lib/univention-appcenter/backups/
```

The file name is

```
appcenter-backup-owncloud:date
```

In it, you find your data and conf folders.

Your database backup is in

```
/var/lib/univention-appcenter/backups/data/backups
```

10.11 Working on Documents in the ownCloud Appliance

Creating and editing documents in ownCloud can be achieved with either Collabora or OnlyOffice. It's your choice which one you prefer to use.

This guide covers the setup and update of the two office apps.

Here is an overview of the process:

1. Access the *Appcenter*
2. Install *Collabora* or *OnlyOffice*
3. *Update* the App

Warning: Access with **HTTPS** using **domain name** is required. Add the IP address and the domain name of your appliance to your */etc/hosts* file, or have it added to your existing DNS server, if you don't want to use the Appliance as your DNS server.

If you encounter the error, "Failed to load the document. Please ensure the file type is supported and not corrupted, and try again.", when trying to open documents, either restart the Collabora Docker container or the appliance.

10.11.1 Appcenter

First you have to get to the Appcenter. Here are the steps to do that:

1. Connect to your appliance using IP address or domain name.

```
https://172.16.40.100  
# or  
https://ucs-2341.CompanyName.com
```

2. Login into the management console
 - Click on the **Domain and System** settings
 - Type in the Administrator as username and the password you set.
3. Now you can access the **Appcenter**".

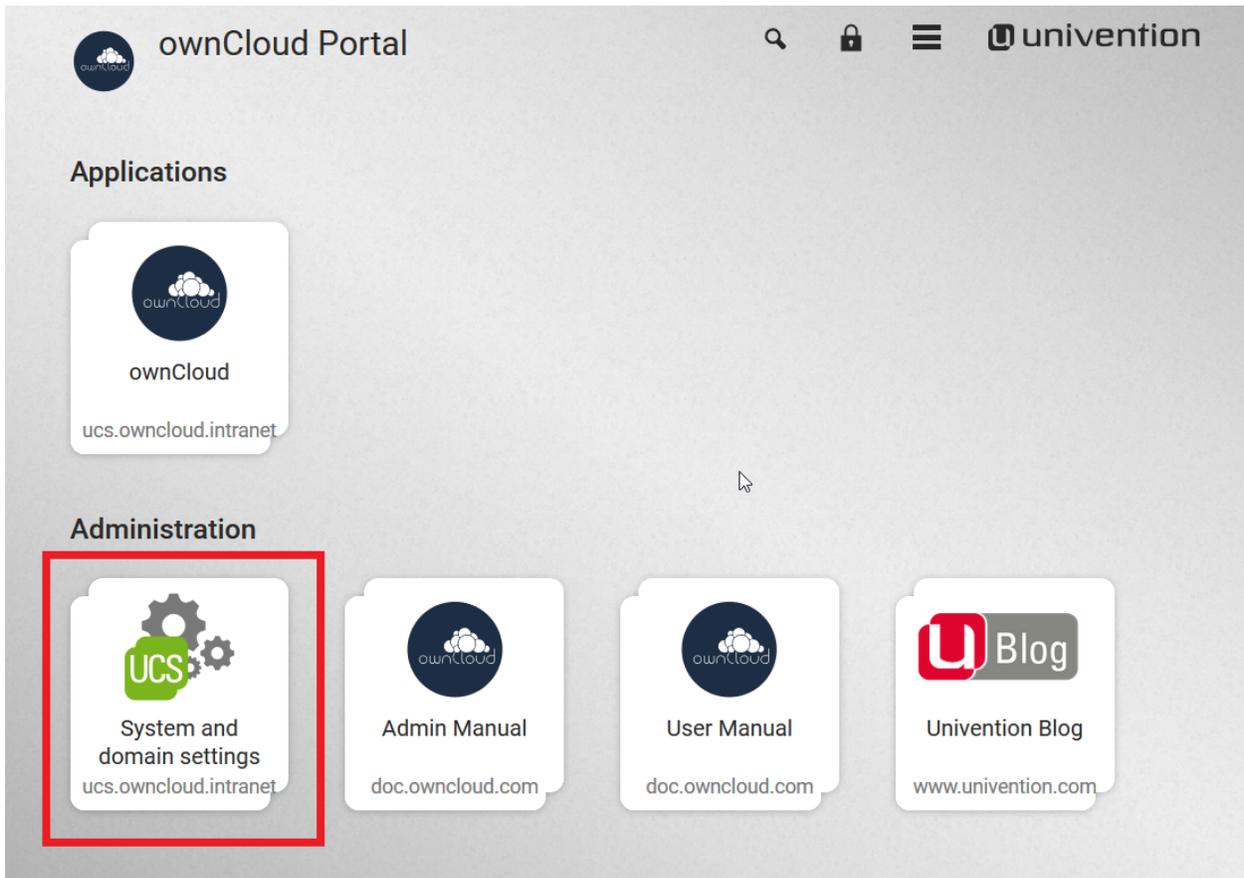
From here on it's your choice to install *Collabora* or *OnlyOffice*.

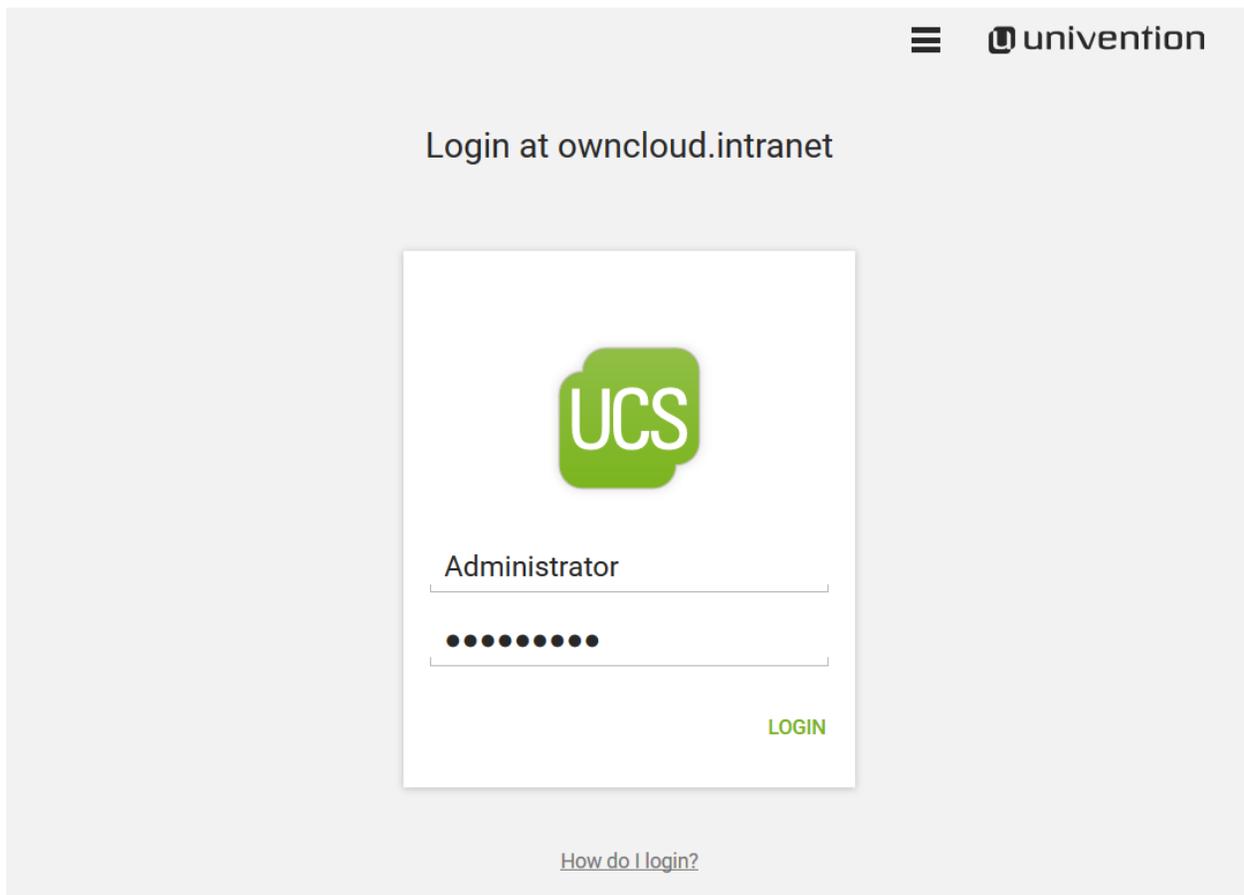
10.11.2 How to Install Collabora

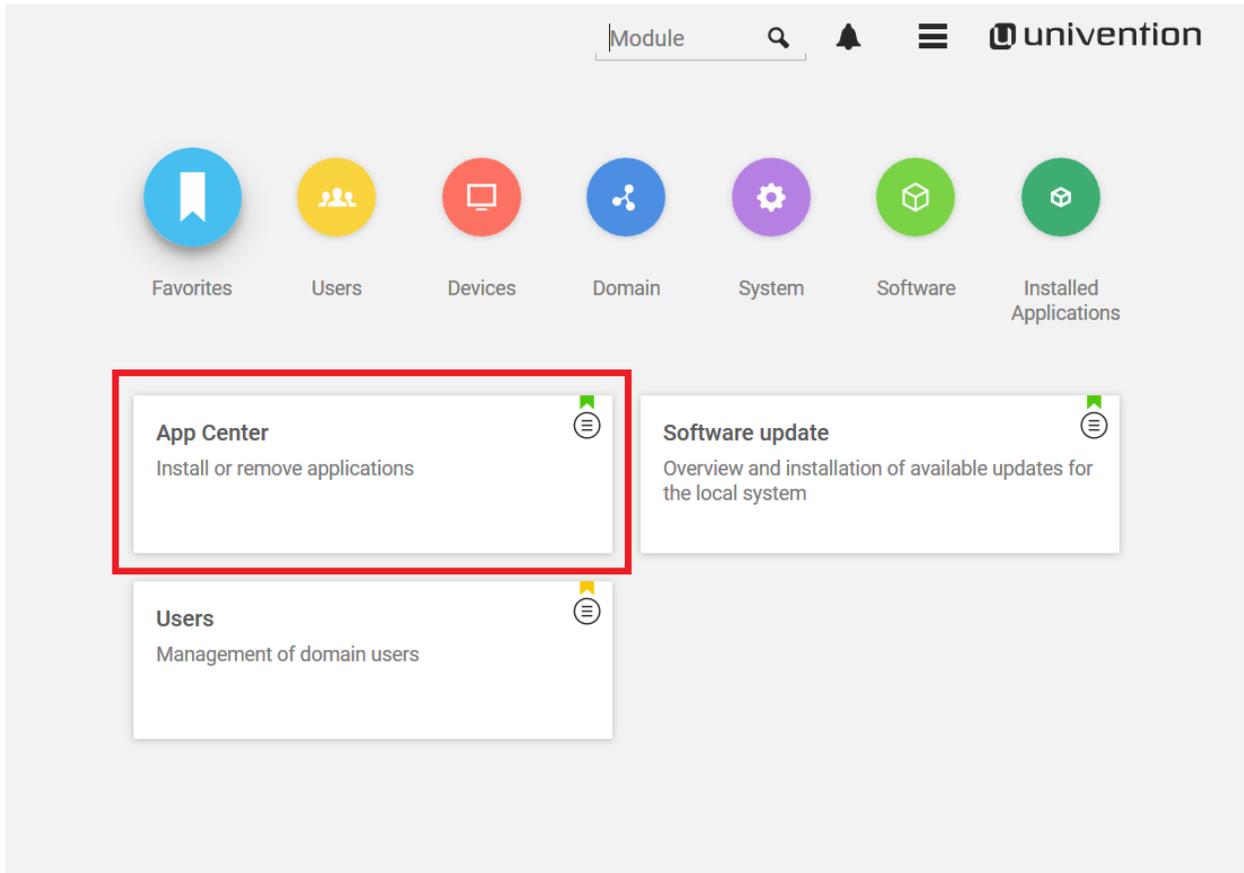
1. Install Collabora in UCS.
3. Enable Collabora in ownCloud.

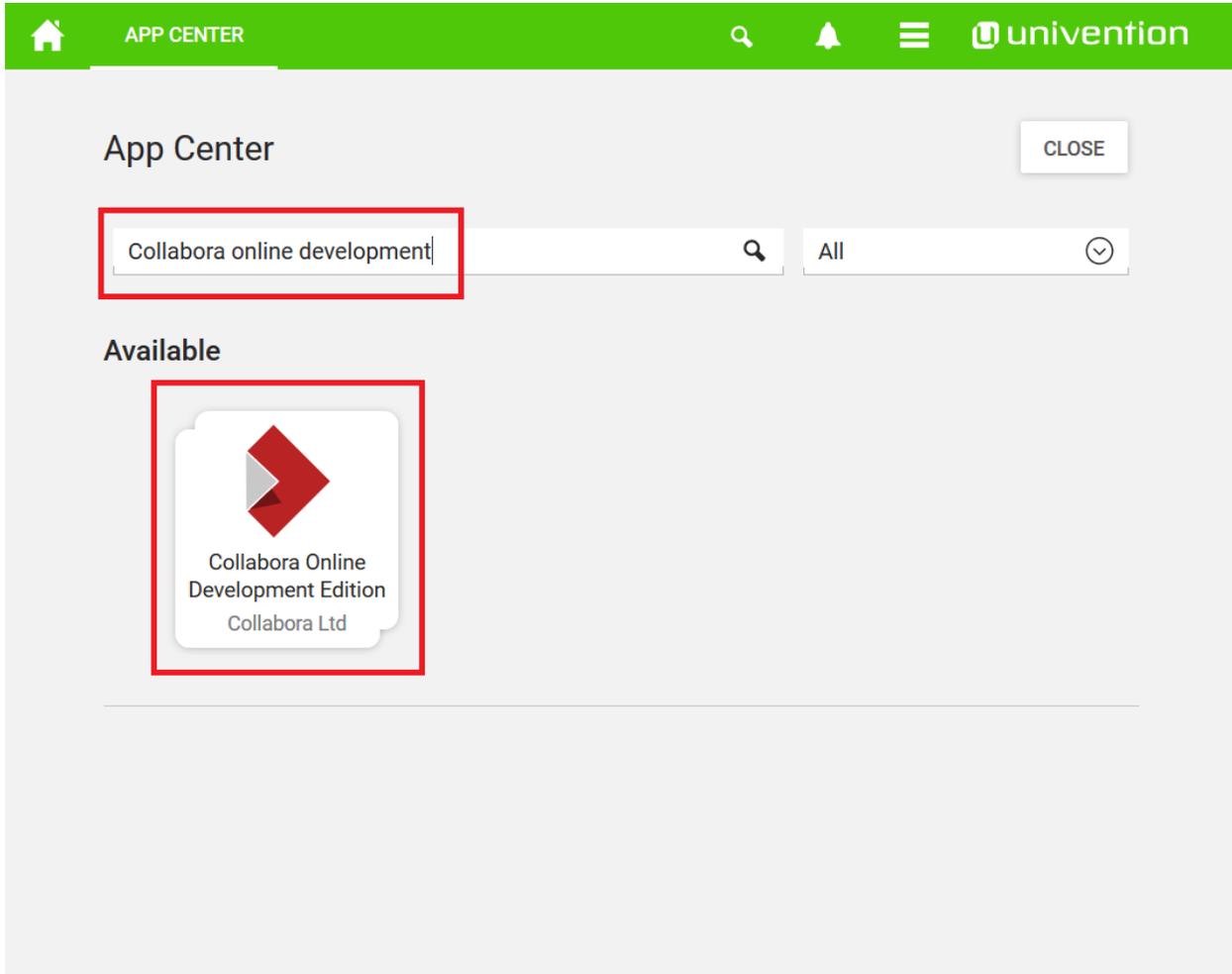
Note: Username and Password are owncloud

Now you can use Collabora within ownCloud. Start by creating a new Document.









COLLABORA ONLINE DEVELOP...

Collabora Online Development Edition

BACK TO OVERVIEW

 Collabora Online Development Edition

[Collabora Ltd](#)
[Collaboration](#) | [Education](#)

INSTALL

Details

Collabora Online is a powerful LibreOffice-based online office that supports all major document, spreadsheet and presentation file formats, which you can integrate in your own infrastructure. Key features are collaborative editing and excellent office file format support.

Collabora Online is excellent for enterprises that need a powerful office suite on-premise, that protects their privacy and allows them to keep full control of their sensitive corporate data.

This app contains the Collabora Online Development

developments, and supports up to 10 concurrent open documents from 20 different connections at the same time.

Key Features

- View and edit text documents, spreadsheets, presentations & more
- Preservation of layout and formatting of documents (WYSIWYG)
- Collaborative editing
- Live notifications of users entering or exiting

Collabora Online Development Edition

CANCEL INSTALLATION

Installation of Collabora Online Development Edition

Please confirm to install the application Collabora Online Development Edition on this host.

Settings

.*

These hosts have access to the Collabora server (host\\.\my
\\.\domain) *

admin

User name for accessing CODE Admin Console (Requires a
restart of the app) *

.....

Password for accessing CODE Admin Console (Requires a
restart of the app) *

.....

Password for accessing CODE Admin Console (Requires a
restart of the app) (retype) *

CANCEL

INSTALL

App installation notes

This App uses a container technology. Containers have to be downloaded once. After that they can be used multiple times.

Depending on your internet connection and on your server performance, the download and the App installation may take up to 15 minutes

Do not show this message again

CONTINUE

The screenshot shows the ownCloud interface with a green header bar. The header contains a home icon, the text "COLLABORA ONLINE DEVELOP...", a search icon, a notification bell icon, a menu icon, and the "univention" logo. The main content area has a light gray background. At the top left, it says "Collabora Online Development Edition". To the right, there is a button labeled "BACK TO OVERVIEW" enclosed in a red rectangular box. Below this, there is a red logo consisting of a square with a white triangle pointing right, followed by the text "Collabora Online Development Edition". Underneath, it says "Collabora Ltd" and "Installed". A section titled "First steps" contains two main parts: "1. Completing the Configuration of Collabora Online" and "3.2. Nextcloud".

Collabora Online Development Edition

[BACK TO OVERVIEW](#)

 Collabora Online
Development Edition

Collabora Ltd
Installed

First steps

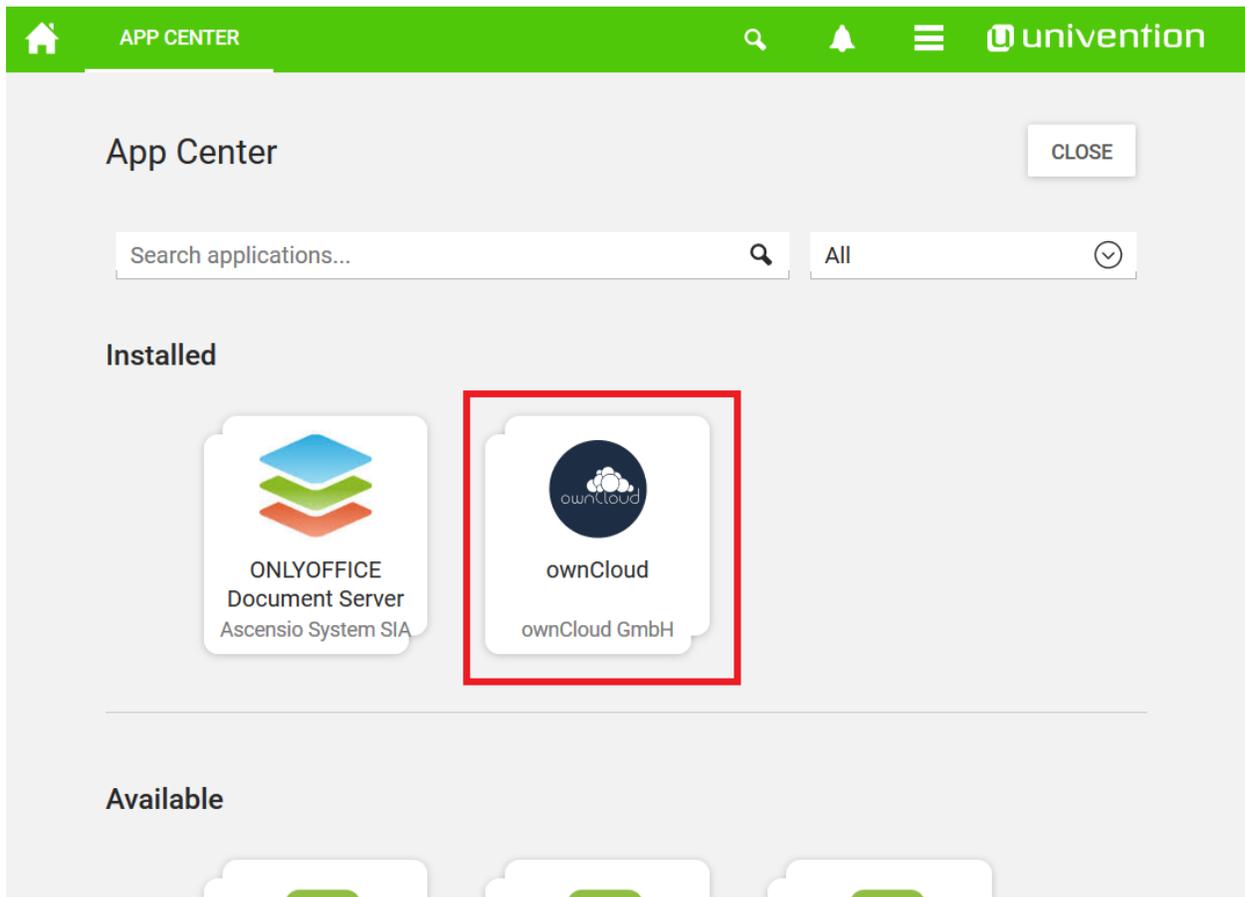
1. Completing the Configuration of Collabora Online

- First, you need a running File Sync and Share solution like EGroupware, Nextcloud or ownCloud (all are available in Univention App Center).
- Next, you need to install the Collabora Plugin in your File Sync and Share solution (see below for more information).
- Then you can give `https://FQDN_OF_THIS_SERVER` without a port number as the WOPIS URL in your preferred File

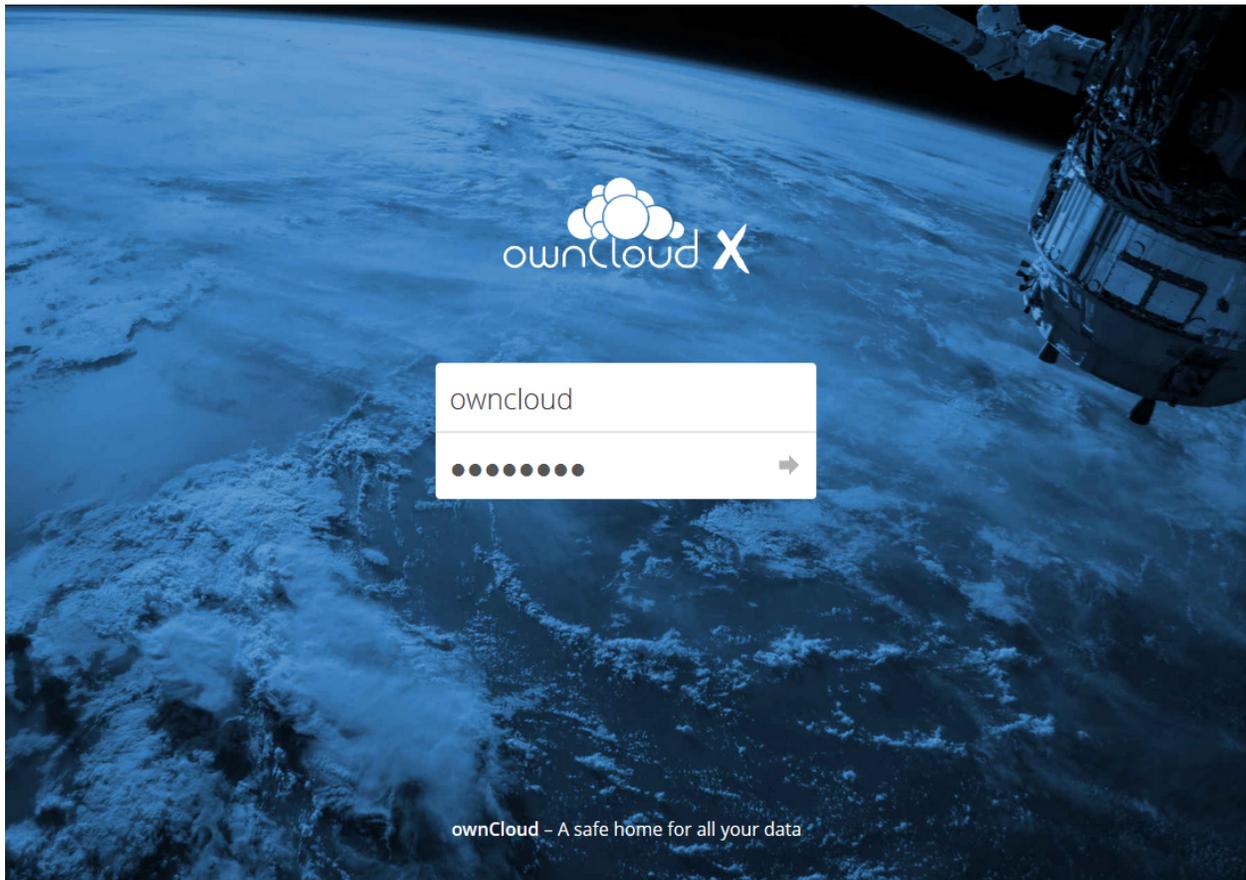
- Next step is to set permissions for groups, which should be able to use Collabora Online. Either edit the User group or use context menu on the user group → Access control and add checkmark for Collabora . So Admin can decide who is able to use Collabora in EGroupware.

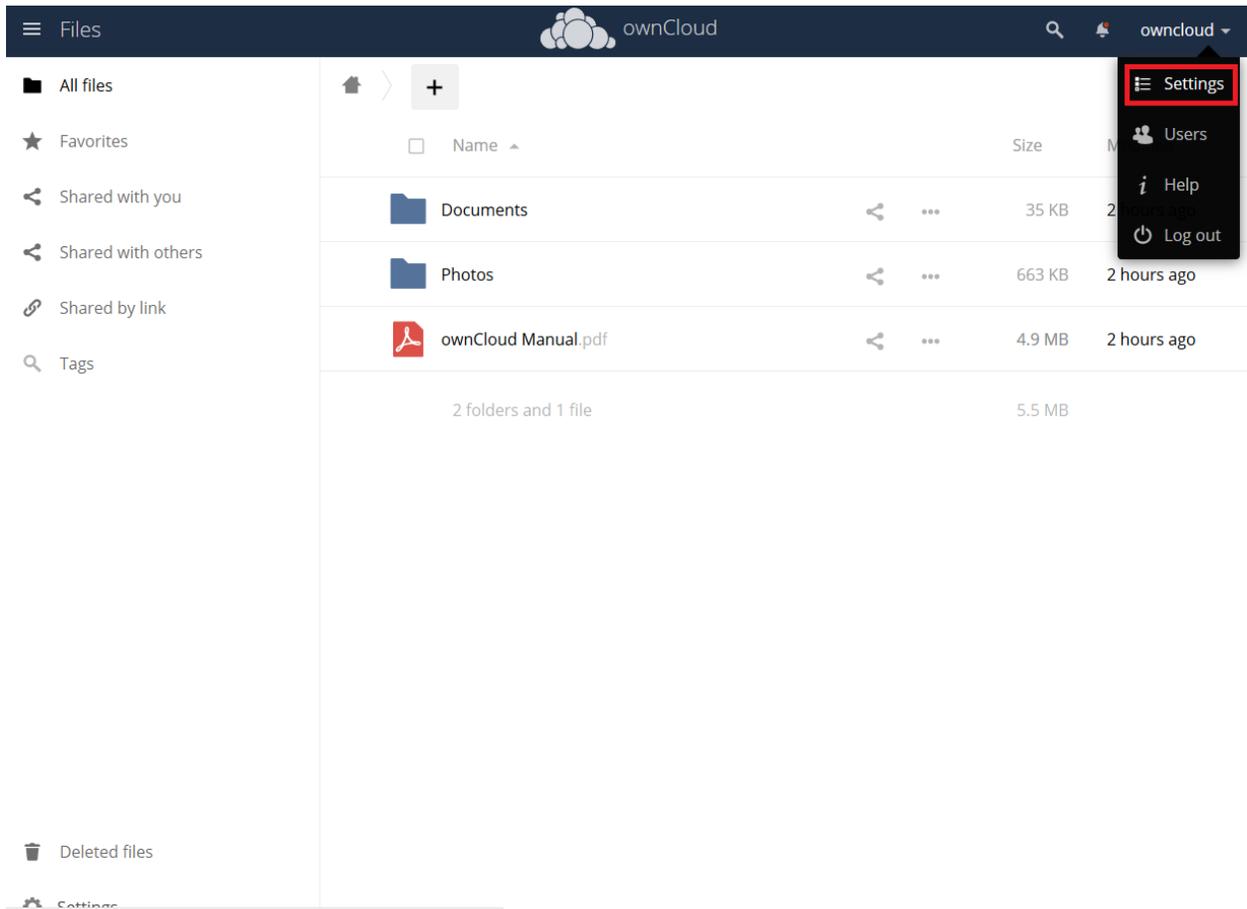
3.2. Nextcloud

- Goto the App Center, select Nextcloud and install it.
- Add the UCS root CA to the Nextcloud App. Run the following command as root user on your



The screenshot shows the univention interface with a green header bar. On the left, there is a home icon and the text 'OWNCLOUD'. On the right, there are icons for search, notifications, a menu, and the univention logo. Below the header, the page title is 'ownCloud'. To the right of the title are three buttons: 'PREVIOUS APP', 'NEXT APP', and 'BACK TO OVERVIEW'. Below the title is a circular logo for ownCloud. Underneath the logo, it says 'ownCloud GmbH' and 'Installed'. To the right of this text is a button labeled 'OPEN', which is highlighted with a red rectangular border. Below this section is a 'First steps' section with a 'Login' subsection. The 'Login' subsection states: 'The default owncloud-administrator account is:' followed by a bulleted list: '• Username: owncloud' and '• Password: owncloud'. To the right of the 'Login' subsection, there is a paragraph: 'Install Collabora Online Development Edition app to use Collabora in ownCloud.' Below the 'Login' subsection is an 'Additional Apps' subsection with a paragraph: 'In order to learn more about ownCloud on UCS - here is our [documentation](#).'





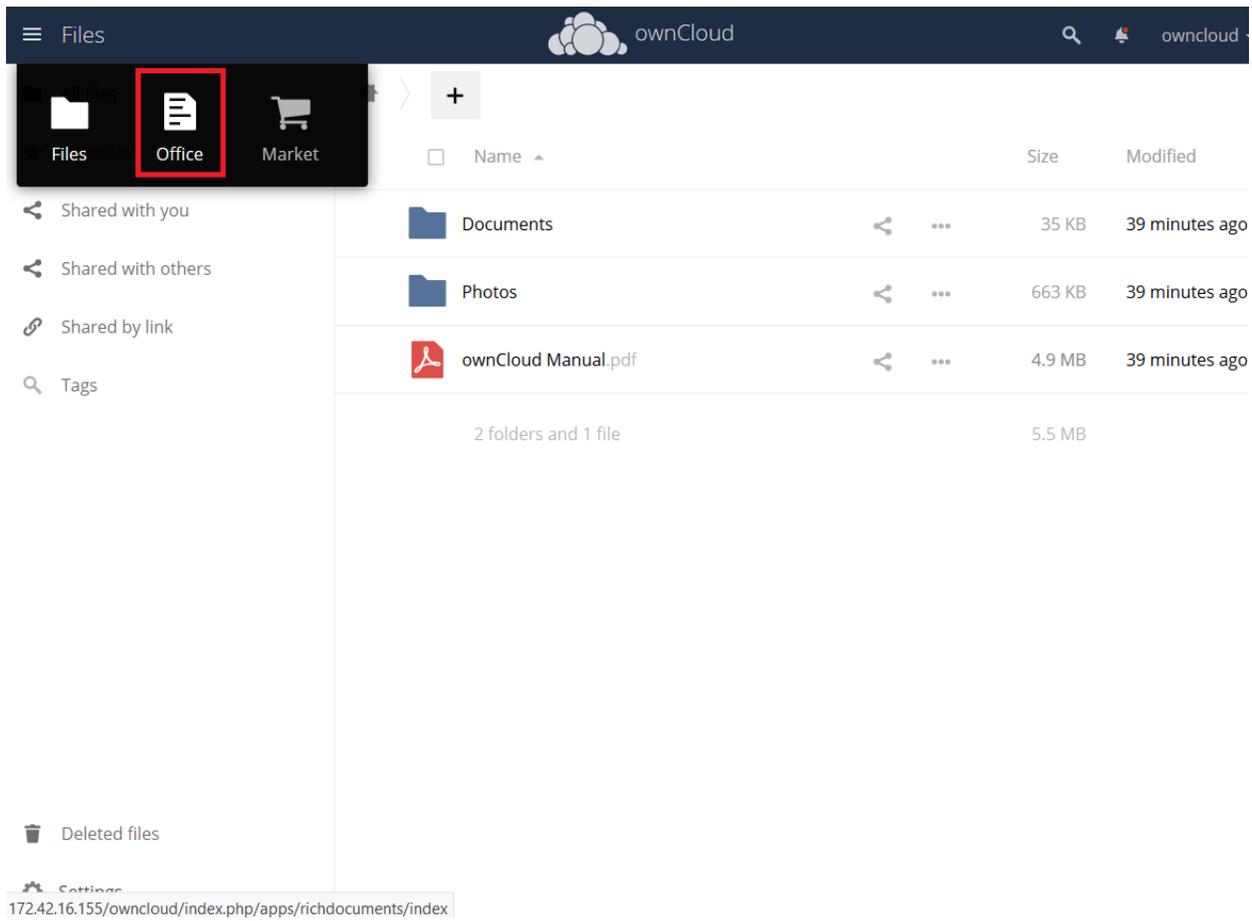
The screenshot shows the ownCloud user settings interface. The top navigation bar includes a hamburger menu, the text 'Settings', the ownCloud logo, and the text 'owncloud'. The left sidebar is divided into 'Personal' and 'Admin' sections. Under 'Personal', there are options for General, Storage, Security, and Additional. Under 'Admin', there are options for Apps, General, Storage, User Authentication, Encryption, Sharing, Help & Tips, and Additional. The 'Apps' option is highlighted with a red box. The main content area displays a storage usage notification: 'You are using 5.5 MB of Unlimited'. Below this, there are sections for Profile picture (with a green circle containing a white 'O'), Full name (input field with 'owncloud'), Email (input field with 'Your email address' and a 'Set email' button), Password (input fields for 'Current password' and 'New password' with a 'Change password' button), Language (a dropdown menu set to 'English' and a 'Help translate' link), and Federated Cloud (text: 'Your Federated Cloud ID: owncloud@ucs-123.owncloud.intranet/owncloud').

The screenshot shows the ownCloud Admin interface. The top navigation bar includes 'Settings', the ownCloud logo, and a search icon. The left sidebar is divided into 'Personal' and 'Admin' sections. The 'Admin' section is expanded to show 'Apps'. The main content area is titled 'Apps Management' and features a 'Show disabled apps' button highlighted with a red box. Below this, six app cards are displayed in a grid:

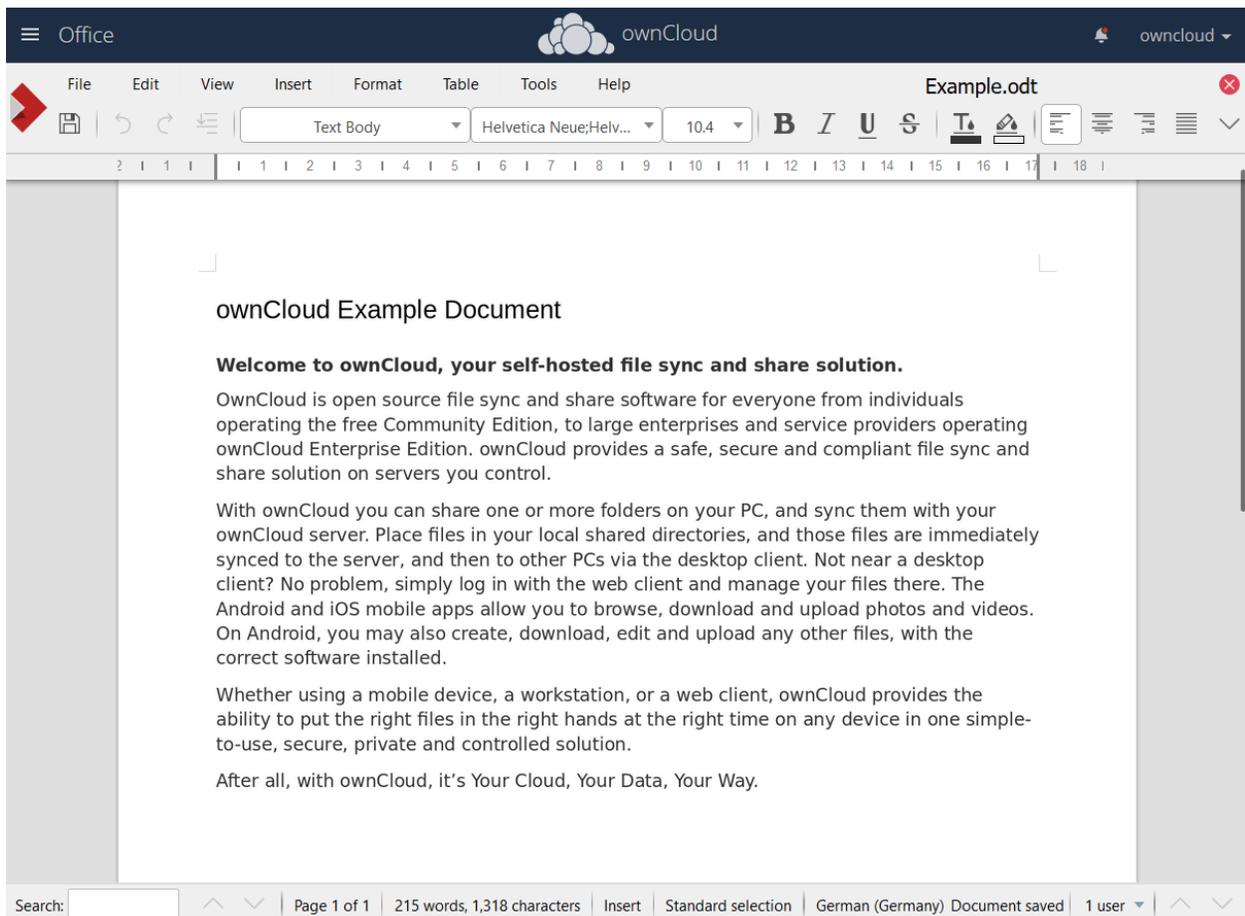
- Admin Config Report** (0.1.1, by owncloud.org): Includes a 'Show description ...' link, an 'Official' badge, and a 'Disable' button.
- Deleted files** (0.9.1, by Bjoern Schiessle): Includes a 'Show description ...' link, an 'Official' badge, and a 'Disable' button.
- Federation** (0.1.0, by Bjoern Schiessle): Includes a 'Show description ...' link, an 'Official' badge, and a 'Disable' button.
- Provisioning API** (0.5.0, by Tom Needham): Includes a 'Show description ...' link, an 'Official' badge, and a 'Disable' button.
- Share Files** (0.10.1, by Michael Gapczynski, Bjoern Schiessle): Includes a 'Show description ...' link, an 'Official' badge, and a 'Disable' button.
- Versions** (1.3.0, by Frank Karlitschek, Bjoern Schiessle): Includes a 'Show description ...' link, an 'Official' badge, and a 'Disable' button.

The screenshot shows the ownCloud Admin interface. The top navigation bar includes 'Settings', the ownCloud logo, and search/notification icons. The left sidebar is divided into 'Personal' (General, Storage, Security, Additional) and 'Admin' (Apps, General, Storage, User Authentication, Encryption, Sharing, Help & Tips, Additional). The main content area is titled 'Apps Management' and displays a list of installed and available apps. The 'Collabora Online' app is highlighted with a red box around its 'Enable' button. Other apps shown include 'Default encryption module', 'Update notification', 'Example ownCloud Theme', and 'External Sites'.

App Name	Version	Author	License	Status	Buttons
Default encryption module	1.3.1	by Bjoern Schiessle, Clark Tomlinson	AGPL-licensed	Official	Enable
Update notification	0.2.1	by Lukas Reschke	AGPL-licensed	Official	Enable
Collabora Online	2.0.5	by Collabora Productivity based on work of Frank Karlitschek, Victor Dubiniuk	AGPL-licensed	Approved	Enable, Uninstall App
Example ownCloud Theme	1.0.0	by Philipp Schaffrath	AGPL-licensed	Approved	Enable, Uninstall App
External Sites	1.2				
External user support					

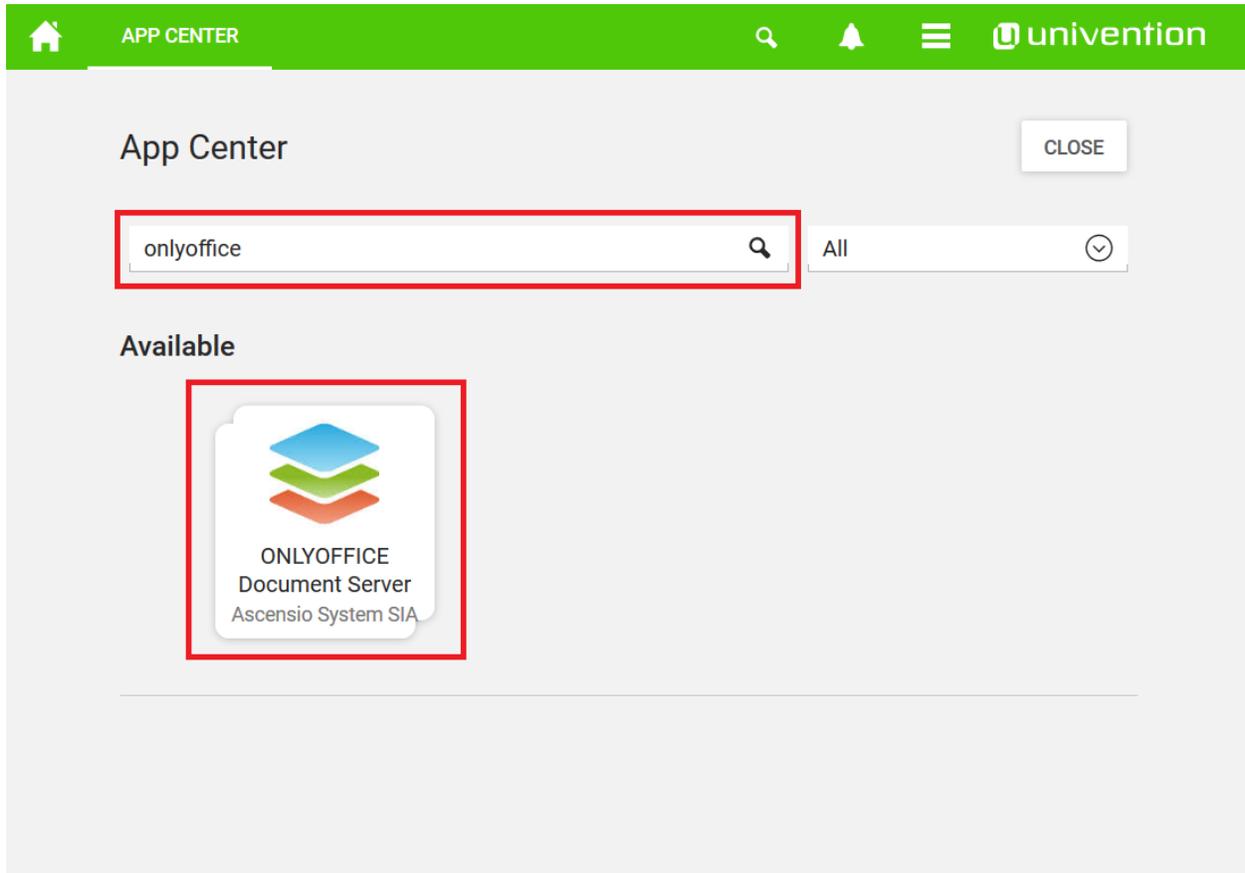






10.11.3 How to Install OnlyOffice

1. Search for “**OnlyOffice**” or select it from the application list in the Appcenter.



2. Install OnlyOffice.

After the installation is complete, return to the Appcenter overview

3. Install the ownCloud OnlyOffice connector App
 - Go to ownCloud

Note: Username and Password are owncloud

- Market
- Tools
- Install OnlyOffice

4. Go to the OnlyOffice settings inside ownCloud.

5. Enter the OnlyOffice server address in the following format and **save** it:

`https://<your-domain-name>/onlyoffice-documentserver/`

7. Now you can create a new document by clicking on the **Plus** button.

Note: PDF documents can also be viewed in OnlyOffice

🏠 ONLYOFFICE DOCUMENT SERVER
🔍 🔔 ☰ univention

ONLYOFFICE Document Server



[BACK TO OVERVIEW](#)

Ascensio System SIA
[Collaboration](#) | [Administration](#) | [Business](#) | [Education](#)

INSTALL

Details ⌵

ONLYOFFICE Document Server is a web-based document, spreadsheet and presentation processing platform, highly compatible with Microsoft Office and OpenDocument file formats. This app offers a powerful feature set that enables you to view, edit and co-author all kinds of Office documents:

- Wide range of formatting features

Use templates, edit your images with Photo Editor, embed YouTube videos and more.

ONLYOFFICE offers the support of all the popular formats: DOC, DOCX, TXT, ODT, RTF, ODP, EPUB, ODS, XLS, XLSX, CSV, PPTX, HTML.

Compared to other online office suites, ONLYOFFICE Document Server provides you with the most complete

License agreement

THE TERMS OF THIS ONLYOFFICE COMMERCIAL LICENSE AGREEMENT (THE "AGREEMENT") REGARDING YOUR USE OF ONLYOFFICE ENTERPRISE EDITION. YOU REPRESENT AND WARRANT THAT YOU HAVE FULL LEGAL AUTHORITY TO BIND THE LICENSEE TO THIS AGREEMENT. IF YOU DO NOT AGREE WITH ALL OF THESE TERMS, DO NOT INSTALL, DOWNLOAD OR OTHERWISE USE ONLYOFFICE.

Definitions

"ONLYOFFICE Community Edition" means open-source office server software provided by Ascensio System SIA, its object code, binary codes, compiled object code as well as any related documentation. It consists of ONLYOFFICE Community Server (released under AGPL v.3 license), ONLYOFFICE Mail Server (released GPL v.2 license) and ONLYOFFICE Document Server (released under AGPL v.3 license). The source codes of ONLYOFFICE Open Source Edition are published at <https://github.com/ONLYOFFICE> and can be modified at any time

[CANCEL](#)

ACCEPT LICENSE

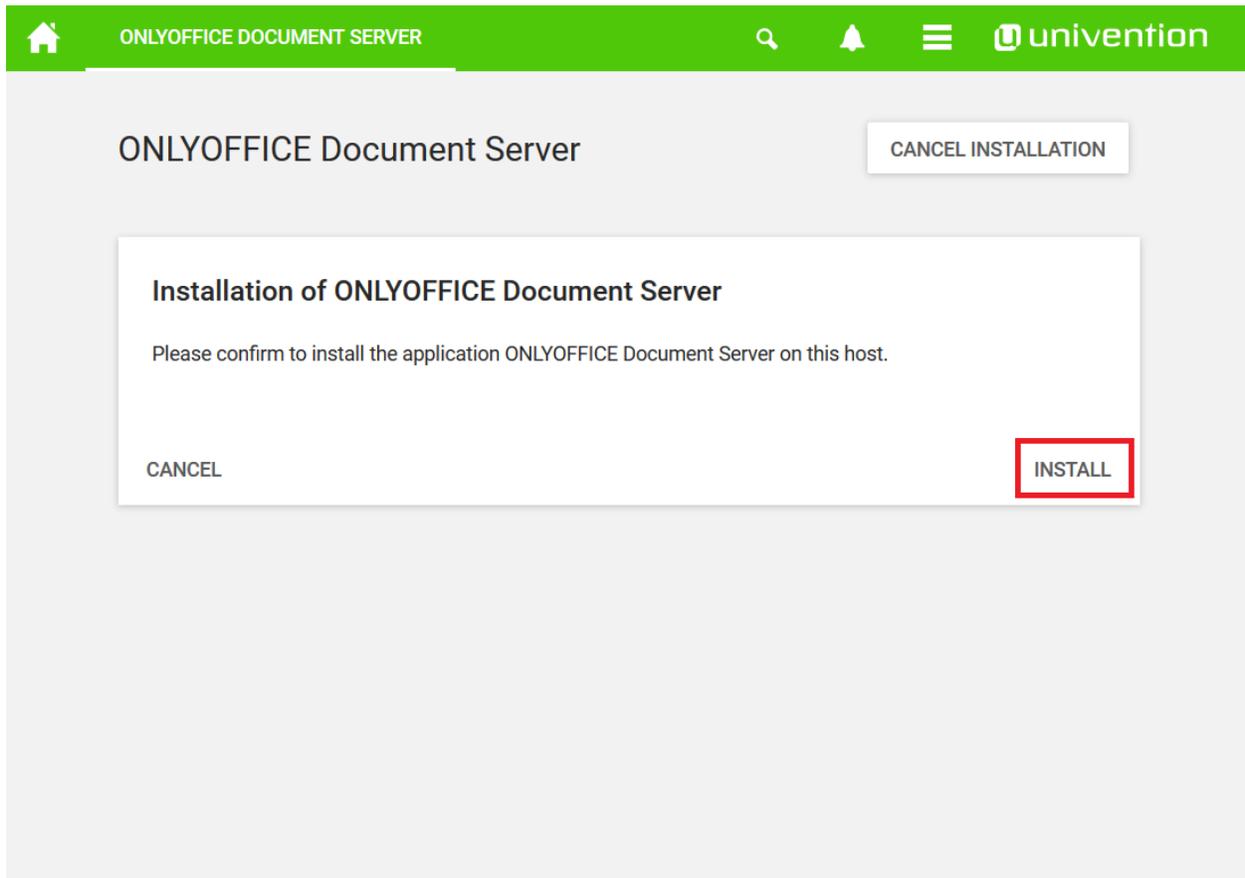
App installation notes

This App uses a container technology. Containers have to be downloaded once. After that they can be used multiple times.

Depending on your internet connection and on your server performance, the download and the App installation may take up to 15 minutes

Do not show this message again

CONTINUE



ONLYOFFICE Document Server

[BACK TO OVERVIEW](#)



[Ascensio System SIA](#)
Installed

First steps

To start using ONLYOFFICE Document Server with Nextcloud or ownCloud, you have to install the respective app and enable the ONLYOFFICE plugin in either app.

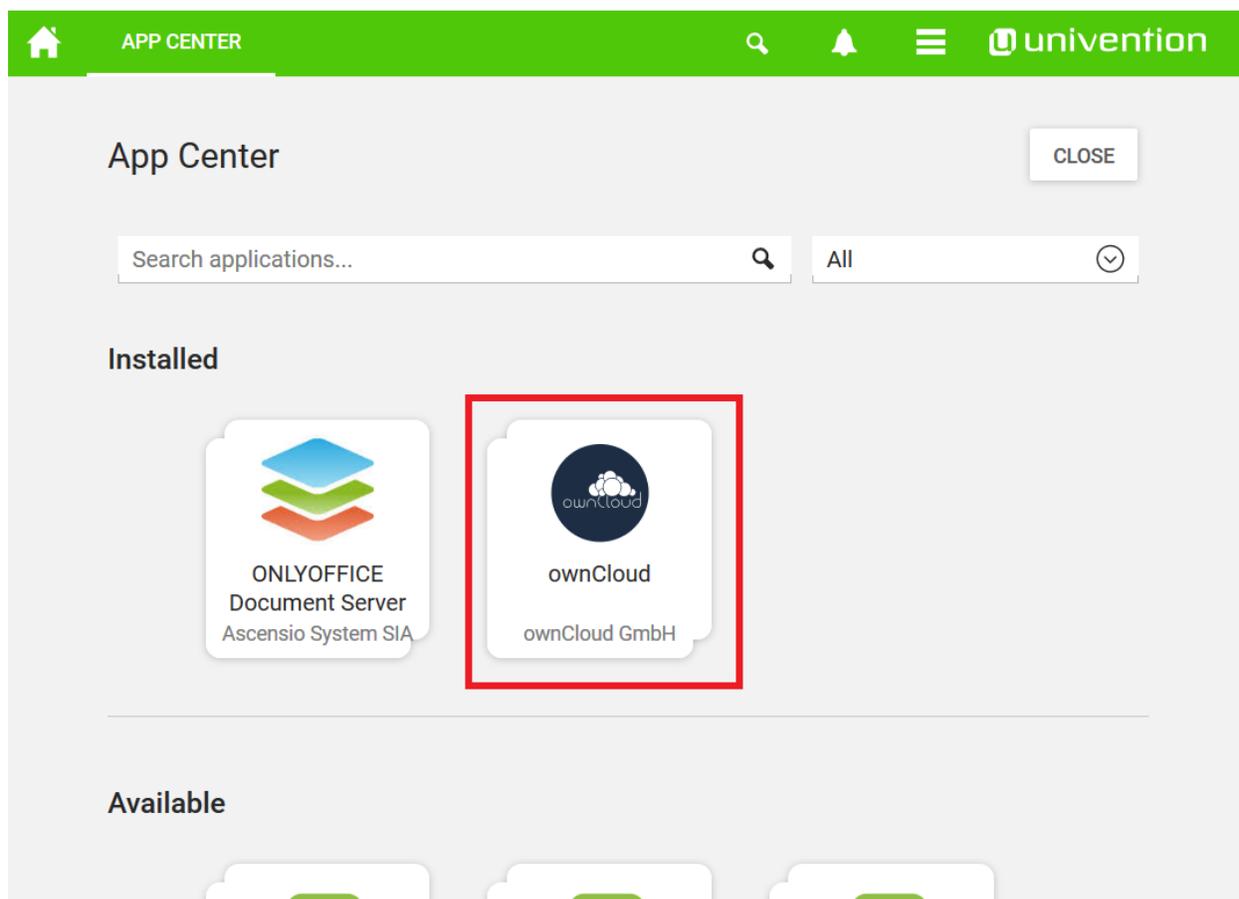
The address to the document server has to be configured inside the plugin. Pleaes note that the parameter **documentserver** is the name (FQDN, without a port number) of the server with the ONLYOFFICE Document Server installed. The address must be accessible for the user browser and from the respective

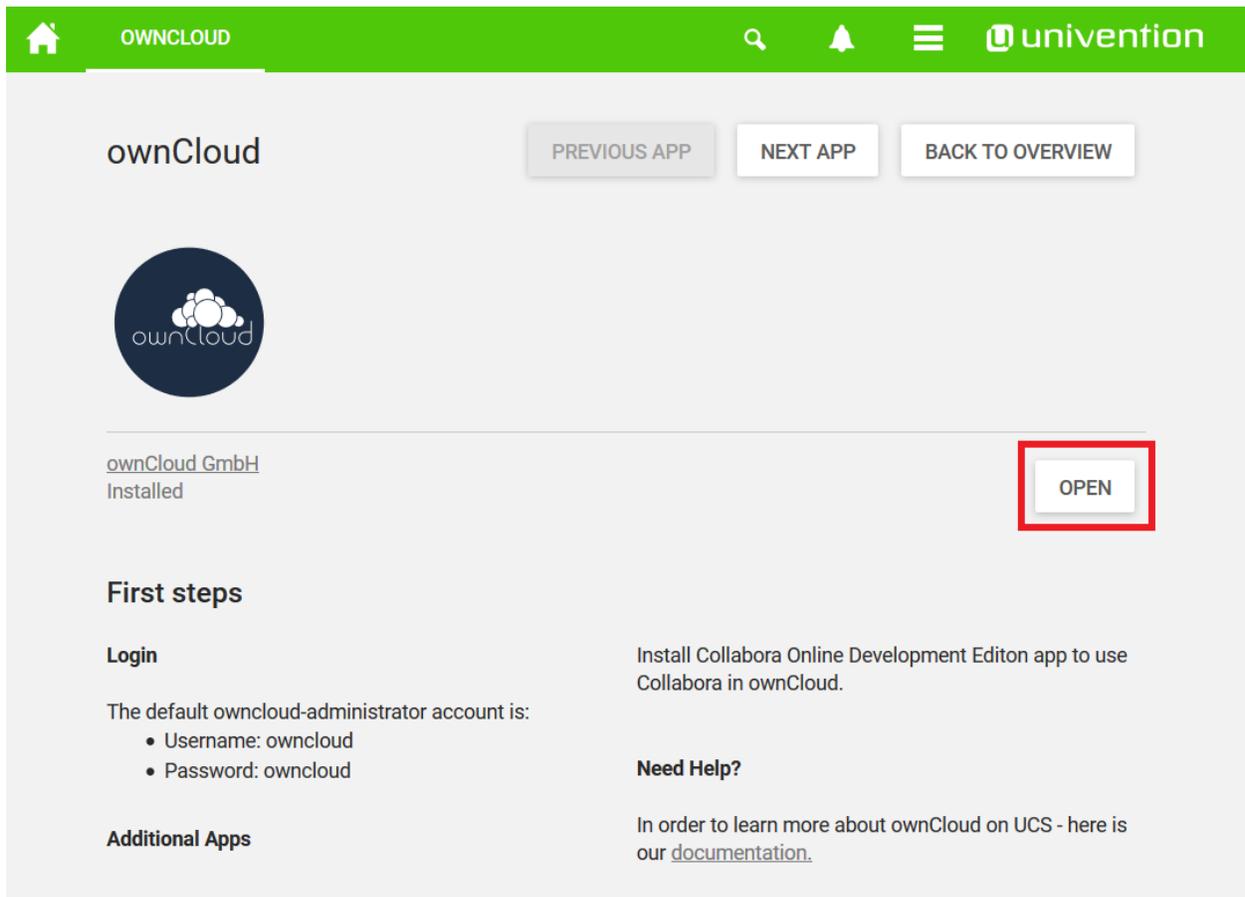
Configuration of ONLYOFFICE plugin in Nextcloud

- Login to Nextcloud as user *Administrator*.
- Goto *Apps* → *Office & Text* → enable *ONLYOFFICE*.
- Goto *Admin* settings and look for *ONLYOFFICE*. There enter the address above to connect the ONLYOFFICE document server and click on *Save*.

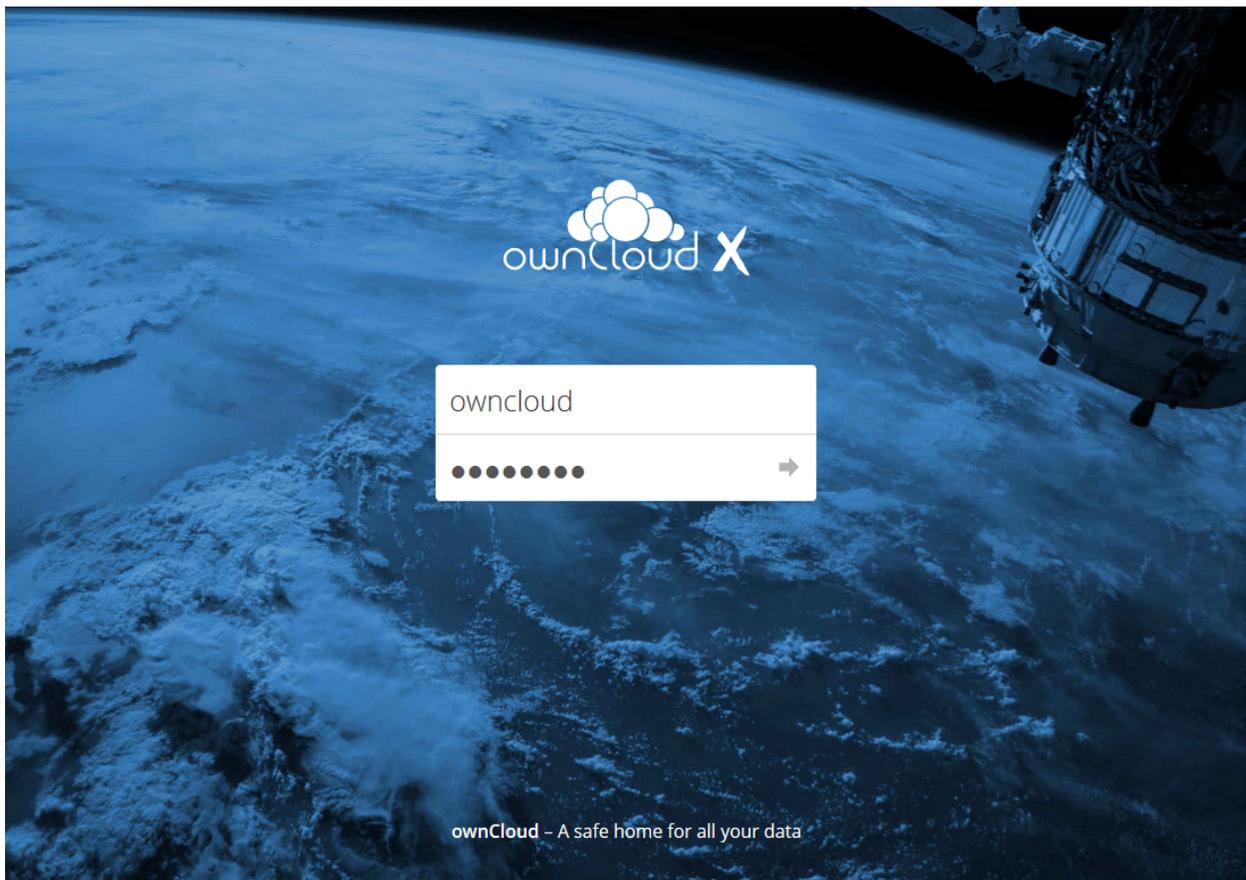
Configuration of ONLYOFFICE plugin in ownCloud

- Login to owncloud as user *owncloud*.
- Goto *Market* → *Tools or Show all* → *ONLYOFFICE*



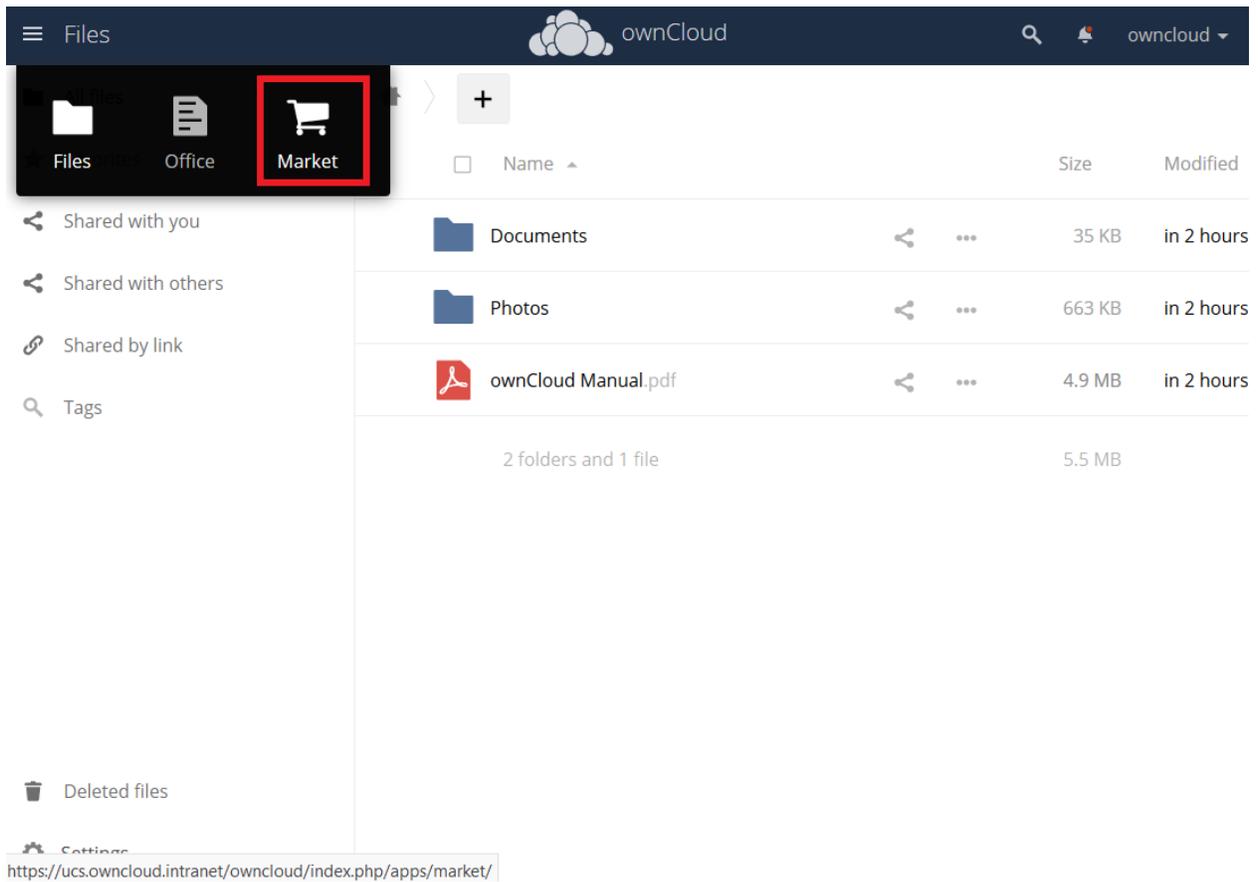


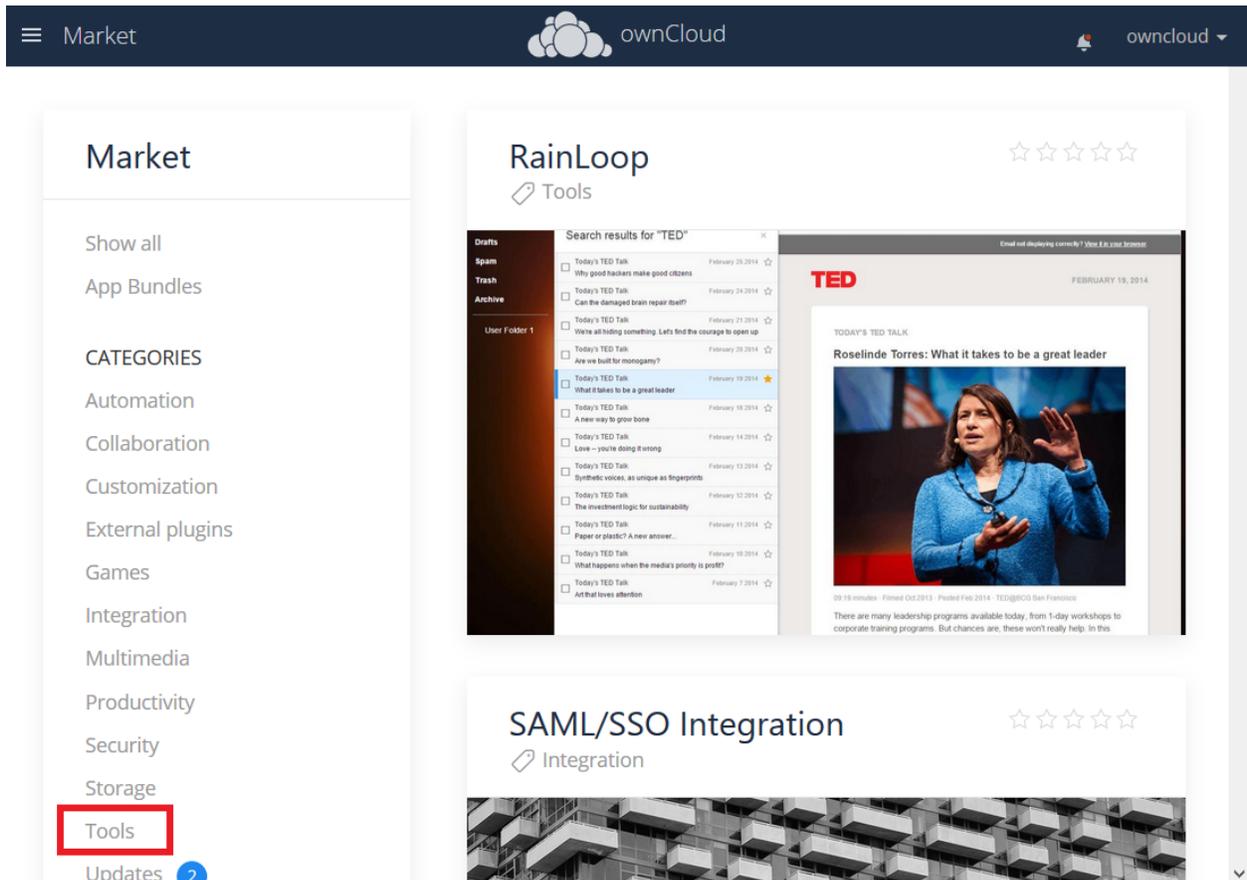
The screenshot shows the univention interface with a green header bar. On the left, there is a home icon and the text 'OWNCLOUD'. On the right, there are icons for search, notifications, a menu, and the univention logo. Below the header, the page title is 'ownCloud'. To the right of the title are three buttons: 'PREVIOUS APP', 'NEXT APP', and 'BACK TO OVERVIEW'. Below the title is a circular logo for ownCloud. Underneath the logo, it says 'ownCloud GmbH' and 'Installed'. To the right of this text is a button labeled 'OPEN', which is highlighted with a red rectangular border. Below this section is a 'First steps' section with a 'Login' subsection. The 'Login' subsection provides the default administrator account information: Username: owncloud and Password: owncloud. To the right of the login information, there is a note: 'Install Collabora Online Development Edition app to use Collabora in ownCloud.' Below the login information is an 'Additional Apps' subsection with a link to 'our documentation'.

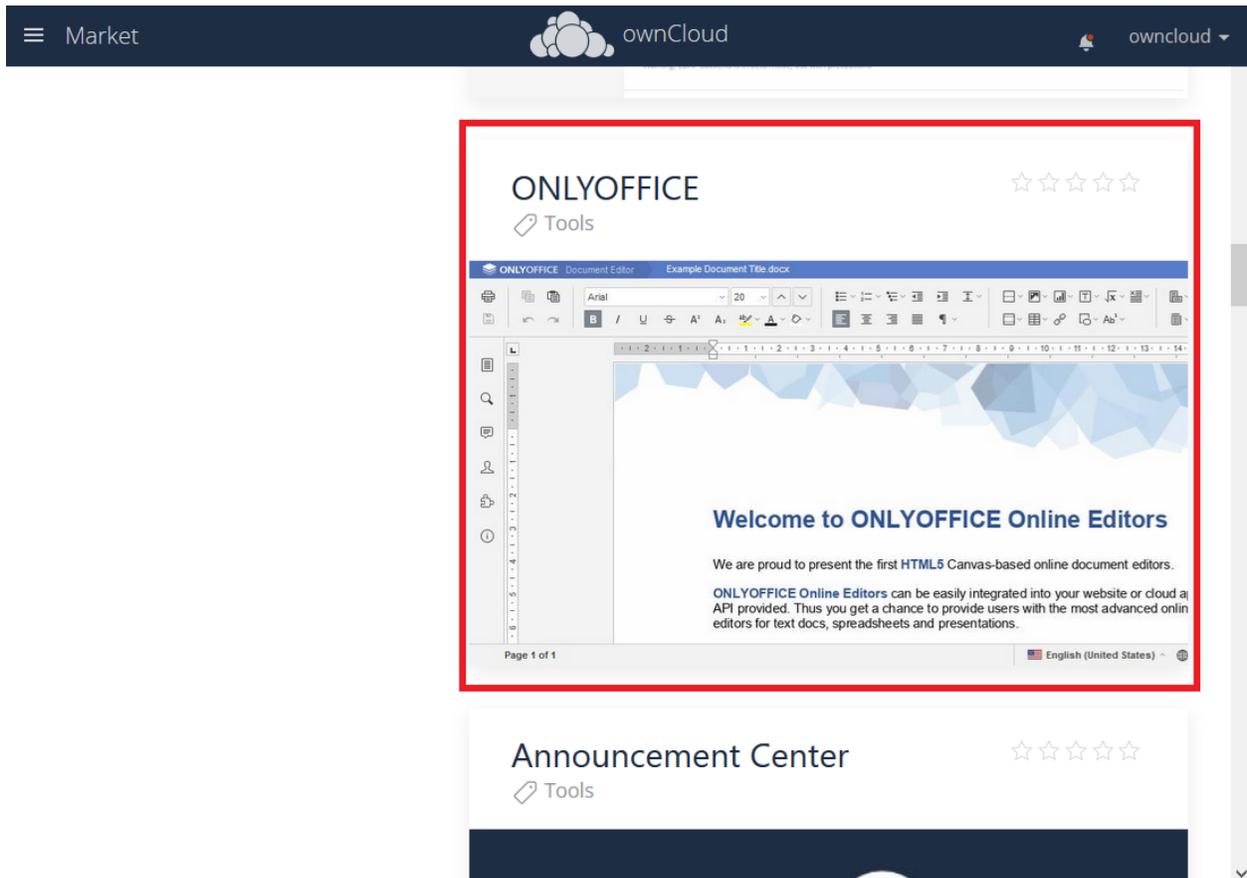


The screenshot shows the ownCloud web interface. At the top, a dark navigation bar contains a menu icon, the word "Files" (highlighted with a red box), the ownCloud logo, and a search icon. Below the navigation bar, a sidebar on the left lists navigation options: "All files", "Favorites", "Shared with you", "Shared with others", "Shared by link", "Tags", "Deleted files", and "Settings". The main content area displays a file browser view with a table of items:

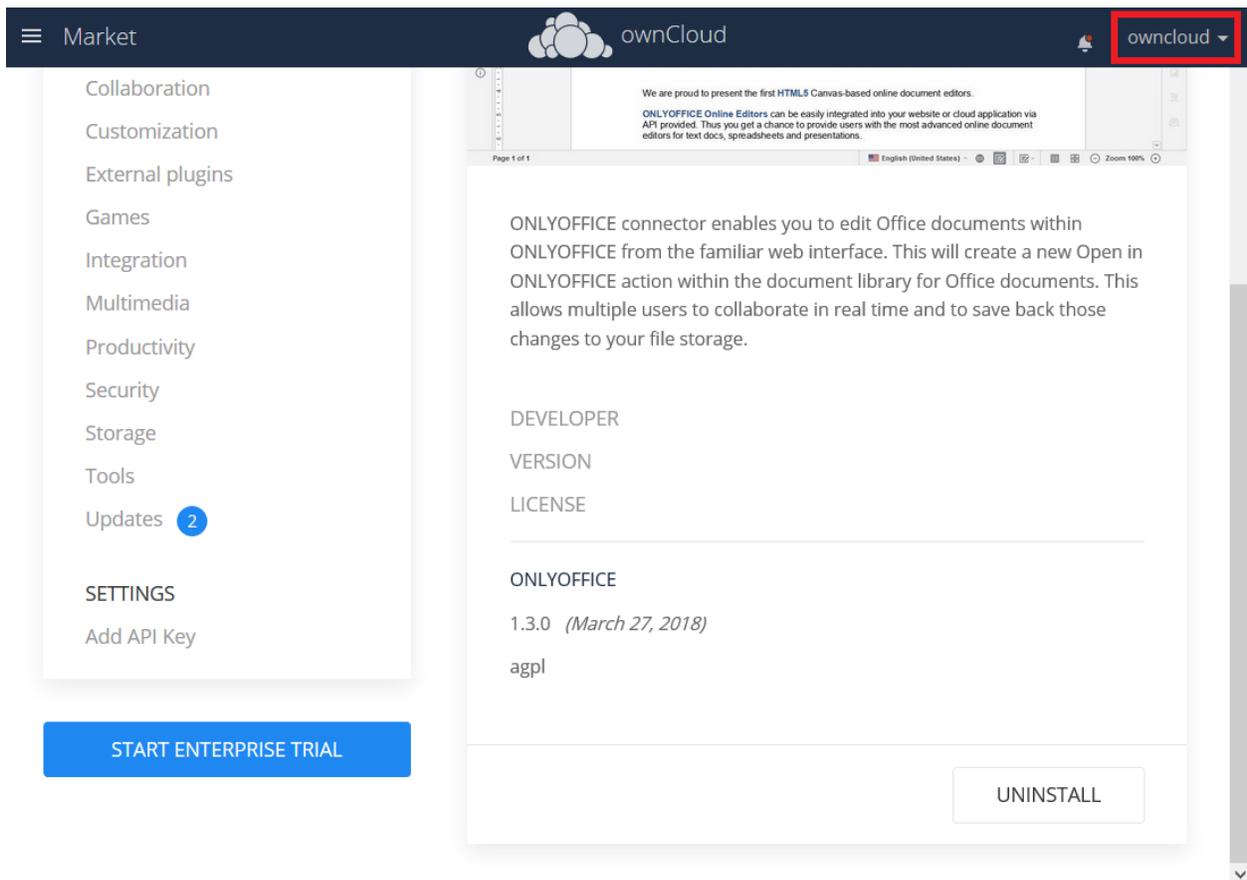
Name	Size	Modified
Documents	35 KB	in 2 hours
Photos	663 KB	in 2 hours
ownCloud Manual.pdf	4.9 MB	in 2 hours
2 folders and 1 file		5.5 MB

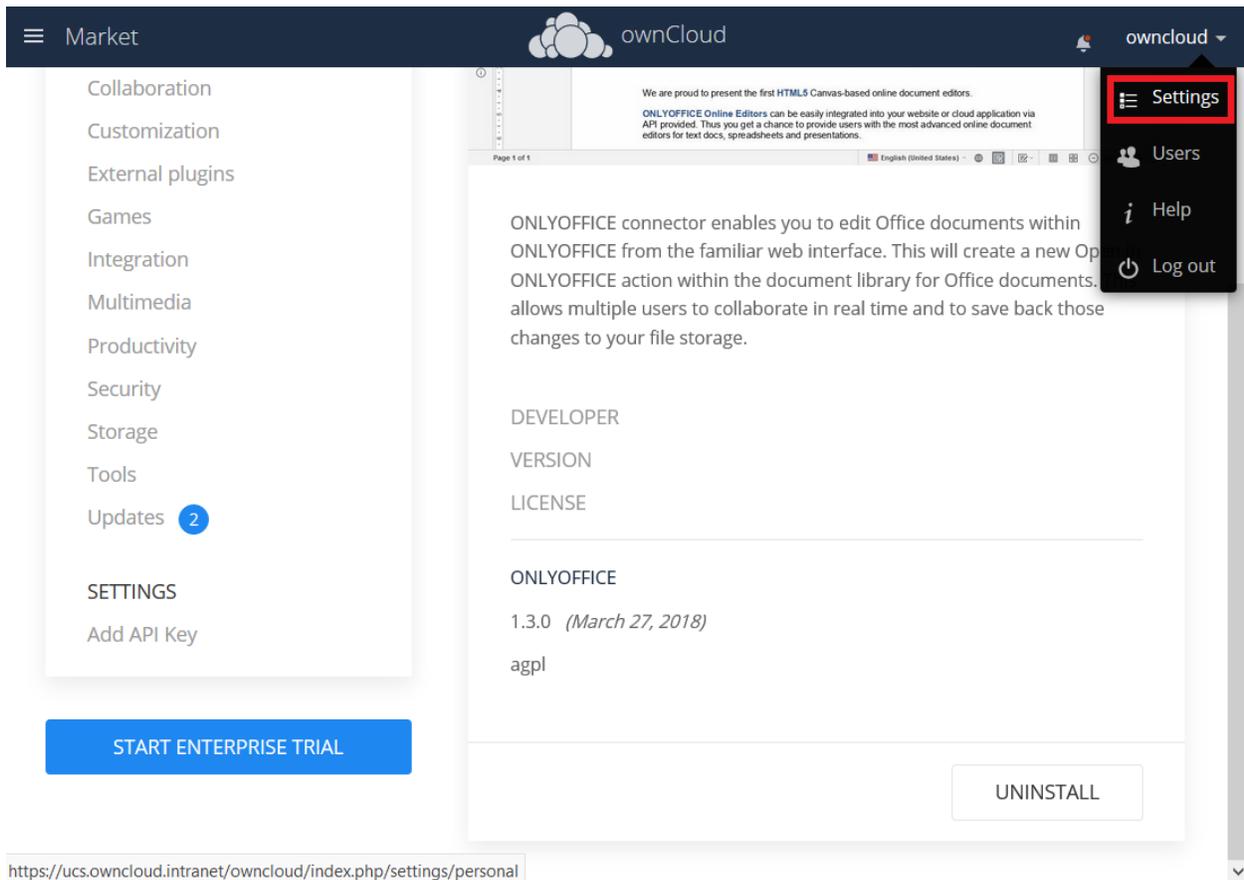




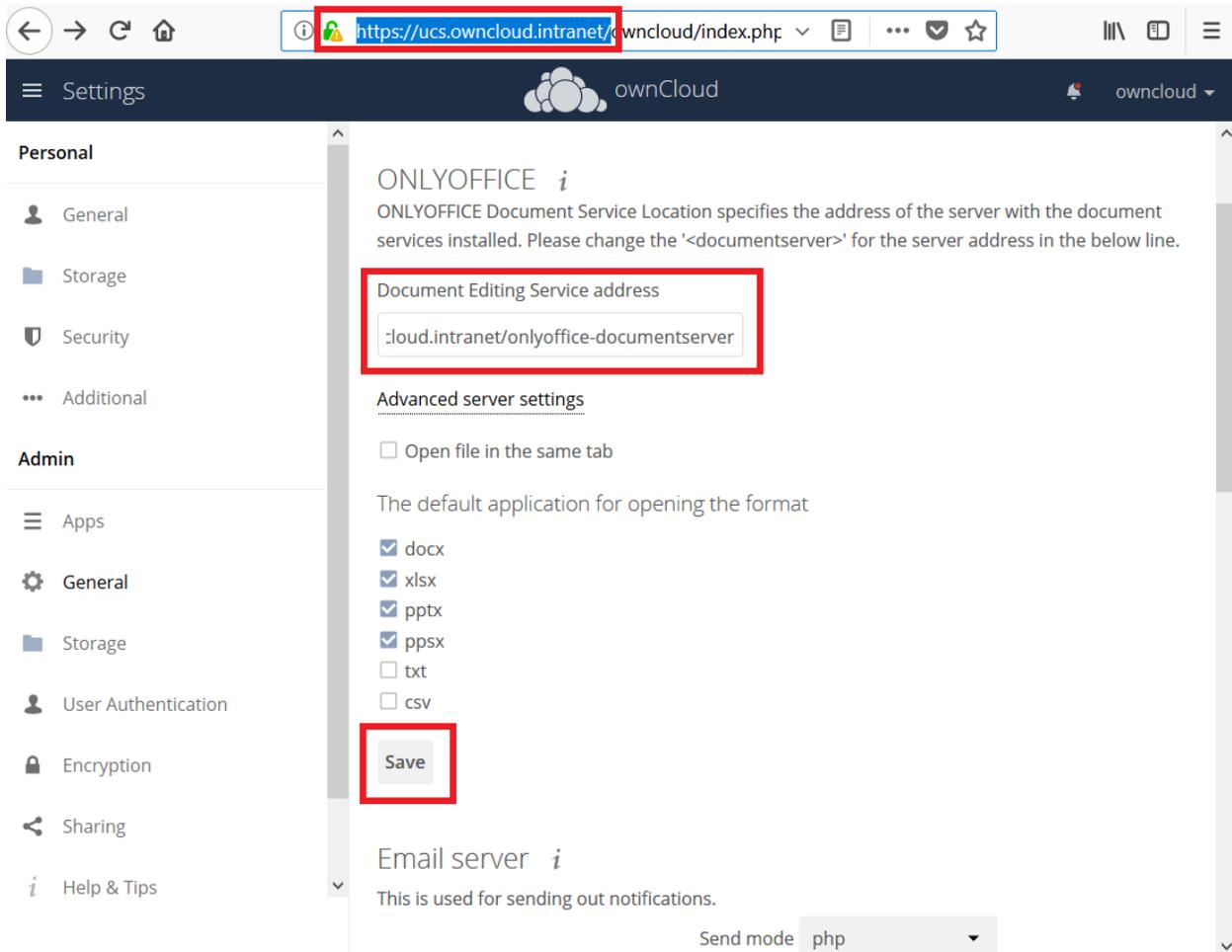


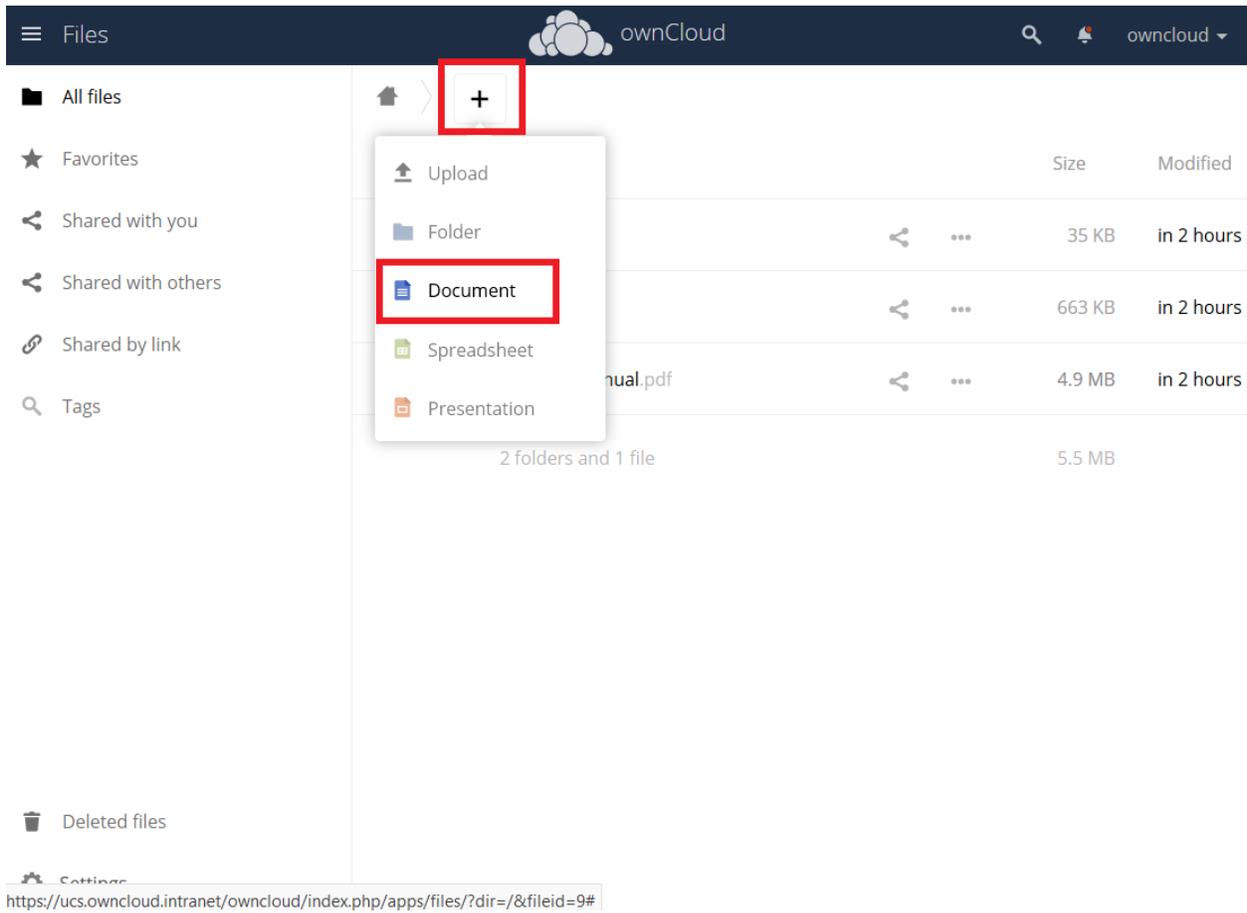
The screenshot displays the ownCloud Market interface. On the left is a navigation menu with categories like Collaboration, Customization, External plugins, Games, Integration, Multimedia, Productivity, Security, Storage, Tools, and Updates (with a '2' badge). Below the menu is a 'START ENTERPRISE TRIAL' button. The main content area shows a preview of a document titled 'ONLYOFFICE connector enables you to edit Office documents within ONLYOFFICE from the familiar web interface...'. Below the preview, there are fields for 'DEVELOPER', 'VERSION', and 'LICENSE'. The 'ONLYOFFICE' section lists version '1.3.0 (March 22, 2018)' and license 'GNU Affero General Public License'. A blue 'INSTALL' button is highlighted with a red border at the bottom right of the preview area.

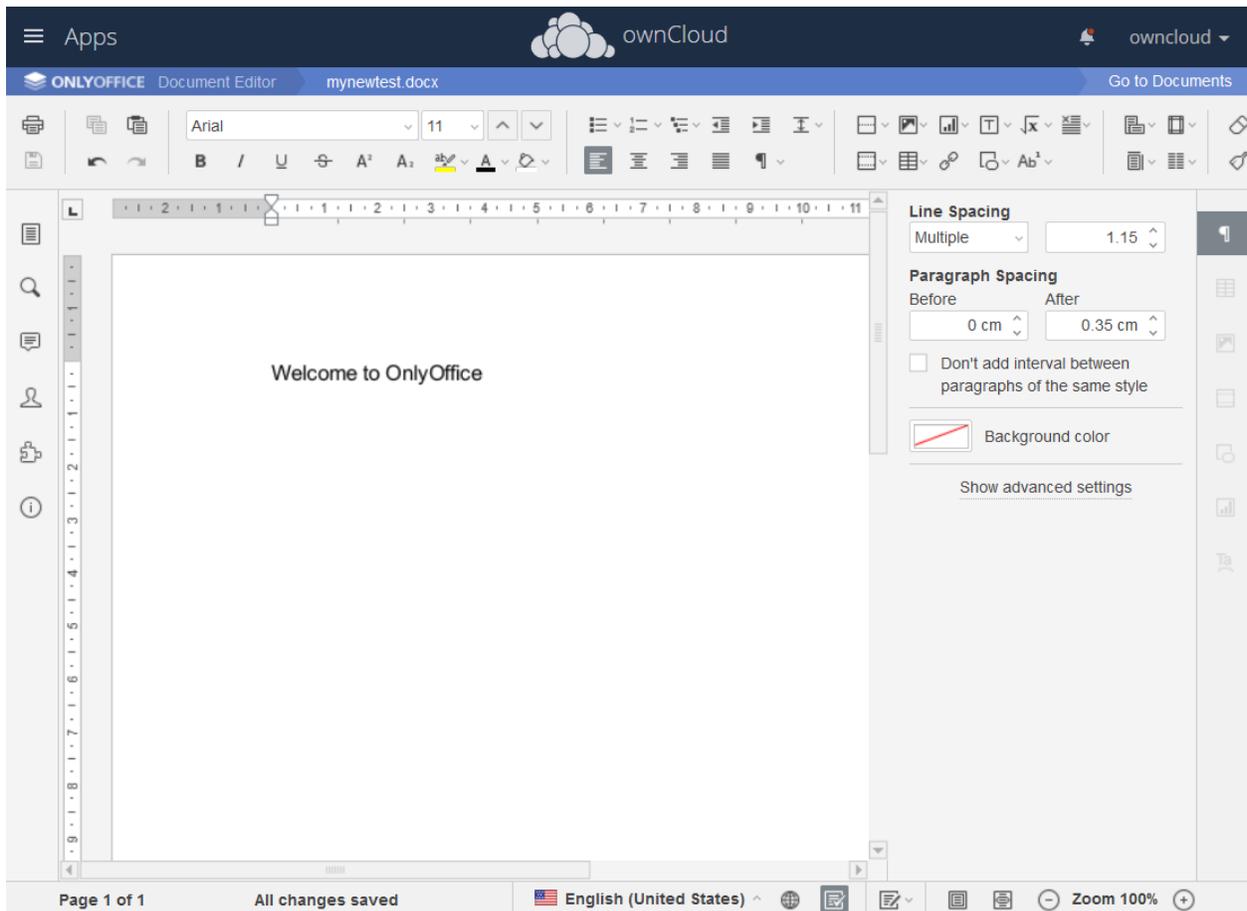


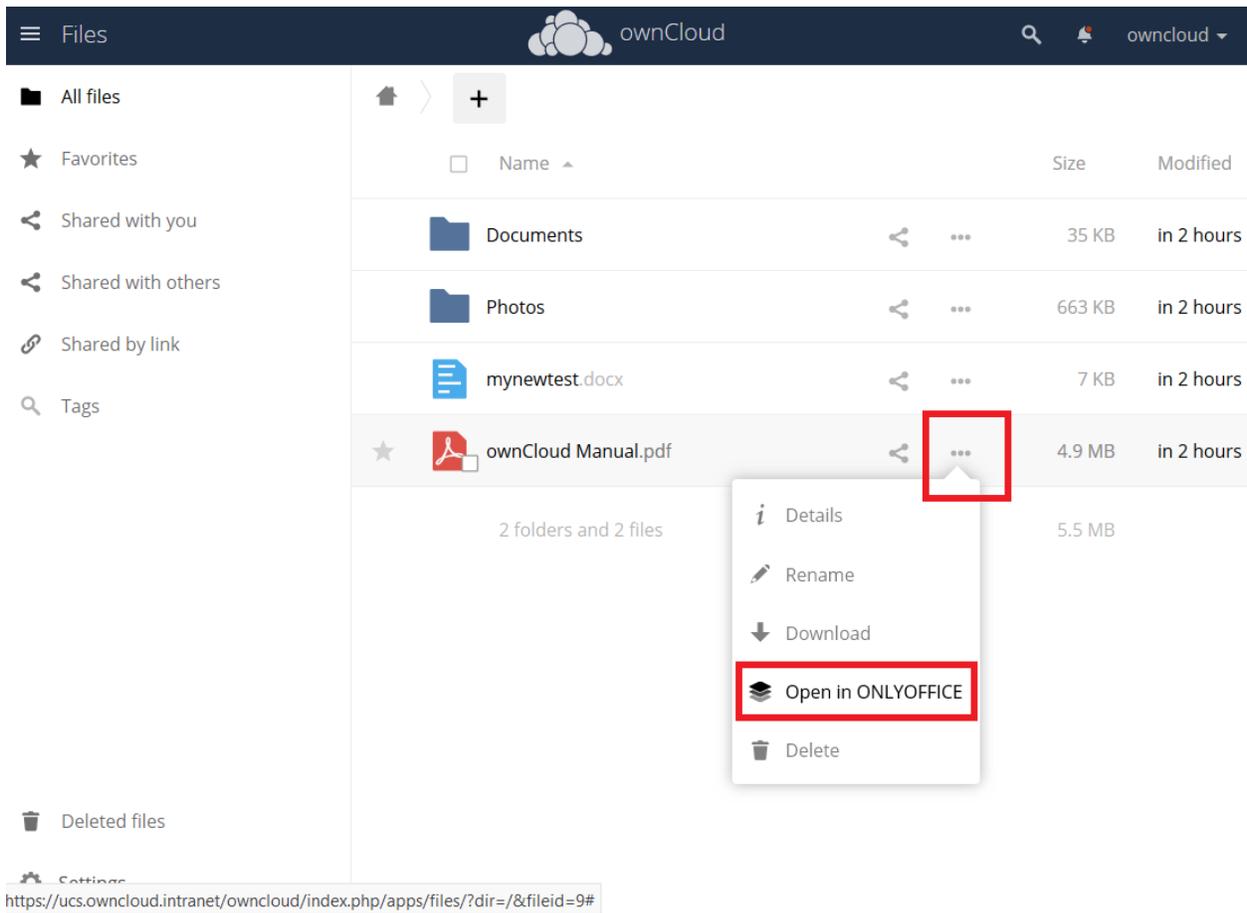


The screenshot displays the ownCloud settings interface. At the top, there is a dark blue header with a hamburger menu icon, the text 'Settings', the ownCloud logo, and the text 'ownCloud'. On the right side of the header, there is a notification bell icon and the text 'owncloud' with a dropdown arrow. Below the header is a left sidebar with two main sections: 'Personal' and 'Admin'. Under 'Personal', there are links for 'General', 'Storage', 'Security', and 'Additional'. Under 'Admin', there are links for 'Apps', 'General' (highlighted with a red box), 'Storage', 'User Authentication', 'Encryption', and 'Sharing'. The main content area shows a storage usage bar at the top indicating 'You are using 5.5 MB of Unlimited'. Below this are sections for 'Profile picture' (with a large green circle containing a white 'O' and an upload button), 'Full name' (with a text input field containing 'owncloud'), 'Email' (with a text input field containing 'Your email address' and a 'Set email' button), and 'Groups' (with the text 'You are member of the following groups: admin'). There is also a 'Password' section with 'Current password' and 'New password' input fields and a 'Change password' button. At the bottom, there is a 'Language' section with a dropdown menu set to 'English' and a 'Help translate' link. The URL at the bottom of the page is 'https://ucs.owncloud.intranet/owncloud/index.php/settings/admin?sectionid=general'.









10.11.4 Updating

When a new App release is available you should update the Office App. Here are the required steps:

- Select **Software update**
- Check if an Update is available
- Select on the App name
- Upgrade the App

10.12 Firewall protected environment

If you are considering setting up the appliance in an environment with a firewall, please create rules that permit access to the following hosts. If your DNS is not working, you can use the IP addresses instead. If you are using Google as your DNS server (IP=8.8.8.8), you have to permit access to it too.

Firewall Rules:

- 8.8.8.8
- software-univention.de
- docker.software-univention.de
- 176.9.114.147
- owncloud.org
- owncloud.com
- marketplace.owncloud.com
- 5.9.68.237

11.1 How do I transfer files from one user to another?

See [transferring files to another user](#).

11.2 How do I deal with problems caused by using self-signed SSL certificates?

See the [security](#) section of the `OCC` command.

11.3 I'm the admin and I lost my password! What do I do now!

See the [reset admin password](#) documentation.

11.4 What is a Federated System?

A Federated System is another [ownCloud](#) or [OpenCloudMesh](#) supporting cloud service.