

ownCloud Administration Manual

The ownCloud Team

Version: 10.9, September 15, 2022

Table of Contents

Introduction	1
ownCloud Videos and Blogs	1
Target Audience	1
Frequently Asked Questions	2
I want to upgrade from Community Version to Enterprise Version. What are the changes?	2
How do I transfer files from one user to another?	2
How do I deal with problems caused by using self-signed SSL certificates?	2
I'm the admin and I lost my password! What do I do now!	2
What is a Federated System?	2
Platform-wide known limitations, excluded files	2
Installation Options	3
Introduction	3
Manual Installation	3
Using a Docker-Based Installation	3
Linux Package Manager Installation	3
Deployment Considerations	3
Deployment Recommendations	6
System Requirements	21
Configuration Notes and Tips	23
Installation Options	27
Troubleshooting	58
Changing Your ownCloud URL	59
Installing and Managing Apps	59
Supported Apps in ownCloud	63
SELinux Configuration	65
Configuration	80
Database	80
Files and Sharing	134
Integration	177
General Topics	186
How to Upgrade Your ownCloud Server	499
Maintenance Mode Configuration	524
Data Exporter	525
Manually Move a Data Directory	527
Migrating to a Different Server	533
What is the Appliance?	538
How to Install the Appliance	538
Troubleshooting	602

ownCloud on QNAP	603
Introduction	603
Minimum Requirements	603
Preparation	603
Installation of ownCloud	605
Configuration	606
Users	607
Enabling ownCloud Apps.....	608
Enterprise Edition and Licensing	609
Accessing your QNAP ownCloud from the Internet	609
Accessing ownCloud via Clients	611
Using External Storage	611
Secure Shell (SSH)	611
occ commands	613
Backing up and Restoring the Database.....	613
Troubleshooting.....	614
Enterprise Edition	616
Installing & Upgrading ownCloud Enterprise Edition	684
General Troubleshooting.....	727
Path and Filename Length Limitations	735
Retrieve Log Files and Configuration Settings	737
Remove Non-Existent Background Jobs.....	738
Have You Found a Mistake In The Documentation?	741

Introduction

Welcome to the ownCloud Classic 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, plus client applications for Microsoft Windows, Mac OS X, Linux, Android and Apple iOS operating systems.

Current editions of ownCloud manuals are always available online at 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.

ownCloud Videos and Blogs

See the [official ownCloud channel](#) and [ownClouders community channel](#) on YouTube for tutorials, overviews, and conference videos. Visit [News](#) to stay up to date.

Target Audience

This guide is for administrators 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. See the developer manual if you would like to contribute:

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

Frequently Asked Questions

I want to upgrade from Community Version to Enterprise Version. What are the changes?

In ownCloud Enterprise you will get access to new apps and features, mainly targeted towards enterprises; apps and features that ensure security, for example.

You can upgrade to the Enterprise version without concern, as your existing files, shares, and users remain as they are.

How do I transfer files from one user to another?

See [transferring files to another user](#).

How do I deal with problems caused by using self-signed SSL certificates?

See the [security section of the OCC command](#).

I'm the admin and I lost my password! What do I do now!

See the [reset admin password documentation](#).

What is a Federated System?

A Federated System is another ownCloud or [OpenCloudMesh](#) supporting cloud service.

Platform-wide known limitations, excluded files

There are known file names that can not be synced with ownCloud, these are:

- Folders and files with a trailing space.
- `.htaccess`.
- `*.part` files.
- File names that exceed 253 characters.
- [client/sync-exclude.list](#).
- `Desktop.ini` in the root directory.
- UNIX/Linux hidden files (files whose names have a leading dot, e.g., `.12345.pdf`). Users must activate "*sync hidden files*" to sync them.

Installation Options

Introduction

This is an overview about the possible installation options for ownCloud Server. You can install ownCloud Server manually or use a Docker-based installation.

Manual Installation

- The [Detailed Installation Guide](#) is a thorough guide for installing ownCloud, containing all the information needed for the prerequisites, the dependencies, the actual installation and the configuration afterwards. The example installation is based on Ubuntu Server.

This guide covers Ubuntu server preparations like dependencies, required packages and other necessary components or configurations including Ubuntu upgrades if necessary, descriptions, explanations and easy copy and paste example commands where possible. You will also get directed to other necessary or recommended sections in the documentation to have a well working ownCloud Server base ready for production.

- The [Quick Installation Guide](#) is a quick guide for installing ownCloud. This guide cannot go into details and has its limits by nature. If you experience issues like with dependencies of PHP or other relevant things like the operating system, web server or database, you have to use the [Detailed Installation Guide](#).

Using a Docker-Based Installation

This guide shows you how to install [ownCloud with Docker](#) using Docker Compose with a YAML file provided by ownCloud.

Linux Package Manager Installation

While this is not a recommended method installing ownCloud Server, this guide shows you how to use the [Linux Package Manager](#) method.

Deployment Considerations

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 primary, multiple replicas 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.

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

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

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

Apache with mod_php is currently the best option. Mod_php is recommended instead of PHP_FPM, because in scale-out deployments separate PHP pools are 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 primary-replica deployment with a MySQL proxy in front of them to send updates to primary, and selects to the replica(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 primary-replica 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.

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. S3 also allows access to Ceph Storage.

Session Storage

- Redis is required for transactional file locking [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](#)).

Deployment Recommendations

Introduction

This document is a guide for technical measures to size your physical environment regarding some general setups described in the scenarios below. It focuses on the software stack and may include some hardware recommendations. You can use any hardware as long the software is capable of running on it and delivers performance that meets your needs.



Independent of the technical measures, you can decide at any time the ownCloud licensing model - the [ownCloud Edition](#).

General 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.



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. Therefore, these recommendations are only rules of thumb based on our experience and customer feedback.

- Operating system: Linux.
- Web server: Apache 2.4.
- Database: MySQL/MariaDB with InnoDB storage engine (MyISAM is not supported, see: [MySQL / MariaDB storage engine](#))
- And a recent PHP Version. See [System Requirements](#)
- Consider setting up a scale-out deployment, or using [Federated Cloud Sharing](#) to keep individual ownCloud instances to a manageable size.



Whatever the size of your organization, always keep one thing in mind:

The amount of data stored in ownCloud will only grow - plan ahead.

ownCloud Administrators Must Have Command Line or Cron Access

We only recommend using hosts that provide the following *to ownCloud administrators*

- command-line access or
- Cron access
- ideally both of the above

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. Default PHP timeout values are often low. Having low timeout settings can break long-running operations, such as moving a huge folder.

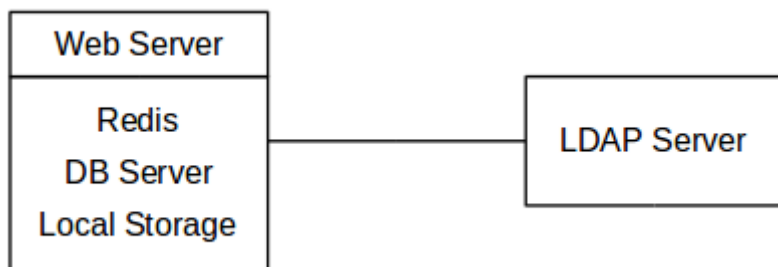
Scenario 1: Small Workgroups and Departments

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	<ul style="list-style-type: none">• 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 Ubuntu 20.04, 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. See the [official Apache documentation](#) or our [Let's Encrypt SSL Certificates](#) 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 because MyISAM is not supported, see: [MySQL / MariaDB storage engine](#)



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 primary 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 [backup](#) and [restore](#) 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

[Redis](#) is recommended and can be used for the session management storage.

Alternatively you can use local session management, see [Local Session Management](#).

Memory Caching

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

Storage

Local storage or Network File System (NFS) if already available.

Recommended Licensing Model

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

Scenario 2: Mid-Sized Enterprises

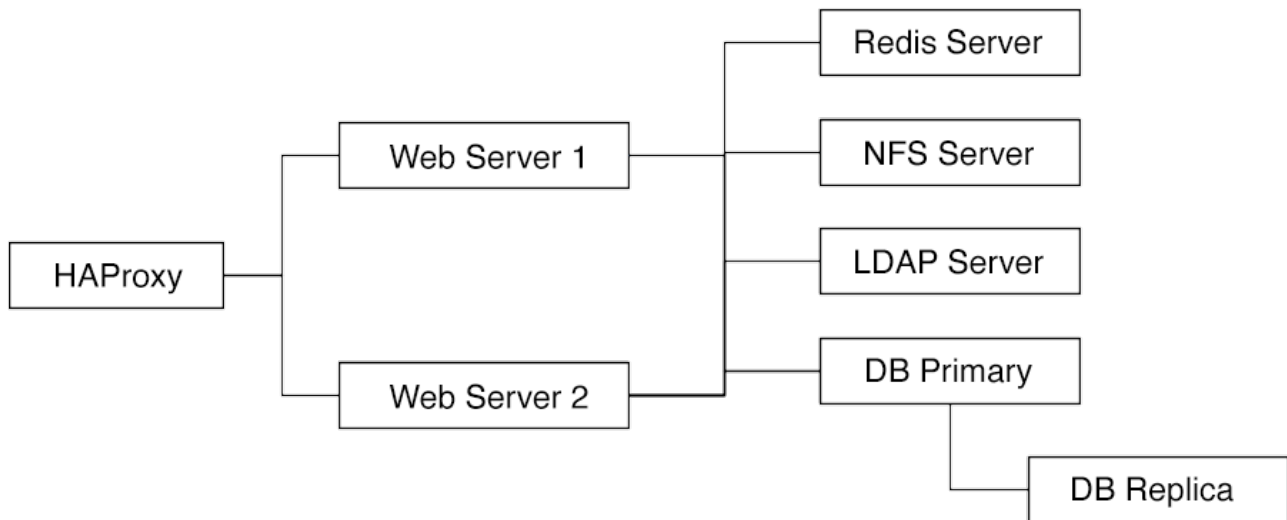
These recommendations apply if you meet the following criteria:

Option	Value
Number of users	150 to 1,000 users.
Storage size	Up to 200TB.
High availability level	<ul style="list-style-type: none"> • 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.
- A Redis server for file locking



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 [primary-replica replication](#). InnoDB storage engine, MyISAM is not supported, see: [MySQL / MariaDB storage engine](#). For mariadb consider: [MariaDB Monitor](#) to configure your setup for a failover Scenario.

Backup

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

- Create a snapshot on the NFS storage server.
- At the same time stop the MySQL replication.
- Create a MySQL dump of the backup replica.
- 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

[Redis](#) is recommended and can be used for the session management storage.

Alternatively you can use local session management, see [Local Session Management](#).

Memory Caching

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

Storage

For accessing a backend storage system via NFS, you can use a dedicated storage system like [NetApp Hybrid Flash Storage Systems](#), or other systems like [IBM Elastic Storage](#) based on their Power8 servers or [RedHat Ceph](#) with their NFS-Ceph gateway.

You may take a look on the [NetApp NFS Best Practice and Implementation Guide](#) for best NFS configuring practices, especially section *9.4 Mount Option Best Practices with NFS* on page 111 and [MySQL Database on NetApp ONTAP](#) which also includes performance measurements.

Recommended Licensing Model

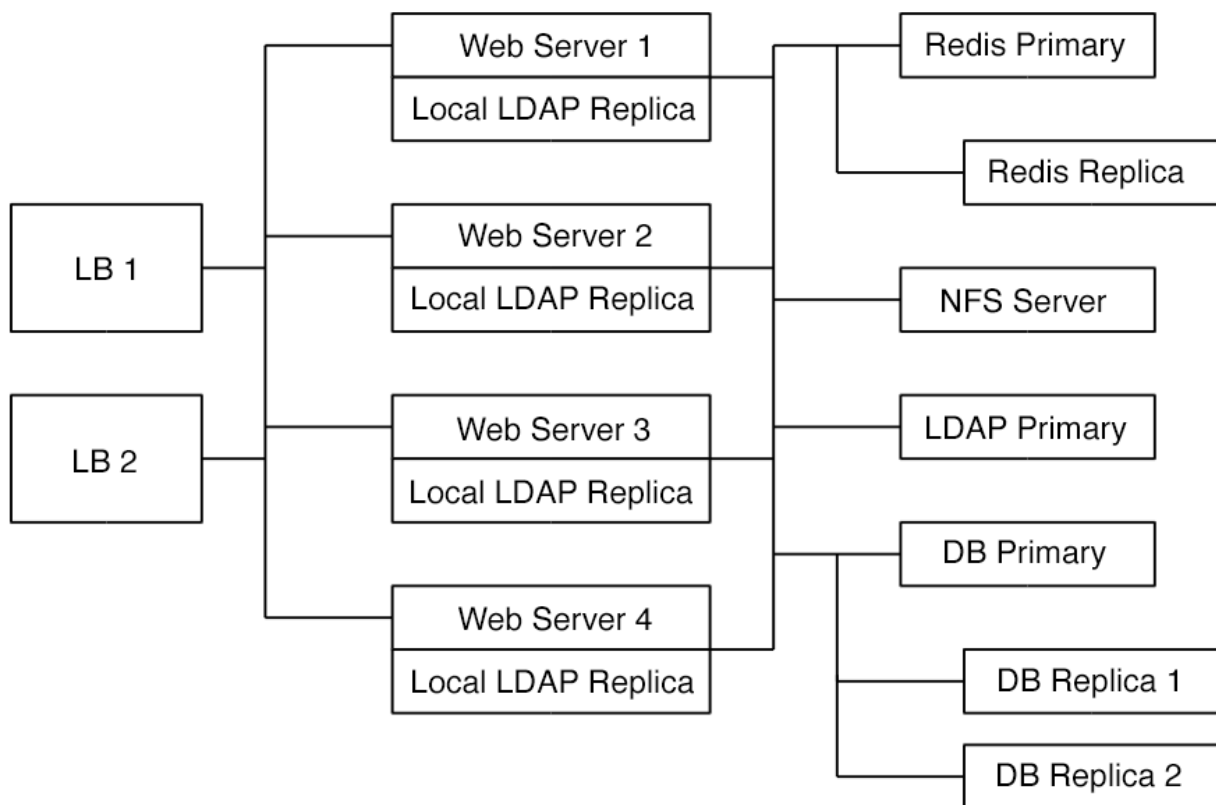
- Enterprise Edition
- See [ownCloud Server or Enterprise Edition](#) for comparisons of the ownCloud editions.

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	<ul style="list-style-type: none"> • 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 primary-replica replication. InnoDB storage engine, MyISAM is not supported, see: [MySQL / MariaDB storage engine](#). For mariadb consider: [MariaDB Monitor](#) to configure your setup for a failover Scenario.

Backup

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

Storage

For accessing a backend storage system via NFS, you can use a dedicated storage system like [NetApp Hybrid Flash Storage Systems](#) or other systems like [IBM Elastic Storage](#) based on their Power8 servers or [RedHat Ceph](#) with their NFS-Ceph gateway. Optionally, an S3 compatible object store can also be used.

You may take a look on the [NetApp NFS Best Practice and Implementation Guide](#) for best NFS configuring practices, especially section *9.4 Mount Option Best Practices with NFS* on page 111 and [MySQL Database on NetApp ONTAP](#) which also includes performance measurements.

Recommended Licensing Model

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

Redis Configuration

Redis in a primary-replica configuration is [a hot failover setup](#) and is usually sufficient. A replica can be omitted if high availability is provided via other means. If that's the case, restarting Redis typically happens fast enough in the event of a failure. 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.

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 transaction
```

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 begun. Once it reaches this point, the node executes the original query.

Why enable it

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



This setting is disabled by default. See the [Galera Cluster WSREP documentation](#) for more details.

General References

- [Database High Availability](#)
- [Performance enhancements for Apache and PHP](#)

Local 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/php*
```

and then add it to the `/etc/fstab` file, for example:

```
Unresolved directive in  
modules/admin_manual/pages/installation/deployment_recommendations.adoc -  
include::example$installation/deployment_recommendations/set_session_path.sh[]
```

Network File System (NFS) Deployment Recommendations

ownCloud recommends using NFS for any scenario other than local storage. It has solid performance and is very stable. This document contains ownCloud's official deployment recommendations.

There can be different scenarios where ownCloud's storage is located on an NFS mount (primary/secondary). In some scenarios, multiple application servers can use the same NFS mount point.



It is advised to use network storage like NFS only in un-routed, switched Gigabit or higher environments.



This guide only covers the NFS client side where ownCloud runs. Follow the storage vendors recommendations to configure the NFS server (storage backend).

General Performance Considerations

Please consider that a network stack runs in ranges of μ s while a storage backend usually runs in ranges of ms. Any tuning considerations should therefore first be attempted on the backend storage layout side, especially under high loads.

NFS Version Comparison Overview

NFSv3	
Exports	All exports are mounted separately
Protocol	Numerous protocols for different aspects collected together. MOUNT, LOCK, STATUS...
Locking	Permanent locks in yet another protocol
Security	UNIX based. SecureNFS. Mode Bit Locking
Communication	One operation per RPC
I18N	All locales must match
Parallel high bandwidth access	None native. (Addition such as MPFS)

NFSv4	
Exports	All exports can be mounted together in a directory tree structure as part of a pseudo-filesystem
Protocol	A single protocol with the addition of OPEN and CLOSE for security auditing
Locking	Lease based locking in the same protocol
Security	Kerberos and ACL based
Communication	Multiple operations per RPC. (Improves performance)
I18N	UTF-8
Parallel high bandwidth access	pNFS

NFSv4

ownCloud recommends using NFSv4 over previous versions for a number of key reasons. These are:

- **Improved Security:** It [mandates a strong security architecture](#). It does not require `rpc.statd` or `lockd`. As a result, it only uses port 2049.
- **Improved Reliability:** Uses TCP by default.
- **Improved Performance:** It uses Multi-Component Messages, which reduce network traffic. It is capable of using a 32KB page size, compared to the default, 1024 bytes.
- Use of [Read/Write Delegations](#).

NFS Mount Options

See the [Ubuntu man pages](#) for a detailed description of the NFS mount options. The following options are default for NFS except if explicitly set differently when mounting: `rw`, `suid`, `dev`, `exec`, `auto`, `nouser`, and `async`.

Depending on the NFS version used, consider the following mount options:

`_netdev`

Use this option to ensure that the network is enabled, before NFS attempts to mount these filesystems. This setting is essential when database files are located on an NFS storage. The database could error or not start correctly, if the mount is not ready before attempting to access its data files.



You can also use `autofs`, to ensure that mounts are always available before attempting to access them.

`nofail`

Using `nofail` allows the boot sequence to continue even if the drive fails to mount. This can happen if the NFS server accessed is down. The boot process will continue after the mount reaches timeout. The default device timeout is 90 seconds. If the option is not set, the boot process will wait until the NFS server is available but can be manually set using the option `x-systemd.mount-timeout=<value in seconds>`.

`bg`

ownCloud recommends using this option. Determines how the mount command behaves if an attempt to mount an export fails. If the `bg` option is specified, a timeout or failure triggers the mount command to fork a child, which will continue to attempt mounting the export. The parent immediately returns with a zero exit code. This is known as a "background" mount. This option is useful for continuous operation without manual intervention if the network connectivity is temporarily down or the storage backend must be rebooted.

`hard`

Default value is *hard*. For business-critical NFS exports, ownCloud recommends using *hard* mounts. ownCloud strongly discourages the use of *soft* mounts.

`retrans`

Default value is 3. This option can be tuned when using option *soft*.

`timeo`

Default value is 600 (60 seconds). This option can be tuned when using option *soft*.

`sync/async`

With the default value of *async*, the NFS client may delay sending application writes to the NFS

server. In other words, under normal circumstances, data written by an application may not immediately appear on the server that hosts the file. **sync** provides greater data cache coherence among clients, but at a **significant performance cost**. Having the database like MySQL or Mariadb on NFS, the default database option value for `innodb_flush_method` is `fsync`, even if it is not explicitly set. This database option forces the mount to immediately write to the NFS server without generally setting the mount `sync` option and avoiding this performance penalty. You may consider further tuning when using clustered server environments.

tcp

ownCloud recommends using this option. Force using TCP as transport protocol. Alternatively you can use `proto=tcp`.

Tune the Read and Write Block Sizes

The allowed block sizes are the packet chunk sizes that NFS uses when reading and writing data. The smaller the size, the greater the number of packets need to be sent to send or receive a file. Conversely, the larger the size, the fewer the number of packets need to be sent to send or receive a file. With NFS Version 3 and 4, you can set the `rsize` and `wsiz` values as high as 65536, when the network transport is TCP. The default value is 32768 and must be a multiple of 4096.



Read and write size must be identical on the NFS server and client.

You can find the set values by working with the output of the `mount` command on a standard server, as in the example below.

```
root@server:~# mount | egrep -o rsize=[0-9]*
```

```
rsize=65536
```

```
root@server:~# mount | egrep -o wsize=[0-9]*
```

```
wsize=65536
```

The information can also be retrieved using the command set of your dedicated storage backend. Once you've determined the best sizes, set them permanently by passing the (`rsize` and `wsize`) options when mounting the share or in the share's mount configuration.

Listing 1. Specifying the read and write block sizes when calling mount

```
mount 192.168.0.104:/data /mnt -o rsize=65536,wsiz=65536
```

Listing 2. Example for a set of NFS mount options:

```
bg,nfsvers=3,wsiz=65536,rsiz=65536,tcp,_netdev
```

Ethernet Configuration Options

MTU (Maximum Transmission Unit) Size

The MTU size dictates the maximum amount of data that can be transferred in one Ethernet frame. If the MTU size is too small, then regardless of the read and write block sizes, the data must still be fragmented across multiple frames. Keep in mind that $MTU = \text{payload (packet size)} + 28$.

Get the Current Set MTU Size

You can find the current MTU size for each interface using *netstat*, *ifconfig*, *ip*, and *cat*, as in the following examples:

Listing 3. Retrieve interface MTU size with *netstat*

```
netstat -i

Kernel Interface table
Iface      MTU      RX-OK RX-ERR RX-DRP RX-OVR      TX-OK TX-ERR TX-DRP TX-OVR Flg
lo         65536   363183      0      0 0        363183      0      0      0 LRU
eth0       1500   3138292      0      0 0       2049155      0      0      0 BMR
```

Listing 4. Retrieve interface MTU size with *ifconfig*

```
ifconfig| grep -i MTU

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
```

Listing 5. Retrieve interface MTU size with *ip*

```
ip addr | grep mtu

1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP group default qlen 1000
```

Listing 6. Retrieve interface MTU size with *cat*

```
cat /sys/class/net/<interface>/mtu
```

Check for MTU Fragmentation

To check if a particular packet size will be fragmented on the way to the target, run the following command:

```
ping <your-storage-backend> -c 3 -M do -s <packetsize>
```

Get the Optimal MTU Size

To get the optimal MTU size, run following command:

```
tracert <your-storage-backend>
```

You can expect to see output like the following:

```
1?: [LOCALHOST]                pmtu 1500 ①
1: <your-storage-backend>      0.263ms reached ②
1: <your-storage-backend>      0.224ms reached ③
Resume: pmtu 1500 hops 1 back 1
```

- ① The first line with localhost shows the given MTS size.
- ② The last line shows the optimal MTU size.
- ③ If both are identical, nothing needs to be done.

Change Your MTU Value

In case you need or want to change the MTU size, under Ubuntu:

- If [NetworkManager](#) is managing all devices on the system, then you can use [nmtui](#) or [nmcli](#) to configure the MTU setting.
- If NetworkManager is not managing all devices on the system, you can set the MTU to 1280 with Netplan, as in the following example.

```
network:
  version: 2
  ethernets:
    eth0:
      mtu: 1280
```

Refer to [the Netplan documentation](#) for further information.



NetworkWorld has [an excellent overview of MTU size issues](#).

System Requirements

Introduction

Read this documentation for a recommended or supported environment for your ownCloud Server. This documentation applies to both a new installation or upgrade of an existing installation.

General Note

There is an important note about a [prerequisite of openssl](#). We highly recommend checking this prerequisite as it needs to be checked regardless of the Operating System chosen.

Officially Recommended Environment

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

Platform	Options
Operating System	Ubuntu 20.04 LTS
Database	MariaDB 10.5 ¹
Web server	Apache 2.4 with prefork and mod_php
PHP Runtime	7.4

(1) MariaDB 10.6 and later is **only supported** with ownCloud release 10.9 and upwards. See the [Install a Database](#) guide and [Database Upgrade](#) guide.

Officially Supported Environments

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

Server

Platform	Options
Operating System (64bit)	<ul style="list-style-type: none">• Debian 10• Red Hat Enterprise Linux 7 and 8 including all 100% compatible derivatives• SUSE Linux Enterprise Server 12 with SP4/5 and 15• Ubuntu 20.04 and 22.04• openSUSE Leap 15.2
Database	<ul style="list-style-type: none">• MySQL 8+ or MariaDB 10.2 through 10.8 ¹ (Recommended)• Oracle 11 and 12 (Enterprise only)• PostgreSQL 9, 10, 11, 12, 13 or 14• SQLite (Not for production)

Platform	Options
Web server	<ul style="list-style-type: none"> • Apache 2.4 with prefork and mod_php
PHP Runtime	<ul style="list-style-type: none"> • 7.3 and 7.4

(1) MariaDB 10.6 and later is **only supported** with ownCloud release 10.9 and upwards. See the [Install a Database](#) guide and [Database Upgrade](#) guide.



For Linux distributions, we support, if technically feasible, the latest two versions per platform and the previous LTS Version.

Hypervisors

- Hyper-V
- VMware ESX - ownCloud must run without overcommitment of cores or RAM for larger installations (1000+ users).
- Xen
- KVM

Web Browser

- Edge (current version on Windows 10)
- IE11 or newer (except Compatibility Mode)
- Firefox 60 ESR+
- Chrome 66+
- Safari 10+

Desktop Sync Client

We always recommend to use the newest sync client with the latest server release.

You can find [detailed system requirements](#) in the documentation for the Desktop Synchronization Client.

Mobile Apps

We always recommend to use the newest mobile apps with the latest server release.

You can find detailed system requirements in the documentation for the mobile apps.

- [iOS system requirements](#)
- [Android system requirements](#)



You can find out more in the [changelog](#).

Database Requirements

The following database settings 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](#))

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.

Configuration Notes and Tips

SELinux

See the [SELinux Configuration Guide](#) for a suggested configuration for SELinux-enabled distributions such as Fedora and CentOS.

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.



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 7.3.0 onward, replace `php_version` with the version number installed, e.g., `7.3` 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.

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.



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.



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: $4896 * 3 * 112 = 1.6MB$ 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.

PHP-FPM

Note that `mod_php` is used exclusively in the development and QA process of the ownCloud server. It's highly recommended to use `mod_php` in your production environment for optimal performance and stability. Any issues with the ownCloud server have to be reproducible with `mod_php`.

SAML SSO with Shibboleth **will not work** with `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	CentOS/Red Hat/Fedora
<code>/etc/php/[php_version]/fpm/</code>	<code>/etc/php-fpm.d/</code>

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 `label-phpinfo`.

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 not to use these modules and recommend `mod_php` instead.

Other Web Servers

- [Other HTTP servers](#)
- [Univention Corporate Server installation](#)

Installation Options

Introduction

This is an overview about the possible installation options for ownCloud Server. You can install ownCloud Server manually or use a Docker-based installation.

Manual Installation

- The [Detailed Installation Guide](#) is a thorough guide for installing ownCloud, containing all the information needed for the prerequisites, the dependencies, the actual installation and the configuration afterwards. The example installation is based on Ubuntu Server.

This guide covers Ubuntu server preparations like dependencies, required packages and other necessary components or configurations including Ubuntu upgrades if necessary, descriptions, explanations and easy copy and paste example commands where possible. You will also get directed to other necessary or recommended sections in the documentation to have a well working ownCloud Server base ready for production.

- The [Quick Installation Guide](#) is a quick guide for installing ownCloud. This guide cannot go into details and has its limits by nature. If you experience issues like with dependencies of PHP or other relevant things like the operating system, web server or database, you have to use the [Detailed Installation Guide](#).

Using a Docker-Based Installation

This guide shows you how to install [ownCloud with Docker](#) using Docker Compose with a YAML file provided by ownCloud.

Linux Package Manager Installation

While this is not a recommended method installing ownCloud Server, this guide shows you how to use the [Linux Package Manager](#) method.

Installing with Docker

Introduction

ownCloud can be installed using the [official ownCloud Docker image](#). This official image works standalone for a quick evaluation but is designed to be used in a docker-compose setup.

Grant docker command privileges to certain users by adding them to the group `docker`:

```
sudo usermod -aG docker <your-user>
```



The changes via `usermod` only take effect after the docker users log in. So you may have to log out and log in again or possibly reboot before you can run docker commands.

Users not added to the `docker` group can run docker commands with a preceding `sudo`. In this section `sudo` is generally omitted before docker commands since we assume you have created a docker user, which is also the only way to run ownCloud's command-line interface `occ` in a docker container. For more information on `occ`, see section [Using the occ Command](#).

An example `occ` command looks like this:

```
docker exec --user www-data <owncloud-container-name> occ <your-command>
```

Quick Evaluation



The commands and links provided in the following descriptions are intended to showcase basic docker usage, but we cannot take responsibility for their proper functioning. If you only want to take a peek and are content with SQLite as database, which is not supported by ownCloud for production purposes, try the following:

```
docker run --rm --name oc-eval -d -e OWNCLOUD_DOMAIN=localhost:8080 -p8080:8080  
owncloud/server
```

This starts a docker container with the name "oc-eval" in the background (option `-d`). `owncloud/server` is the docker image downloaded from Docker Hub. If you don't start the container with option `-d`, the logs will be displayed in the shell. If you are running it in the background as in the example above, you can display the logs with the command:

```
docker logs oc-eval
```

With the command `docker ps` you can list your running docker containers and should see the entry for oc-eval.

You can log in to your ownCloud instance via a browser at `http://localhost:8080` with the preconfigured user `admin` and password `admin`.



Access only works with http, not https.

Now, if you like what you see but want a supported installation with MariaDB, you should remove the eval version before proceeding with the next section.

```
docker kill oc-eval
```

This removes the container if you used the option `--rm` as suggested in the example above. If you omitted that option, you need to first run the command:

```
docker rm oc-eval
```

If you now run `docker ps` again, the entry for `oc-eval` should be gone.

Docker Compose

The configuration:

- Exposes ports 8080, allowing for HTTP connections.
- Uses separate *MariaDB* and *Redis* containers.
- Mounts the data and MySQL data directories on the host for persistent storage.

The following instructions assume you install locally. For remote access, the value of `OWNCLOUD_DOMAIN` must be adapted.

1. Create a new project directory. Then copy and paste the sample `docker-compose.yml` from this page into that new directory.
2. 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:8080</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>



`ADMIN_USERNAME` and `ADMIN_PASSWORD` will not change between deploys even if you change the values in the `.env` file. To change them, you'll need to do `docker volume prune`, which **will delete all your data**.

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

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/docs-
server/master/modules/admin_manual/examples/installation/docker/docker-compose.yml
```

Create the environment configuration file

```
cat << EOF > .env
OWNCLOUD_VERSION=10.9
OWNCLOUD_DOMAIN=localhost:8080
ADMIN_USERNAME=admin
ADMIN_PASSWORD=admin
HTTP_PORT=8080
EOF
```

Build and start the container

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

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

Name	Command	State	Ports
owncloud_maria db	docker-entrypoint.sh --max ...	Up (healthy)	3306/tcp
owncloud_redis	docker-entrypoint.sh --dat ...	Up (healthy)	6379/tcp
owncloud_server	/usr/bin/entrypoint /usr/b ...	Up (healthy)	0.0.0.0:8080 → 8080/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.



All files stored in this setup are contained in Docker volumes rather than a physical filesystem tree. It is the admin's responsibility to make the files persistent.

To inspect the volumes run:

```
docker volume ls | grep files
```

The volume name depends on the project name which builds the first part of the volume and the name of the volume in the docker file. The naming pattern of the volume is `<COMPOSE_PROJECT_NAME>_<VOLUME_NAME>`. An environment variable for `COMPOSE_PROJECT_NAME` can be set and also be defined in a `.env` file. If not specified, the directory in which docker-compose is executed will be used as a name.

To export the files of the project "owncloud-docker-server" as a tar archive run:

```
docker run -v <YOUR_DOCKER_VOLUME>:/mnt \
  ubuntu tar cf - -C /mnt . > files.tar
```

Although the containers are up and running, it may still take a few minutes until ownCloud is fully functional.

To inspect the log output:



```
docker-compose logs --follow owncloud
```

Wait until the output shows **Starting apache daemon...** before you access the web UI.

Although all important data persists after:

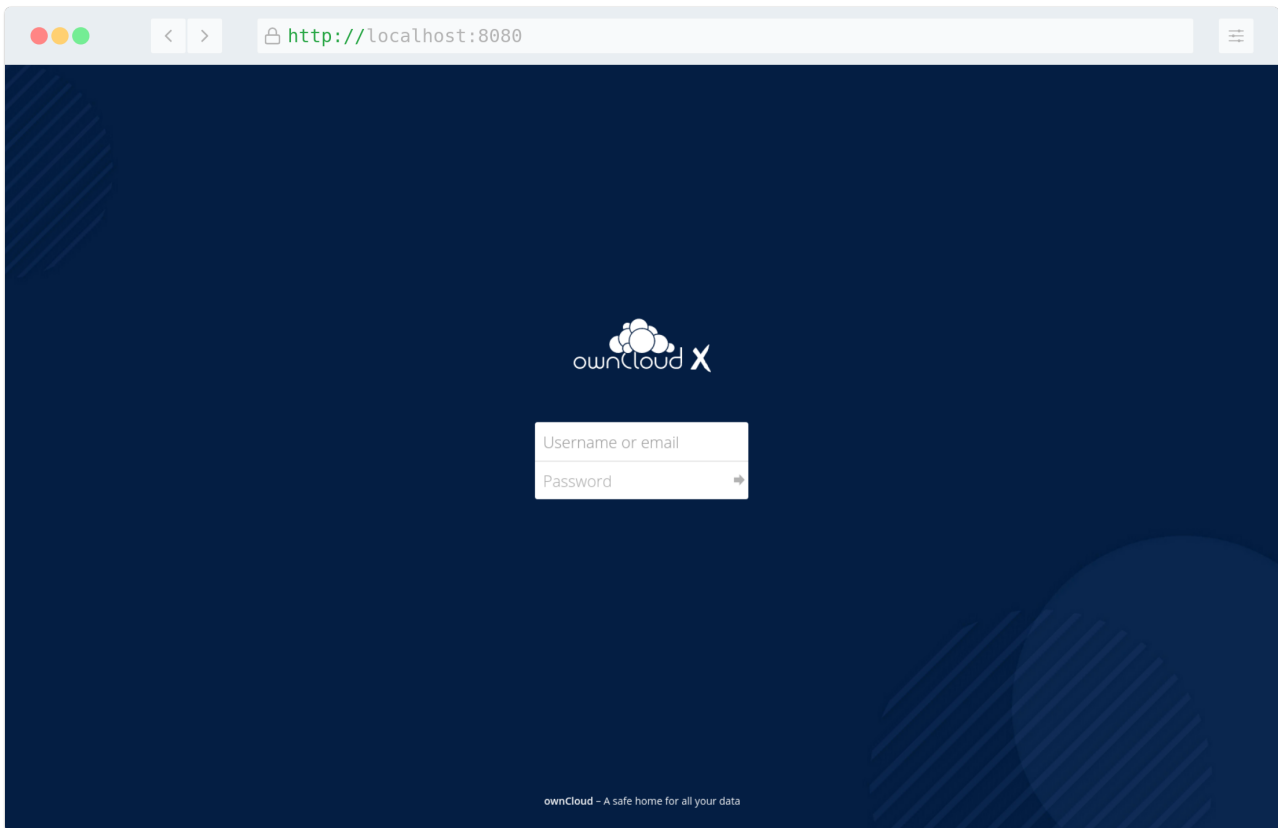


```
docker-compose down; docker-compose up -d
```

there are certain details that get lost, e.g., default apps may re-appear after they were uninstalled.

Logging In

To log in to the ownCloud UI, open <http://localhost:8080> in your browser of choice, where you see the standard ownCloud login screen as in the image below.



The username and password are the credentials which you stored in `.env` earlier. Note that these will not change between deploys even if you change the values in `.env`.

Stopping the Containers

Again we assume you used `docker-compose` like in the previous example. To stop the containers use:

```
docker-compose stop
```

To stop and remove containers along with the related networks, images and volumes:

```
docker-compose down --rmi all --volumes
```

Running occ commands

If you want to run an occ command, first go to the directory where your `.yaml` or `.env` file is located. Here, you are able to run any command referring to [Using the occ Command](#) by entering:

```
docker-compose exec owncloud occ <command>
```



Don't use the `php` command prefix, this leads to several errors and is not intended to run in docker environments.

Upgrading ownCloud on Docker

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

1. Go to your docker directory where your `.yaml` and `.env` files exist.
2. Put ownCloud into maintenance mode with the following command:

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

3. Create a backup of the database in case something goes wrong during the upgrade process, using the following command:

```
docker-compose exec mariadb \  
  /usr/bin/mysqldump \  
  -u root \  
  --password=owncloud \  
  --single-transaction \  
  owncloud > owncloud_$(date +%Y%m%d).sql
```



You need to adjust the password and database name if you have changed it in your deployment.

4. Shutdown the containers:

```
docker-compose down
```

5. Update the version number of ownCloud in your `.env` 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
```

6. View the file to ensure the change has been implemented.

```
cat .env
```

7. Start your docker instance again.

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

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

container will automatically run `occ upgrade` when starting up. If you notice the container starting over and over again, you can check the update log with the following command:

```
docker-compose logs --timestamp owncloud
```

8. If all went well, end maintenance mode:

```
docker-compose exec owncloud occ maintenance:mode --off
```

Docker Compose YAML File

The file `docker-compose.yml` contains the configuration of your ownCloud container.



Since ownCloud Server 10.5, the dedicated enterprise docker image `registry.owncloud.com/owncloud/enterprise` is deprecated. All supported enterprise features and apps are now included in the public image `owncloud/server` available on Docker Hub. A login to our registry `registry.owncloud.com` is no longer required.

```
Unresolved directive in modules/admin_manual/pages/installation/docker/index.adoc -
include::example$installation/docker/docker-compose.yml[Example Docker Compose YAML
configuration file for ownCloud Server.]
```

Troubleshooting

Admin Settings

When running under docker, the admin user cannot control certain settings in the WebUI, instead they are now controlled by environment variables. Changing these variables requires stopping and restarting the container with extra `docker -e ...` parameters or with new entries in the `.env` file for docker-compose.

Logging

The loglevel is set to the fixed value 2: "Warnings, errors, and fatal issues".

Listing 7. To get the highest log level "Everything" (including debug output), use:

```
OWNCLOUD_LOGLEVEL=0
```

Raspberry Pi

If your container fails to start on Raspberry Pi or other ARM devices, you most likely have an old version of `libseccomp2` on your host. This should only affect distros based on Rasbian Buster 32 bit. Install a newer version with the following command:

```
cd /tmp
```

```
wget http://ftp.us.debian.org/debian/pool/main/libs/libseccomp/libseccomp2_2.5.1-1_armhf.deb
sudo dpkg -i libseccomp2_2.5.1-1_armhf.deb
```

Alternatively you can add the backports repo for Debian Buster:

```
sudo apt-key adv --keyserver keyserver.ubuntu.com \
  --recv-keys 04EE7237B7D453EC 648ACFD622F3D138
echo "deb http://deb.debian.org/debian buster-backports main" | \
  sudo tee -a /etc/apt/sources.list.d/buster-backports.list
sudo apt update
sudo apt install -t buster-backports libseccomp2
```

In any case, you should restart the container after confirming you have `libseccomp2.4.4` installed.

For more information see: [Linux Server Docs](#)

Terminating containers

If your container is terminating for whatever reason, you will not be able to run `docker(-compose) exec` to make investigations inside the container as there will be no running container. Instead you need to use `docker(-compose) run`. It's important that you prefix any command to be run by `/usr/bin/owncloud`, otherwise the container will not be initialized correctly. See the example command below:

```
docker(-compose) run <containername> /usr/bin/owncloud bash
```

Detailed Installation Guide

Introduction

This document describes:

- How to prepare your server
- Prerequisites and how to download ownCloud
- Installation of ownCloud

The following descriptions focus on the Ubuntu distribution. Even if we try to make these steps as easy as possible by offering ready to use commands and scripts, you need to have sufficient knowledge about administrating a server environment which provides web services.



This document does not offer proposals about how to secure your server. Therefore, we strongly recommend checking out the [Hardening and Security Guidance](#) before the installation and to keep it on hand throughout.

Prepare Your Server

For more information on the requirements of your server, read the [general prerequisites guide](#). The following sections describe the procedures in detail.

Ubuntu 20.04 LTS Server

To prepare your Ubuntu 20.04 server for the use with ownCloud, follow the [Ubuntu 20.04 preparation guide](#). This guide installs PHP 7.4

Ubuntu 22.04 LTS Server

To prepare your Ubuntu 22.04 server for the use with ownCloud, follow the [Ubuntu 22.04 preparation guide](#).



Ubuntu 22.04 only provides PHP 8.x which is currently not supported by ownCloud. Therefore PHP 7.4 is installed via PPA.

Install a Database

If you do not already have a supported database installed, follow the [Manual Database Installation guide](#).

Configure the Web Server

To configure your Apache web server for use with ownCloud, follow the [Apache preparation guide](#).

Installation of ownCloud Binaries

To install ownCloud binaries, you have to download the required package. After doing so, you can perform the following steps manually or use the provided scripts. These scripts are convenient since they can also be used for upgrading which eases the process a lot.

Download ownCloud

Before downloading ownCloud, change to a directory where you want to save the file temporarily. This can be, for example `/tmp`. In further examples, we use tar archives or the complete ownCloud bundle. The name for the complete archive looks like this: `owncloud-complete-yyyyymmdd.archive_type`.

Download the archive of the latest ownCloud version:

1. Go to the [ownCloud Download Page](#) and select the package that fits your needs. You can download either the `.tar.bz2` or `.zip` archive. Based on the example below, copy the link of the selected file and run the following command to download it:

```
wget https://download.owncloud.com/server/stable/owncloud-complete-latest.tar.bz2
```

2. Download the corresponding checksum file like:

```
wget https://download.owncloud.com/server/stable/owncloud-complete-
latest.tar.bz2.md5
or
wget https://download.owncloud.com/server/stable/owncloud-complete-
latest.tar.bz2.sha256
```

3. Verify the MD5 or SHA256 sum:

```
sudo md5sum -c owncloud-complete-latest.tar.bz2.md5 < owncloud-complete-
latest.tar.bz2
or
sudo sha256sum -c owncloud-complete-latesttar.bz2.sha256 < owncloud-complete-
latest.tar.bz2
```

4. You can also verify the PGP signature:

```
wget https://download.owncloud.com/server/stable/owncloud-complete-
latest.tar.bz2.asc
gpg --verify owncloud-complete-latest.tar.bz2.asc owncloud-complete-latest.tar.bz2
```

Script-Guided Installation

Use the [Script-Guided Installation](#) if you want to easily **install** or **upgrade** ownCloud or **manage ownership and permissions**. The page contains detailed instructions about downloading and usage.



Using the *Script Guided Installation*, you can handle many useful installation and update options automatically.

Command Line Installation

Use the following commands if you want to do the basic setup without any changes and physical installation options. Consider using the [Script-Guided Installation](#) if you plan to improve your setup from step one.

- Extract the archive contents and run the unpacking command for your tar archive:

```
tar -xjf owncloud-complete-latest.tar.bz2
```

- tar unpacks to a single **owncloud** directory. Copy the ownCloud directory to its final destination. If you are running the Apache HTTP server, you may safely install ownCloud in your Apache document root. Assuming your document root is in **/var/www**.


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

After the installation, set the correct ownership and permissions according to the needs of your environment. While you can do that manually, we suggest using the scripts from the [Script-Guided Installation](#) which ease the process a lot.

Complete the Installation

After restarting Apache, you must complete your installation by running either the Graphical Installation Wizard or on the command line with the `occ` command.

After finalizing the installation, re-run the script provided in [Script-Guided Installation](#) to secure your `.htaccess` files. Your ownCloud instance is now ready to use.

Finalize Using the Graphical Installation Wizard

To finalize the installation using the graphical installation wizard, refer to the [Graphical Installation Wizard](#).

Finalize Using the Command Line

If you want to finalize the installation via the command line, use the following example command. The command assumes that you have unpacked the source to `/var/www/owncloud/`. Replace all the parameters according to your needs.

```
cd /var/www/owncloud/  
sudo -u www-data ./occ maintenance:install \  
  --database "mysql" \  
  --database-name "owncloud" \  
  --database-user "root"\  
  --database-pass "password" \  
  --admin-user "admin" \  
  --admin-pass "password"
```

On how to use `occ`, refer to the [occ command reference](#).



Admins of SELinux-enabled distributions may need to write new SELinux rules to complete their ownCloud installation; see the [SELinux Configuration Guide](#) for a suggested configuration.

Post Installation Configuration

After installing ownCloud successfully, ownCloud recommends that you perform some post installation tasks. These tasks help configure background jobs or improve performance by caching.



At this point, we'd also like to remind you to consult the [Hardening and Security Guidance](#) section.

Background Jobs

To read more about background jobs and how to configure them, read the [Background Job Configuration](#) guide.

Configure Caching

It is recommended to install and enable caching (PHP opcode cache and/or data cache), which significantly improves performance. For more information, read the [Caching Configuration](#) guide.

Notes

Headers



ownCloud has a mechanism to set headers programmatically. These headers are set with the `always` directive to avoid errors when there are additional headers set in the web server's configuration file like `http.conf`. More information on headers can be found in the `mod_headers` documentation.

Managing Trusted Domains

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



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

A typical configuration may look like this:

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

The loopback address, `127.0.0.1`, is automatically white-listed, 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.



For further information on improving the quality of your ownCloud installation, see [the configuration notes and tips guide](#).



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 Configuration Guide](#) for a suggested configuration.

Install ownCloud on Ubuntu 20.04

Introduction

This is a short guide to installing ownCloud on a fresh installation of Ubuntu 20.04. Run the following commands in your terminal to complete the installation.

This guide can not go into details and has its limits by nature. If you experience issues like with dependencies of PHP or other relevant things like the operating system, web server or database, look at the [Detailed Installation Guide](#) for more information.

Prerequisites and Notes

- A fresh installation of [Ubuntu 20.04](#) with SSH enabled.
- This guide assumes that you are working as the root user.
- Your ownCloud directory will be located in `/var/www/owncloud/`.
- php 7.4 is the default version installable with Ubuntu 20.04.
- Use the correct [Multi-Processing Module \(MPM\)](#).
- Read the [openssl Version](#) notes which are important when planning to use encryption.

Preparation

Set Your Domain Name

```
my_domain="Your.Domain.tld"
echo $my_domain

hostnamectl set-hostname $my_domain
hostname -f
```

Generate Strong Passwords

```
sec_admin_pwd=$(openssl rand -base64 18)
echo $sec_admin_pwd > /etc/.sec_admin_pwd.txt

sec_db_pwd=$(openssl rand -base64 18)
echo $sec_db_pwd > /etc/.sec_db_pwd.txt
```

Update Your System

First, ensure that all the installed packages are entirely up to date and that PHP is available in the APT repository. To do so, follow the instructions below:

```
apt update && \
  apt upgrade -y
```

Create the occ Helper Script

Create a helper script to simplify running [occ commands](#):

```
FILE="/usr/local/bin/occ"
cat <<EOM >$FILE
#!/bin/bash
cd /var/www/owncloud
sudo -E -u www-data /usr/bin/php /var/www/owncloud/occ "$@"
EOM
```

Make the helper script executable:

```
chmod +x $FILE
```

Install the Required Packages

```
apt install -y \
  apache2 libapache2-mod-php \
  mariadb-server openssl redis-server wget php-imagick \
  php-common php-curl php-gd php-gmp php-bcmath php-imap \
  php-intl php-json php-mbstring php-mysql php-ssh2 php-xml \
  php-zip php-apcu php-redis php-ldap php-phpseclib
```

Install smbclient php Module

If you want to connect to external storage via SMB you need to install the smbclient php module.

First install the required packages:

```
apt-get install -y libsmbclient-dev php-dev php-pear
```

Then install smbclient php module using pecl:

```
pecl channel-update pecl.php.net
mkdir -p /tmp/pear/cache
pecl install smbclient-stable
echo "extension=smbclient.so" > /etc/php/7.4/mods-available/smbclient.ini
phpenmod smbclient
systemctl restart apache2
```

Check if it was successfully activated:

```
php -m | grep smbclient
```

This should show the following output:

```
libsmbclient
smbclient
```

Install the Recommended Packages

Additional useful tools helpful for debugging:

```
apt install -y \
  unzip bzip2 rsync curl jq \
  inetutils-ping ldap-utils\
  smbclient
```

Configure Apache

Create a Virtual Host Configuration

```
FILE="/etc/apache2/sites-available/owncloud.conf"
cat <<EOM >${FILE}
<VirtualHost *:80>
# uncomment the line below if variable was set
#ServerName $my_domain
DirectoryIndex index.php index.html
DocumentRoot /var/www/owncloud
<Directory /var/www/owncloud>
  Options +FollowSymLinks -Indexes
  AllowOverride All
  Require all granted

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

  SetEnv HOME /var/www/owncloud
  SetEnv HTTP_HOME /var/www/owncloud
</Directory>
</VirtualHost>
EOM
```

Enable the Virtual Host Configuration

```
a2dissite 000-default
a2ensite owncloud.conf
```

Configure the Database



It's recommended to execute `mysql_secure_installation` to secure the mariadb installation and set a strong password for the database user.

Ensure transaction-isolation level is set and `performance_schema` on.

```
sed -i "\[mysqld\]/transaction-isolation = READ-COMMITTED\nperformance_schema = on"
/etc/mysql/mariadb.conf.d/50-server.cnf
systemctl start mariadb
mysql -u root -e "CREATE DATABASE IF NOT EXISTS owncloud; \
GRANT ALL PRIVILEGES ON owncloud.* \
TO owncloud@localhost \
IDENTIFIED BY '${sec_db_pwd}'";
```

It is recommended to run `mysqldtuner` script to analyse database configuration after running with load for several days.

Enable the Recommended Apache Modules

```
a2enmod dir env headers mime rewrite setenvif
systemctl restart apache2
```

Installation

Download ownCloud

```
cd /var/www/
wget https://download.owncloud.com/server/stable/owncloud-complete-latest.tar.bz2 && \
tar -xjf owncloud-complete-latest.tar.bz2 && \
chown -R www-data:owncloud
```

Install ownCloud



Remember to set a strong password for your owncloud admin user and provide the previously set password for the database user as the `--database-pass` argument.

```
occ maintenance:install \
--database "mysql" \
--database-name "owncloud" \
--database-user "owncloud" \
--database-pass ${sec_db_pwd} \
--data-dir "/var/www/owncloud/data" \
--admin-user "admin" \
```

```
--admin-pass ${sec_admin_pwd}
```

Configure ownCloud's Trusted Domains

```
my_ip=$(hostname -I|cut -f1 -d ' ')\nocc config:system:set trusted_domains 1 --value="$my_ip"\nocc config:system:set trusted_domains 2 --value="$my_domain"
```

Configure the cron Jobs

Set your background job mode to cron:

```
occ background:cron
```

Configure the execution of the cron job to every 15 min and the cleanup of chunks every night at 2 am:

```
echo "*/*15 * * * * /var/www/owncloud/occ system:cron" \  
| sudo -u www-data -g crontab tee -a \  
/var/spool/cron/crontabs/www-data\necho "0 2 * * * /var/www/owncloud/occ dav:cleanup-chunks" \  
| sudo -u www-data -g crontab tee -a \  
/var/spool/cron/crontabs/www-data
```



If you need to sync your users from an LDAP or Active Directory Server, add this additional [Cron job](#). Every 4 hours this cron job will sync LDAP users in ownCloud and disable the ones who are not available for ownCloud. Additionally, you get a log file in `/var/log/ldap-sync/user-sync.log` for debugging.

```
echo "1 */6 * * * /var/www/owncloud/occ user:sync \  
'OCA\User_LDAP\User_Proxy' -m disable -vvv >> \  
/var/log/ldap-sync/user-sync.log 2>&1" \  
| sudo -u www-data -g crontab tee -a \  
/var/spool/cron/crontabs/www-data\nmkdir -p /var/log/ldap-sync\ntouch /var/log/ldap-sync/user-sync.log\nchown www-data. /var/log/ldap-sync/user-sync.log
```

Configure Caching and File Locking

```
occ config:system:set \  
memcache.local \  
--value '\OC\Memcache\APCu'\nocc config:system:set \  

```

```
memcache.locking \  
  --value '\OC\Memcache\Redis'  
occ config:system:set \  
  redis \  
  --value '{"host": "127.0.0.1", "port": "6379"}' \  
  --type json
```

Configure Log Rotation

```
FILE="/etc/logrotate.d/owncloud"  
sudo cat <<EOM >$FILE  
/var/www/owncloud/data/owncloud.log {  
  size 10M  
  rotate 12  
  copytruncate  
  missingok  
  compress  
  compresscmd /bin/gzip  
}  
EOM
```

Finalize the Installation

Make sure the permissions are correct:

```
cd /var/www/  
chown -R www-data. owncloud
```

ownCloud is now installed. You can confirm that it is ready to enable HTTPS (for example using [Let's Encrypt](#)) by pointing your web browser to your ownCloud installation.

To check if you have installed the correct version of ownCloud and that the occ command is working, execute the following:

```
occ -V  
echo "Your Admin password is: "$sec_admin_pwd  
echo "It's documented at /etc/.sec_admin_pwd.txt"  
echo "Your Database Password is: "$sec_db_pwd  
echo "It's documented at /etc/.sec_db_pwd.txt and in your config.php"  
echo "Your ownCloud is accessible under: "$my_domain  
echo "The Installation is complete."
```



We recommend you check out the section [Hardening and Security Guidance](#) next.

Install ownCloud on Ubuntu 22.04

Introduction

This is a short guide to installing ownCloud on a fresh installation of Ubuntu 22.04. Run the following commands in your terminal to complete the installation.

This guide can not go into details and has its limits by nature. If you experience issues like with dependencies of PHP or other relevant things like the operating system, web server or database, look at the [Detailed Installation Guide](#) for more information.

Prerequisites and Notes

- A fresh installation of [Ubuntu 22.04](#) with SSH enabled.
- This guide assumes that you are working as the root user.
- Your ownCloud directory will be located in `/var/www/owncloud/`.
- php 7.4 from the `ondrej/php` PPA is going to be installed on Ubuntu 22.04.
- Use the correct [Multi-Processing Module \(MPM\)](#).
- Read the [openssl Version](#) notes which are important when planning to use encryption.

Preparation

Set Your Domain Name

```
my_domain="Your.Domain.tld"
echo $my_domain

hostnamectl set-hostname $my_domain
hostname -f
```

Generate Strong Passwords

```
sec_admin_pwd=$(openssl rand -base64 18)
echo $sec_admin_pwd > /etc/.sec_admin_pwd.txt

sec_db_pwd=$(openssl rand -base64 18)
echo $sec_db_pwd > /etc/.sec_db_pwd.txt
```

Update Your System

First, ensure that all the installed packages are entirely up to date and that PHP is available in the APT repository. To do so, follow the instructions below:

```
apt update && \
  apt upgrade -y
```

Create the occ Helper Script

Create a helper script to simplify running [occ commands](#):

```
FILE="/usr/local/bin/occ"
cat <<EOM >$FILE
#!/bin/bash
cd /var/www/owncloud
sudo -E -u www-data /usr/bin/php /var/www/owncloud/occ "$@"
EOM
```

Make the helper script executable:

```
chmod +x $FILE
```

Install the Required Packages

```
sudo add-apt-repository ppa:ondrej/php -y
sudo apt update && sudo apt upgrade

apt install -y \
  apache2 \
  libapache2-mod-php7.4 \
  mariadb-server openssl redis-server wget \
  php7.4 php7.4-imagick php7.4-common php7.4-curl \
  php7.4-gd php7.4-imag php7.4-intl php7.4-json \
  php7.4-mbstring php7.4-gmp php7.4-bcmath php7.4-mysql \
  php7.4-ssh2 php7.4-xml php7.4-zip php7.4-apcu \
  php7.4-redis php7.4-ldap php-phpseclib\
```

Install smbclient php Module

If you want to connect to external storage via SMB you need to install the smbclient php module.

```
apt-get install -y php7.4-smbclient
echo "extension=smbclient.so" > /etc/php/7.4/mods-available/smbclient.ini
phpenmod smbclient
systemctl restart apache2
```

Check if it was successfully activated:

```
php -m | grep smbclient
```

This should show the following output:

```
libsmbclient
smbclient
```

Install the Recommended Packages

Additional useful tools helpful for debugging:

```
apt install -y \  
  unzip bzip2 rsync curl jq \  
  inetutils-ping ldap-utils\  
  smbclient
```

Configure Apache

Create a Virtual Host Configuration

```
FILE="/etc/apache2/sites-available/owncloud.conf"  
cat <<EOM >${FILE}  
<VirtualHost *:80>  
# uncomment the line below if variable was set  
#ServerName $my_domain  
DirectoryIndex index.php index.html  
DocumentRoot /var/www/owncloud  
<Directory /var/www/owncloud>  
  Options +FollowSymlinks -Indexes  
  AllowOverride All  
  Require all granted  
  
<IfModule mod_dav.c>  
  Dav off  
</IfModule>  
  
  SetEnv HOME /var/www/owncloud  
  SetEnv HTTP_HOME /var/www/owncloud  
</Directory>  
</VirtualHost>  
EOM
```

Enable the Virtual Host Configuration

```
a2dissite 000-default  
a2ensite owncloud.conf
```

Configure the Database



It's recommended to execute `mysql_secure_installation` to secure the mariadb installation and set a strong password for the database user.

Ensure transaction-isolation level is set and `performance_schema` on.

```
sed -i "\[mysqld\]/transaction-isolation = READ-COMMITTED\nperformance_schema = on"
/etc/mysql/mariadb.conf.d/50-server.cnf
systemctl start mariadb
mysql -u root -e "CREATE DATABASE IF NOT EXISTS owncloud; \
GRANT ALL PRIVILEGES ON owncloud.* \
TO owncloud@localhost \
IDENTIFIED BY '${sec_db_pwd}'";
```

It is recommended to run the `mysqldtuner` script to analyze the database configuration after running with load for several days.

Enable the Recommended Apache Modules

```
a2enmod dir env headers mime rewrite setenvif
systemctl restart apache2
```

Installation

Download ownCloud

```
cd /var/www/
wget https://download.owncloud.com/server/stable/owncloud-complete-latest.tar.bz2 && \
tar -xjf owncloud-complete-latest.tar.bz2 && \
chown -R www-data. owncloud
```

Install ownCloud



Remember to set a strong password for your ownCloud admin user and provide the previously set password for the database user as the `--database-pass` argument.

```
occ maintenance:install \
--database "mysql" \
--database-name "owncloud" \
--database-user "owncloud" \
--database-pass ${sec_db_pwd} \
--data-dir "/var/www/owncloud/data" \
--admin-user "admin" \
```

```
--admin-pass ${sec_admin_pwd}
```

Configure ownCloud's Trusted Domains

```
my_ip=$(hostname -I|cut -f1 -d ' ')
occ config:system:set trusted_domains 1 --value="$my_ip"
occ config:system:set trusted_domains 2 --value="$my_domain"
```

Configure the cron Jobs

Set your background job mode to cron:

```
occ background:cron
```

Set the execution of the cron job to every 15 minutes and the cleanup of chunks every night at 2 am:

```
echo "*/*15 * * * * /var/www/owncloud/occ system:cron" \
| sudo -u www-data -g crontab tee -a \
/var/spool/cron/crontabs/www-data
echo "0 2 * * * /var/www/owncloud/occ dav:cleanup-chunks" \
| sudo -u www-data -g crontab tee -a \
/var/spool/cron/crontabs/www-data
```



If you need to sync your users from an LDAP or Active Directory Server, add this additional [cron job](#). Every 4 hours this cron job will sync LDAP users in ownCloud and disable the ones who are not available for ownCloud. Additionally, you get a log file in `/var/log/ldap-sync/user-sync.log` for debugging.

```
echo "1 */6 * * * /var/www/owncloud/occ user:sync \
'OCA\User_LDAP\User_Proxy' -m disable -vvv >> \
/var/log/ldap-sync/user-sync.log 2>&1" \
| sudo -u www-data -g crontab tee -a \
/var/spool/cron/crontabs/www-data
mkdir -p /var/log/ldap-sync
touch /var/log/ldap-sync/user-sync.log
chown www-data. /var/log/ldap-sync/user-sync.log
```

Configure Caching and File Locking

```
occ config:system:set \
  memcache.local \
  --value '\OC\Memcache\APCu'
occ config:system:set \
```

```
memcache.locking \  
--value '\OC\Memcache\Redis'  
occ config:system:set \  
redis \  
--value '{"host": "127.0.0.1", "port": "6379"}' \  
--type json
```

Configure Log Rotation

```
FILE="/etc/logrotate.d/owncloud"  
sudo cat <<EOM >$FILE  
/var/www/owncloud/data/owncloud.log {  
    size 10M  
    rotate 12  
    copytruncate  
    missingok  
    compress  
    compresscmd /bin/gzip  
}  
EOM
```

Finalize the Installation

Make sure the permissions are correct:

```
cd /var/www/  
chown -R www-data. owncloud
```

ownCloud is now installed. You can confirm that it is ready to enable HTTPS (for example using [Let's Encrypt](#)) by pointing your web browser to your ownCloud installation.

To check if you have installed the correct version of ownCloud and that the occ command is working, execute the following:

```
occ -V  
echo "Your Admin password is: "$sec_admin_pwd  
echo "It's documented at /etc/.sec_admin_pwd.txt"  
echo "Your Database Password is: "$sec_db_pwd  
echo "It's documented at /etc/.sec_db_pwd.txt and in your config.php"  
echo "Your ownCloud is accessible under: "$my_domain  
echo "The Installation is complete."
```



We recommend you check out the section [Hardening and Security Guidance](#) next.

Linux Package Manager Installation

Introduction

You can use the `packetmanager` installation, but it is not recommended to do so. This is because sometimes dependencies are acting against each other like `ownCloud` version, minimum PHP version and Linux distribution restrictions. Anyone who runs a package manager installation should consider migrating to a manual installation to overcome this situation.

Add the ownCloud Repository

Before you can install `owncloud-files`, you need to add [ownCloud's package repository](#) to your distribution's package manager.



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

Available Packages

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

Avoid Automatic Upgrades

If you are installing ownCloud using one of the various Linux package managers, we **strongly** recommend that you avoid automatically updating the `owncloud-complete-files` package, when running a system update or upgrade and when upgrading other packages. That way, there are no surprise changes (whether positive or negative) to your ownCloud installation.

Here are the ways to do so for [APT](#), [Yum](#), and [Zypper](#).

APT

If you are using APT, use `apt-mark hold` to mark the `owncloud-complete-files` package as held. Here's an example of how to do so:

```
apt-mark hold owncloud-complete-files
```

To see if `owncloud-complete-files` has already been held, use the `showhold` command, as in the following example. If it's printed out to the console, then it's being held.

```
apt-mark showhold owncloud-complete-files
```

To unset `owncloud-complete-files` as held back, use the `unhold` command, as in the example below.

```
apt-mark unhold owncloud-complete-files
```

Yum

If you are using Yum, there are two options that you can take to lock packages from being upgraded. You can:

1. Add `exclude=owncloud-complete-files` to `/etc/yum.conf`
2. Use [the versionlock plugin](#) for Yum.

The VersionLock Plugin

If the `versionlock` plugin is not installed, install it by running:

```
yum install yum-plugin-versionlock
```

When it is installed, you can lock `owncloud-complete-files` run:

```
yum versionlock add owncloud-complete-files
```

To confirm that it is locked, run:

```
yum versionlock list
```

To unlock `owncloud-complete-files`, run:

```
yum versionlock delete owncloud-complete-files
```

Zypper

If you are using Zypper, use the `addlock` or `al` commands. Similar to `apt-mark hold` these add a package lock that prevents the package from being modified. The example below shows how to use the command to lock `owncloud-complete-files`.

```
zypper addlock owncloud-complete-files
```

To see if the package has already been locked, use the `locks` command. If `owncloud-complete-files` is already locked, then you will see output similar to the below example.

```
# | Name | Type | Repository
---+-----+-----+-----
1 | owncloud-complete-files | package | (any)
```

To unlock `owncloud-complete-files`, if it is already locked, use the `removelocks` or `rl` commands, as in the example below.

Installing ownCloud Community Edition

The package comes without dependencies which means, that the server will not directly run after installing it.

To get the dependencies installed and configured, follow one of the guides provided in section [Manual Installation on Linux](#)



See the `system_requirements` for the recommended ownCloud setup and supported platforms.

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 download and install from [ownCloud's package repository](#)

The ownCloud server is designed to work with different databases and different web-servers, in a large range of configurations.



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 10.9.1. 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 10.0.2, 10.0.3, 10.0.4 or 10.9.1. 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.

Installing ownCloud Enterprise Edition

See [the enterprise installation guide](#) for instructions on installing ownCloud Enterprise edition.

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.

Additional Guides and Notes

See `installation_wizard` for important steps, such as choosing the best database and setting correct directory permissions. See the [SELinux Configuration Guide](#) 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 [client stable version](#) is in the official community repository, more packages are in the [Arch User 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](#).

The Installation Wizard

Introduction

When you have installed ownCloud physically, you can either finalize the installation from the command line or the installation wizard. This guide focuses on using the installation wizard.

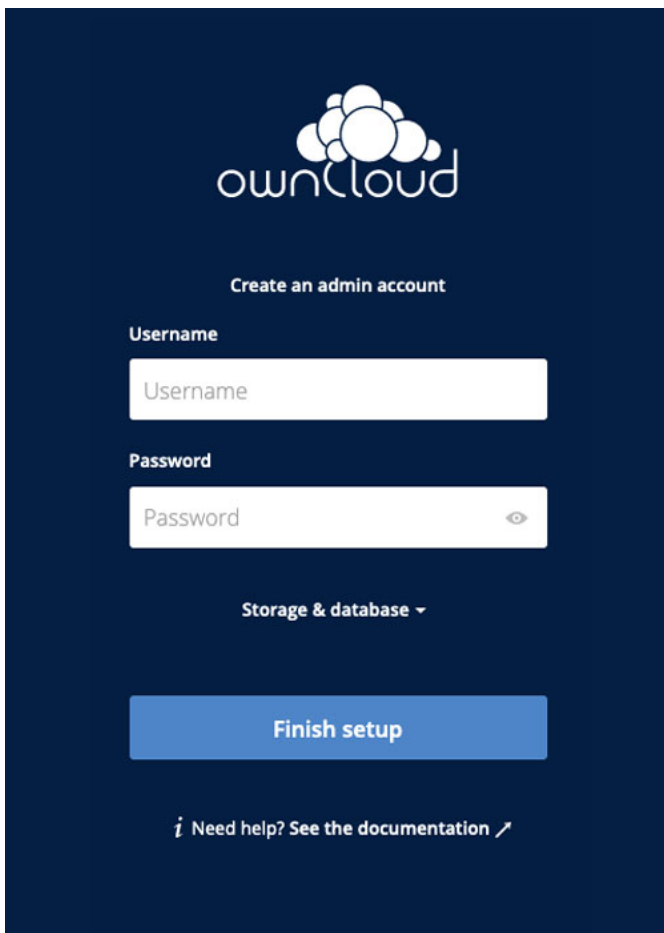


If you are planning to use the installation wizard, we **strongly** encourage you to protect it through some form of [password authentication](#) or [access control](#). If the installer is left unprotected when exposed to the internet, there is the possibility that a malicious actor could finish the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

Quick Start

When the ownCloud prerequisites are fulfilled and all ownCloud files are installed, run the Installation Wizard. This involves just three steps:

1. Point your web browser to <http://<your-owncloud-domain>>.
2. Enter your desired administrator's username and password.
3. Click [**Finish Setup**].



Now you can start using your new ownCloud server. Of course, there is much more that you could 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.

Detailed Guide

This section provides a more detailed guide to the installation wizard and the three main topics:

1. [Post-Installation Steps](#)
2. [Configuration Options](#)
3. [Database Setup by ownCloud](#)

Post-Installation Steps

For hardened security and proper server operation, ownCloud recommends setting the permissions on your ownCloud directories as strictly as possible. This should be done immediately after the initial installation and before running the setup.

Your HTTP user must own the directories `config/`, `data/`, `apps/` and, if applicable, `apps-external/` 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 `label-phpinfo`. 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`.



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 could cause problems if the NFS mount is lost.

An easy way to set the correct permissions is to use the scripts provided in the [Script-Guided Installation](#).

Configuration Options

Click **[Storage and Database]** to expose additional installation configuration options for your ownCloud data directory and to select the database and configure the access.

The screenshot shows the 'Storage & database' configuration screen. It features a dark blue background with white text and input fields. At the top, there is a dropdown menu labeled 'Storage & database'. Below it, the 'Data folder' section has a text input field containing '/var/oc_data'. The 'Configure the database' section has three tabs: 'SQLite', 'MySQL/MariaDB' (which is selected), and 'PostgreSQL'. Below the tabs are five input fields: 'Database user' (containing 'Database user'), 'Database password' (containing 'Database password' and a toggle icon), 'Database name' (containing 'Database name'), and 'Database host' (containing 'localhost'). At the bottom, there is a note: 'Please specify the port number along with the host name (e.g., localhost: 5432).', a blue 'Finish setup' button, and a footer with an information icon, the text 'Need help? See the documentation', and the slogan 'ownCloud - A safe home for all your data'.



For security reasons, the `data` directory of your ownCloud should be located

outside the webroot of your server.

The location of the `data` directory can either be defined by entering the path here or when installing the ownCloud files. For more information on the latter, see the [Script-Guided Installation](#).

If you define the path here, the respective setting in your `config.php` file will be adjusted. Alternatively, you can create a link `data` pointing to the directory containing the actual files. In this case, the `config.php` setting for the data directory remains unchanged.



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 webserver user.

Database Setup by ownCloud



Your database and PHP connectors must be installed **before** you run the Installation Wizard.

After you enter your administrative login for your database, the installer creates a special database user with privileges limited to the ownCloud database.

Afterward, ownCloud only needs this special ownCloud database user and drops the administrative database login you used before. This new user's name is based on 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.

Troubleshooting

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.'

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/>.



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.

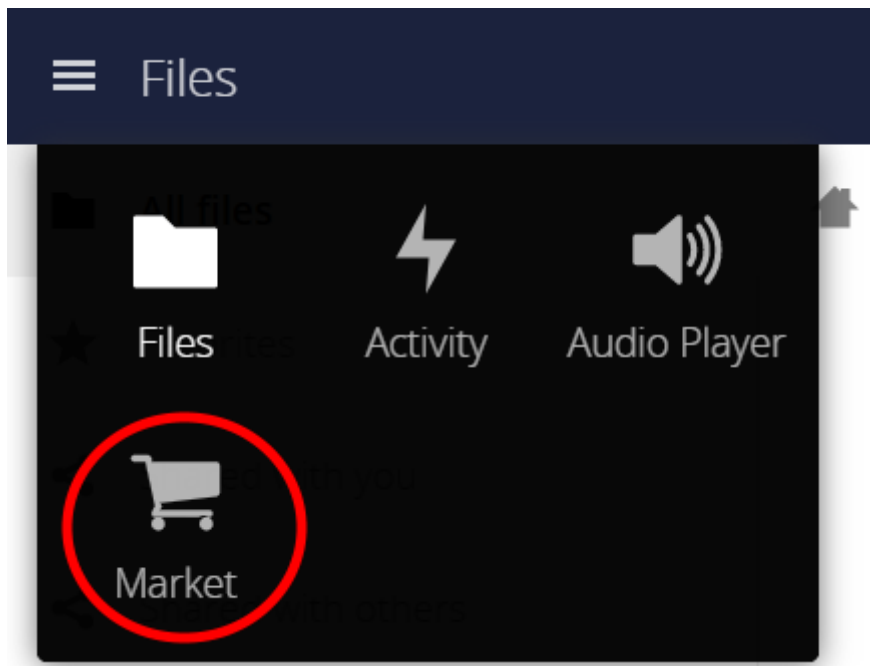
Installing and Managing Apps

Introduction

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

Installing and Managing Apps

Installing Apps Via the ownCloud Marketplace



To add an app, use the *Market* app, which is accessible from the top-level navigation bar, on the left-hand side of the page. Once in the Market app, click an app's name to view more details about it. Once you have done this, you can also install it by clicking [**Install**]. Clicking *Install*, downloads it from the ownCloud Marketplace, installs, and enables it.

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, they are not installed.



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

Installing Apps Manually

To install an app manually, instead of by using the Market app, extract the app tarball into your ownCloud installation's default app folder (`</path/to/owncloud>/apps`) or, ideally, into [a custom app directory](#).

Once the tarball has been extracted into the default app folder. Enable the application,

- by Navigating to **Settings** > **Admin** > **Apps** and clicking [**Enable**]; or the
- [occ app command](#).

Managing Apps

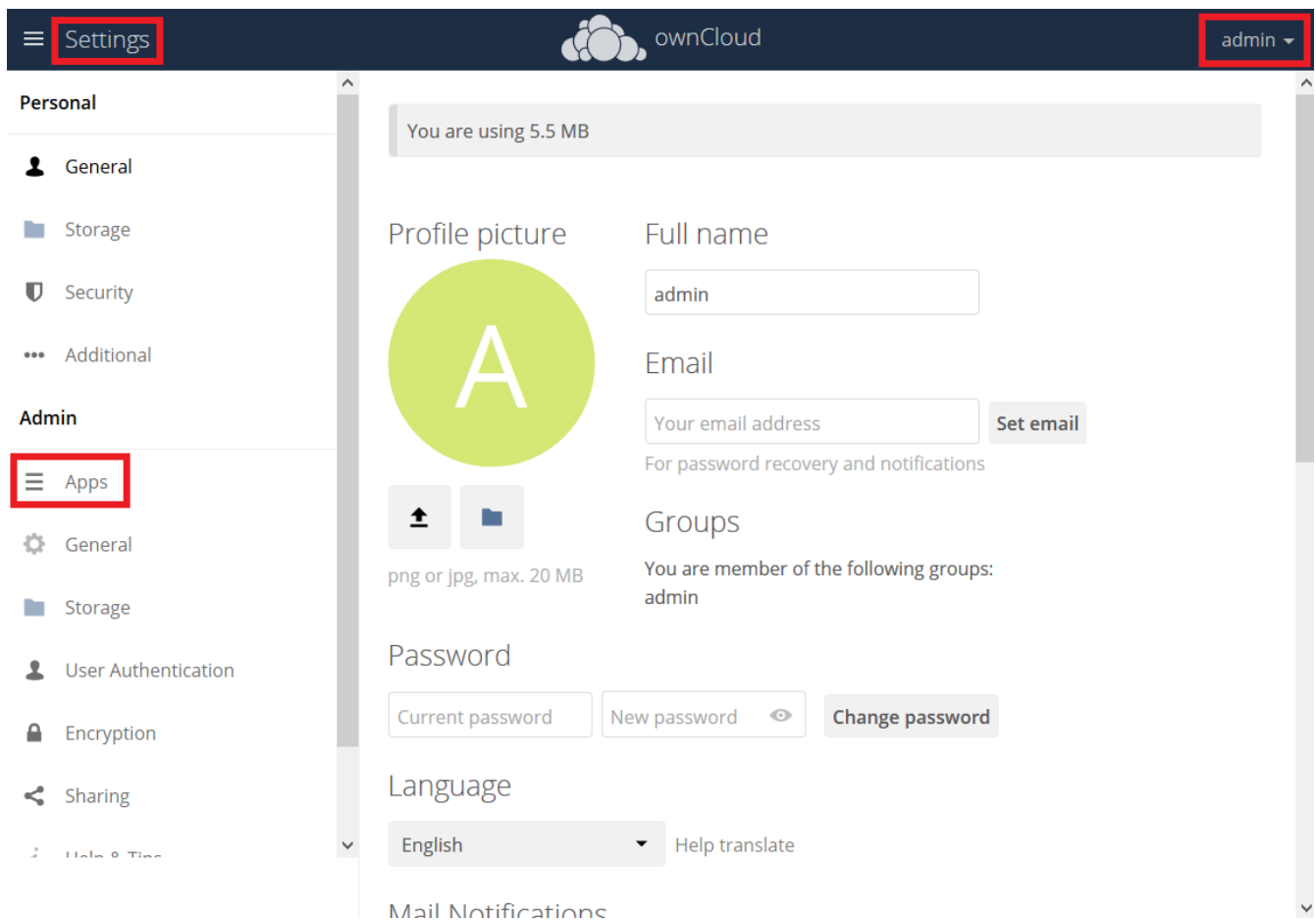
Some apps are installed and enabled during ownCloud installation, while other apps can be installed and enabled post-installation.



Supported Enterprise Apps

See [supported apps](#) for a list of supported Enterprise edition apps.

View App Status



The screenshot displays the ownCloud user interface. At the top, the 'Settings' menu item is highlighted with a red box. In the top right corner, the user's name 'admin' is also highlighted with a red box. The left sidebar shows the 'Admin' section, with the 'Apps' menu item highlighted by a red box. The main content area shows the user's profile for 'admin'. It includes a storage usage indicator (5.5 MB), a profile picture, and fields for 'Full name' (admin), 'Email' (Your email address), and 'Groups' (admin). There are also sections for 'Password' and 'Language' (English).

To see the status of your installation's applications, go to your Apps page, via **Settings** › **Admin** › **Apps**. 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.

Enabling and Disabling Apps

On the Apps page (**Settings** › **Admin** › **Apps**), you can enable or disable applications. By default, enabled apps are displayed. To disable an app, click **[Disable]** under its details.

To display disabled apps, click **[Show disabled apps]**. To enable an app, click **[Enable]** under its details.

Configuring Apps

Some apps have configurable options on the Apps page, such as **Enable only for specific groups**. However, this is the exception. Apps are mainly configured from your ownCloud Personal or Admin settings page, or in `config.php`.

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. Having non-core apps in a directory separate to the core app directory makes them 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 webroot, prefixed with `/`.

writable

Whether users can install apps in that folder.

After adding the configuration, ownCloud only installs apps in directories where `writable` is set to `true`. The configuration example below shows how to add a second directory, called `apps-external`.

```
Unresolved directive in modules/admin_manual/pages/installation
/apps_management_installation.adoc - include::example$installation/custom-app-
directory-configuration.php[]
```

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](#).

Multiple Servers

We recommend having your `apps-external` and your `config` directory on a network storage in order to prevent conflicts when installing or updating apps.

Supported Apps in ownCloud

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 Media Viewer](#)



Before Files Media Viewer 1.0.4, the *Gallery* and *Files VideoPlayer* apps need to be **uninstalled before installing** the Media Viewer app. Starting with Files Media Viewer 1.0.4, the *Gallery* and *Files VideoPlayer* apps need to be **disabled before using** the Files Media Viewer app.

- Files PDF Viewer
- Files Sharing
- Files TextEditor
- Files Trashbin
- Files Versions
- First Run Wizard
- Notifications
- Provisioning API
- Template Editor (for notification emails)
- Update Notifications
- User External
- User LDAP

Enterprise-Only Apps

- [Auditing](#)
- [Collaborative Tags Management](#)

- [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](#)

Media Viewer App

Introduction

The [Media Viewer App](#) is a simple viewer for pictures and videos integrated into the files app, which supersedes the former Gallery and Video Player apps.



- Before installing the Media Viewer app, the Gallery and Video Player apps need to be removed, or at the very least disabled. When removing or disabling, ensure that any [gallery link shares are redirected](#).
- Gallery and Video Player are no longer supported and will not receive any further security or bug fixes.
- Users are strongly encouraged to switch to Media Player.

Add Support For More Media Types

To add support for additional media types, in addition to the default set, ensure that [ImageMagick](#) and its [PECL extension](#) are installed and enabled. Next, add new entries to the `enabledPreviewProviders` in `config/config.php`. Below, is an example of how to configure it.

```
'enabledPreviewProviders' => [
    'OC\\Preview\\PNG',
    'OC\\Preview\\JPEG',
    'OC\\Preview\\GIF',
    'OC\\Preview\\Illustrator',
    'OC\\Preview\\Postscript',
    'OC\\Preview\\Photoshop',
    'OC\\Preview\\TIFF'
],
```



Support for playing Apple QuickTime (*.mov) does not work in Chrome - however it is supported in Safari and Mozilla.



Look at the sample configuration ([config.sample.php](#)) in your config folder, for more information about this configuration key.

SELinux Configuration

Introduction

[Security-Enhanced Linux \(SELinux\)](#) is a Linux kernel security module that provides a mechanism for supporting access control security policies, including mandatory access controls (MAC).

Preparation

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/apps-external(/.*)?'
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/apps-external(/.*)?'
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  
/var/www/html/owncloud/apps-external
```

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
```

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
```

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
```

Allow access to LDAP server

Use this setting to allow LDAP connections:

```
setsebool -P httpd_can_connect_ldap on
```

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
```

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
```

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
```

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
```

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
```

Allow access to GPG for Rainloop

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

```
setsebool -P httpd_use_gpg on
```

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 to configure 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
```

Unresolved directive in modules/admin_manual/pages/installation/letsencrypt/index.adoc - include::partial\$section_page.adoc[]

- [Using Let's Encrypt SSL Certificates](#)
- [Configure Apache with Let's Encrypt](#)

Using Let's Encrypt SSL Certificates

Introduction

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

- For ease of handling, SSL-specific directives have been moved into a separate file to be included. This can help with first-time certificate issuance as well as with reusing configurations.
- 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 at the earliest 30 days before expiring. Certbot can be forced to renew via options at any time as long as the certificate is valid.



Raymii.org provides [raymii-ssl-url](#)[an excellent introduction to strong SSL security measures with Apache], if you would like to know more.

Requirements & Dependencies

You require a domain name with a valid [A-Record](#) pointing back to your server's IP address. In case your server is behind a firewall, ensure that your server is accessible from the internet by adding the required firewall and port forwarding rules.

Install Let's Encrypt's Certbot Client



certbot has updated the prerequisites and the way to install the certbot script. You can find how to install it on [certbot instructions](#). Follow one of the possible ways and continue when ready.



If you have used `certbot-auto` before, read how to upgrade in the [certbot-auto](#) section.

In general, to run Certbot, use the following command:

```
sudo certbot
```

Updating Certbot

Because certbot is using snap for Ubuntu, there is no need to manually check for updates. Snap checks this automatically and does not require admin intervention, although you can configure the update behavior. For details see the [Snap getting started](#) documentation.

Register Your Email Address

First Time Registration

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 a question similar to the following, which you can answer "Yes" or "No":

```
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.

Update Your Registration

In case you want to update your registered email address use following command:



This will affect all the certificates issued using this account.

```
sudo certbot register --update-registration --email <your-email-address>
```

When that completes, you'll see a message similar to the following:

```
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: y
```

IMPORTANT NOTES:

- Your e-mail address was updated to `<your-email-address>`

Create Let's Encrypt's Config Files

Because remembering all the possible options for certbot is difficult, the following scripts ease the use for common tasks because of their self-descriptive name.

- Create the following files in the Let's Encrypt directory which can usually be found in `/etc/letsencrypt`. Rename `<your-domain-name>.sh` with the name of the domain(s) you want to issue a certificate for.

```
cd /etc/letsencrypt
```

```
sudo touch cli.ini list.sh renew.sh renew-cron.sh delete.sh <your-domain-name>.sh
```

- Make all files created executable *except* `cli.ini` by running

```
sudo chmod +x *.sh
```

- Use `sudo` when running the scripts (unless you are already logged in as the root user)

All scripts have to be executed with `sudo` as certbot [requires enhanced privileges](#).



If you're logged in to your server as a user other than root, you'll likely need to put `sudo` before your Certbot commands so that they run as root (for example, `sudo certbot` instead of just `certbot`)

cli.ini

This file defines some default settings used by Certbot. Use the email address you registered with. Comment or uncomment the post-hook parameter depending on if you want to run post hooks. Running post hooks will reload the web server configuration automatically if a certificate has been renewed.

```
Unresolved directive in
modules/admin_manual/pages/installation/letsencrypt/using_letsencrypt.adoc -
include::example$installation/lets_encrypt/cli.ini[]
```



For the following scripts, replace the path to Certbot and the Certbot script name based on your installation. You can find it by running:

```
which certbot
```

list.sh

This script lists all your issued certificates.

```
Unresolved directive in
modules/admin_manual/pages/installation/letsencrypt/using_letsencrypt.adoc -
include::example$installation/lets_encrypt/list.sh[]
```

renew.sh

This script:

- Renews all your issued certificates.
- In case you have enabled the post hook for your web server in `cli.ini`, it will reload the web server configuration automatically if a certificate has been renewed.

```
Unresolved directive in
modules/admin_manual/pages/installation/letsencrypt/using_letsencrypt.adoc -
include::example$installation/lets_encrypt/renew.sh[]
```

renew-cron.sh

This script:

- Renews all your issued certificates but does not upgrade Certbot.
- In case you have enabled the post hook for your web server in `cli.ini`, it will reload the web server configuration automatically if a certificate has been renewed.



This script is intended for use via Cron.

```
Unresolved directive in
modules/admin_manual/pages/installation/letsencrypt/using_letsencrypt.adoc -
include::example$installation/lets_encrypt/renew-cron.sh[]
```

delete.sh

This script deletes an issued certificate.
Use the `list.sh` script to list issued certificates.

```
Unresolved directive in
modules/admin_manual/pages/installation/letsencrypt/using_letsencrypt.adoc -
include::example$installation/lets_encrypt/delete.sh[]
```

<your-domain-name>.sh

The following example script creates a certificate for a domain or sub-domains, which can be added or removed as necessary. Replace (sub-domain.)example.com with your domain or sub-domain names. The first (sub)domain name in the script is used for naming the directories created by Certbot.



You can create different certificates for different sub-domains, such as `example.com`, `www.example.com`, and `subdomain.example.com` by creating different scripts.

```
Unresolved directive in
modules/admin_manual/pages/installation/letsencrypt/using_letsencrypt.adoc -
include::example$installation/lets_encrypt/your-domain-name.sh[]
```



You can enable the `--dry-run` option which does a test run of the client only.

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 has been successfully created and that it will expire on 2018-06-18.

Listing Existing Certificates

If you want to list (view) 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
```

Web Server Setup

Refer to the [Apache setup guide](#), to set up your web server and issue a certificate.

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.

The screenshot shows the Qualys SSL Labs report interface. At the top, there is a navigation bar with the Qualys logo and links for Home, Projects, Qualys.com, and Contact. Below the navigation bar, the report title is "SSL Report:" followed by a redacted domain name. The assessment date is "Sat, 17 Mar 2018 14:27:01 UTC | HIDDEN | Clear cache" and there is a "Scan Another »" link. The main content area is titled "Summary" and features a large green "A+" rating box. To the right of the rating is a horizontal bar chart showing scores for Certificate (100), Protocol Support (95), Key Exchange (90), and Cipher Strength (90). Below the chart, there is a yellow banner with a link to the documentation page and a green banner indicating that HTTP Strict Transport Security (HSTS) is deployed on the server.

Renewing SSL Certificates

As Let's Encrypt certificates expire every 90 days, 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
```



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.



If you want to use different values, you can check them e.g. at crontab.guru and modify the script with your preferred options.

Add Extra Domains to the Certificate

If you want to add an extra domain, like `subdomain.example.com`, 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 for your ownCloud instance to sub-domain access.



This means you need to comment the `include` directive (see the relevant [web server setup](#)) and follow the steps afterwards.

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 by displaying a list of the currently available SSL certificate domain names, as in the example below, and then prompt you to supply the certificate 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.  
-----
```

Configure Apache with Let's Encrypt

Introduction

This guide shows how to configure Apache with Let's Encrypt.

Dependencies

To follow this guide, your server needs to have the following dependencies installed:

- Apache 2.4.8 or later
- OpenSSL 1.0.2 or later
- [Let's Encrypt](#)

Assumptions

This guide assumes these things:

1. That you are using Ubuntu.
If you are not using Ubuntu, please adjust the instructions to suit your distribution or operating system.
2. That your ownCloud installation is configured using a [VirtualHost \(vhost\)](#) configuration instead of being configured in the main Apache configuration.
3. That the vhost configuration file is stored under `/etc/apache2/sites-available/`.
Not all distributions use this location, however. Refer to your distribution's Apache documentation, to know where to store yours.



See the [SSL Configuration Generator](#) for setup details depending on your environment, especially the different results based on the selected *Mozilla*

Create and Configure a Diffie-Hellman Params File



A Diffie-Hellman (DH) params file is necessary for Forward Secrecy and for securing your TLS setup. Read [Perfect Forward Secrecy Explained](#) or [Perfect Forward Secrecy - An Introduction](#) for more details.

When using Apache 2.4.8 or later and OpenSSL 1.0.2 or later, you can generate and specify a [Diffie-Hellman](#) (DH) params file. If not already present in your VirtualHost (vhost) file, add an [SSLOpenSSLConfCmd](#) directive and a new certificate with stronger keys, which improves Forward Secrecy.



The following OpenSSL command may take quite a while to complete, so be patient.

You can place the generated SSL certificate into any directory of your choice by running the following command and changing the value supplied to the `-out` option. We recommend storing it in `/etc/apache2/` in this guide, solely for simplicity.

```
sudo openssl dhparam -out /etc/apache2/dh4096.pem 4096
```

Once the command completes, add the following directive to your common SSL configuration:

```
SSLOpenSSLConfCmd DHParameters /etc/apache2/dh4096.pem
```

Let's Encrypt ACME-Challenge

After that, add an Alias directive for the `/.well-known/acme-challenge` location in your HTTP VirtualHost configuration, as in line four in the following example.

```
<VirtualHost *.80>
  ServerName mydom.tld

  Alias /.well-known/acme-challenge/ /var/www/letsencrypt/.well-known/acme-challenge/
  <Directory "/var/www/letsencrypt/.well-known/acme-challenge/">
    Options None
    AllowOverride None
    ForceType text/plain
    RedirectMatch 404 "^(?!/\.well-known/acme-challenge/[\w-]{43}$)"
  </Directory>

  # ... remaining configuration
</VirtualHost>
```


Create an SSL VirtualHost Configuration

We recommend creating a separate file for storing the **SSL** directives for each site. If these directives already exist on the virtual host for the site, delete them and include the file instead. This way, after the certificate has been created, you can use the file in any virtual host configuration with SSL enabled for which the certificate is valid without reissuing the SSL certificate. It also eases the management for the web site certificate files, as you can easily include or exclude the file in the virtual config with a single remark and it keeps the files' contents compact.

```
cd /etc/apache2/  
sudo mkdir ssl_rules  
touch ssl_rules/ssl_mydom.tld
```

Listing 8. `/etc/apache2/ssl_rules/ssl_mydom.tld`

```
# Eases letsencrypt initial cert issuing  
  
SSLEngine on  
SSLCertificateChainFile /etc/letsencrypt/live/mydom.tld/fullchain.pem  
SSLCertificateKeyFile /etc/letsencrypt/live/mydom.tld/privkey.pem  
SSLCertificateFile /etc/letsencrypt/live/mydom.tld/cert.pem
```



To improve SSL performance, we recommend that you use the [SSLUseStapling](#) and [SSLStaplingCache](#) directives. Here's an example configuration:

```
SSLUseStapling on  
SSLStaplingCache shmcb:/tmp/stapling_cache(2097152)
```

With the files created and filled-out, update your HTTPS VirtualHost configuration:

```
<VirtualHost *:443>  
  ServerName mydom.tld  
  
  # ssl letsencrypt  
  # Include /etc/apache2/ssl_rules/ssl_mydom.tld  
  
  #...  
</VirtualHost>
```



For the moment, comment out the **Include** directive, as the certificate files do not, currently, exist.

Test and Enable the Apache Configuration

With the configuration created, test it by running one of the following two commands:

```
sudo apache2ctl configtest
sudo apache2ctl -t
```

It should not display any errors. If it doesn't, load your new Apache configuration by running the following command:

```
sudo apache2ctl graceful
```

Create the SSL Certificates

See the Let's Encrypt [Create an SSL Certificate](#) documentation for how to create the SSL certificates.

See the Let's Encrypt [Listing Existing Certificates](#) documentation for how to list the SSL certificates.

As the certificate files exist, you can uncomment the `Include` directive in your HTTPS VirtualHost configuration to use them.

```
<VirtualHost *:443>
  ServerName mydom.tld

  # ssl letsencrypt
  Include /etc/apache2/ssl_rules/ssl_mydom.tld

  #...
</VirtualHost>
```

Reload the Apache Configuration

Finally, reload (or restart) Apache.

It is now ready to serve HTTPS request for the given domain using the issued certificates.

```
sudo service apache2 reload
```

Configuration

In this section, you will find all the information you need for configuring ownCloud.

Database

In this section, you can find out about

- [Converting your Database Type](#)
- [Database Configuration on Linux](#)

Converting Database Type

Introduction

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](#).



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`:



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_log_file_size=256M
innodb_log_buffer_size = 128M
innodb_buffer_pool_size=2048M
innodb_buffer_pool_instances=3
innodb_io_capacity = 500
innodb_file_format=Barracuda
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 -u www-data ./occ db:convert-type [options] type username hostname database
```



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 -u www-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](#)

Database Configuration on Linux

Introduction

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.



After physically installing ownCloud, the setup of the owncloud database is either done with the [installation wizard](#) or via the command line. For more information see the [Complete the Installation](#) section in the Manual Installation documentation.

Requirements

Choosing to use MySQL / MariaDB, PostgreSQL, or Oracle as your database requires, that you install and set up the server software first.



Oracle users, see [the Oracle Database Configuration guide](#).

The steps for configuring a third party database are beyond the scope of this document. Please refer to the documentation below, for your database vendor.

- The [MariaDB Knowledge Base](#)
- The [MySQL documentation](#)
- The [Oracle Database documentation](#)
- The [PostgreSQL documentation](#)

Enabling Binary Logging

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
'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.'
```

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.

Set **READ COMMITTED** as the 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.

Configuring the Storage Engine

Since ownCloud 7, only InnoDB is supported as a storage engine. Some shared hosts do not support InnoDB and only MyISAM. Running ownCloud in 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 exceptional 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.

MySQL / MariaDB

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).

MariaDB is backward 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/php/7.4/apache2/conf.d/20-mysql.ini` could look like this:

```
# configuration for PHP MySQL module
extension=pdo_mysql.so

[mysql]
mysql.allow_local_infile=0n
mysql.allow_persistent=0n
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
```

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 [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, both MySQL (or MariaDB) **and** ownCloud need to be configured to use 4-byte Unicode support instead of the default 3-byte.

If you are setting up

- a new ownCloud installation, using version 10.0 or above, **and**

- you're using a *minimum* MySQL version of 5.7

then you don't need to do anything, as support is checked during setup and used if available.

However, if

- you have an existing ownCloud installation that you need to convert to use 4-byte Unicode support **or**
- you are working with a MySQL version *earlier* than version 5.7

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
```

2. Run the following occ command:

```
sudo -u www-data ./occ db:convert-mysql-charset
```

When this is done, tables will be created with:

- A `utf8mb4` character set.
- A `utf8mb4_bin` collation.
- `row_format` set to compressed.



For more information, please either refer to [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/library/innodb-system-variables/#innodb_large_prefix
- <http://www.tocker.ca/benchmarking-innodb-page-compression-performance.html>
- <http://dev.mysql.com/doc/refman/5.7/en/charset-unicode-utf8mb4.html>
- <https://dev.mysql.com/doc/refman/5.7/en/innodb-file-format.html>
- https://dev.mysql.com/doc/refman/5.7/en/innodb-parameters.html#sysvar_innodb_large_prefix

PostgreSQL

If you decide to use a PostgreSQL database, make sure that you have installed and enabled the [PostgreSQL extension](#) and the [PostgreSQL PDO extension](#) in PHP. The PHP configuration in `/etc/php/7.4/apache2/conf.d/20-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 PostgreSQL command-line mode use:

```
sudo -u postgres psql -d template1
```

Then a `template1=#` prompt will appear. You can now enter your commands as required. When finished, you can quit the prompt by entering:

```
\q
```

An ownCloud instance configured with PostgreSQL will 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 Installation Wizard](#) would 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. It's 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 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 [the sample PHP configuration 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 hostname (`db.server.com` in this example):

```
ping db.server.com

PING db.server.com (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 hostname:

```
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 PostgreSQL installation on a different machine, add the `-h` option with the applicable hostname:

```
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	PostgreSQL
<code>SELECT User,Host FROM mysql.user;</code>	<code>SELECT * FROM pg_user;</code>

Show Available Databases

MySQL	PostgreSQL
<code>SHOW DATABASES;</code>	<code>\l</code>

Show ownCloud Tables in Database

MySQL	PostgreSQL
<code>USE owncloud; SHOW TABLES;</code>	<code>\c owncloud; \d</code>

Quit Database

MySQL	PostgreSQL
<code>quit;</code>	<code>\q</code>

How to Solve Deadlock Errors

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

Explanation

This error occurs when two transactions write and commit to the same rows in separate cluster nodes. Only one of them can successfully commit. The failing one will be aborted. For cluster level aborts, Galera Cluster returns a deadlock error.

Solution

The solution, for Galera Cluster, would be to send all write requests to a single DB node, instead of all of them. Here is [a useful guide](#), when using [HAProxy](#).

The same concept applies when [MaxScale](#) is used as a DB proxy. It needs to be configured to send all write requests to a single DB node instead all of them and balance read statements across the rest of the nodes. Here is [a useful guide](#) on how to configure MaxScale with Read/Write splitting.

Enabling Causality Checks

Additionally, to solve this issue, when using Galera Cluster, customers should try to set `wsrep_sync_wait=1`. When enabled, the node triggers causality checks in response to certain types of queries. This is disabled by default.

Unresolved directive in modules/admin_manual/pages/configuration/files/encryption/index.adoc - include::partial\$section_page.adoc[]

Encryption Configuration

Introduction

The primary purpose of the ownCloud server-side encryption is to protect users' files when they're located on remote storage sites such as Dropbox and Google Drive, smoothly and seamlessly from within ownCloud.

General Notes

Since ownCloud 9.0, server-side encryption for local and remote storage can operate independently. This allows encrypting a remote storage independent of the home storage on the ownCloud server.



Starting with ownCloud 9.0 we support Authenticated Encryption for all newly encrypted files. See [Exploiting unauthenticated encryption mode](#) 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. This way, a malicious external storage administrator cannot add new files to the storage without your knowledge. However, you may not use this setting *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 storage sites 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 any users that you shared them with.



- Encrypting files increases their size by an 8KB header plus 100 bytes per each 8KB block of the file. Remember to take this into account when you are both provisioning storage and setting storage quotas.
- If you are *running* the encryption app before version 1.5.0 or *started* with an encryption app version before 1.5.0, BASE64 encoding was used and might still be used for old files if untouched since then. In these cases, old encrypted files increased their size by roughly 35%. We recommend to update the ownCloud system to be able to use the benefits of reduced file sizes for new and rewritten files. Note that the encryption app version lower than 1.5.0 was delivered as part of the ownCloud system lower than 10.7.
- User quotas are based on the *unencrypted* file size — **not** the encrypted size. This means that admins need to calculate with higher disk space requirements on the backend.
- You **CANNOT** use encryption for your *primary storage* if the primary storage is an Amazon S3 compatible object storage. This is disabled by default, also see [S3 Compatible Object Storage as Primary Storage Location](#)

When files on an external storage are encrypted in ownCloud, you cannot share them directly from the external storage services, but 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 the user's password. 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 but not filenames and directory structures.

Location of Encryption Keys

The encryption keys are stored in the following directories:

Type	Directory	Description
Master Key	<code>data/files_encryption/OC_DEFAULT_MODULE</code>	Location of the master key necessary to decrypt files.

Type	Directory	Description
User Key (Deprecated)	<code>data/<USER>/files_encryption/keys/files</code>	Location of the user key and share key per file necessary to decrypt files.



You can move the keys to a different location. To do so, refer to the [Move Key Location](#) section of the documentation.



You should regularly back up all encryption keys to prevent permanent data loss.

Rules and Restrictions

When encryption is enabled, all files are encrypted and decrypted by the ownCloud application and stored encrypted on your local or remote storage. The latter protects your data on externally hosted storage. An ownCloud admin and a storage admin will only see encrypted files when directly browsing backend storage.

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.



SSL terminates at the same time or before the web server 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](#).

```
Unresolved directive in
modules/admin_manual/pages/configuration/files/encryption/encryption_configuration.adoc -
include::partial$/configuration/files/encryption/not-encrypted-files.adoc[]
```


Using a Hardware Security Module (HSM)

When using a HSM, see the additional information provided at [The HSM \(Hardware Security Module\) Daemon \(hsmdaemon\)](#)

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.
--------------------	--

User-Key:	Every user has their own private/public key pairs, and the private key is protected by the user's password.
	User-Key encryption has been deprecated with ownCloud release 10.7



These encryption types are **not compatible**.

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's encryption options](#).



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!**

Enable the Encryption App

Before you can use encryption, you must enable the encryption app. You can do this either on the command-line or in the Web-UI.

Enable Encryption From the Command-Line

To enable the encryption app, run the following command:

```
sudo -u www-data ./occ app:enable encryption
```

```
sudo -u www-data ./occ encryption:enable
```

```
sudo -u www-data ./occ encryption:select-encryption-type masterkey -y
```

If the encryption app is successfully enabled, you should see the following confirmations:

```
encryption enabled  
Encryption enabled
```

```
Default module: OC_DEFAULT_MODULE  
Master key successfully enabled.
```

Enable Encryption in the Web-UI

To enable encryption in the Web-UI:

1. Go to **Settings** › **Admin** › **Apps** and click on `Show disabled apps`
2. When the disabled apps are rendered, click **[Enable]** under *"Default encryption module"*.

Basic Configuration via the Web-UI

You can do basic configuration of encryption via the Web-UI, but it is recommended to use the CLI.

1. Go to **Settings** › **Admin** › **Encryption**, and enable **[Enable server-side encryption]**.
2. Select the *"Default encryption module"*, either *"Master Key"* (recommended) or *"User-key"* (depreciated).
3. When User-specific encryption is enabled, users must log out and log back in to trigger the automatic personal encryption key generation process.

Master-Key-Based Encryption

Enabling Master Key Based Encryption from the Command-Line

To be safe and avoid any issues on a running instance, put your server in single user mode with the following command:

```
sudo -u www-data ./occ maintenance:singleuser --on
```

Enabling encryption via the command line involves several commands. If not already done, enable the default encryption module app with the following command:

```
sudo -u www-data ./occ app:enable encryption
```

Then enable encryption, using the following command:

```
sudo -u www-data ./occ encryption:enable
```

After that, enable the master key, using the following command:

```
sudo -u www-data ./occ encryption:select-encryption-type masterkey
```



The master key mode has to be set up in a newly created instance.

Finally, encrypt all data, using the following command:


```
sudo -u www-data ./occ encryption:encrypt-all --yes
```



This command is not typically required as the master key is often enabled at installation time. As a result when enabling it, there should be no data to encrypt. In case it's being enabled after the installation and there are files which are unencrypted, [encrypt-all](#) can be used to encrypt them. Depending on the amount of existing data and the location, this operation can take a long time.

Now you can turn off the single user mode:

```
sudo -u www-data ./occ maintenance:singleuser --off
```

View Current Encryption Status

Get the current encryption status and the loaded encryption module:

```
sudo -u www-data ./occ encryption:status
```

Replacing an Existing Master Key

If the master key needs replacement, for example because it has been compromised, an `occ` command is available. The command is [encryption:recreate-master-key](#). It replaces an existing master key with a 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.

```
sudo -u www-data ./occ maintenance:singleuser --on
```

```
Single user mode is currently enabled
```

Decrypt all user data files, or optionally a single user:

```
sudo -u www-data ./occ encryption:decrypt-all [username]
```

Disable Encryption

To disable encryption, put your ownCloud server into single-user mode, and then disable your encryption module with these commands:

```
sudo -u www-data ./occ maintenance:singleuser --on
```

```
sudo -u www-data ./occ encryption:disable
```

Take it out of single-user mode when you are finished, by using the following command:

```
sudo -u www-data ./occ maintenance:singleuser --off
```



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 if user key encryption was selected.

User-Key-Based Encryption (Deprecated)

Limitations of User-Key-Based Encryption

- Deprecated with [ownCloud release 10.7](#)
- Users added to groups cannot decrypt files on existing shares.
- OnlyOffice will not work.
- Impersonate will not work.
- OAuth2 will not work.
- Elasticsearch will not work.
- Users getting access to an external storage which already contains encrypted files cannot get access to said files for reasons such as the group case above.
- When having data shared with a group and group membership changes after the share is established, subsequently added users will not be able to open the shared data unless the owner will share it again.

Enabling User-Key-Based Encryption From the Command-line

To avoid any issues on a running instance, put your server in single user mode with the following command:

```
sudo -u www-data ./occ maintenance:singleuser --on
```

If not already done, enable the default encryption module app, using the following command:

```
sudo -u www-data ./occ app:enable encryption
```

After that, enable encryption, using the following command:

```
sudo -u www-data ./occ encryption:enable
```

Then, enable the user-key, using the following command:

```
sudo -u www-data ./occ encryption:select-encryption-type user-keys
```

Finally, encrypt all data, using the following command:

```
sudo -u www-data ./occ encryption:encrypt-all --yes
```

Now you can turn off the single user mode:

```
sudo -u www-data ./occ maintenance:singleuser --off
```

View Current Encryption Status

Get the current encryption status and the loaded encryption module:

```
sudo -u www-data ./occ encryption:status
```

Enable Users' File Recovery Keys

If users encrypt their files and lose their ownCloud password, they lose access to their encrypted files as the files will be unrecoverable. It is not possible to reset a user's password using the standard reset process if the user's files are encrypted.

In such a case, 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.

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

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 grants the admin the right to decrypt their data for recovery purposes. If they do *not* do this, the Recovery Key won't work for them.

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

Users who have enabled password recovery you can provide with a new password and recovery access to their encrypted files by supplying the Recovery Key on their page.

<input type="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

You may change your recovery key password.

Change recovery key password:

<input type="password"/>	Old Recovery key password
<input type="password"/>	New Recovery key password
<input type="password"/>	Repeat New Recovery key password
<input type="button" value="Change Password"/>	



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.



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. Otherwise admins could hijack the recovery key from each other.



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.

```
sudo -u www-data ./occ maintenance:singleuser --on
```

```
Single user mode is currently enabled
```

Disable Encryption

You may disable encryption only with `occ`. Make sure you have backups of all the encryption keys, including those for all users. Next, put your ownCloud server into single-user mode, and then disable your encryption module with this command:

```
sudo -u www-data ./occ maintenance:singleuser --on
```

```
sudo -u www-data ./occ encryption:disable
```



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:

```
sudo -u www-data ./occ maintenance:singleuser --off
```

It is possible to disable encryption with the file recovery key *if* every user has enabled it. In this case, "decrypt all" will decrypt all files of all users.



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:

```
sudo -u www-data ./occ encryption:show-key-storage-root
```

```
Current key storage root: default storage location (data/)
```

You can move the keys to another folder inside your data directory. Moving your keys outside of your data folder is not supported. The folder must already exist, be owned by and restricted to root and the webserver group. This example is for Ubuntu Linux. Note that the new folder is relative to your data directory:

```
mkdir /var/www/owncloud/data/new_keys
```

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

```
chmod -R 0770 /var/www/owncloud/data/new_keys
```

```
sudo -u www-data ./occ encryption:change-key-storage-root new_keys
```

Change key storage root from default storage location to new_keys

Start to move keys:

```
4 [=====]
```

Key storage root successfully changed to new_keys

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 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](#).

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.

Encryption Configuration Quick Guide

Introduction

This quick guide gives a brief summary of the commands needed without going into the details and backgrounds. See the [full encryption configuration guide](#) for more details.

Master-Key-Based Encryption

Overview

- The **recommended** type of encryption.
- Best to activate on new instances with no data.
- If you have existing data, use the **occ encryption:encrypt-all** command. Depending on the amount of existing data and the location, this operation can take a long time.

Activate Master Key-Based Encryption

```
sudo -u www-data ./occ maintenance:singleuser --on
sudo -u www-data ./occ app:enable encryption
sudo -u www-data ./occ encryption:enable
sudo -u www-data ./occ encryption:select-encryption-type masterkey -y
sudo -u www-data ./occ encryption:encrypt-all --yes
sudo -u www-data ./occ maintenance:singleuser --off
```

View the Encryption Status

```
sudo -u www-data ./occ encryption:status
```

Decrypt Encrypted Files

Depending on the amount of existing data, this operation can take a long time.

```
sudo -u www-data ./occ maintenance:singleuser --on
sudo -u www-data ./occ encryption:decrypt-all
sudo -u www-data ./occ maintenance:singleuser --off
```

Deactivate Master-Key-Based Encryption

```
sudo -u www-data ./occ encryption:disable

# ignore the "already disabled" message
sudo -u www-data ./occ app:disable encryption
```

If the master key has been compromised or exposed, you can replace it. You will need the current

master key for it.

```
sudo -u www-data ./occ encryption:recreate-master-key
```

Clean up Your Database

Access your ownCloud database and remove the remaining entries that have not been automatically removed with this command:

```
DELETE FROM oc_appconfig WHERE appid='encryption';
```

Clean up Your Storage

The removal of remaining encryption keys is a manual process. You have to delete all encryption keys on the storage by running the following command. Modify the path to your data directory according to your installation. The `find` command limits the search to exactly one directory below the user level and for security reasons prompts before each deletion:

```
find /var/www/owncloud/data/ -mindepth 2 -maxdepth 2 -type d -name "files_encryption" -exec rm -R -i {} +
```

```
Unresolved directive in
modules/admin_manual/pages/configuration/files/external_storage/index.adoc -
include::partial$section_page.adoc[]
```

External Storage Configuration

Introduction

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.

Starting with ownCloud 9.0, a new set of `occ` commands for [managing external storage](#) is introduced.

This also includes an option for the ownCloud admin to enable or disable sharing on individual [external mountpoints](#). Sharing on such mountpoints is disabled by default.

Enabling External Storage Support

Tick the checkbox under `Settings > Storage > "Enable External Storage"`.

External Storage

Enable external storage

Storage Configuration



Before adding a storage in a production environment make sure its configuration is correct. Removal of the external storage or change of its configuration does not remove metadata entries from the database belonging to the previous 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.

The screenshot shows the 'Settings' application interface. On the left is a navigation sidebar with sections for 'Personal' (General, Storage, Security, Additional) and 'Admin' (Apps, General, Storage, Encryption). The main content area is titled 'External Storage' and contains the following elements:

- Enable external storage
- External storage has been disabled by the administrator
- A table with columns: Folder name, External storage, and Authentication.
- Under 'Folder name': an input field with the placeholder text 'Folder name'.
- Under 'External storage': a dropdown menu labeled 'Add storage' with a list of options: Amazon S3, Google Drive, OpenStack Object Storage, ownCloud, SFTP, SMB / CIFS, and WebDAV.
- Under 'Authentication': an input field.
- Allow users to mount external s

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/auth_mechanisms](#) for more detailed information.

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
<input type="text" value="SFTP"/>	SFTP	<div style="border: 1px solid black; padding: 2px;"><div style="border-bottom: 1px solid black; padding: 2px;">Username and password</div><div style="padding: 2px; background-color: #007bff; color: white;">Username and password</div><div style="padding: 2px;">Log-in credentials, save in session</div><div style="padding: 2px;">RSA public key</div></div>	<div style="border: 1px solid red; padding: 2px;">Host</div> <div style="border: 1px solid red; padding: 2px;">Root</div> <div style="border: 1px solid red; padding: 2px;">Username</div> <div style="border: 1px solid red; padding: 2px;">Password</div>

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 a connection issue with the target 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

x guest0x admin (group)

B BlueDragon

R rootA

T test1

T test2



Adding a storage for users or groups you don't have access rights to, an error notification will be shown and a red square icon appears on the mount.

Mount Options

Hover your cursor to the right of any storage configuration to expose the settings button and trashcan. When clicking the trashcan icon, you delete the mountpoint. The settings button allows you to configure each storage mount individually with the following options:

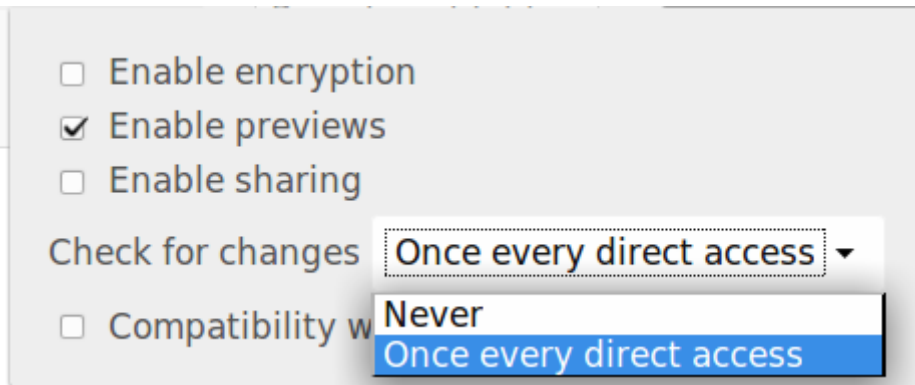
- Encryption

- Read Only
- 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.



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



Be careful with the choices that you enable, as it allows a user to make potentially arbitrary connections to other services on your network!

Detecting Files Added to External Storages

We recommend [configuring the background job Webcron or Cron](#) to enable ownCloud to automatically detect files added to your external storages.



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 ./occ files:scan --all`
```

Alternatively, replace `--all` with the user name to trigger a rescan of the user's files periodically, for example every 15 minutes, which includes the mounted external storage.



See [the occ's file operations](#) for more information.

Known limitations

- Removal of the external storage or change of its configuration does not remove metadata entries belonging to the previous storage configuration. This may impact performance of the installation as previous configuration metadata entries get orphaned. Removal of orphaned entries requires manual deletion of orphaned storage cache by its storage id.

External Storage Authentication Mechanisms

Introduction

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.

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.



here is a workaround that allows background file scanning when using **Log-in credentials, save in session**, and that is using [Ajax cron mode](#). 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.



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.

Authentication Configuration

RSA public key

Host Root Username ssh-rsa AAAAB3NzaC1

Generate keys

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 are provided and then entered into ownCloud. Then ownCloud can perform an authentication request, establishing the storage connection.

sharedropbox Dropbox

rt

.....

All Users x

Access granted

If ownCloud clients are unable to connect to your ownCloud server, check that the bearer authorization header [is not being stripped out](#).

Amazon S3

Introduction

Amazon S3 is used to connect owncloud to your Amazon S3 bucket.



If your installation uses S3 as an external storage in any version before ownCloud 10.3, you have to install and enable [files_external_s3](#). Otherwise, files stored on existing S3 external storages will **not** be fully accessible.

Configuration

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 it 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	AKIAIOSHDC77WFI oc-files-wc Hostname (optional) Port (optional) Region (optional) <input checked="" type="checkbox"/> Enable SSL <input checked="" type="checkbox"/> Enable Path Style	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 [External Storage Configuration](#) for additional mount options and information, and [External Storage Authentication mechanisms](#) for more information on authentication schemes.

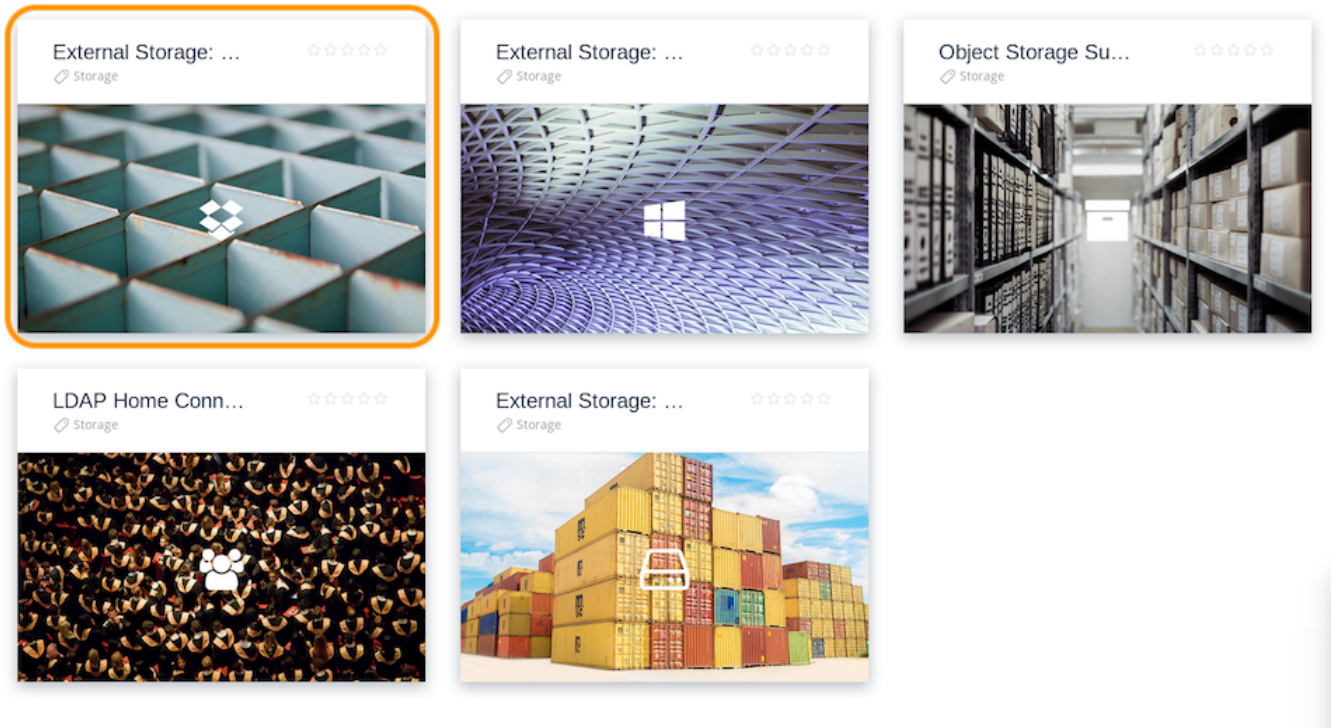
Dropbox

Introduction

Connecting Dropbox to your ownCloud installation requires only a few steps. Then you can easily keep a Dropbox folder in sync with an ownCloud folder. This guide assumes you already have a Dropbox account.

Install the ownCloud Dropbox app

Install the External Storage Dropbox app from the ownCloud Marketplace



1. Click [**Market**] in the ownCloud web UI drop-down menu on the left side
2. Go to the **Storage** category
3. Select **External Storage: Dropbox App**
4. Click [**INSTALL**]

Create a Dropbox app

Next, you need to create a Dropbox app. To do that, [open the new app creation form](#), where you see three settings:

1. "Choose an API" -> "Scoped access"
2. "Choose the type of access" -> "App folder"
3. "Name your app"

Read and agree to the Dropbox API Terms and Conditions before clicking the blue [**Create app**] button. After you do that, the settings page for the application loads.

App folder name	owncloud_x_share	Change
App key	[Redacted]	
App secret	Show	
OAuth 2	Redirect URIs	
	<input type="text" value="https:// (http allowed for localhost)"/>	Add



Redirect URI: Here you must enter the exact URL of the page where you configure the storage.

Examples:

When configuring as an **admin**:

```
http(s)://<<Server_Address>>/settings/admin?sectionid=storage
```

When configuring as a **user**:

```
http(s)://<<Server_Address>>/settings/personal?sectionid=storage
```

Take note of the App key and App secret since you'll need them in the next step.

Create a Dropbox Share

Return to the ownCloud web interface. Under **Admin > Settings > Storage**, check the **[Enable external storage]** checkbox if it's not already checked. Then, in the drop-down list under **External storage**, select Dropbox V2.

Then, you need to provide a name for the folder in the "Folder name" field and a "client key" and "client secret" under "Configuration". The client key and client secret values are the "App key" and "App secret" which you saw earlier in your Dropbox app configuration settings.

After you have entered these values, click **[Grant access]**. ownCloud then interacts with the Dropbox 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 name.



Other Options

If you want to grant access to the share to a select list of users and groups, you can add them to the field in the "Available for" column.

Using the Dropbox Share

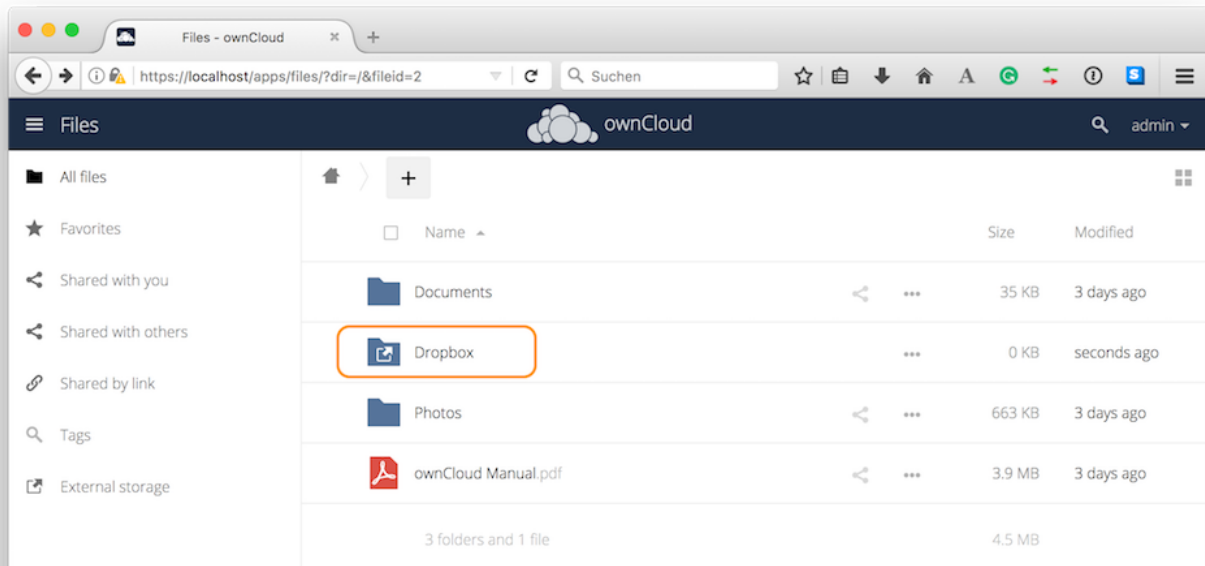
After a Dropbox share is created, a new folder is available under "All Files" with the name you provided when you created the share. It is represented by an external share folder icon as in the image below.

External Storage

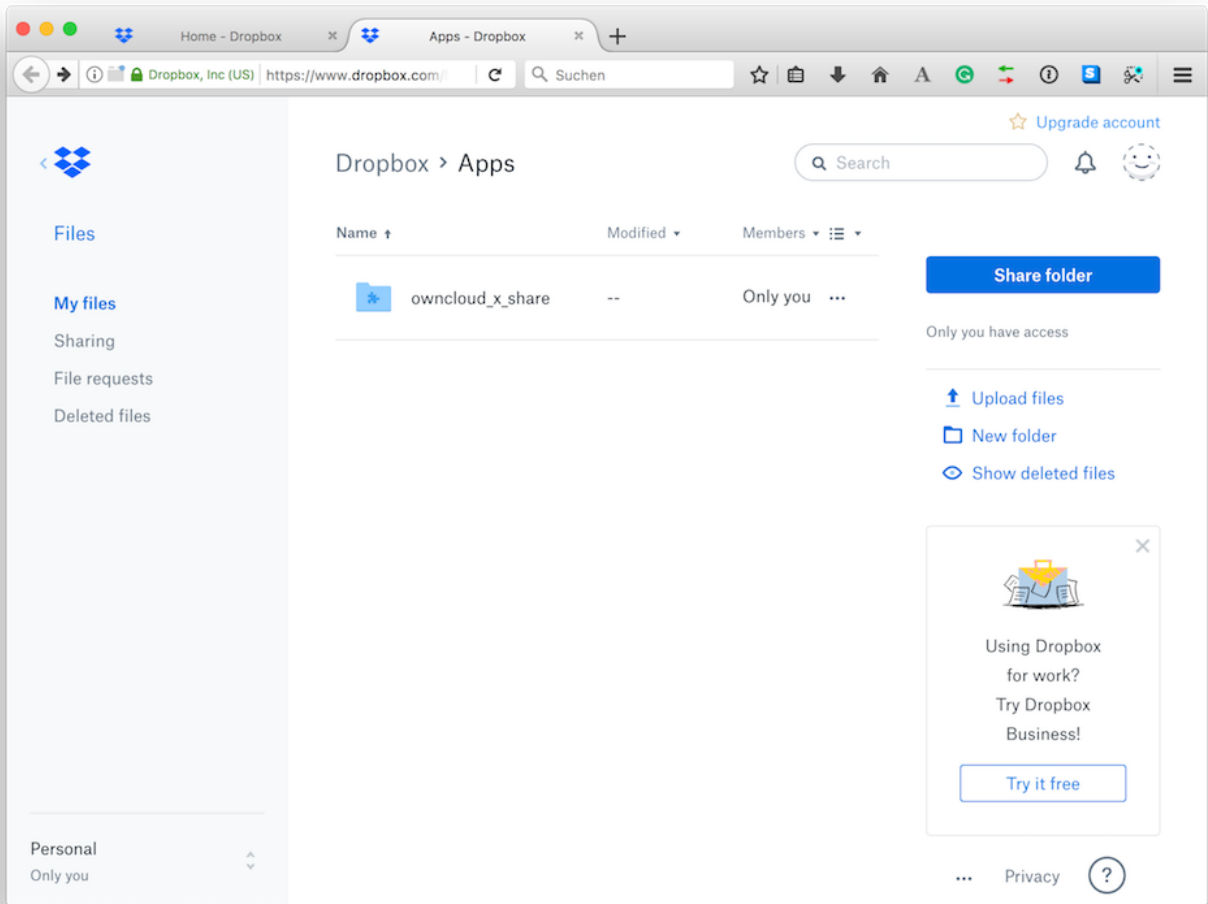
Enable external storage

Folder name	External storage	Authentication	Configuration	Available for
<input type="text" value="Dropbox"/>	Dropbox	OAuth2	<input type="text" value=""/>	<input type="text" value="All users. Type to select user or group."/>
<input type="text" value=""/>	<input type="text" value="Add storage"/>			

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, they will be visible in both after they've been synced.



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 Market interface. On the left, a sidebar lists various categories, with 'External plugins' highlighted in a red box. The main content area displays the 'FTP storage support' plugin page, which includes the ownCloud logo, a description of the plugin as an 'FTP backend for files_external', and a table of metadata. The table lists the developer as 'ownCloud', the version as '0.2.0', the release date as 'Apr 25, 2017', and the license as 'GNU Affero General Public License'. An 'INSTALL' button is located at the bottom right of the plugin page.

DEVELOPER	VERSION	RELEASE DATE	LICENSE
ownCloud	0.2.0	Apr 25, 2017	GNU Affero General Public License


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](#) for more information.

External Storage

Folder name	External storage	Configuration	Available for
 FTP	FTP	ftp.example.com:22 username ●●●●●●●● public.html/ <input checked="" type="checkbox"/> Secure ftps://	× support(group)

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 [External Storage Configuration](#) for additional mount options and information.

FTP uses the password authentication scheme; see [External Storage Authentication mechanisms](#) for more information on authentication schemes.

Google Drive

Introduction

Using the Google Drive external storage in ownCloud, you can mount all or a subfolder of Google Drive.

For subfolders, use the following scheme:

- subfolder = empty (mounting the root, all of Google Drive will be used)
- subfolder = `$user` (`$user` variable represents the current logged in ownCloud username)
- subfolder = name (a folder name, can be cascaded like `name1/name2` or `name/$user`)



If the subfolder is not present in Google Drive, no Google Drive mount will be shown in the users file list.



Using subfolders is beneficial if you want to selectively encrypt Google Drive mount points



The variable `$user` is the substitute for the current logged-in user. The subfolder with the username must be created manually in 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.

In the examples used, `<your domain>` represents how you access your ownCloud server, where you

see the login screen. This may look like:

```
https://example.com
or
http://example.com
or
IP/owncloud
```

Preparations in the Google Cloud Console

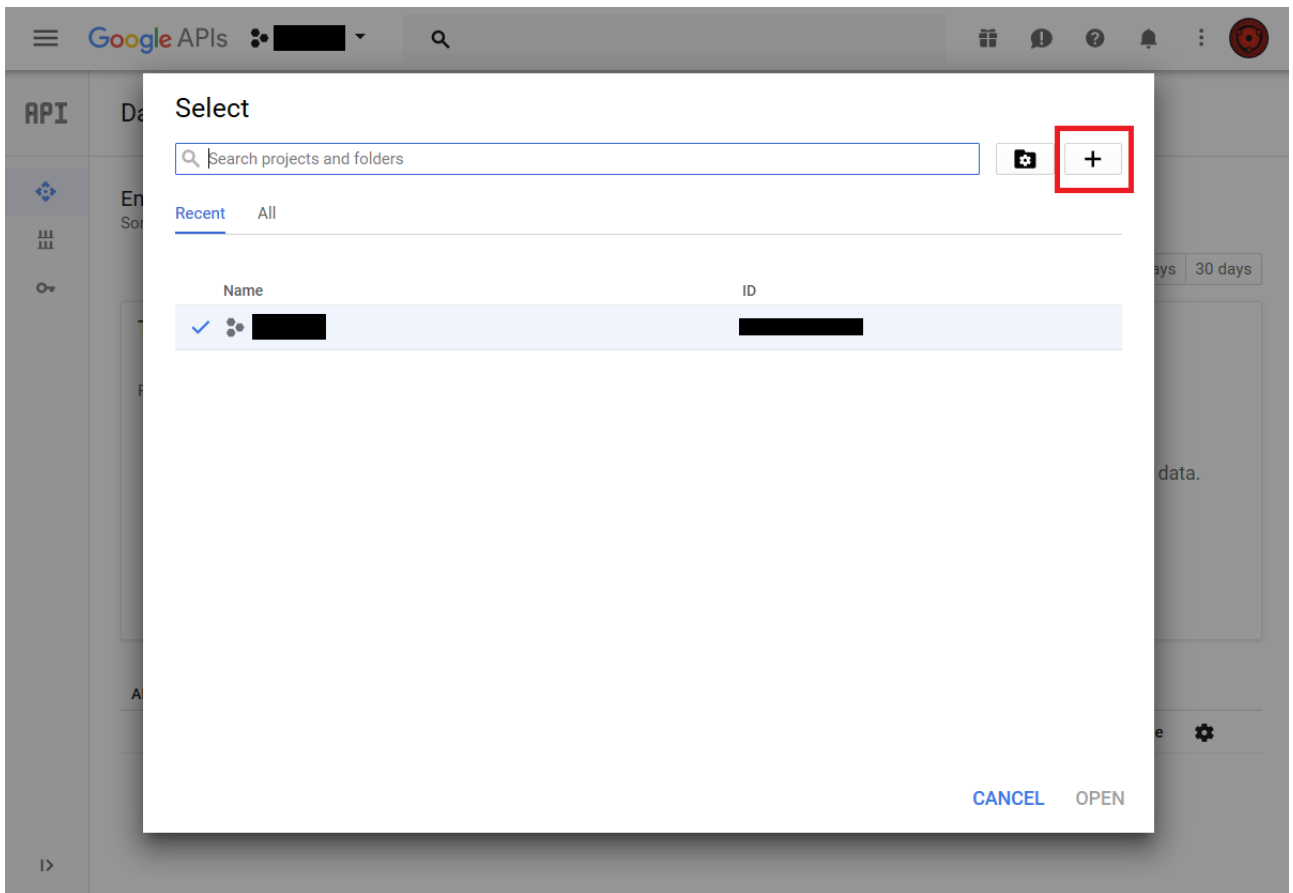
Create a Google Drive Project

1. You can use your existing Google account such as Groups, Drive, or Mail, or create a new one and log into the [Google Cloud Console](#). After logging in click the [**Create Project**] button on the top right side.

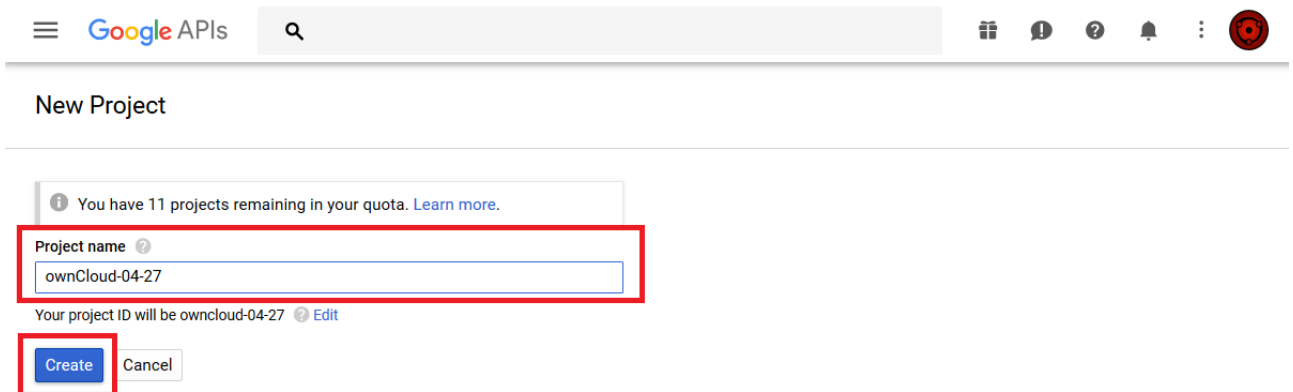
The screenshot shows the Google Cloud Console interface. At the top, there is a search bar with a project ID (partially obscured by a red box) and a search icon. Below the search bar is the 'Dashboard' section with a '+ ENABLE APIS AND SERVICES' button. The main content area is titled 'Enabled APIs and services' and includes a sub-header 'Some APIs and services are enabled automatically'. There are time range filters: 1 hour, 6 hours, 12 hours, 1 day, 2 days, 4 days, 7 days, 14 days, and 30 days. Three charts are displayed: 'Traffic' (Requests/sec), 'Errors' (Percent of requests), and 'Median latency' (Milliseconds). All three charts show 'There is no data for this time period.' Below the charts is a table with the following columns: API, Requests, Errors, Error ratio, Latency, median, Latency, 98%, and a 'Disable' button with a gear icon. The table contains one row for 'Google Drive API' with dashes in the data columns.

API	Requests	Errors	Error ratio	Latency, median	Latency, 98%	
Google Drive API	-	-	-	-	-	Disable

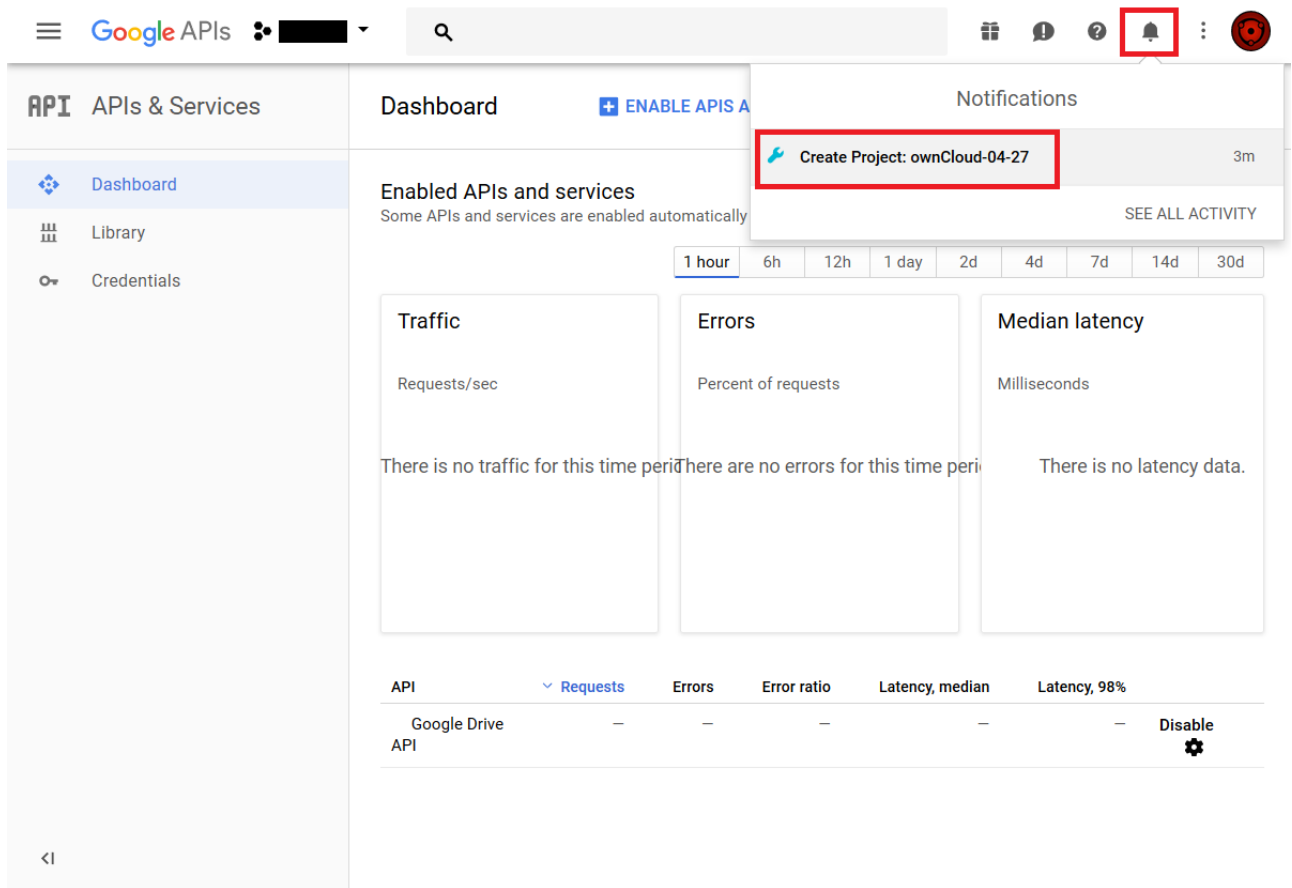
2. Add a new project by clicking the [+] button on the top right side.



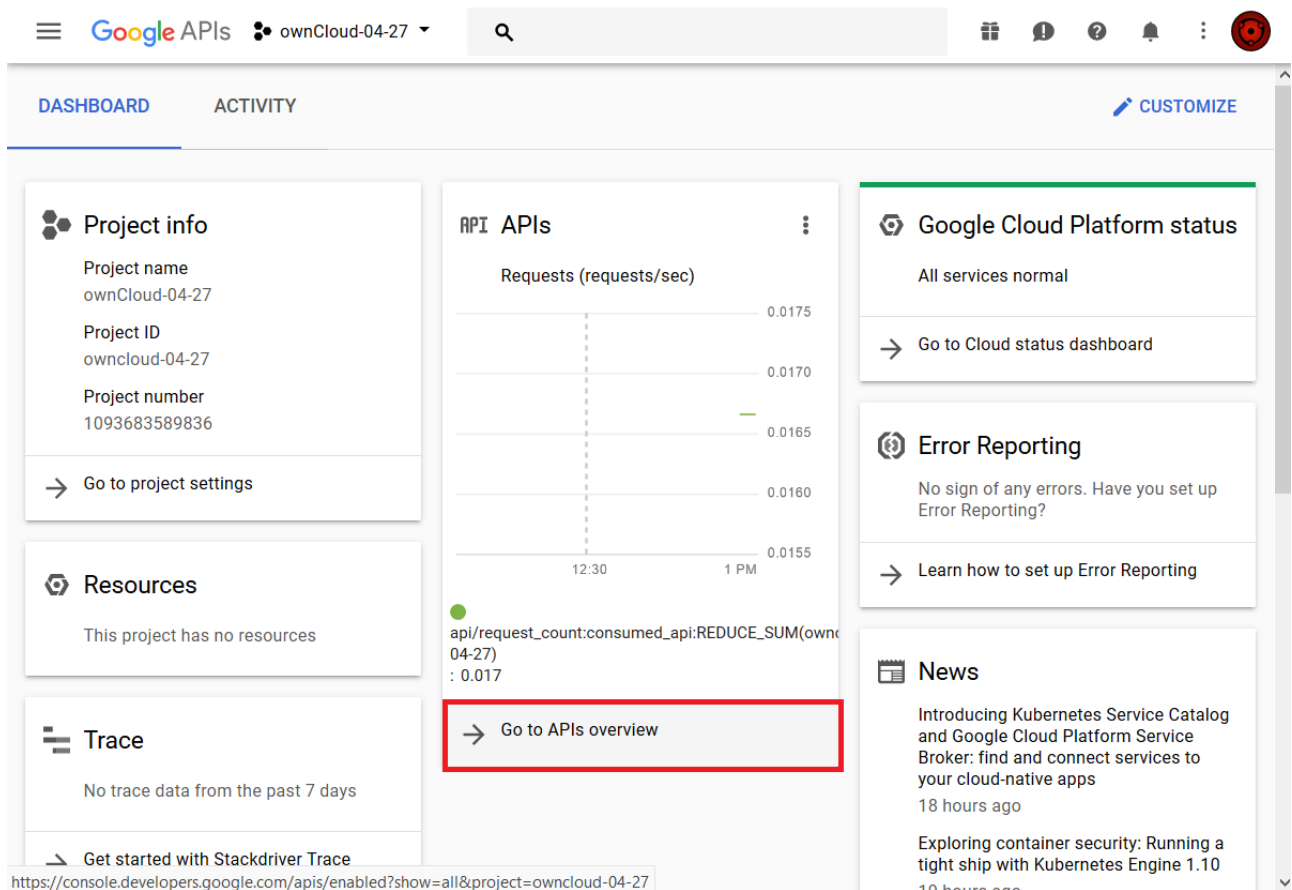
3. Give your project a name, and either accept the default **Project ID** or create your own, then click the **[Create]** button. For this example a random name was chosen, "owncloud-04-27". However, feel free to choose your own name.



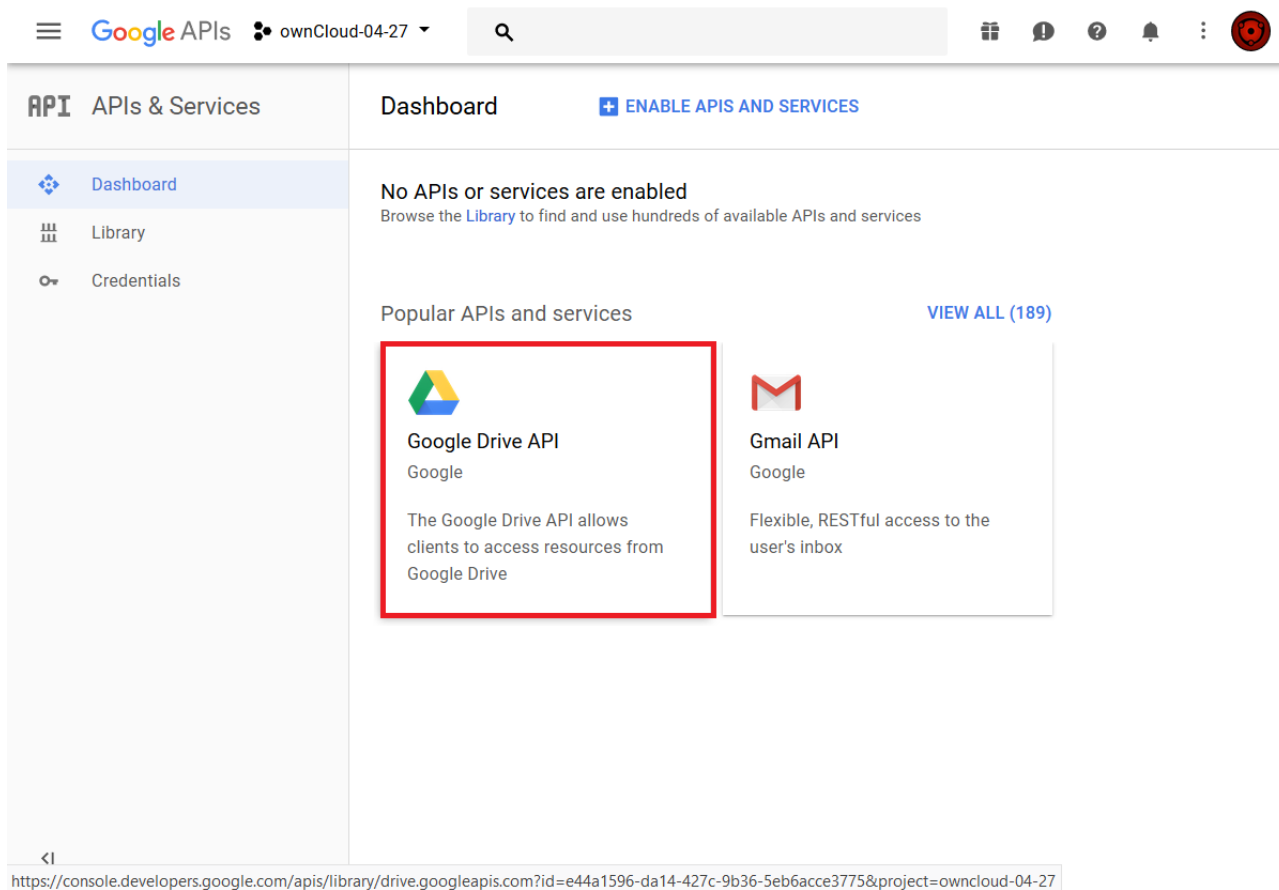
4. After your project is created, click on the [notifications bell] and select your project.



5. Go to Api overview to select google's API.

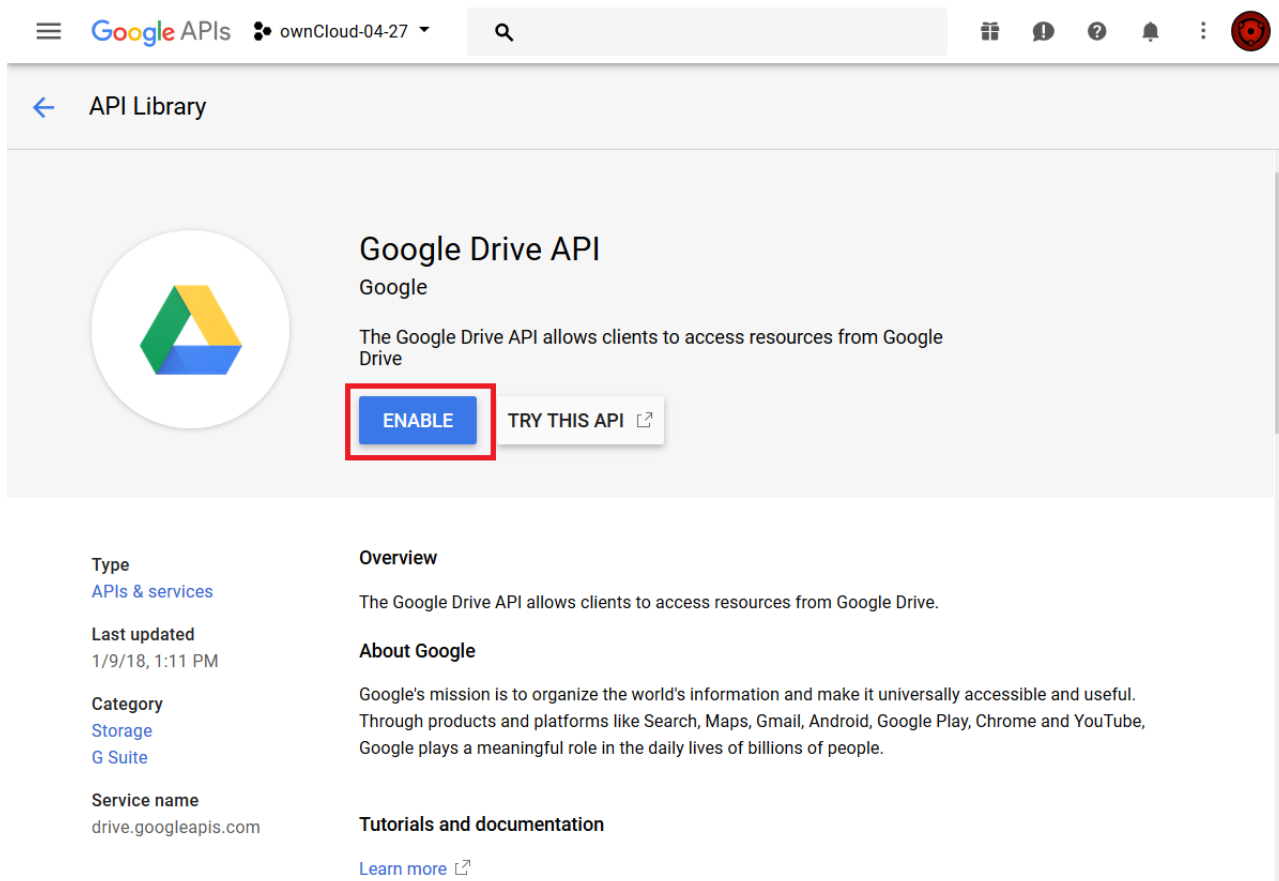


6. Select Google Drive API



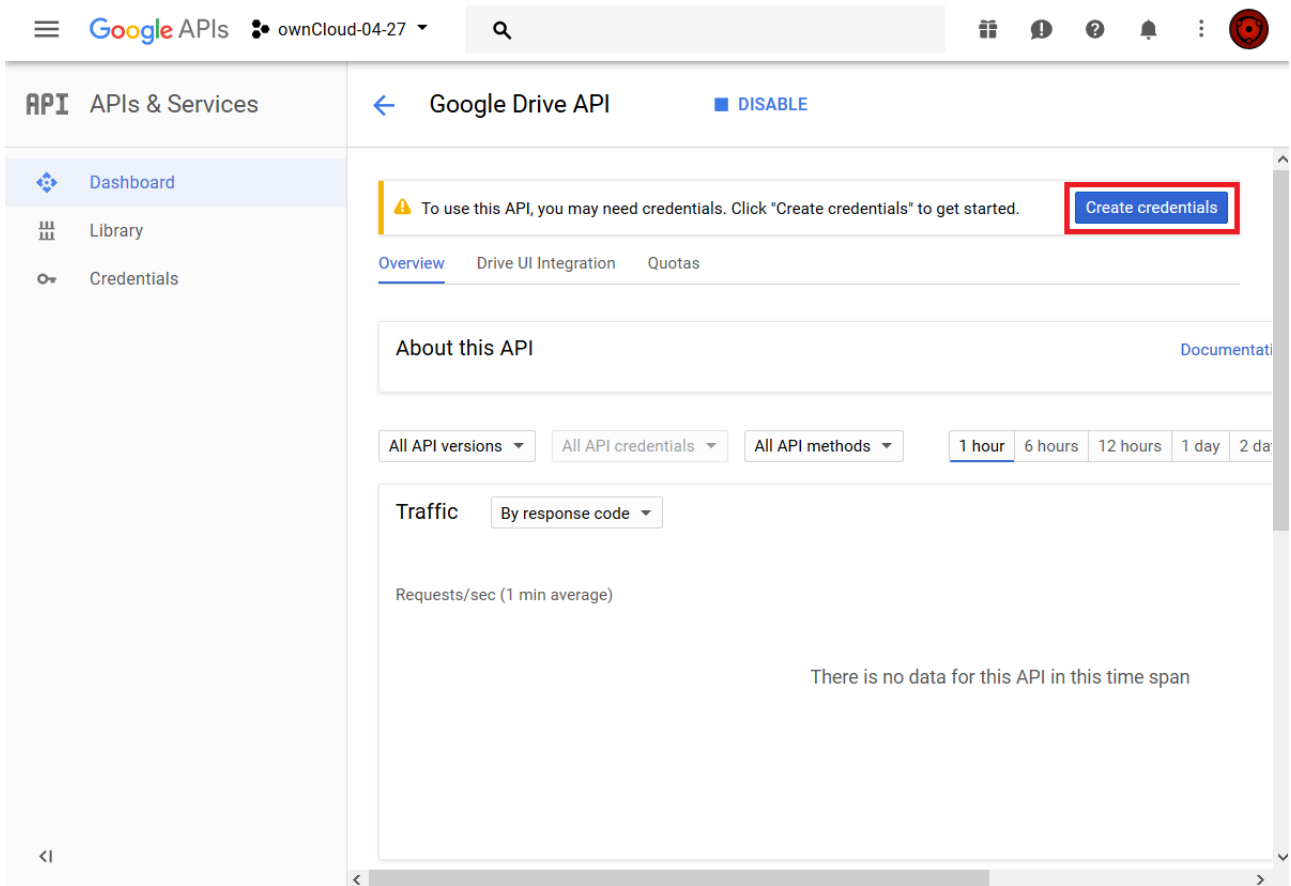
The screenshot shows the Google APIs & Services Dashboard for the project 'ownCloud-04-27'. The 'APIs & Services' sidebar is on the left, with 'Dashboard' selected. The main content area shows a message: 'No APIs or services are enabled. Browse the Library to find and use hundreds of available APIs and services'. Below this, there is a section for 'Popular APIs and services' with a 'VIEW ALL (189)' link. Two API cards are visible: 'Google Drive API' and 'Gmail API'. The 'Google Drive API' card is highlighted with a red border. It features the Google Drive logo, the text 'Google Drive API', 'Google', and a description: 'The Google Drive API allows clients to access resources from Google Drive'. The 'Gmail API' card features the Gmail logo, 'Gmail API', 'Google', and the description: 'Flexible, RESTful access to the user's inbox'. The URL at the bottom is <https://console.developers.google.com/apis/library/drive.googleapis.com?id=e44a1596-da14-427c-9b36-5eb6acce3775&project=owncloud-04-27>

7. Enable the Google Drive API

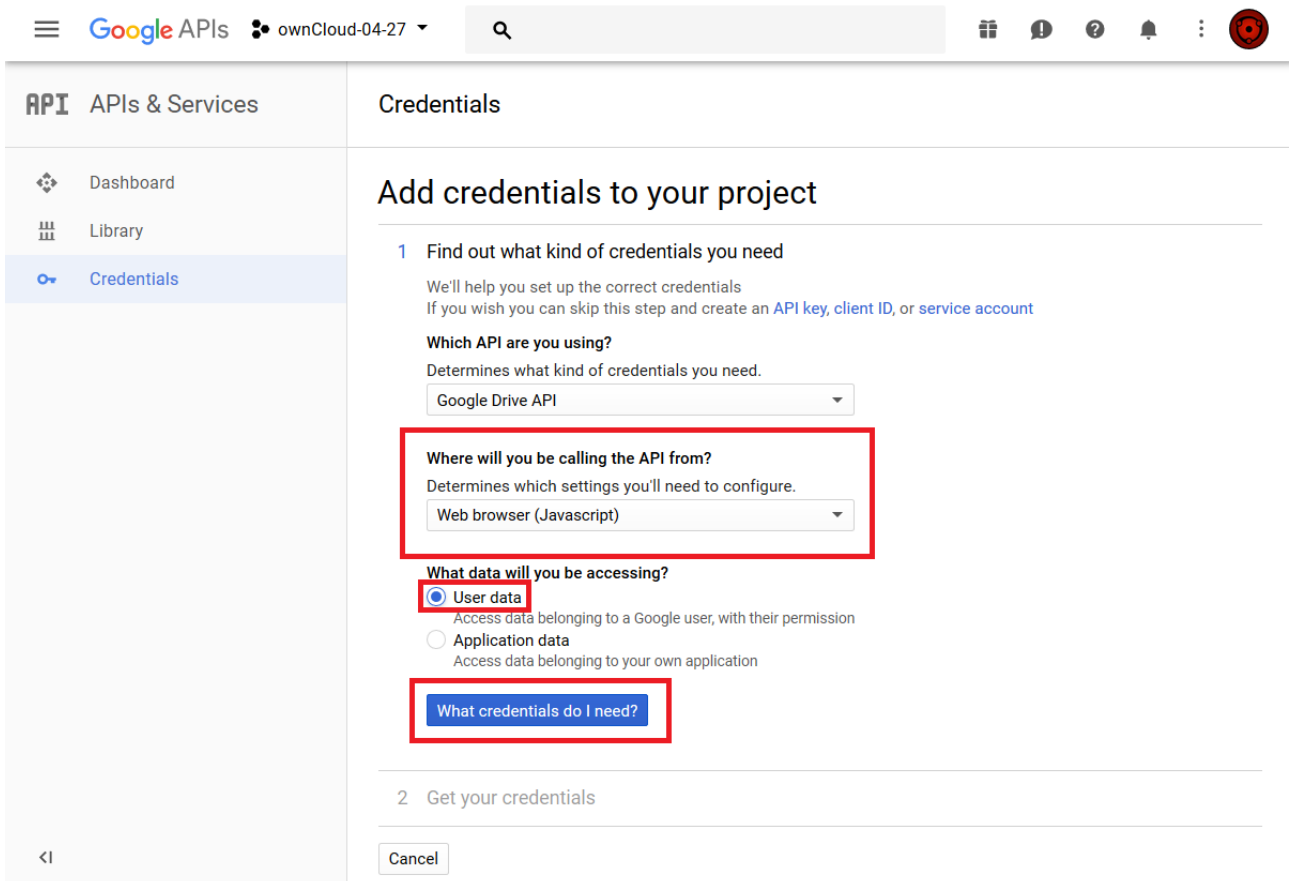


The screenshot shows the 'API Library' page for the 'Google Drive API'. The page header includes a back arrow, 'API Library', and the project name 'ownCloud-04-27'. The main content area features the Google Drive logo, the title 'Google Drive API', and the provider 'Google'. A description states: 'The Google Drive API allows clients to access resources from Google Drive'. Below the description, there are two buttons: 'ENABLE' (highlighted with a red border) and 'TRY THIS API' with an external link icon. The page is divided into two columns. The left column contains metadata: 'Type: APIs & services', 'Last updated: 1/9/18, 1:11 PM', 'Category: Storage, G Suite', and 'Service name: drive.googleapis.com'. The right column contains an 'Overview' section with the same description, an 'About Google' section with the company's mission statement, and a 'Tutorials and documentation' section with a 'Learn more' link.

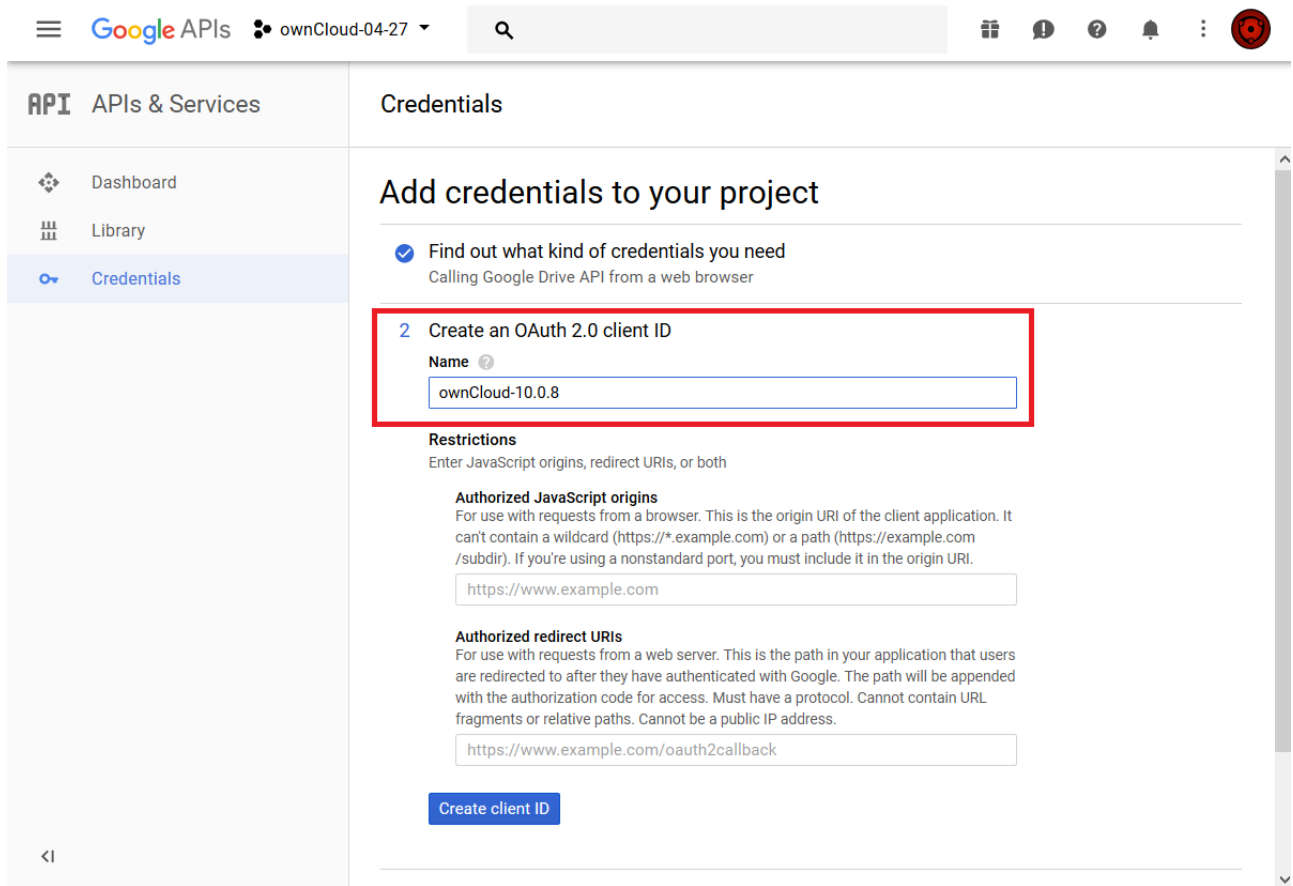
8. You now must create your credentials.



9. First, select [Web Browser] and [User data].



10. The next screen that opens is **Create OAuth 2.0 Client ID**. Enter your app name.



Configure Authorisations

These authorisations are necessary to tell Google which source URI requests are allowed. You can configure multiple Authorized URIs if you wish to enable admin and personal access at the same time for different purposes.

Authorized Redirect URIs

To configure *Authorized Redirect URIs*, select one of the two possible URI Schemes. If you are configuring storage as an administrator - choose the admin URI, if you are a user and configure your personal storage - pick the personal URI.

```
https://<your domain>/index.php/settings/admin?sectionid=storage  
or  
https://<your domain>/index.php/settings/personal?sectionid=storage
```

Authorized JavaScript Origins

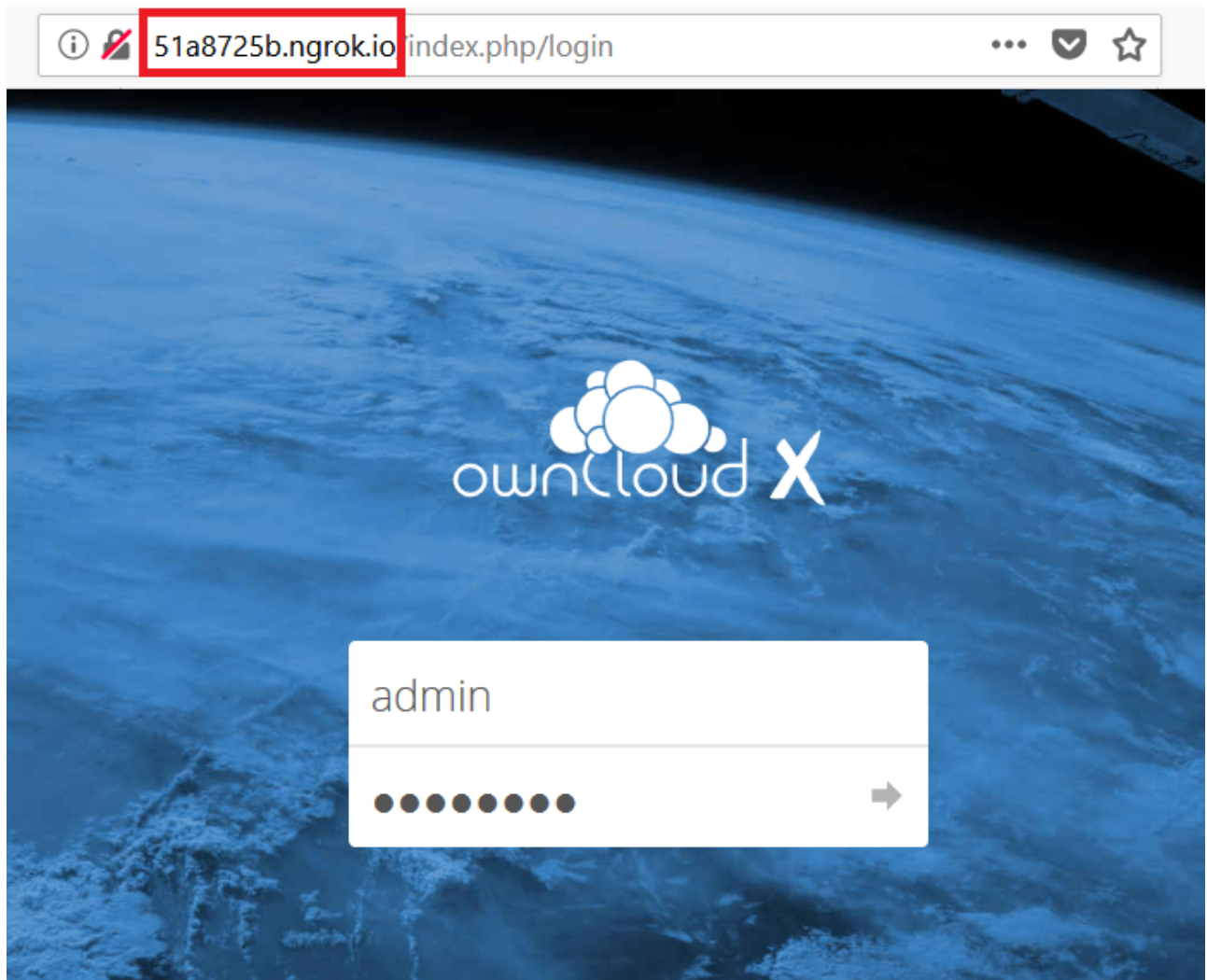
This is just `https://<your domain>` which represents how you access your ownCloud server, where you see the login screen.

Configure to connect to Google Drive

The following example procedure configures an admin based storage mount. The domain used in

this example is <http://51a8725b.ngrok.io>

1. Login to your ownCloud account



2. Go to Storage in the Settings

Admin

☰ Apps

⚙️ General

📁 Storage

👤 User Authentication

🔒 Encryption

3. Enable external Storage

External Storage

Enable external storage

4. Select Google Drive

Folder name

Add storage ▼

- Amazon S3
- Google Drive
- OpenStack Object Storage
- ownCloud
- SFTP
- SMB / CIFS
- WebDAV

Allow users to mount external storage

5. The Google Drive App is enabled

Give the mount point a meaningful name. We have used **Google Drive** in this example.

GoogleDrive

Google Drive ⚙️

OAuth2 ▼

SubFolder

Client ID

Client secret

Grant access

All users. Type to select user or group. ⚙️ 🗑️

6. Copy the Authorized Redirect URI from the browser

51a8725b.ngrok.io/index.php/settings/admin?sectionid=storage

7. Enter it the Google Drive Console here

Google APIs ownCloud-04-27

APIs & Services

- Dashboard
- Library
- Credentials**

Credentials

Find out what kind of credentials you need
Calling Google Drive API from a web browser

2 Create an OAuth 2.0 client ID

Name ?

Restrictions
Enter JavaScript origins, redirect URIs, or both

Authorized JavaScript origins
For use with requests from a browser. This is the origin URI of the client application. It can't contain a wildcard (https://*.example.com) or a path (https://example.com/subdir). If you're using a nonstandard port, you must include it in the origin URI.

Authorized redirect URIs
For use with requests from a web server. This is the path in your application that users are redirected to after they have authenticated with Google. The path will be appended with the authorization code for access. Must have a protocol. Cannot contain URL fragments or relative paths. Cannot be a public IP address.

Create client ID

8. Choose a project name for the consent screen.

A consent screen has to be created. This is the information in the screen Google shows you when you connect your ownCloud Google Drive app to Google the first time.

Add credentials to your project

- ✓ Find out what kind of credentials you need
Calling Google Drive API from a web browser

- ✓ Create an OAuth 2.0 client ID
Created OAuth client 'ownCloud-10.0.8'

3 Set up the OAuth 2.0 consent screen

Email address [?]

Product name shown to users [?]

[More customization options](#)



The consent screen will be shown to users whenever you request access to their private data using your client ID. It will be shown for all applications registered in this project.

You must provide an email address and product name for OAuth to work.

9. Download the credentials as JSON file.

Credentials

Add credentials to your project

- ✓ Find out what kind of credentials you need
Calling Google Drive API from a web browser

- ✓ Create an OAuth 2.0 client ID
Created OAuth client 'ownCloud-10.0.8'

- ✓ Set up the OAuth 2.0 consent screen

4 Download credentials

Client ID 1093683589836-8666mgmfamqcbqqgicgej7lrrpjth5ba.apps.googleusercontent.com

Download this credential information in JSON format. This is always available for you on the credentials page.

[I'll do this later](#)

You can either open this file with the editor of your choice (SublimeText for example), or you can put in your web browser to view it. You can always download this data from your Google Drive project at a later time for other Google Drive mounts.

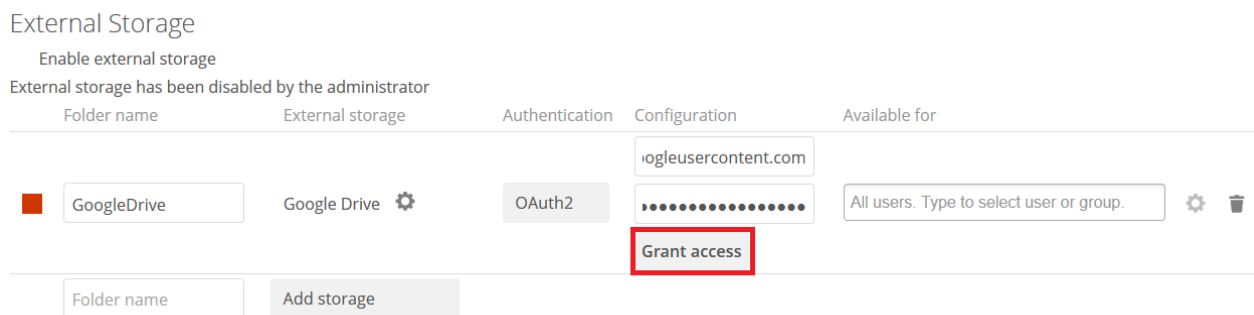
Here is an example output:

```
web:
  client_id: "1093683589836-8666mgnfamqcbqqgicgej7lrrpjth5ba.apps.googleusercontent.com"
  project_id: ownCloud-04-27
  auth_uri: "https://accounts.google.com/o/oauth2/auth"
  token_uri: "https://accounts.google.com/o/oauth2/token"
  auth_provider_x509_cert_url: "https://www.googleapis.com/oauth2/v1/certs"
  client_secret: "CrIkSysecuRL1nViyJiytPWh"
  redirect_uris:
    0: "http://51a8725b.ngrok.io/index.php/settings/admin?sectionid=storage"
  javascript_origins:
    0: "http://51a8725b.ngrok.io"
```

10. Client ID and Client Secret

Enter the Client ID and Client Secret in the ownCloud Google Drive mount screen and click **[Grant Access]**. Now you have everything you need to mount your Google Drive in ownCloud. Your consent page appears when ownCloud makes a successful connection.

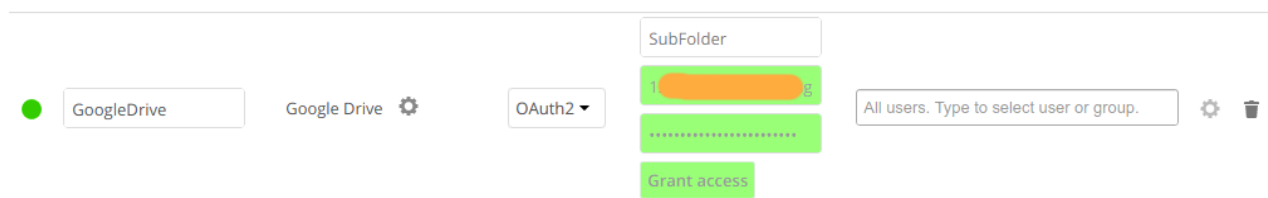
Click **[Allow]** when the consent screen appears.



11. Success

You are finished when you see the green light confirming a successful connection.

See the [External Storage Configuration](#) for additional mount options and information.



12. Files View

Go to your files view. You will see the newly mounted Google Drive.

Name	Size	Modified
Documents	35 KB	13 minutes ago
GoogleDrive	Pending	5 years ago
Photos	663 KB	13 minutes ago
ownCloud Manual.pdf	4.8 MB	13 minutes ago

3 folders and 1 file Pending

Local Storage

Introduction



Using local storage is a security risk, only use it if you know what you are doing.

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 web server user

Details

As this setup diffuses the difference between ownCloud Admin and sysadmin, this is a significant security risk and therefore off by default.



- **Only enable local storage if ownCloud Admin and sysadmin are the same person on purpose.**
- A local ownCloud mount does not work well with external storages like SMB or FTP mounted in the Linux filesystem. If such a Linux mounted storage goes away, ownCloud is likely to see the underlying empty mountpoint as a perfectly valid folder and will *silently* propagate content deletion, instead of forwarding error messages to the end users.

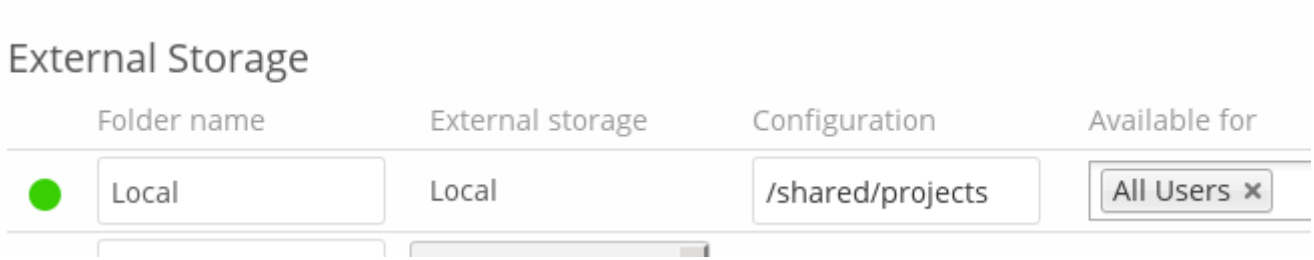
In any case, local storage is only configurable via the ownCloud admin settings. Non-admin users cannot create local storage mounts.

See [Set Correct Permissions](#) for information on correct file permissions, and find your HTTP user [PHP Version and Information](#).

To enable Local storage, you must first enable it by editing your ownCloud installation's `config/config.php` file adding the following configuration key:

```
'files_external_allow_create_new_local' => 'true',
```

To manage local storage, navigate to **Settings** › **Admin** › **Storage**. You can see an example in the screenshot below.



	Folder name	External storage	Configuration	Available for
●	Local	Local	/shared/projects	All Users ×

1. In the **Folder name** field enter the folder name that you want to appear on your ownCloud Files page.
2. In the **Configuration** field enter the full file path of the directory you want to mount.
3. In the **Available for** field enter the users or groups who have permission to access the mount; by default all users have access.

See [External Storage Configuration](#) for additional mount options and information, and [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 [External Storage Configuration](#) for additional mount options and information.
- See [External Storage Authentication Mechanisms](#) for more information on authentication schemes

S3 Compatible Object Storage as Primary Storage Location

Introduction

Administrators can configure Amazon S3 compatible object storages as the primary ownCloud storage location with the [S3 Primary Object Storage](#) app. The referencing name is `files_primary_s3`. Using `files_primary_s3` replaces the default ownCloud `owncloud/data` directory. However, 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.



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, [Object Storage Support \(objectstore\)](#) is still available, but the [S3 Primary Object Storage](#) app is the preferred and only supported way to provide S3 storage support as primary storage. ownCloud provides consulting for migrations from `objectstore` → `files_primary_s3`.

Consider the following differentiation:



External Storage: S3

Integrate S3 object storages as external storages

S3 Primary Object Storage

Leverage object storage via S3 as primary storage



OpenStack Swift has been deprecated.

When using `files_primary_s3`, the Amazon S3 bucket to be used needs to be created manually first, according to the [Amazon S3 developer documentation](#) and versioning needs to be enabled for this bucket.

Implications

Read the following implications carefully **BEFORE** you start using `files_primary_s3`:

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. In "object store" mode as primary storage access, ownCloud 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 file system. An excellent example is the [Encryption app](#), which fetches critical files in addition to any requested file, which results in significant overhead.

Therefore encrypting the S3 primary storage via ownCloud has been disabled and can not be enabled

4. When requiring encryption for the bucket containing the primary storage, use the bucket built-in encryption provided by the S3 API. See the configuration examples below how to enable it.
5. 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 file IDs are changed during such cross-storage move operations.

Configuration

Copy the following relevant example 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:

```
<?php
$CONFIG = [
    'objectstore' => [
        'class' =>
'Implementation\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' => 'owncloud123456',
                    'secret' => 'secret123456',
                ],
            ],
        ],
    ],
];
```

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' => '',
                // replace key, secret and bucket with your credentials
                'credentials' => [
                    // replace key and secret with your credentials
                    'key' => 'owncloud123456',
                    'secret' => 'secret123456',
                ],
                // replace the ceph endpoint with your rgw url
                'endpoint' => 'http://ceph:80/',
                // Use path style when talking to ceph
                'use_path_style_endpoint' => true,
            ],
        ],
    ],
];

```

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' => 'owncloud123456',
                ],
            ],
        ],
    ],
];

```

```

        'secret' => 'secret123456',
    ],
    'use_path_style_endpoint' => true,
    'endpoint' => 'http://scality:8000/',
],
],
];

```

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"/>	SFTP	<input type="text" value="Username and password"/> <ul style="list-style-type: none"> Username and password Log-in credentials, save in session 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 [External Storage Configuration](#) for additional mount options and information.
- See [External Storage Authentication Mechanisms](#) for more information on authentication schemes

Samba File Server Configuration (SMB/CIFS)

Introduction

ownCloud can connect to Windows file servers, and other SMB-compatible servers (e.g., [Samba](#)), by using the [SMB/CIFS](#) backend.

Dependencies

To connect ownCloud to an SMB file server, you need to prepare your server. Please see the [Manual Installation on Linux](#) guides for more information, prerequisites and requirements.

Access Testing

To ensure that you can connect to your file server with SMB, do a small test upfront like the following.

```
sudo smbclient -L <file_server_name> -U <full_domain_name>/<user_name>
```

Please fix any issues before you connect ownCloud to a SMB file server.

Configuration

When configuring ownCloud, you will need the following information:

- The folder name, which will be your local mount point.
- The URL of the Samba server.
- The username or domain/username used to login to the Samba server.
- The password to login to the Samba server.
- The share name to mount on the remote Samba server.
- The remote subfolder inside the remote Samba share to mount. This is optional, as it defaults to `/.`



To assign the ownCloud logon username automatically to the subfolder, use `$user` instead of a subfolder name. The `foldername=username` must be present and is not created on access.

- 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 Active Directory (AD), or when using session credentials where the username cannot be modified. This is concatenated with the username, so the backend gets `domain\username`

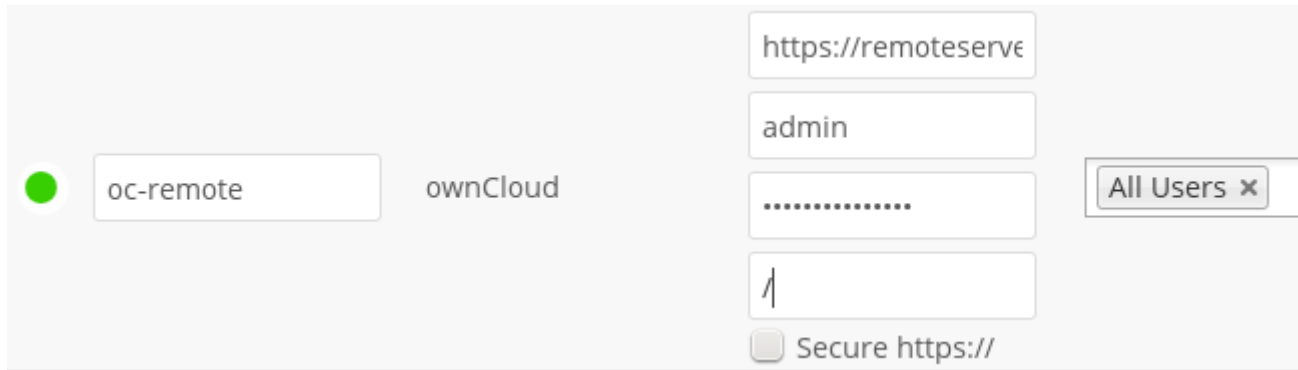
The screenshot shows the configuration interface for SMB / CIFS. It includes a green status indicator and the label 'smbcifs'. The main configuration area is titled 'SMB / CIFS' and contains several input fields: 'smbserver', 'users', '/shared', and 'Domain'. A dropdown menu is open for 'Session credentials', with 'Username and password' and 'Session credentials' as options. To the right, there is a search box labeled 'All users. Type to select'.

Further Information

- [External Storage Configuration](#) for additional mount options and information.
- [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:

- The name of your local mountpoint. Optionally, a **Remote Subfolder** can be specified to change the destination directory. The default is to use the whole root.
- The URL of the WebDAV or ownCloud server.
- The username and password for the remote server.



We always recommend **https://** for security reasons, so encourage you to enable [**Secure https://**].



CPanel users should install [Web Disk](#) to enable WebDAV functionality.

Further Reading

- See [External Storage Configuration](#) for additional mount options and information.
- See [External Storage Authentication Mechanisms](#) for more information on authentication schemes.

Files and Sharing

This section contains all of the file and sharing related configuration documentation. It includes such topics as:

- [Default Files Configuration](#)
- [File Sharing Configuration](#).
- [Federated Cloud Sharing Configuration](#).
- [Manual File Locking](#).

Big File Upload Configuration

Introduction

If you're expecting big file uploads, some considerations have to be taken into account. Setups based on your needs can be configured.

General Considerations

- Make sure that a version of PHP [supported by ownCloud](#) is installed.
- Consider that user quotas may prevent big file uploads due to a user reaching the space limitation.
- Though ownCloud already disables the PHP setting **Output Buffering** in the shipped `.htaccess` and `.user.ini` to prevent PHP memory-related errors, it can be the case that you must manually set it in your `php.ini` or `VirtualHosts` when the other two configuration files can't be used in your environment.
- The directory used for `upload_tmp_dir` must be fully accessible by PHP / the webserver user, usually `www-data`.
- Your temp directory or partition has to be big enough to hold multiple parallel uploads from multiple users. The formula for this is `temp_space = concurrent_uploads * chunk_size`
For example, if the chunk size is **10MB** (which is the default but might vary between different clients) and the average number of users uploading at the same time is **25**, then you'll need 250MB of temp space, as the formula below shows.

```
10MB x 25 users = 250MB required temp space
```

- The user's upload directory, usually in `<datadirectory>/<username>/uploads` (see [Sample Config PHP Parameters](#) for details) also has to be big enough. The formula is a bit different, as this directory collects all chunks of a file for that upload for that user until the upload is completed. The space needed for this directory is temporarily the same size as for the final file size. As an example, if a user wants to upload a 4GB file, temporarily 4GB of space needs to be available in the upload directory to hold the chunks. When the upload has finished, all chunks are written to the final destination and the chunks are deleted afterwards freeing that temporary space. The formula for the upload directory's temp space for all users is: `temp_space = concurrent_uploads * average_upload_size_per_user`. The location of the upload directory can be defined via the config setting `dav.chunk_base_dir`.

The space temporarily consumed in the upload directory will not count against the user quota. If a user has no quota left in his personal storage and the quota excludes external mounts, uploads to a windows network drive share as example will succeed. The file temporarily created in the upload directory will not count against his personal storage.

- In Centos and RHEL, Apache has a few more default configurations within `systemd`.



You will have to set the `temp` directory in two places:

1. In `php.ini`, e.g., `sys_temp_dir = "/scratch/tmp"`
2. In Apache systemd file e.g. `sudo systemctl edit httpd` and change/add:

```
PrivateTmp=false
```

When done, you need to reload the daemon and restart the service:

```
sudo systemctl daemon-reload
sudo systemctl restart httpd
```

Please **do not** change `/usr/lib/systemd/system/httpd.service` directly, only use `sudo systemctl edit httpd`. If not doing so, a `httpd` package upgrade may revert your changes.

Configuration via `.htaccess/user.ini`



ownCloud comes with its own `owncloud/.htaccess` file. When using `php-fpm`, PHP settings in `.htaccess` are not accessed. These settings must then be set in the `.user.ini` file. `php-fpm` will read settings from any `.user.ini` file in the same directory as the `.php` file that is being served via a web server.

Set the following parameters inside the corresponding file using your own desired values, as in the following examples, both files are located in the ownCloud root folder:

`.user.ini`

```
post_max_size=16G
output_buffering=0
upload_max_filesize=16G
upload_tmp_dir=/mnt/php_big_temp/
```

`.htaccess`

```
php_value post_max_size=16G
php_value output_buffering=0
php_value upload_max_filesize=16G
php_value upload_tmp_dir=/mnt/php_big_temp/
```

If you see PHP timeouts in your log files, increase the timeout values, which are in seconds, as in the example below. Use the `php_value` prefix like above when configuring the `.htaccess` file:

```
max_input_time=3600
max_execution_time=3600
```



Consider that any settings made in `.htaccess` or `.user.ini` may need to be repopulated after an upgrade of ownCloud.

Configuring via PHP Global Settings

If you don't want to use the ownCloud `.htaccess` or `.user.ini` file, you may configure PHP globally instead. Make sure to comment out or remove any lines in `.htaccess` if you added any like in the section above.



If you are running ownCloud on a 32-bit system, any `open_basedir` directive in your `php.ini` file needs to be commented out.

See the **Loaded Configuration File** section of [PHP Version and Information](#) to find your relevant `php.ini` files.

Set the following parameters inside the corresponding `php.ini` file using your own desired file size values, as in the following example:

```
post_max_size=16G
output_buffering=0
upload_max_filesize=16G
upload_tmp_dir=/mnt/php_big_temp/
```

If you see PHP timeouts in your log files, increase the timeout values, which are in seconds, as in the example below:

```
max_input_time=3600
max_execution_time=3600
```

Configuring via a Virtual Host

You can configure php parameters also per virtual host - if you have access to the Apache configuration file. This eliminates the need to maintain custom settings in a `.user.ini` or `.htaccess` file especially on upgrades. Note the mandatory prefix `php_admin_value` before the php parameter.

```
<VirtualHost *:443>

    DocumentRoot /var/www/owncloud
    ServerName myowncloud.com

    php_admin_value post_max_size 16G
    php_admin_value output_buffering 0
    php_admin_value upload_max_filesize 16G
    php_admin_value upload_tmp_dir /mnt/php_big_temp/
```



If you see PHP timeouts in your log files, increase the timeout values, which are in seconds, as in the example below:

```
php_admin_value max_input_time 3600
php_admin_value max_execution_time 3600
```

Configuring via 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 some parameters in `config.php`.

- Set a temporary location for uploaded files by using the `tempdirectory` setting.
- If you have configured the `session_lifetime` setting in your `config.php`, see [Sample Config PHP Parameters](#), 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 entirely from your configuration to reset it to the default shown in the `config.sample.php`.

General Upload Issues

Various environmental factors could cause a restriction of the upload size. Examples are:

- The `LVE Manager` of `CloudLinux` which sets an `I/O limit`.
- Some services like `Cloudflare` are also known to cause uploading issues.
- Upload limits enforced by proxies used by your clients.
- Other web server modules like described in [General Troubleshooting](#).

Apache Directives

- [LimitRequestBody](#)
- [SSLRenegBufferSize](#)

Apache with `mod_reqtimeout`

The `mod_reqtimeout` Apache module could also stop large uploads from completing. If you're using this module and uploads of large files fail, either disable it in your Apache config or increase the configured `RequestReadTimeout` values.

Disable `mod_reqtimeout` on Ubuntu

On Ubuntu, you can disable the module by running the following command:

```
sudo a2dismod reqtimeout
```

Disable `mod_reqtimeout` on CentOS

On CentOS, comment out the following line in `/etc/httpd/conf/httpd.conf`:

```
LoadModule reqtimeout_module modules/mod_reqtimeout.so
```

When you have run `asdismod` or updated `/etc/httpd/conf/httpd.conf`, restart Apache.



There are also several other configuration options in your web server config which could prevent the upload of larger files. Refer to your web server's manual for how to configure those values correctly:

Apache with mod_fcgid

- [FcgidMaxRequestInMem](#)
- [FcgidMaxRequestLen](#)



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 usual may no longer be necessary, once bug #51747 is fixed.

Long-Running Uploads

For very long-running uploads **those lasting longer than 1h** to public folders, *when chunking is not in effect*, `filelocking.ttl` should be set to a significantly large value in `config.php`. If not, large file uploads will fail with a file locking error, because the Redis garbage collection will delete the initially acquired file lock after 1 hour by default.

To estimate a good value, use the following formula:

```
time_in_seconds = (maximum_upload_file_size / slowest_assumed_upload_connection).
```

For the value of "*slowest assumed upload connection*", take the **upload** speed of the user with the slowest connection and divide it by two. For example, let's assume that the user with the slowest connection has an 8MBit/s DSL connection; which usually indicates the download speed. This type of connection would, usually, have 1MBit/s upload speed (but confirm with the ISP). Divide this value in half, to have a buffer when there is network congestion, to arrive at 512KBit/s as the final value.

Manual File Locking

Introduction

Manual file locking allows users, if enabled, to lock files in shared areas while working on them in order to prevent concurrent changes from other users (check-in/check-out).

The feature builds on the WebDAV Locks backend which has been introduced with Server 10.1 and is now available in the ownCloud Web Interface. All storages are supported as locking takes place on the WebDAV level. The locks will only be available via ownCloud, not when a user works directly on the storage. Using the context menu of files, every user who has access can lock them. Users can recognize locked files by the means of a new lock indicator. While a file is locked, other users can still access it but they can not make any changes. Locked files can manually be unlocked by the lock owner (the user who locked the file; exclusive locking) using the "Locks" tab in the file details view (right sidebar).

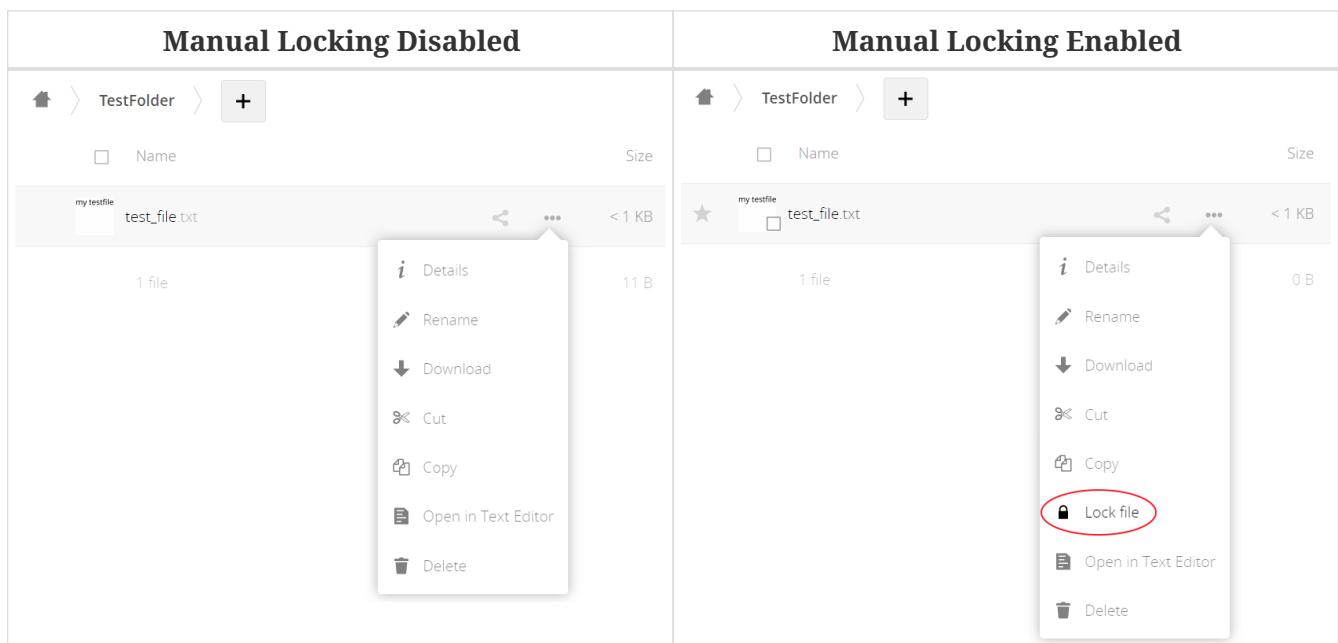
Enable or Disable the UI Component



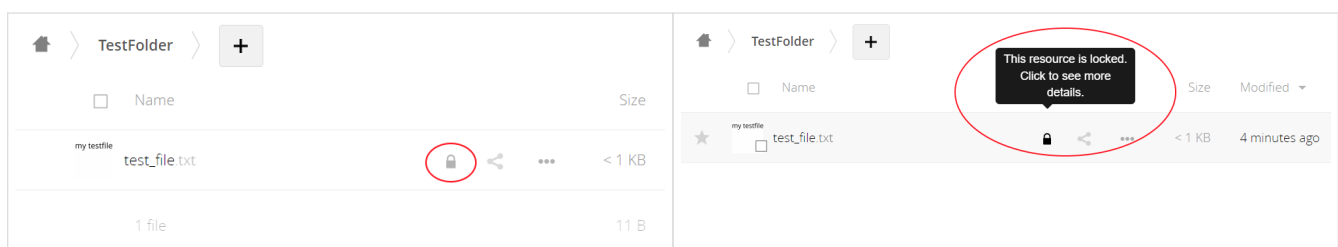
The *user-facing* components in the web interface are disabled by default because this feature allows users to lock other users' files **exclusively**. Even the owner of the file can't unlock them. Lock releasing can only be done by the locking user, a user who is a member of a lock breaking group (if defined), or until the lock expires.

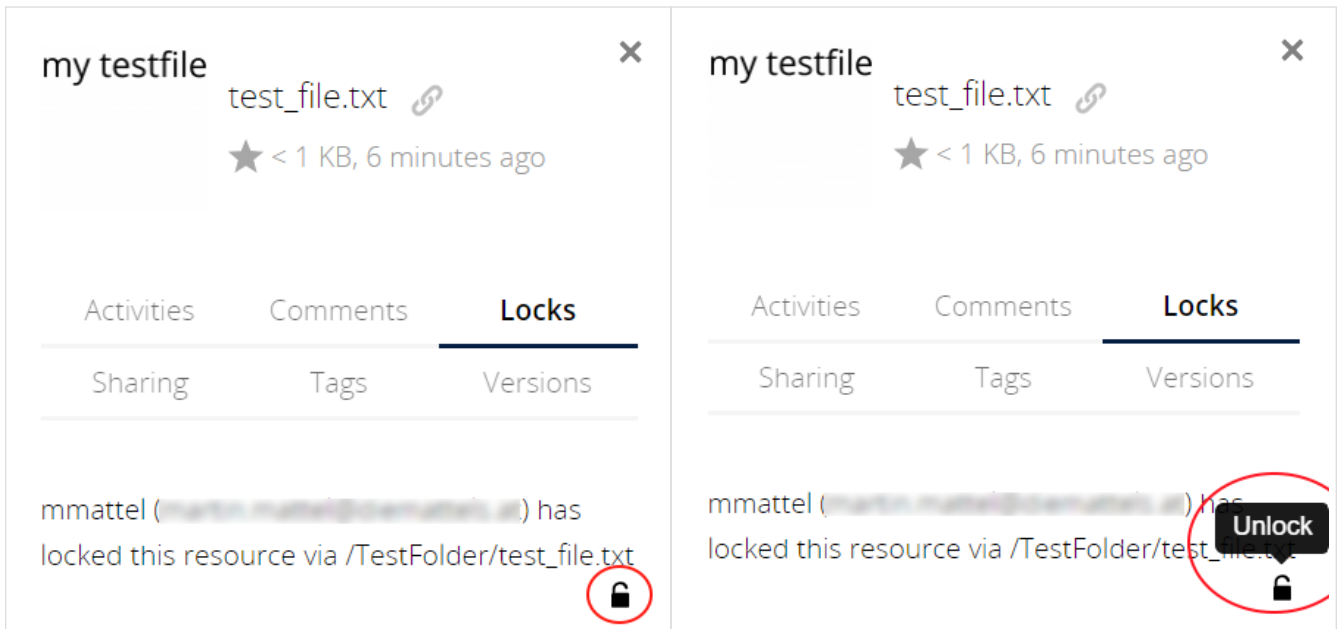
By default, locks set by the user in the web interface will expire after 30 minutes. The maximum lock time by default is 24 hours.

The main user-facing component in the web interface looks like in the following screenshots. If *Manual File Locking* is disabled, the additional user-facing components are not present:



If manual locking is enabled, the following additional user-facing components are present:





Administrators can enable *Manual File Locking* for users either via the web interface or by executing an occ command:

Web interface

Go to **Settings** > **Admin** > **General**

Manual File Locking

Default timeout for the locks if not specified (in seconds)

Maximum timeout for the locks (in seconds)

Enable manual file locking in the web interface

Allow users in the following groups to unlock files they have access to:

Users in these groups can unlock files even if they are not the owner of the lock.

Using the occ command

```
sudo -u www-data ./occ config:app:set files enable_lock_file_action --value yes
```

Configuration

To prevent files being locked infinitely, there is a mechanism that automatically expires locks after a certain time. The expiration time of locks can either be configured via the web interface or using occ commands. In addition, administrators can define groups whose members can break locks.

The default timeout for the locks is, if not specified (in seconds):

Maximum lifetime of a lock set via the web interface (or by not specifying a timeout value when calling the WebDAV Locks API).

The maximum timeout for the locks (in seconds):

Maximum lifetime of locks which is allowed to be set by calling the WebDAV Locks API.

Define lock breaker groups:

Users who are a member of these groups can break locks set by another user.

Web interface

Go to **Settings > Admin > General**

The image is the same as shown above when enabling or disabling *Manual File Locking*.

Using the occ command

- Default locks timeout

```
sudo -u www-data ./occ config:app:set files lock_timeout_default --value 1800
```

- Maximum locks timeout

```
sudo -u www-data ./occ config:app:set files lock_timeout_max --value 86400
```

- Define lock breaker groups

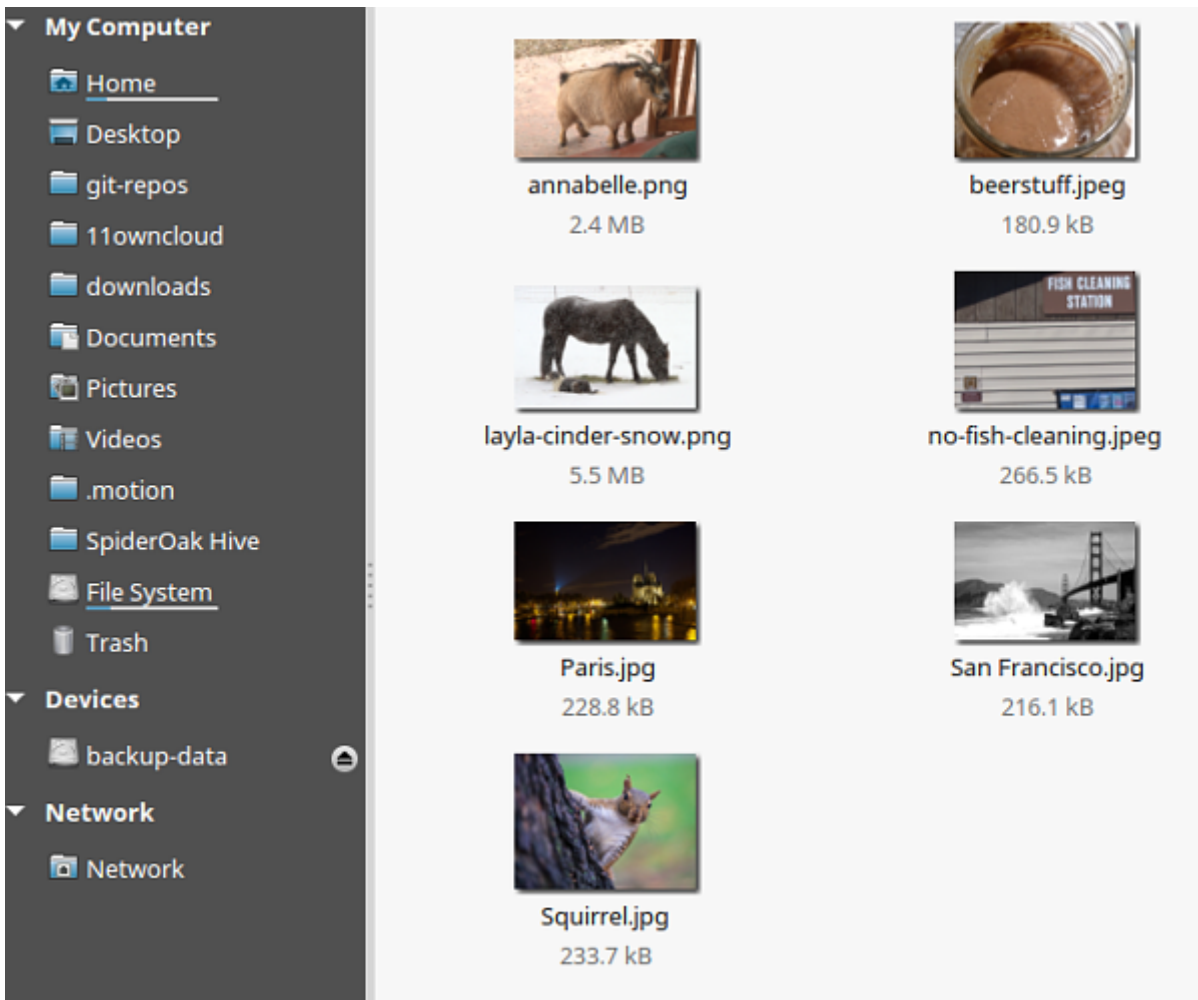
The example below defines two lock breaker groups named `unlockers` and `admin`.

```
sudo -u www-data ./occ config:app:set core lock-breaker-groups --value  
'["unlockers","admin"]'
```

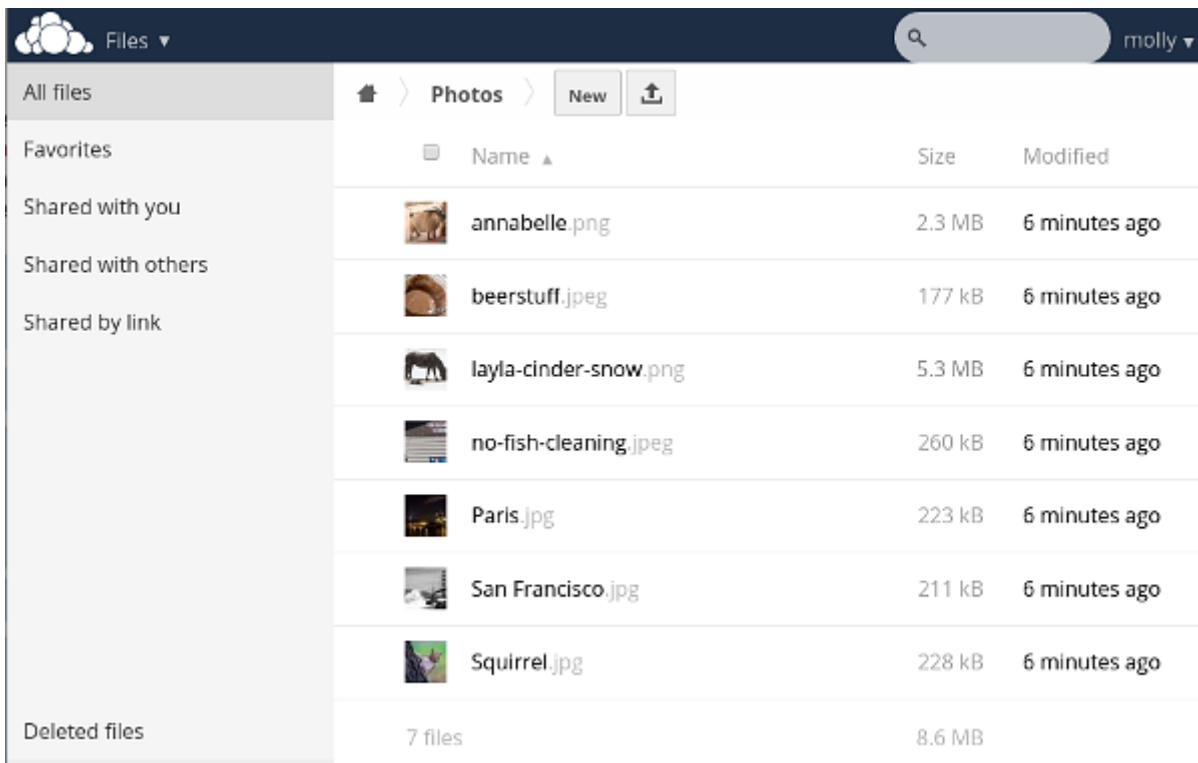
Providing Default Files

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` 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 this directory empty if you do not want to copy any skeleton files.

The value of the `skeletondirectory` key **must not be empty** if you decide to use it in your `config.php`.



See [Sample Config PHP Parameters](#) for more the complete list of `config.php` options.

Configuring Federation Sharing

Introduction

Federated Cloud Sharing is managed by the Federation app. When you enable the Federation app you can easily and securely link file shares between ownCloud servers, in effect creating a "cloud" of ownCloud installations.



For security reasons federated sharing **strictly requires HTTPS (SSL/TLS)**.



We strongly recommend using HTTP for development and testing purposes. However, to do so, you have to set `'sharing.federation.allowHttpFallback' => true`, in `config/config.php`.

Configuration

Follow these steps to establish a trusted connection between two servers.

1. Verify that both servers have SSL certificates. If you open the server URL in your browser and see a lock icon on the left-hand side of the address bar, the certificate is valid.

Lock icon in the address bars in Firefox, Google Chrome, and Safari.

Firefox



Google Chrome



Safari



2. Verify that the `'overwrite.cli.url' => 'https://<SERVER_URL>'` setting is configured to the correct URL, instead of `'localhost'`, in `config.php`.
3. Reset the federation job in your `oc_jobs` table. This job is required to get the verification token

from the other server to establish a federation connection between two servers. The resetting ensures that it will be executed when we run `system:cron` later.

```
mysql -u root -e "update oc_jobs set last_run=0 where class='OCA\\Federation
\\SyncJob';" owncloud;
mysql -u root -e "update oc_jobs set last_checked=0 where class='OCA\\Federation
\\SyncJob';" owncloud;
```

4. Navigate to **admin settings** → **sharing** → **Federation**
5. Add **server 1** to the trusted servers on **server 2**.
6. Add **server 2** to the trusted servers on **server 1**.
7. Now run the cron job in your ownCloud directory (for example `/var/www/owncloud/`).

```
sudo -u www-data ./occ system:cron
```

8. Now the check should be green
9. Sync now your users with

```
sudo -u www-data ./occ dav:sync-system-addressbook
sudo -u www-data ./occ federation:sync-addressbook
```

10. Configure automatic acceptance of new federated shares.

```
sudo -u www-data ./occ config:app:set federation auto_accept_trusted --value '0'
sudo -u www-data ./occ config:app:set federatedfilesharing auto_accept_trusted
--value 'yes'
```

Working With Proxies

There are ownCloud instances that are not connected to the internet. They have no possibility to reach the public network. Therefore Federation will not work without a proxy.

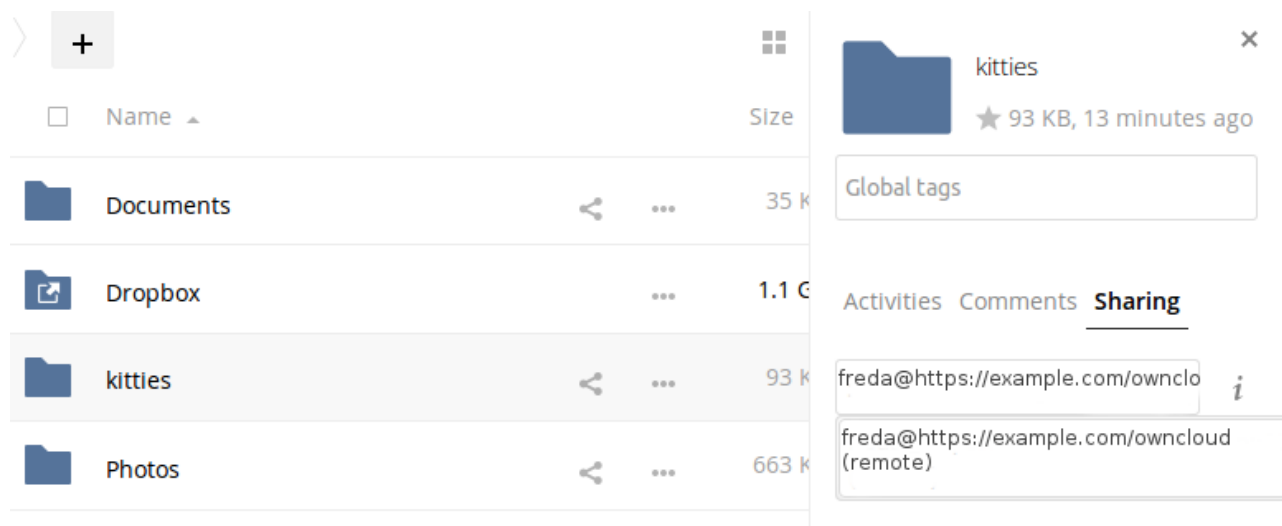
To set the `proxy` and `proxyuserpwd` configuration variables, in `config/config.php`. `proxy` sets the proxy's hostname, and `proxyuserpwd` sets the username and password credentials, in `username:password` format.

Creating a New Federation Share

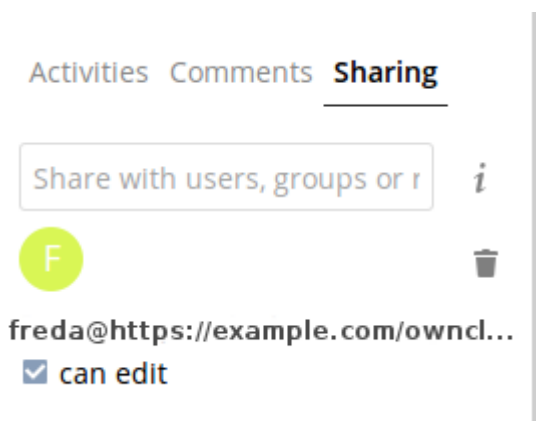
Follow these steps to create a new Federation share between two ownCloud servers. This requires no action by the user on the remote server; all it takes is a few steps on the originating server.

1. Enable the Federation app.
2. Then, create a federated share by entering `username@serveraddress` in the sharing dialog (for example `freda@https://example.com/owncloud`). When ownCloud verifies the link, it displays it

with the **(federated)** label. Click on this label to establish the link.



3. 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.

Federated Sharing Scanner CronJob Configuration



As part of the migration step to 10.5, before enabling the cronjob described below, make sure to remove the system cron job from your crontab that executes legacy **occ incoming-shares:poll**

The Federated Sharing Scanner is a background job used to scan the federated shares to ensure the integrity of the file cache.

On each run the scanner will select federated shares that satisfy these requirements:

1. ensure that within a single cron run, at max [cronjob_scan_external_batch] scans will be performed out of all accepted external shares (default 100)
2. a scan of that external share has not been performed within the last [cronjob_scan_external_min_scan] seconds (default 3 hours)
3. the user still exists, and has been active recently, meaning logged in within the last [cronjob_scan_external_min_login] seconds (default 24 hours)

4. there has been a change in the federated remote share root etag or mtime, signaling a mandatory rescan

To enable the cronjob, go to **Settings > Admin Settings > Federated Cloud Sharing** and enable the checkbox

Federated Cloud Sharing *i*

Periodically synchronize outdated federated shares for active users

Federated Cloud Sharing *i*

Periodically synchronize outdated federated shares for active users

Alternatively you can use the command line:

```
sudo -u www-data ./occ config:app:set files_sharing cronjob_scan_external_enabled  
--value 'yes'
```

You can also configure these settings of the cronjob:

1. the minimum amount of time since last login of a user so that a scan is triggered (ensures only active users get fed shares synced)

```
sudo -u www-data ./occ config:app:set files_sharing cronjob_scan_external_min_login  
--value <integer-seconds>
```

1. the minimum amount of time since last scanned so that the next scan is triggered (avoid frequent scan when active collaboration)

```
sudo -u www-data ./occ config:app:set files_sharing cronjob_scan_external_min_scan  
--value <integer-seconds>
```

1. the maximum number of federated share scans per 10 minutes (scan performed only if fed share files got updated)

```
sudo -u www-data ./occ config:app:set files_sharing cronjob_scan_external_batch  
--value <integer-number>
```

Use the following command to force a run of the scanner cronjob:

```
sudo -u www-data ./occ background:queue:execute --force --accept-warning <id-of-fed-  
scanner-job>
```

Known Issues

Persistent Locks Are Not Guaranteed

There is a known bug propagated persistent locks to federated instances. If a user creates an exclusive lock on a share, no other users should be able to modify it, nor its contents, and all users should see a lock icon on the share.

However, this isn't the case. The following functionality has been recorded:

- The user who created the lock sees the lock icon throughout the share.
- The top-level of the share for receivers shows the lock icon.
- Sub-items of the share **do not show the lock icon**.
- The share and its contents **can still be modified by all users**; specifically:
 - Sub-items **can be deleted**.
 - Sub-items **can be created**.

Tips

VCARD properties

It is possible to configure the VCARD properties that are searched in order to retrieve a list of federated users in the share dialog. By default, ownCloud uses CLOUD and FN properties, however this list may be configured by the admin:

```
sudo -u www-data ./occ config:app:set dav remote_search_properties --value  
=CLOUD,FN,EMAIL
```

Possible options are:

- VERSION
- UID
- FN
- N
- EMAIL
- CLOUD

Listing Federated Shares

In case you want to see which federated shares exist on your server, you can use this command to list them.

Currently there is no ownCloud `occ` command to list federated shares, that's why you have to use these database queries to obtain the information.

Federated shares are saved in your database.

```
sudo mysql -u <ownCloud_DB_User> -p<ownCloud_DB_Password> -h <ownCloud_DB_Host>
<ownCloud_DB_Name>
```

Incoming shares can be listed with the following query:

```
select * from oc_share where share_type=6;
```

Each unique ID gives you an incoming federated share.

Outgoing shares can be listed with the following query: (replace `cloud.example.com` with your instance URL)

```
select * from oc_share_external where remote NOT IN ('https://cloud.example.com');
```

Each unique ID gives you an outgoing federated share.

Exit the database console with this command:

```
quit
```

File Sharing

Introduction

This section describes how to set general configuration rules for sharing files.

General Notes

The sharing policy is configured at **Settings > Admin > Sharing**.



If you don't see the sharing section:

- Check if you have installed an Adblock browser plugin.

If so, disable the plugin and recheck.

Sharing *i*

Allow apps to use the Share API

Allow users to share via link

Allow public uploads

Enforce password protection for read-only links

Enforce password protection for read & write links

Enforce password protection for upload-only (File Drop) links

Set default expiration date

Allow users to send mail notification for shared files

Language used for public mail notifications for shared files Owner language ▼

Allow users to share file via social media

Automatically accept new incoming local user shares

Allow resharing

Allow sharing with groups

Restrict users to only share with users in their groups

Restrict users to only share with groups they are member of

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

Default user and group share permissions

Create Change Delete Share

Extra field to display in autocomplete results

Email address ▼

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, for more details see [Federated Cloud Sharing Configuration](#).
- Create public link 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 link shares
 - Allow public uploads to public link shares
 - Enforce password protection on public link shares

- Set default expiration date on public link shares
- Allow users to send mail notification for shared files
- Set the language used for public mail notification for shared files
- Allow users to share file via social media
- Set default expiration date for user shares
 - Set the number of days to expire after
 - Enforce as maximum expiration date
- Set default expiration date for group shares
 - Set the number of days to expire after
 - Enforce as maximum expiration date
- Set default expiration date for remote shares
 - Set the number of days to expire after
 - Enforce as maximum expiration date
- Automatically accept new incoming local user shares
- Allow resharing
- Allow sharing with groups
- Restrict users to only share with users in their groups
- Restrict users to only share with groups they are a member of
- Allow users to send mail notification for shared files to other users
- Exclude groups from creating shares
- Allow username autocompletion in share dialog
 - Restrict enumeration to group members
- Default user and group share permissions
- Extra field to display in autocomplete results



ownCloud includes a [Share Link Password Policy app](#).

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 link shares for people who are not ownCloud users via hyperlink.

Allow public uploads

Check this option to allow anyone to upload files to public link shares.

Enforce password protection of public link shares

Check these options to force users to set a password on public link shares. Passwords can be enforced on any or all of read-only, read-write, read-write-delete and upload-only (File Drop) public link shares. This does not apply to local user and group shares.

Set default expiration date of public link shares

Check this option to set a default expiration date on public link shares. Check *Enforce as maximum expiration date* to limit the maximum expiration date to be the default. Users can choose an earlier expiration date if they wish.

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 ./occ \
  config:app:set \
  core \
  shareapi_public_notification_lang \
  --value '<language code>'
```



In the example above, the `<language code>` is an [ISO 3166-1 alpha-2 two-letter country code](#), such as **de**, **gb**, **us**, **es** or others.



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 for user shares

Check this option to set a default expiration date when sharing with another user. The user can change or remove the default expiration date of a share.

Set the number of days to expire after

Set the default number of days that user shares will expire. The default value is 7 days.

Enforce as maximum expiration date

Check this option to limit the maximum expiration date to be the default. Users can choose an earlier expiration date if they wish.

Set default expiration date for group shares

Check this option to set a default expiration date when sharing with a group. The user can change or remove the default expiration date of a share.

Set the number of days to expire after

Set the default number of days that group shares will expire. The default value is 7 days.

Enforce as maximum expiration date

Check this option to limit the maximum expiration date to be the default. Users can choose an earlier expiration date if they wish.

Set default expiration date for remote shares

Check this option to set a default expiration date when sharing with a remote user. The user can change or remove the default expiration date of a share.

Set the number of days to expire after

Set the default number of days that remote shares will expire. The default value is 7 days.

Enforce as maximum expiration date

Check this option to limit the maximum expiration date to be the default. Users can choose an earlier expiration date if they wish.

Automatically accept new incoming local user shares

Disabling this option activates the "Pending Shares" feature. Users will be notified and have to

accept new incoming user shares before they appear in the file list and are available for access giving them more control over their account. More information about [pending shares](#) can be found in the release notes.

Allow resharing

Check this option to enable users to re-share files shared with them.

Allow sharing with groups

Check this option to enable users to share with groups.

Default user and group share permissions

Administrators can define the permissions for user/group shares that are set by default when users create new shares. As shares are created instantly after choosing the recipient, administrators can set the default to e.g. read-only to avoid creating shares with too many permissions unintentionally.

Restrict users to only share with users in their groups

Check this option to confine sharing within group memberships.



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.

Restrict users to only share with groups they are a member of

When this option is enabled, users can only share with groups they are a member of. They can still share with all users of the instance but not with groups they are not a member of. To restrict sharing to users in groups the sharer is a member of, the option *Restrict users to only share with users in their groups* can be used. More information about [granular sharing restrictions](#) can be found in the release notes.

Allow users to send mail notification for shared files to other users

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. When you check this, you will 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.

Extra field to display in autocomplete results

The autocomplete dropdowns in ownCloud usually show the display name of other users when it is set. If it's not set, they show the user ID / login name, as display names are not unique you can run into situations where you cannot distinguish the proposed users. This option enables to add mail addresses or user ID's to make them distinguishable.

Blacklist Groups From Receiving Shares

Sometimes it is 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 is a system group, it can be advisable to block it from receiving shares. In these cases, ownCloud administrators can blacklist one or more groups so that they cannot receive shares.

To blacklist one or more groups via the Web UI, under **Settings > Admin > 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.

Group Sharing Blacklist

Exclude groups from receiving shares

These groups will not be available to share with. Members of the group are not restricted in initiating shares and can receive shares with other groups they are a member of as usual.

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 outgoing shares and metadata info associated with those files (shares, tags, and comments, etc). Incoming shares are *not* moved, as the sharing user holds the ownership of the respective files. This is useful when you have to transfer a user's files to another user before you delete them.

Trashbin contents are not transferred.

Here is an example of how to transfer all files from one user to another.

```
sudo -u www-data ./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 ./occ files:transfer-ownership \  
  --path="folder/to/move" \  
  <source-user> \  
  <destination-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 will 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 the [occ command reference](#), for a complete list of `occ` commands.



If an exception occurred during the transfer ownership command or the command terminated prematurely, it is advised to run following command for the source **and** target user:

```
sudo -u www-data ./occ files:troubleshoot-transfer-ownership --uid <uid>
```

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. This means, whatever happens to the file owner also happens to the files.

One solution to get around this issue 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 the share is independent which users come and go, the file shares will remain. Because all files added to the share or edited in it are automatically 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 [occ files_external documentation](#).

Personal Share

```
sudo -u www-data ./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
```

or

```
sudo -u www-data ./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 ./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'}
```

or

```
sudo -u www-data ./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 ./occ files_external:import \  
/import.json
```


Personal Share

```
sudo -u www-data ./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": []  
}
```



Share Permissions

Permissions Masks

Permission	Value	web UI Value
READ	1	
UPDATE	2	<i>can update</i>
CREATE	4	<i>can create</i>
DELETE	8	<i>can delete</i>
SHARE	16	<i>can reshare</i>

File Operations Shorthand for the Later Table

Operation	Description
download	Download/read/get a file or display a folder's contents.
upload	A new file can be uploaded/created (file target does not exist).
upload_overwrite	A file can overwrite an existing one.

Operation	Description
rename	Rename file to new name, all within the shared folder.
move_in	Move a file from outside the shared folder into the shared folder.
move_in_overwrite	Move a file from outside the shared folder and overwrite a file inside the shared folder. <div style="display: flex; align-items: center;">  <p>SabreDAV automatically deletes the target file first before moving, so requires DELETE permission too.</p> </div>
move_in_subdir	Move a file already in the shared folder into a subdirectory within the shared folder.
move_in_subdir_overwrite	Move a file already in the shared folder into a subdirectory within the shared folder and overwrite an existing file there.
move_out	Move a file to outside of the shared folder.
move_out_subdir	Move a file out of a subdirectory of the shared folder into the shared folder.
copy_in	Copy a file from outside the shared folder into the shared folder.
copy_in_overwrite	Copy a file from outside the shared folder and overwrite a file inside the shared folder. <div style="display: flex; align-items: center;">  <p>SabreDAV automatically deletes the target file first before copying, so requires DELETE permission too.</p> </div>
delete	Delete a file inside the shared folder.
mkdir	Create a folder inside the shared folder.
rmdir	Delete folder inside the shared folder

The following lists what operations are allowed for the different permission combinations (share permission is omitted as it is not relevant to file operations):

Operation(s)	Permission Combinations
READ (aka read-only)	<ul style="list-style-type: none"> • download

Operation(s)	Permission Combinations
READ + CREATE	<ul style="list-style-type: none"> • download • upload • move_in • copy_in • mkdir
READ + UPDATE	<ul style="list-style-type: none"> • download • upload_overwrite • rename
READ + DELETE	<ul style="list-style-type: none"> • download • move_out • delete • rmdir
READ + CREATE + UPDATE	<ul style="list-style-type: none"> • download • upload • upload_overwrite • rename • move_in • copy_in • mkdir
READ + CREATE + DELETE	<ul style="list-style-type: none"> • download • upload • move_in • move_in_overwrite • move_in_subdir • move_in_subdir_overwrite • move_out • move_out_subdir • copy_in • copy_in_overwrite • delete • mkdir • rmdir

Operation(s)	Permission Combinations
READ + UPDATE + DELETE	<ul style="list-style-type: none"> • download • upload_overwrite • rename • move_out • delete • rmdir
READ + CREATE + UPDATE + DELETE (all permissions)	<ul style="list-style-type: none"> • download • upload • upload_overwrite • rename • move_in • move_in_overwrite • move_in_subdir • move_in_subdir_overwrite • move_out • move_out_subdir • copy_in • copy_in_overwrite • delete • mkdir • rmdir

Files Versions

Introduction

Every time when a file gets rewritten to the storage, the versions app (`files_versions`) creates a new backup copy of the file. Versions are visible for the user in the webinterface only and do not get synced to clients. An admin can control the retention behaviour of versioned files.

How Versions are Created

When a backup copy is created, it is stored inside a folder `files_versions` which is inside the users root folder. The app will add the suffix `.v` followed by the unix timestamp of the creation date of the backup copy.



File versioning only gets triggered if the change is made via the ownCloud ecosystem. It does not get triggered if the change is made at a mounted filesystem directly.

Versions are displayed in the WebUI in the details view in the right sidebar if you click on the file row in the file listing. You can restore the current file to one of the earlier backup copies in the list, by clicking on the **[restore]** icon of the specific version.

The screenshot shows the ownCloud WebUI interface. The main content area displays a file listing for 'welcome.txt' with columns for Name, Size, and Modified. The file is 28 B and was modified 14 minutes ago. The right sidebar shows the details view for 'welcome.txt', including a 'Versions' tab with a list of 11 previous versions. Each version entry shows the date and time (e.g., 'Do 25 Apr 14 minutes ago') and the file size ('< 1 KB'). A 'restore' icon is visible next to each version entry.

How Versions are Deleted

The versions app deletes old file versions automatically to ensure that users do not exceed their storage quotas. This is done by automatic background jobs which clean up the versions following a specific pattern. This pattern defines the expiration date for each backup version.

Default Versions Delete Patterns

This is the default pattern used to delete old versions:

- For the last second we keep one version
- For the last 10 seconds ownCloud keeps one version every 2 seconds
- For the last minute ownCloud keeps one version every 10 seconds
- For the last hour ownCloud keeps one version every minute
- For the last 24 hours ownCloud keeps one version every hour
- For the last 30 days ownCloud keeps one version every day
- If the versions are older than 30 days ownCloud keeps one version every week

The versions are adjusted along this pattern every time a new version is created and the background job was executed.

Example

Time Period before last Expiration	Maximum Number of Versions:
1 second	1
10 seconds	5
1 minute	6
1 hour	59
1 day	23
30 days	30



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.



Adjust the `'versions_retention_obligation'` setting in `config.php` to avoid filling up the user's quota.

Change the Expiration Settings

You may alter the default pattern in `config.php`. The default setting is `auto`, which sets the default pattern:

```
'versions_retention_obligation' => 'auto',
```

Possible Config Values

<code>auto</code>	Default value if nothing is set
-------------------	---------------------------------

<code>D, auto</code>	Keep versions at least for D days, apply expiration rules to all versions that are older than D days
<code>auto, D</code>	Delete all versions that are older than D days automatically, delete other versions according to expiration rules
<code>D1, D2</code>	Keep versions for at least <code>D1</code> days and delete when they exceed <code>D2</code> days.
<code>disabled</code>	Disable Versions; no files will be deleted.

Example 1:

Keep all versions for at least 10 days, apply expiration rules to all versions that are older than 10 days. This will keep a lot more versions during the last 10 days compared to the default pattern.

```
'versions_retention_obligation' => '10, auto',
```

Example 2:

Apply expiration rules to all versions that are created during the last 30 days and do not keep any versions older than 30 days.

```
'versions_retention_obligation' => 'auto, 30',
```

Example 3:

Do not apply any expiration rules. Delete all versions after 30 days.

```
'versions_retention_obligation' => '30, 30',
```

Enterprise File Retention

Enterprise customers have additional tools for managing file retention policies; see [Advanced File Tagging With the Workflow App](#).

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.



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.

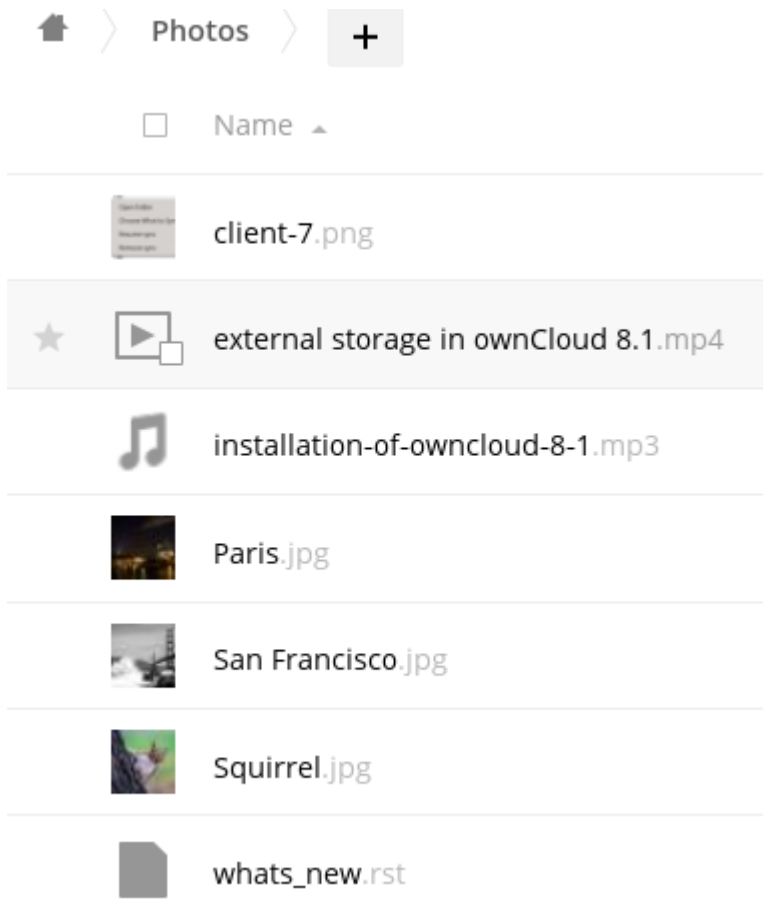
File locking is enabled by default, using the database locking backend. This places a significant load on your database. Using `memcache.locking` relieves the database load and improves performance. Admins of ownCloud servers with heavy workloads should install [a memory cache](#) .

Previews Configuration

Introduction

The ownCloud preview system generates thumbnails and previews of files for all ownCloud apps that display files such as the Files or the Files Mediaviewer app.

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

ownCloud supports the preview generation of file types such as PDF, SVG or various office documents. These document types can be a security issue as they can have javascript or other code either embedded or linked.



Be careful enabling preview thumbnail generation for documents which could contain or reference executable code! ownCloud does NOT take any responsibility for any issues.

Important Considerations

1. Rendering takes place when the user accesses the folder and the preview has not been generated before. This means that each first folder access may create additional load on the server.
2. Previews are not a shared resource but rendered for each user individually.
3. Preview generation can only be set for the system and not for individual mounts.
4. When enabling preview generation for SVG, the preview code checks for the existence of `xlink` or `href` and disallows creating a preview. This minimizes the risk but does not eliminate it. Such

a check is not made for PDF or Office documents and enabling the creation of previews for those documents can be therefore a *serious security issue*.

5. When enabling preview generation for videos (or huge image files), consider the following points:
 - a. Because the video needs to be downloaded before a preview can be created, this may impact general accessibility of files for other users if the video resides on an external mount point with limited bandwidth like Google Drive.
 - b. The server may report timeouts if there are multiple videos to render and/or if the video is big.
 - c. Preview generation for videos is in general a resource intensive process.

Default Preview Providers

Please note that the ownCloud preview system comes already with sensible defaults, and therefore it is usually not necessary to adjust those configuration values. If you want to configure previews, add or change the following parameters in `config/config.php`.

The default list of enabled preview providers which do not need to be explicitly enabled in the config are:

```
OC\Preview\BMP
OC\Preview\GIF
OC\Preview\JPEG
OC\Preview\WEBP
OC\Preview\MarkDown
OC\Preview\MP3
OC\Preview\PNG
OC\Preview\TXT
OC\Preview\XBitmap
```

If you want to add or change the default list, you **MUST** define all elements used. If you just declare an additional item, only this item will be taken and none of the default list.

Prerequisites

When defining your own preview providers, some things need to be considered. For some file types, ownCloud uses ImageMagick to generate previews. By default, the delivered version of ImageMagick for Ubuntu 20.04 is version 6, and the wrapper for php is version 3.4. This version of ImageMagick is *not* capable of processing additional file formats like SVG or HEIC and many others. If you want to use those providers, you must upgrade ImageMagick to version 7 and the php wrapper to version 3.5. See the [php-imagick Library](#) section in the installation guide for more information.

Notes for PDF Preview Generation

If you handle the security risk and decide to allow creating previews for PDF files, change the following imagick security policy. Use an editor of your choice like `nano` and change the following

file, adapt the path if using ImageMagick 7:

```
sudo nano /etc/ImageMagick-6/policy.xml  
or  
sudo nano /etc/ImageMagick-7/policy.xml
```

Search for the following content:

```
<policy domain="coder" rights="none" pattern="PDF" />
```

and change:

```
rights="none" --> rights="read|write"
```

After changing the policy file for ImageMagic, restart your Apache web server or your php-fpm service.

Notes for Video Preview Generation

To be able to create previews for video files when using the `OC\Preview\Movie` provider, you must install `ffmpeg`. There can be significant load on the server during conversion when video thumbnail generation is enabled.

```
sudo apt install -y ffmpeg
```

List Extensions Used for the Preview Generation

To get a list of file extensions linked to the image or video provider, change into the `owncloud` directory and run the following example command. Use a different filter for other provider types.

```
cat resources/config/mimetypermapping.dist.json | grep image
```

Preview Format Requirements

The following providers require the php `imagick` extension:

```
OC\Preview\AI  
OC\Preview\EPS  
OC\Preview\Heic  
OC\Preview\PDF  
OC\Preview\PSD  
OC\Preview\SGI  
OC\Preview\SVG  
OC\Preview\TIFF
```

```
OC\Preview\TTF
```

The following providers are only available if either LibreOffice or OpenOffice is installed on the server:

```
OC\Preview\MSOfficeDoc
OC\Preview\MSOffice2003
OC\Preview\MSOffice2007
OC\Preview\OpenDocument
OC\Preview\StarOffice
```

The following providers are available, but disabled by default due to performance or privacy/security concerns:

```
OC\Preview\Font
OC\Preview\Illustrator
OC\Preview\Movie
OC\Preview\MSOfficeDoc
OC\Preview\MSOffice2003
OC\Preview\MSOffice2007
OC\Preview\OpenDocument
OC\Preview\StarOffice
OC\Preview\SVG
OC\Preview\PDF
OC\Preview\Photoshop
OC\Preview\Postscript
OC\Preview\TIFF
```

Managing Your Preview Settings

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 and will display generic icons instead of thumbnails.

Set the configuration option `enable_previews` to `false`:

```
'enable_previews' => false,
```

Adding a Preview Provider

The example below adds the preview provider for `SGI` and `HEIC` images:

```
'enabledPreviewProviders' => [
  'OC\Preview\SGI',
```

```
'OC\Preview\Heic',  
'OC\Preview\BMP',  
'OC\Preview\GIF',  
'OC\Preview\JPEG',  
'OC\Preview\MarkDown',  
'OC\Preview\MP3',  
'OC\Preview\PNG',  
'OC\Preview\TXT',  
'OC\Preview\XBitmap',  
],
```



You have to add all default providers if you do not want to disable them.

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. The default value you can reference in `config/config.sample.php` is set to 2048.

The following example would limit previews to a maximum size of 100 px × 100 px:

```
'preview_max_x' => 100,  
'preview_max_y' => 100,
```



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:

```
'preview_max_scale_factor' => 10,
```

If you want to disable scaling at all, you can set the config value to `1`:

```
'preview_max_scale_factor' => 1,
```

If you want to disable the maximum scaling factor, you can set the config value to `null`:

```
'preview_max_scale_factor' => null,
```

Define the JPEG Preview Quality

The JP(E)G image quality can be defined in [%] for displaying thumbnails and image previews for

apps like Files or Files Mediaviewer. Note that this setting is for displaying only and has no impact on the stored thumbnail / preview quality or size.

```
'previewJPEGImageDisplayQuality' => -1,
```

The scale ranges from 1 to 100, where 1 is the lowest and 100 the highest. It defaults to -1 which is equivalent to approximately 75% of the original image quality. Consider that any value over 80 may result in an unnecessary increase of the displayed image and has larger response sizes when requesting images, without much increase of the image quality. Usually it is not necessary to have a quality setting over 75, but it can be increased if there is the need to display previews in high quality with the cost that every image requested generates a higher response load. Note that this setting does not affect downloading images. Setting a value takes immediate effect and nothing needs to be regenerated as it is for display requests only.

For more information see: [PHP imagejpeg — Output image to browser or file](#)

Mimetypes Management

Introduction

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, e.g. if you want a custom audio icon for audio mimetypes instead of the default file icon.

Mimetype Aliases

ownCloud's default mimetype configuration is defined in

```
owncloud/resources/config/mimetypealiases.dist.json
```

Below you can see a snippet of the file where 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",
}
```

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
```

and save it as

```
config/mimetypealiases.json
```

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.



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

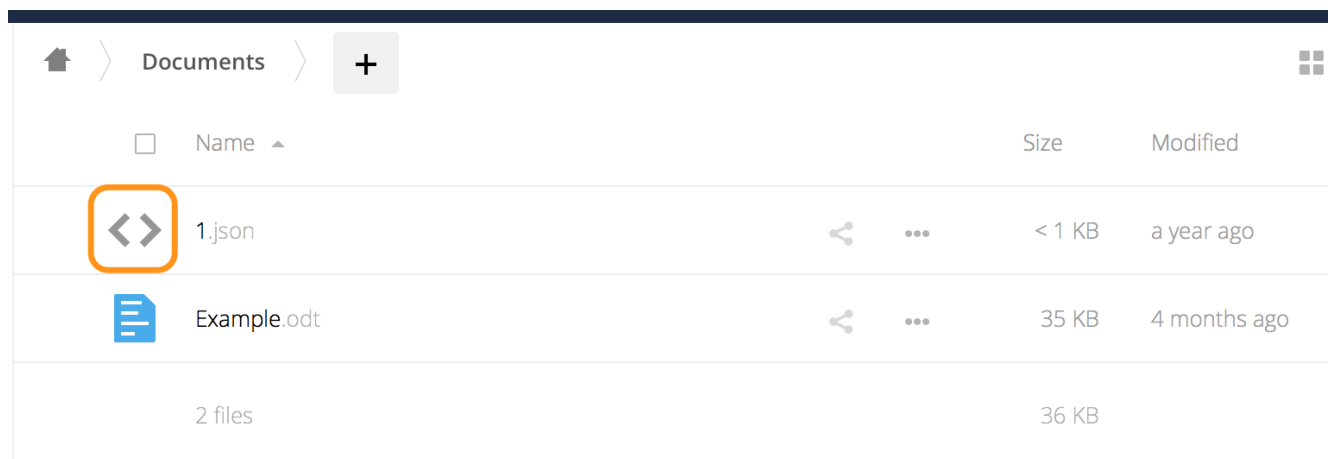
Once you have made changes to

```
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 ./occ maintenance:mimetype:update-js
```

Example - Changing the JSON File Icon



Let's go through an example of to change 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`.

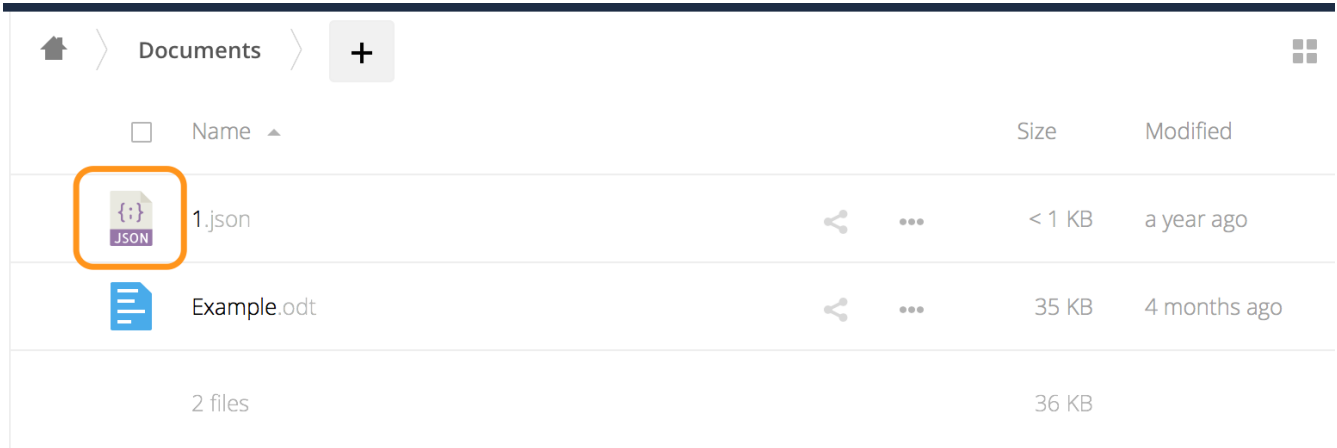


The name and location of the file are important. * The location is because the `core/img/filetypes` directory stores the mimetype file icons. * The name is important as it's a rough mapping between the alias name and the icon's file name, i.e., `text/json` becomes `text-json`.

4. Run the following command to update the mimetype alias database.

```
sudo -u www-data ./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.



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/mimetypemapping.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-draw"],
  "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/mimetypemapping.dist.json
```

and save it as

```
config/mimetypemapping.json
```

Then, in this new file, make any changes required.



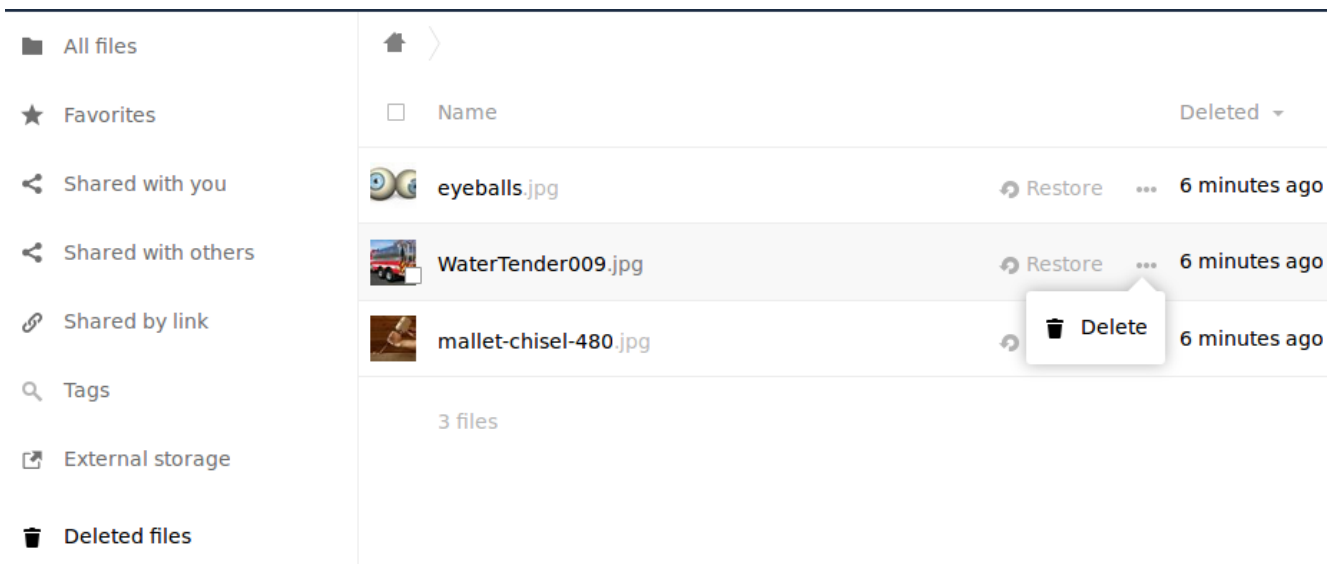
Please refer to the [ownCloud theming documentation](#) for where to put the new image files.

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.

Managing the Trash Bin

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 ./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 ./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 ./occ trashbin:cleanup user1 user2
Remove deleted files of user1
Remove deleted files of user2
```

See the **Deleted Files** section in [Sample PHP Configuration Parameters](#), and the [Trash Bin](#) section of the occ commands.

Integration

This section is dedicated to integrating ownCloud with other products.

- [Microsoft Teams](#)
- [ownCloud App for Splunk](#)

Integrate ownCloud into Microsoft Teams

Introduction

If you're using Microsoft Teams in your organization or for private purposes, you will likely want to access your ownCloud installation from your Microsoft Teams account. For this purpose, we created the [ownCloud Generator for Admins](#) with which you can generate a customized Microsoft Teams app for your users accessing your ownCloud services. Each ownCloud domain to be accessed requires a separate generated Microsoft Teams app for your users. The generated app must then be uploaded in your organization's app catalog.



As a prerequisite, the OpenID Connect app is required. If you already have a OpenID Connect configuration made with another service, you have to reconfigure with Microsoft Azure AD, as only one identity provider configuration is allowed.

Prerequisites

To get this working, you need to install and/or configure the following components:

Option 1 "Enterprise": With Single Sign-On (SSO) and ownCloud Enterprise Edition

1. Microsoft Azure Active Directory
2. ownCloud apps:
 - a. [OpenID Connect](#)
 - b. [MS-Teams Bridge App](#)
3. The custom app(s) you have generated with [ownCloud Generator for Admins](#)
4. Microsoft Teams

Option 2 "Standard": With Basic Authentication and ownCloud Standard Edition

1. ownCloud apps:

a. OpenID Connect

2. The custom Microsoft Teams app(s) you have generated with the [ownCloud Generator for Admins](#)
3. Microsoft Teams

Note: If you are using the Standard Edition, you can skip the following steps that describe the configuration of Azure AD and the MS-Teams Bridge App.

ownCloud

Installation

Assuming you have an ownCloud server version 10.7 or higher already running in your company or for personal use, perform the following steps:

1. Install and enable the MS-Teams Bridge app, minimum required version: v1.0.0.
2. Install and enable the [OpenID Connect](#) app from the ownCloud marketplace, minimum required version: v2.0.0.

Configure the MS-Teams Bridge App

You need to configure the MS-Teams Bridge app in two steps:

1. Add a *header* directive to the Apache `.htaccess` configuration located in your ownCloud web root in section `<IfModule mod_env.c>`

```
Header merge Content-Security-Policy "frame-ancestors 'self' teams.microsoft.com *.teams.microsoft.com"
```

Using `merge`, the response header is appended to any existing header of the same name, unless the value to be appended already appears in the header's comma-delimited list of values. When a new value is merged onto an existing header it is separated from the existing header with a comma. Merging avoids that headers of the same type and content being sent multiple times. This can happen if headers are also set on other locations.



For the time being, if you add the header to the ownCloud's `.htaccess` file in the ownCloud web root, you have to manually add that header again after an ownCloud upgrade.

2. Add a config key to your `config.php` file

This key is necessary for security reasons. Users will be asked to click a login button each time when accessing the ownCloud app after a fresh start of their Microsoft Teams app or after idle time. This behavior is by design. The button name can be freely set based on your requirements.

```
'msteamsbridge' => [  
    "loginButtonName" => "Login to ownCloud with Azure AD",
```

],

3. Enable [index.php less URL's](#) on your web server.

Microsoft

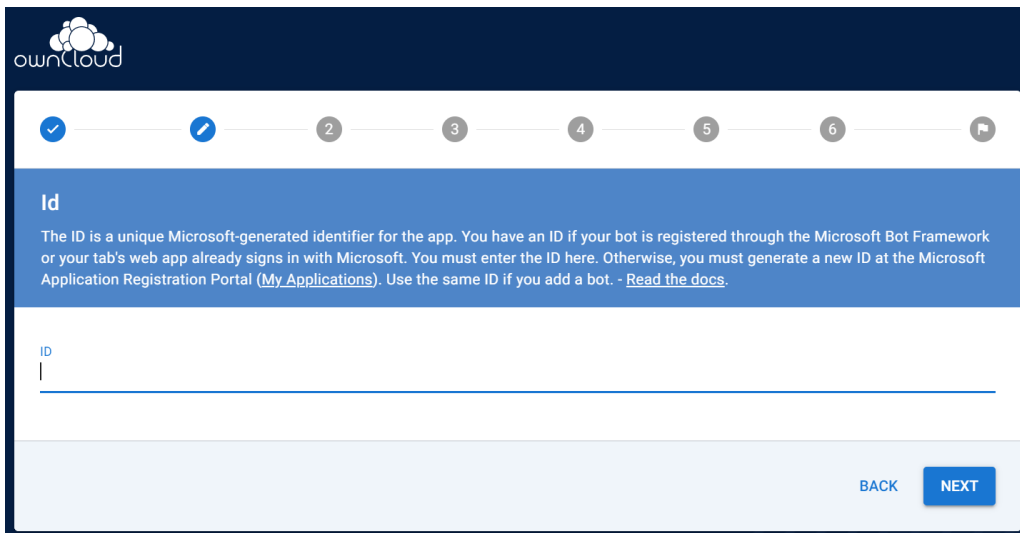
Microsoft Azure and OpenID Connect

Before you start to create your Microsoft Teams App, follow the procedure described in [Example Setup Using Microsoft Azure](#) to configure Microsoft Azure AD and OpenID Connect.

Create Your Microsoft Teams App

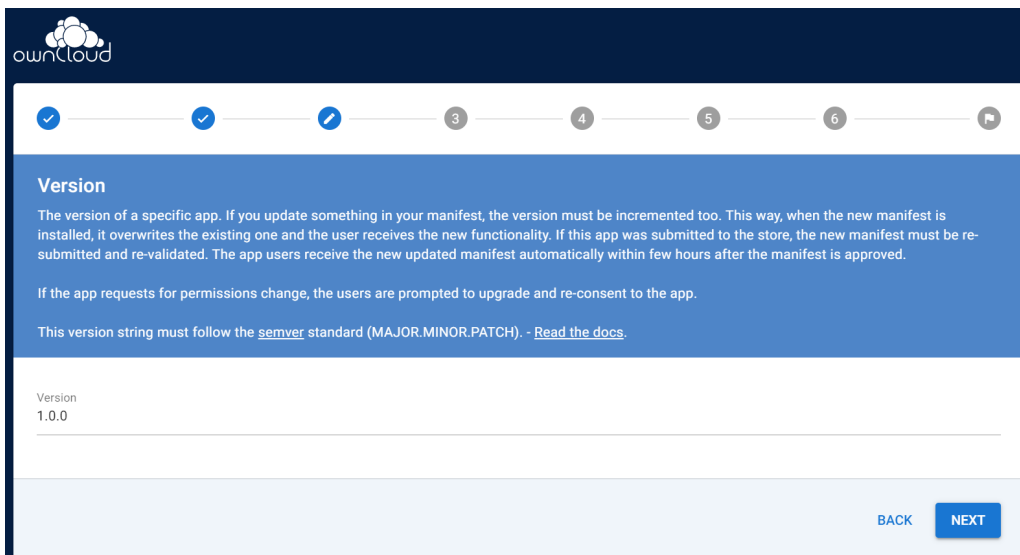
The following procedure creates an ownCloud app ready to be used by your users with Microsoft Teams in your environment.

1. In [ownCloud Generator for Admins](#) follow the guided instructions step by step.
2. Enter the Microsoft App/Client ID for your app. The ID's to be entered **must** be the [CLIENT-ID](#) from Microsoft Azure.



The screenshot shows the 'ownCloud' logo in the top left corner. Below it is a progress bar with seven steps: 1 (checked), 2 (pencil icon), 3 (grey), 4 (grey), 5 (grey), 6 (grey), and 7 (pencil icon). The main content area has a blue header with the title 'Id'. Below the header is a text box containing the following text: 'The ID is a unique Microsoft-generated identifier for the app. You have an ID if your bot is registered through the Microsoft Bot Framework or your tab's web app already signs in with Microsoft. You must enter the ID here. Otherwise, you must generate a new ID at the Microsoft Application Registration Portal ([My Applications](#)). Use the same ID if you add a bot. - [Read the docs](#).' Below this text is a text input field with the label 'ID' and a single character 'I' entered. At the bottom right of the form are two buttons: 'BACK' and 'NEXT'.

3. Enter the version of the app you create.



The screenshot shows the 'ownCloud' logo in the top left corner. Below it is a progress bar with seven steps: 1 (checked), 2 (checked), 3 (pencil icon), 4 (grey), 5 (grey), 6 (grey), and 7 (pencil icon). The main content area has a blue header with the title 'Version'. Below the header is a text box containing the following text: 'The version of a specific app. If you update something in your manifest, the version must be incremented too. This way, when the new manifest is installed, it overwrites the existing one and the user receives the new functionality. If this app was submitted to the store, the new manifest must be re-submitted and re-validated. The app users receive the new updated manifest automatically within few hours after the manifest is approved. If the app requests for permissions change, the users are prompted to upgrade and re-consent to the app. This version string must follow the [semver](#) standard (MAJOR.MINOR.PATCH). - [Read the docs](#).' Below this text is a text input field with the label 'Version' and the text '1.0.0' entered. At the bottom right of the form are two buttons: 'BACK' and 'NEXT'.

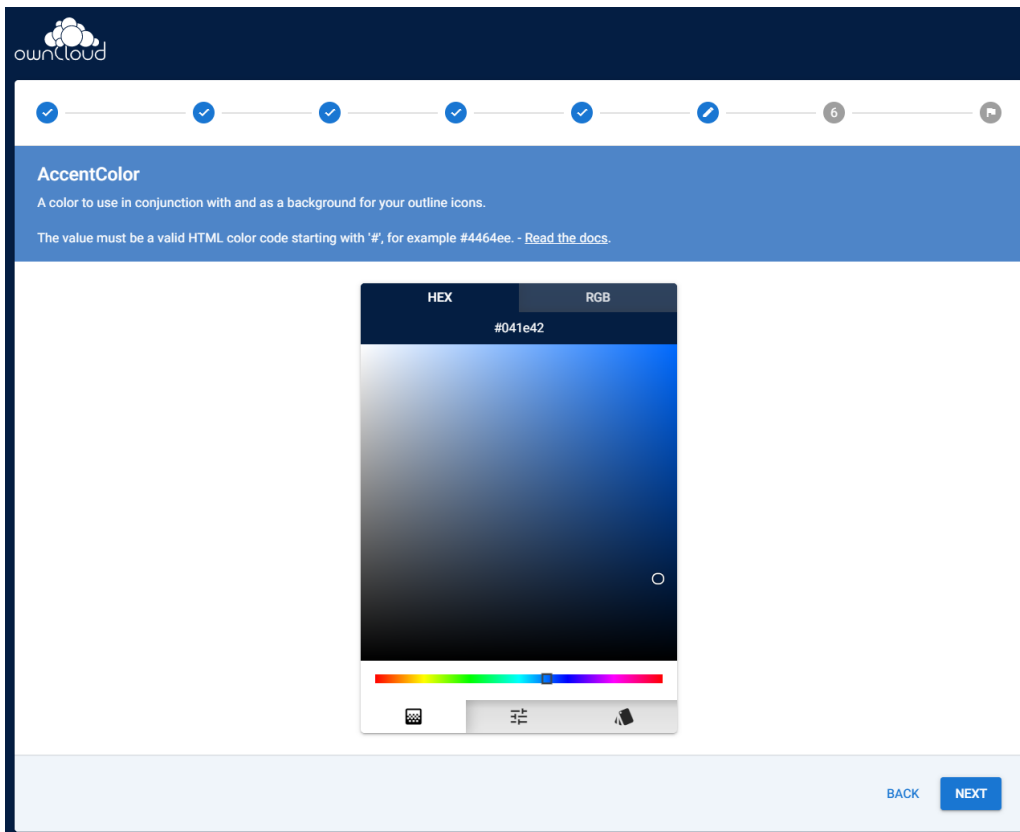
4. Enter the name of the app you create. Take care about how to name your app. It **cannot** be changed later on. We recommend naming it **ownCloud for Teams** for easy identification.

The screenshot shows the 'Name' configuration step in the ownCloud app wizard. At the top, the ownCloud logo is visible. Below it is a progress bar with seven steps: steps 1, 2, and 3 are marked with blue checkmarks; step 4 is the current step, marked with a pencil icon; steps 5 and 6 are marked with grey circles; and step 7 is marked with a grey circle and a right-pointing arrow. The main content area has a blue header with the title 'Name'. Below the header, there is explanatory text: 'The name of your app experience, displayed to users in the Teams experience. For apps submitted to AppSource, these values must match the information in your AppSource entry. The values of short and full must be different. - [Read the docs.](#)'. There are two text input fields: 'Short' with the value 'ownCloud for Teams' and 'Full' which is empty. At the bottom right, there are 'BACK' and 'NEXT' buttons.

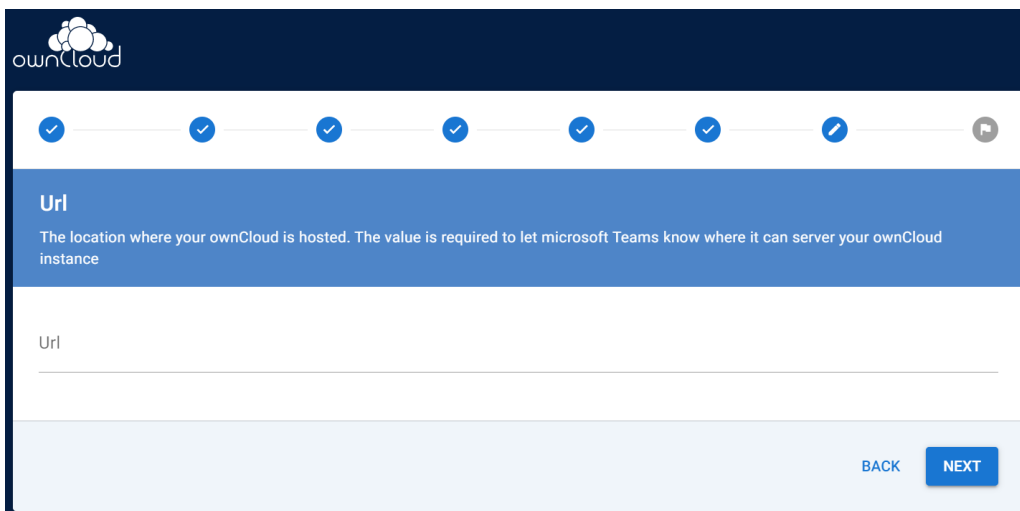
5. Enter the description of the app you create.

The screenshot shows the 'Description' configuration step in the ownCloud app wizard. The progress bar at the top is identical to the previous step, with step 5 now marked with a pencil icon. The main content area has a blue header with the title 'Description'. Below the header, there is explanatory text: 'Describes your app to users. For apps submitted to AppSource, these values must match the information in your AppSource entry. Ensure that your description accurately describes your experience and provides information to help potential customers understand what your experience does. You must note in the full description, if an external account is required for use. The values of short and full must be different. Your short description must not be repeated within the long description and must not include any other app name. - [Read the docs.](#)'. There are two text input fields: 'Short' with the value 'Access your ownCloud without leaving Teams.' and 'Full' with the value 'Integrate your ownCloud instance in Teams to access your files easily. ownCloud will be integrated as a tab in Teams so you can quickly reach your files.' At the bottom right, there are 'BACK' and 'NEXT' buttons.

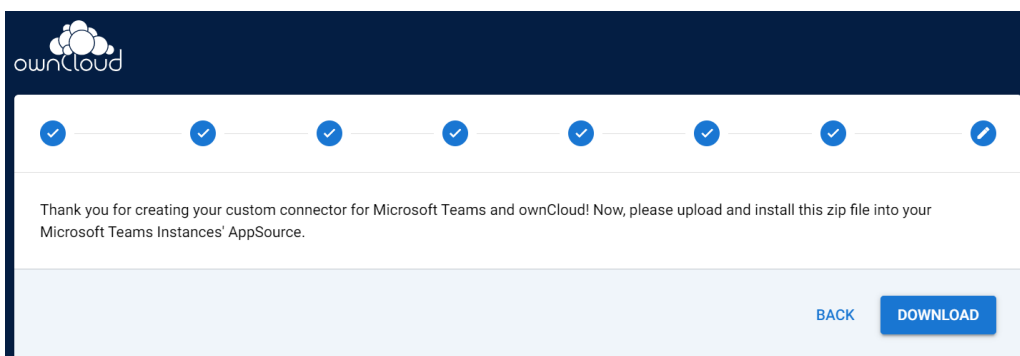
6. Set the AccentColor of the app you create.



7. Enter the URL how you access your owncloud instance like <https://cloud.example.com>.



8. After performing all the steps, click the **download** button and store the generated zip file locally.



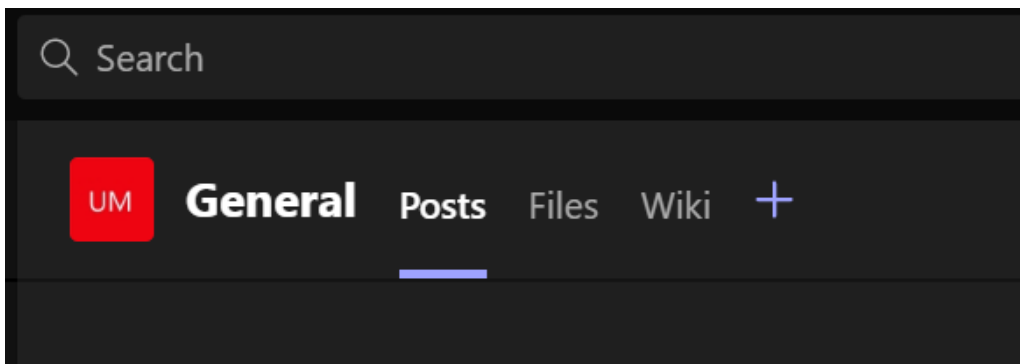
9. Go to the app section of Microsoft Teams and upload the generated zip file to your organization's app catalogue. Follow the [Publish a custom app by uploading an app package](#) guide for more information.
10. The new app is now available to users in your organization's app catalog.
11. See the following documents on how to pin the app, set the order how apps appear or how to install apps on behalf of users.
 - a. [Manage your apps in the Microsoft Teams admin center](#)
 - b. [Manage app setup policies in Microsoft Teams](#)

See the [users documentation](#) about their necessary steps how to integrate ownCloud into Microsoft Teams.

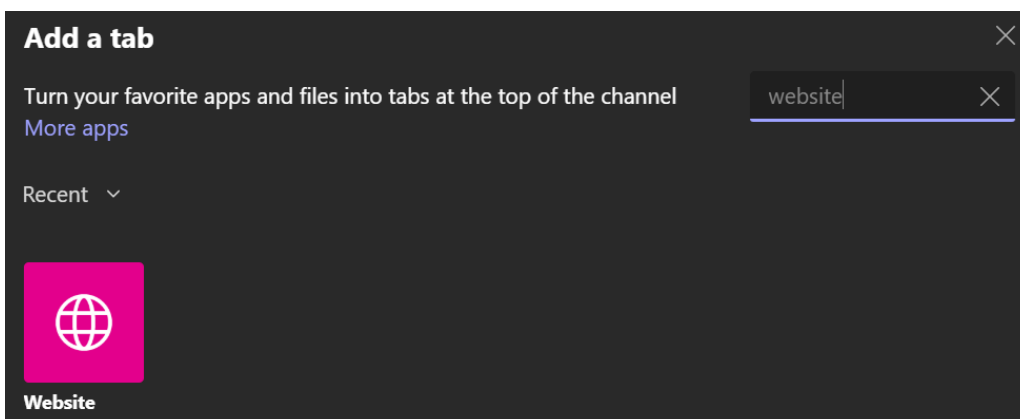
Alternative ownCloud Website Tab

As an alternative to creating an app for Microsoft Teams, it's also possible to embed ownCloud as a Microsoft Teams tab website. Tabs are Teams-aware webpages embedded in Microsoft Teams. See the [What are Microsoft Teams tabs](#) documentation to find out more.

1. Press the [+] plus button at the top of the Teams window.



2. Search for **website** and add by clicking on it.



3. Add a meaningful name and the following URL replacing "cloud.example.com" with how you access your ownCloud instance.

Website About X

Tab name

ownCloud for Teams ✓

URL*

Paste your link here

*Make sure you're only linking to sites that start with 'https://' and contain trustworthy web content. That way, you and your team can stay secure.

Post to the channel about this tab

Back Save

`https://cloud.example.com/apps/msteamsbridge`

Support

If you encounter problems with the integration of ownCloud and Teams, please contact us via eMail at support@owncloud.com or look for answers to those problems at the [Forum](#)

ownCloud App for Splunk

Introduction

The *ownCloud App for Splunk* provides a sophisticated reporting and auditing tool for ownCloud service operators. It makes use of both ownCloud's technical logs (owncloud.log), audit logs and the *ownCloud Metrics* API to provide insights. It shows information about users as well as storage and sharing usage across the instance and per user. It also makes audit evaluations quicker and more efficient. The app configures Splunk to retrieve and store the data and to provide visualizations, log filtering tools and pre-defined alerts for certain events.

By aggregating, evaluating and visualizing the data provided by ownCloud, the *ownCloud App for Splunk* allows service providers to gain insights into how their ownCloud platform is used and adopted (e.g., user, storage and sharing growth). Automatically gathering and processing ownCloud data enables a continuous reporting tool to be built up for stakeholders. For auditing purposes, the app provides very fine-grained and flexible tools that allow tracing actions by user, by operation or even by a single file and more.

The app makes all relevant ownCloud data available in Splunk. The dashboards and tools can easily be extended or modified. With just a few clicks, they can be adapted to specific needs, using the filtering and visualization features provided by Splunk.

Prerequisites

To set up the *ownCloud App for Splunk*, a number of prerequisites have to be fulfilled.

- ownCloud Server has a minimum version of 10.5.
- Splunk has a minimum version of 7.2.
- The [Metrics App](#) is installed, configured and enabled on ownCloud Server.
- The [Auditing App](#) is installed, configured and enabled on ownCloud Server.
- Both components of the *ownCloud App for Splunk*, the app and the add-on, are installed and configured. See below for further information on these components.

Setup & Configuration

ownCloud

1. Install and set up the [Auditing App](#) as [documented](#). Take note of the log file paths (owncloud.log and admin_audit.log) as those will be required in the Splunk configuration below.
2. Install and set up the [Metrics App](#) as [documented](#). Take special care to set the Metrics API key as it will be required in the Splunk configuration below.

Splunk

The *ownCloud App for Splunk* consists of two components that have to be installed and configured in Splunk.

- The [ownCloud Add-on for Splunk](#) gathers and stores the ownCloud data in Splunk.
- The [ownCloud App for Splunk](#) adds dashboards and other functionalities to the Splunk web interface.

Both can be installed from the Splunkbase app store. You will find the necessary initial configuration below.

ownCloud Add-on for Splunk (TA_owncloud)

The [ownCloud Add-on for Splunk](#) (TA_owncloud) takes care of gathering the data from ownCloud as well as storing and indexing it in Splunk. It requires a Splunk Universal Forwarder to be installed on the ownCloud host.

To get started, please follow the steps below.

1. Create an index for your ownCloud data (e.g., `index=owncloud`).

The *ownCloud Add-on for Splunk* does not ship with an index. You have to create an index on your Splunk instance or Splunk index cluster. For further help, refer to the respective [Splunk documentation](#).

2. Install a Splunk Universal Forwarder on your ownCloud host. For further information, consult the [Splunk documentation](#).
3. Install the *ownCloud Add-on for Splunk*
 - If you're using a standalone Splunk instance, you have to install the *ownCloud Add-on for Splunk*.

- If you're using a distributed Splunk installation, it depends on your setup:
- Search Heads: Installation of the *ownCloud Add-on for Splunk* is required.
- Indexers: Installation of the *ownCloud Add-on for Splunk* is conditional. It is not required if you use Heavy Forwarders to collect data. It is required if you use Universal Forwarders to collect data.
- Universal or Heavy Forwarders: Installation of the *ownCloud Add-on for Splunk* required. In addition data and scripted input must be enabled as described below.

4. Enable data and scripted input with a configuration file.

On your Universal Forwarder or Heavy Forwarder instance, you must enable input using the configuration files.

1. Copy `$SPLUNK_HOME/etc/apps/TA_owncloud/default/inputs.conf.example` to `$SPLUNK_HOME/etc/apps/TA_owncloud/local` directory and rename the file to `inputs.conf`.
2. Open `$SPLUNK_HOME/etc/apps/TA_owncloud/local/inputs.conf` for editing.
3. Check all `index = owncloud` settings and change the index name if needed.
4. Check the ownCloud logs locations (default: `/var/www/owncloud/data/`) and change them to the values you configured on the ownCloud Server.
5. Save the `$SPLUNK_HOME/etc/apps/TA_owncloud/local/inputs.conf` file.
6. Copy `$SPLUNK_HOME/etc/apps/TA_owncloud/default/owncloud.conf.example` to `$SPLUNK_HOME/etc/apps/TA_owncloud/local` directory and rename the file to `owncloud.conf`.
7. Open `$SPLUNK_HOME/etc/apps/TA_owncloud/local/owncloud.conf` for editing.
8. Change the `METRICSAPIKEY` setting to the Metrics API key value you configured on the ownCloud Server.
9. Change the `API_HOST` setting to your ownCloud instance domain name or IP address. This value is used to query the Metrics API for data.
10. Save the `$SPLUNK_HOME/etc/apps/TA_owncloud/local/owncloud.conf` file.
11. Restart the Splunk instance.

ownCloud App for Splunk (owncloud_app)

The *ownCloud App for Splunk* (`owncloud_app`) adds the dashboards, visualizations and other functionalities to the Splunk web interface based on the indexed data.

- Install the *ownCloud App for Splunk* from Splunkbase. You only have to install it on Search Heads.
- If you created a custom index for ownCloud data, you have to modify a macro to include this index. You can do this in the Splunk web interface by navigating to **Settings** > **Advanced search** > **Search macros** and changing `owncloud-indexes` to your dedicated index (default: `index=owncloud`).

General Topics

In this section you will find information about:

- [Code Signing](#)
- [Impersonating Users](#)
- [Full Text Search](#)

Code Signing

Introduction

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.

All the possible errors and their explanations can be found [here](#)

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.

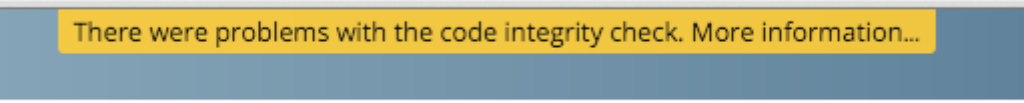
For custom distributions of ownCloud it is recommended to change the release version branch in version.php to something else than "stable".

Is Code Signing Mandatory For Apps?

Code signing is optional for all third-party applications.

Fixing Invalid Code Integrity Messages

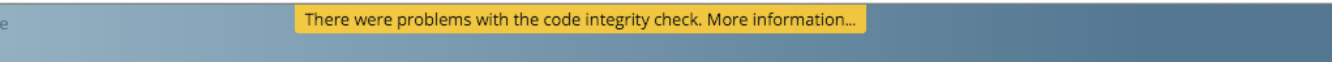
A code integrity error message (There were problems with the code integrity check. More information...) appears in a yellow banner at the top of your ownCloud Web interface:



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.



Security & setup warnings

1

2

3

- Some files have not passed the integrity check. Further information on how to resolve this issue can be found in our documentation. (List of invalid files... / 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] =>
                88a3a92c11db91dec1ac3be0e1c87f862c95ba6ffaaa3f2c3
                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.
        )
    )
[web] => Array
(
    [FILE_MISSING] => Array
        (
            [.htaccess] => Array
                (
                    [expected] =>
85ad7b1b88ad984f11f7f24f84e6aa9935eb75a36c50bf08efdbc5c295e67b3762a1bfacd8f981fb33e5c7
c30d65eff7ebd6a47cb1f0de24e936a71cca2f023e
                    [current] =>
                )
            )
        )
    )
)

```

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.
5. The file `.htaccess` is missing.

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.
5. Download the official server tar ball and copy the `.htaccess` into your instance.

For other means on how to receive support please take a look at the [Docs & Guides page](#). After fixing these problems verify by clicking [**Rescan**].



When using a FTP client to upload those files make sure it is using the **Binary** transfer mode instead of the **ASCII** transfer mode.

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:

```
sudo -u www-data ./occ integrity:check-core
sudo -u www-data ./occ integrity:check-app <appid>
```



See [the occ command](#) to learn more about using `occ`.

Errors

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.
- **FILE_MISSING**
 - 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.

Impersonating Users

Introduction

To help users debug an issue or to get a better understanding of what they see when they use their ownCloud account, you can impersonate their ownCloud user. The ability to do so is a feature delivered via an ownCloud app called [Impersonate](#).

Limitations

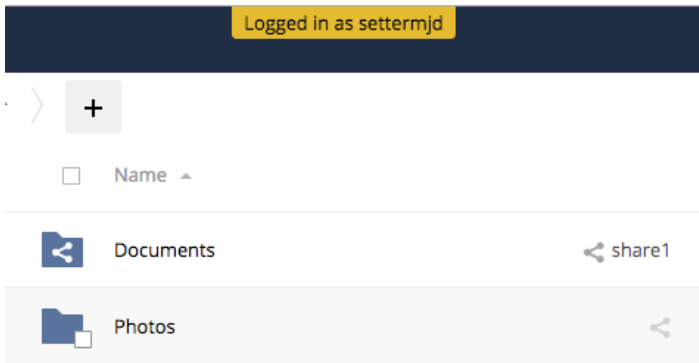
- This functionality is available to administrators only.
- Impersonating is not possible when using Shibboleth or OpenID.

Impersonating a User

When installed, you can then impersonate users; in effect, you will be logged in as a specific 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		settermjd	share1, share2, share3, sha.
share1		share1	no group
share2		share2	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.



Anything that you see until you log out will be what that user would see.

Ending an Impersonation

When you're ready to stop impersonating the user, log out and you will return to your normal user session.

Allow Some or All Group Administrators to Impersonate Users

As a security measure, the application lets ownCloud administrators restrict the ability to impersonate users to:

- All group administrators.
- Specific group administrators.



By default, when the Impersonate app is installed, only the ownCloud administrator will be allowed to impersonate users. When the app is installed and configured, ownCloud administrators retain the ability to impersonate all users of an ownCloud instance.

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.

To configure it, go to the administrator settings panel, which you can find under **User Name > Settings > Admin > User Authentication**. You'll see a section titled: **[Impersonate Settings]**.

- If you want to allow group admins to impersonate users within groups which they administer, click **[Allow all group admins to impersonate users within the groups they are admins of]**.

Impersonate Settings



Allow all group admins to impersonate users within the groups they are admins of



Allow group admins of specific groups to impersonate the users within those groups

- If you want to limit impersonation to specific group admins, first click **[Allow group admins of specific groups to impersonate the users within those groups]**. With the option checked,

click into the textbox underneath it. You will see a list of all groups on your ownCloud installation, which will change, based on what you type in the textbox to search for specific groups.

Impersonate Settings

- Allow all group admins to impersonate users within the groups they are admins of
- Allow group admins of specific groups to impersonate the users within those groups

Choose one or more groups from the list, and they will be added to the textbox, restricting this functionality to only those groups.

Full Text Search

Introduction

ownCloud offers the ability to use full text search via the Full Text Search app connecting to an Elasticsearch Server. This allows users to search not only for file names but also for content within files stored in ownCloud.

The [Full Text Search](#) app integrates full text search into ownCloud, powered by Elasticsearch. This document describes how to setup the ownCloud part of the Full Text Search app.

Prerequisites

1. A fully functioning [Elasticsearch Server 7](#). Follow the [Installation and Upgrade Guide](#) for your environment.



- Version 1.0.0 of the Full Text Search app only works with Elasticsearch version 5.6.
- With version $\geq 2.0.0$ of the app, Elasticsearch version 7 is supported and required.

2. The [Ingest Attachment Processor Plugin](#) lets Elasticsearch extract metadata and text from over a thousand different file types such as PPT, XLS, PDF and more. To install the processor, run the following command from your Elasticsearch installation directory:

```
sudo bin/elasticsearch-plugin install ingest-attachment
```

Post installing the Plugin, you need to restart the Elasticsearch server:

```
sudo service elasticsearch restart
```

Installation

To install the app, use the Marketplace app on your ownCloud server or proceed manually:

1. Download and extract the tarball of the [Full Text Search app](#) to the apps directory (or [custom apps directory, preferred](#)) of your ownCloud instance.
2. Use the [App Commands](#) to enable the `search_elastic` application with:

```
sudo -u www-data ./occ app:enable search_elastic
```

or enable it via the GUI **Settings** › **Admin** › **Apps** › **Full Text Search** › **Enable**.

Configuration

To configure the Full Text Search, go to **Settings** › **Admin** › **Search**.

Authentication Methods

Independent of the authentication method selected below, you need to provide the URL of the Elasticsearch server. For any of the authentication methods selected, your Elasticsearch server must be prepared upfront.

For the URL, both **HTTP** and **HTTPS** including the address and port can be used.

The app provides several authentication methods. Select the one of your choice and check out the details for the respective authentication method below:

Elasticsearch

http://172.17.0.3:9200

Username and Password

No Authentication

Username and Password

API Key

Save Configuration Reset index Scan external storages

8 nodes marked as indexed, 8 documents in index using 133874 bytes

No Authentication

When using **No Authentication**, just fill in the URL of the ES server.

Elasticsearch

No Authentication ▾

Save Configuration Reset index Scan external storages

8 nodes marked as indexed, 8 documents in index using 133874 bytes

User / Password Authentication

When using **User / Password Authentication**, enter the credentials set up on the ES server. Note that the password will be stored encrypted in the ownCloud database.

Elasticsearch

Username and Password ▾

Save Configuration Reset index Scan external storages

8 nodes marked as indexed, 8 documents in index using 133874 bytes

API Key Authentication

When using **API Key Authentication**, enter the API Key with which the ES server was set up.

Elasticsearch

API Key ▾

Save Configuration Reset index Scan external storages

15 nodes marked as indexed, 15 documents in index using 79268 bytes



The API Key needs to be the *encoded* one, **not** the *api_key* string. For details see the [Create API key API](#) at the ES documentation.

Search External Storage

Define if external storage should be included in ES indexing by setting the checkmark accordingly with [**Scan external Storages**].

Save the Configuration

Save the configuration with the [**Save configuration**] button.

Set up the ES Index

When everything is set up, you can click the button **[Setup index]** which will tell the ES server to create the plain empty index and other related internal settings.



This step is important, because the red dot will turn green showing that everything has been set up correctly.

Resetting the ES Index

You can at any time reset the index if required by clicking on **[Reset index]** or with an `occ` command. The index will be recreated afterwards.

```
sudo -u www-data ./occ search:index:reset
```

Using `occ` Commands

You can use the:

- [occ Full Text Search command set](#) to manage the app. These commands let administrators *create*, *rebuild*, *reset*, and *update* the search index. For example, the following command resets and recreates the index for all users:

```
sudo -u www-data ./occ search:index:reset
```

- [occ Config Commands command set](#) to configure the app.

Examples:

List app settings

```
sudo -u www-data ./occ config:list search_elastic
```

```
{
  "apps": {
    "search_elastic": {
      "enabled": "yes",
      "group": "content_searchers",
      "installed_version": "2.1.0",
      "nocontent": "false",
      "scanExternalStorages": "1",
      "servers": "elastic:xxxxxxx@172.17.0.3:9200",
      "types": "filesystem"
    }
  }
}
```

Set app options

```
sudo -u www-data ./occ config:app:set \  
search_elastic scanExternalStorages --value 0
```

or

```
sudo -u www-data ./occ config:app:set \  
search_elastic scanExternalStorages --value 1
```

App Modes

The Full Text Search app provides two modes, which are **active** and **passive**.

Active Mode

After enabling the app, it will be by default in *active mode*

- File changes will be indexed in background jobs. System cron is recommended, otherwise a lot of jobs might queue up.
- Search results will be based on Elasticsearch.
- Search functionality based on ownCloud core database queries will no longer be used.



Active mode can cause a downtime for search when indexing starts on an already heavily used instance, because it takes a while until all files have been indexed.

Passive Mode

To do an initial full indexing without the app interfering, it can be put in *passive mode*

- The administrator can run occ commands changing the search configuration without notice to the users.
- The app will not index any changes by itself.
- Search results will still be based on ownCloud core database queries.

Changing the App Mode

```
sudo -u www-data ./occ config:app:set \  
search_elastic mode --value passive
```

or

```
sudo -u www-data ./occ config:app:set \  
search_elastic mode --value active
```


Restrict Search Results

Index Metadata Only

If you only want to use the Full Text Search app as a more scalable search on filenames, you can disable content indexing by setting the option `nocontent` to `true`, which defaults to `false`:

```
sudo -u www-data ./occ config:app:set \  
  search_elastic nocontent --value true
```



- You have to reindex all files if you change this back to `false`. Setting it to `true` does not require reindexing.
- It may be a more flexible way to go with limiting full text search to certain groups by setting the option `group.nocontent`, see [below](#) for details.

Limit Metadata Search for Groups

If you only want to use search for shared filenames, you can disable full text search for specific groups by setting the option `group.nocontent` to the groups whose users should *only* receive results based on filenames (not the full path), like users in the group `nofulltext` as in the example below:

```
sudo -u www-data ./occ config:app:set \  
  search_elastic group.nocontent \  
  --value nofulltext
```

You can also configure multiple groups by separating them with comma:

```
sudo -u www-data ./occ config:app:set \  
  search_elastic group.nocontent \  
  --value nofulltext,anothergroup,"group with blanks"
```

This allows a scalable search in shared files without clouding the results with content based hits.

Create the Index

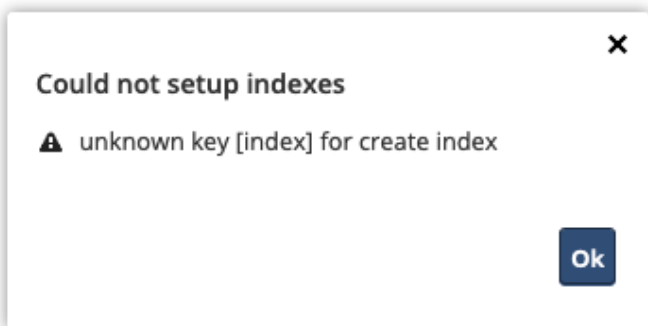
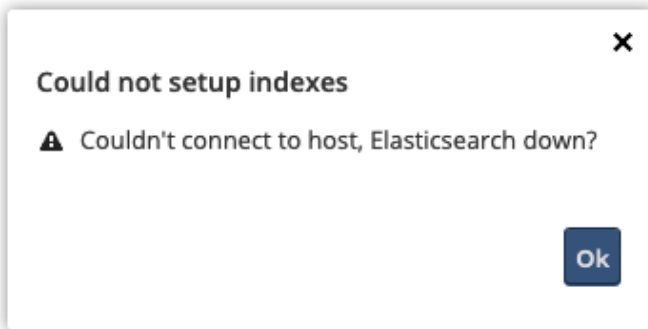
When everything has been set up and configured, you can initiate creating the index. This must be done with an `occ` command. Depending on using *active* or *passive* mode, you either have to:

- **active mode:** wait until the job has finished and search is available to users, or
- **passive mode:** users continue to search with ownCloud embedded search and you switch over to active mode when the `occ` command has finished indexing.

```
sudo -u www-data ./occ search:index:create
```

Issues

When the Elasticsearch server is down or the index has not been set up, you may get the following message. Check if the ES server is reachable or if the index was set up properly as one solution to fix the issue.



User Manual

To find out more about the usage, check out the section in the User Manual: [Search & Full Text Search](#).

Known Limitations

Currently, the app has the following known limitations:

- If a shared file is renamed by the sharee (share receiver), the sharee cannot find the file using the new filename.
- Search results are not updated when a text file is rolled back to an earlier version.
- The app does not return results for received federated share files.
- When using encryption, the app only works with the default **Master Key** encryption module.

Unresolved directive in modules/admin_manual/pages/configuration/server/index.adoc - include::partial\$section_page.adoc[]

Configuring the Activity App

Introduction

You can configure your ownCloud server to automatically send out email notifications to your users for various events.

These events include:

- A file or folder has been shared
- A file or folder has been changed
- A file or folder has been deleted
- A new file or folder has been created

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, go to **Settings › Admin › Apps** to enable it.

Configuring your ownCloud for the Activity App



A working email configuration is required to configure your ownCloud to send out email notifications. Furthermore, it is recommended to configure the [background job](#) `Webcron` or `Cron`.

Email notifications for shared files can be enabled/disabled by administrators with the "*Allow users to send mail notifications for shared files to other users*" option, available in **Settings › Admin › Sharing**. There is also a [configuration option](#) `activity_expire_days` available in your `config.php` which allows you to clean up older activities from the database.

Time Base

- Whenever a default date is enabled and set for expiring shares (e.g. after 7 days), the time base for default dates is the time of the ownCloud server, not the time of the client accessing the ownCloud server.
- When a client receives an expiry notification for a share, the expiry is effective at the end of the day based on the time of the ownCloud server and not the time of the client accessing the ownCloud server.

Background Jobs

Introduction

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. To run Cron jobs with ownCloud, we recommend that you use the `occ system:cron` command.

Use the [occ background command set](#) to select which scheduler you want to use for controlling.

As an example:

```
sudo -u www-data ./occ background:cron
```

Is the same as using the **Cron** section on your ownCloud Admin page.

Docker Note

If you are using the official docker images you don't need to take care about the configuration for background jobs, the docker image is already configured to use cron internally. If required, this can also be adjusted by the [environment variables](#) `OWNCLOUD_CROND_ENABLED` and `OWNCLOUD_CROND_SCHEDULE`.

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:

1. 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.
2. While Webcron is better than AJAX, it has limitations too.
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.



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 15 minutes (recommended), under the default web server user (often, `www-data` or `wwwrun`) you must set up the following Cron job to call the `occ system:cron` command:

```
sudo crontab -u www-data -e
*/15 * * * * /usr/bin/php -f /path/to/your/owncloud/occ system:cron
```

You can verify if the cron job has been added and scheduled by executing:

```
sudo crontab -u www-data -l
*/15 * * * * /usr/bin/php -f /path/to/your/owncloud/occ system:cron
```



You have to make sure that PHP is found by Cron; hence why we've deliberately added the full path.

Please refer to [the crontab man page](#) for the exact command syntax if you don't want to have it run every 15 minutes.



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.



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 `background:cron` multiple times. Depending on the process which you are 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

```
sudo -u www-data ./occ system:cron
```

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.

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.



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 trashbin` command:

```
sudo -u www-data ./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 versions` command:

```
sudo -u www-data ./occ versions:expire
```



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 dav` command:

```
sudo -u www-data ./occ dav:sync-system-addressbook
```

SyncJob (Federation)

`OCAFederationSyncJob`

It can be run, as follows, using the `OCC federation sync` command:

```
sudo -u www-data ./occ federation:sync-addressbooks
```

Troubleshooting

Remove Non-Existent Background Jobs

See the [Remove Non-Existent Background Jobs](#) section in the general troubleshooting documentation for more details.

Forbidden error for `Scanner.php`

If you find a **Forbidden** error message in your log files, with a reference to the `Scanner.php` file, then you should:

- Check if you have any shares with the status `pending`.
- Configure `conditional logging` for cron to see more output.

Memory Caching

Introduction

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 (opcodes) so they don't need to be parsed and compiled every time they are called. These compiled PHP scripts are stored in shared 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.

In addition, we suggest to use **External Transactional File Locking** which reduces load on the database significantly.

Supported Caching Backends

The caching backends supported by ownCloud are:

- [Opcache](#)
This is an opcode cache only and does **not** cache any data. Opcache is bundled with PHP from version 5.5.0 and later.
- [APCu](#)
This is a data cache only and does **not** cache any opcode. APCu 4.0.6 and up is required.
- [Redis](#)
This is an in-memory data structure store (cache) for single and multi-server ownCloud installations, which provides file locking and can be set up in local or distributed environments. Consider Redis younger, richer in features and more configurable than memcached. At least version 2.2.6 or higher of the PHP Redis extension is required.
- [Memcached](#)
This is a distributed cache for multi-server ownCloud installations and has **no** file locking capabilities.

See the following page to learn more about the [Redis vs. Memcached – 2021 Comparison](#).



You may use *both* a local and a distributed cache. The recommended ownCloud caches are APCu and Redis. 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 your configuration for different locations. For details see the [Define the location of the cache folder](#) description.

Cache Types

Opcache

Opcache should be enabled by default in your php installation. To check it, run the following command:

```
php -r 'phpinfo();' | grep opcache.enable
```

APCu

The easiest cache to use is APCu, because it is a pure data cache, very fast as it is memory-based only and *nothing needs to be configured*. APCu can not be used when running on an external server like in a distributed environment.

Installing APCu

On Ubuntu/Debian/Mint systems, if not already done:

```
sudo apt install php-apcu
```

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 performance of Redis when used with a socket connection can get close to the performance of APCu.



The Redis PHP module must be at least version 2.2.6 or higher.

- For Ubuntu 20.04, the default shipped Redis Server version and the php-redis extension is 5.x.
- For Ubuntu 22.04, the default shipped Redis Server version is 6.0.16.
- For Ubuntu 22.04, the php7.4-redis extension has version 5.3.x.
- With Redis version 6, a new authentication mechanism has been introduced named ACL (Access Control Lists). ownCloud does currently not support Redis ACLs, but does support the password protection available with current Redis versions.



Installing Redis

On Ubuntu/Debian/Mint systems, if not already done:

```
sudo apt install redis-server php-redis
```

The installer will automatically launch Redis and configure it to launch at startup.

After that, assuming that you don't encounter any errors, restart Apache and the extension is ready to use.

Redis Performance Consideration

- Because Redis writes data to disk, it is recommended to use a high performance backend like SSD.
- If you do not have a distributed environment where the Redis server is installed at a different machine, you can configure Redis to be [socket-based](#) instead of TCP-based to [increase performance](#).

Additional notes for Redis vs. APCu on Memory Caching

- APCu is faster at local caching than Redis when using TCP since APCu is memory-based only.
- If you have enough memory, use APCu for in memory caching and Redis for file locking.
- If you are limited in memory or only want to have one caching backend, use Redis for both.
- Consider using sockets instead of TCP when you decide on Redis but do not have a distributed caching environment.

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 the Redis database where the cache is stored. It is zero by default at ownCloud. To check what yours is currently set to for ownCloud, check the `dbindex` value in `config/config.php`. To change it, see the [Memory caching backend configuration](#)



Out of the box, every Redis instance supports 16 databases so `<dbIndex>` has to be set between 0 and 15.

Please read more about the instructions for the [select](#) and [flushdb](#) command.

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.



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 Ubuntu/Debian/Mint

On Ubuntu/Debian/Mint run the following command:

```
sudo apt-get install memcached php-memcached
```



The installer will automatically start **memcached** and configure it to launch at startup.

Configuration File Paths

PHP Version	Filename
7.4	<code>/etc/php/7.4/mods-available/memcached.ini</code>

Note that the PHP version depends on your environment.

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 log in, run the [flush_all command](#), and log out:

```
telnet localhost 11211
flush_all
quit
```

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 the [Memory caching backend configuration](#) for an overview of all possible config parameters, as the examples below only show basic configuration settings. After installing and enabling your chosen memory cache, verify that it is active by viewing the [PHP configuration details](#).

OpCache Configuration

OpCache should already be configured with PHP 7, see the [opcache documentation](#) for details.

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

Redis is very configurable; consult the [Redis documentation](#) to learn more.

Regardless of whether you have set up Redis to use TCP or a Unix socket, we recommend adding the following for best performance. This enables [External Transactional File Locking](#) based on Redis:

```
'filelocking.enabled' => true,  
'memcache.locking' => '\OC\Memcache\Redis',
```

Redis Configuration Using TCP

The following example `config.php` configuration connects to a Redis cache via TCP:

```
'memcache.local' => '\OC\Memcache\Redis',  
'redis' => [  
    'host' => 'localhost', // For a Unix domain socket, use  
    '/var/run/redis/redis.sock'  
    'port' => 6379, // Set to 0 when using a Unix socket  
    'timeout' => 0, // Optional, keep connection open forever  
    '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.  
],
```

Redis Configuration Using Unix Sockets

If Redis is running on the same server as ownCloud, it is recommended to configure it to use Unix sockets for increased performance. Follow these steps to do so:

1. Add the `www-data` user to the `redis` group:

```
sudo usermod -G redis -a www-data
```

2. Create your Redis folder that the Unix socket will be in:

```
sudo mkdir -p /var/run/redis/
```

3. Set the permissions so the `redis` user and `www-data` group own it:

```
sudo chown -R redis:www-data /var/run/redis
```

4. Open an editor of your choice and change/add the following parameters to the Redis configuration file. Note that in the example `vi` is used as editor:

```
sudo vi /etc/redis/redis.conf
```

```
# create a unix domain socket to listen on
unixsocket /var/run/redis/redis.sock

# set permissions for the socket
unixsocketperm 770
```

5. Restart Redis to make the changes effective:

```
sudo service redis-server restart
```

6. Check if the Redis Unix socket was created:

```
ls -lh /var/run/redis
```

The output should be like the following:

```
srwxrwx--- 1 redis redis 0 May 12 12:26 redis.sock
```

Then, configure ownCloud to communicate with the Redis socket as in the following example.

```
# Change the host value, based on the socket's location in your distribution
'memcache.local' => '\OC\Memcache\Redis',
'redis' => [
  'host' => '/var/run/redis/redis.sock',
  'port' => 0,          // Set to 0 when using a Unix socket
  '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.
],
```

Redis Performance Comparison TCP vs Socket

To see a benchmark comparison, run:

```
sudo redis-benchmark -q -n 100000
sudo redis-benchmark -s /var/run/redis/redis-server.sock -q -n 100000
```

In the following table, you will see an example gain of about +20% when using sockets compared to TCP on localhost. The values can differ in your environment. Please do a local check.

Test	TCP (requests/s)	Socket (requests/s)	Gain (%)
PING_INLINE	15527.95	23518.35	+34
PING_BULK	16946.28	23239.60	+27
SET	18351.99	22789.43	+19
GET	18850.14	22747.95	+17
INCR	18663.68	22914.76	+18
LPUSH	19109.50	24183.79	+21
RPUSH	19076.69	23196.47	+18
LPOP	18460.40	23485.21	+21
RPOP	19058.51	24752.47	+23
SADD	18932.22	22391.40	+15
HSET	18491.12	20785.70	+11
SPOP	19069.41	23282.89	+18
LPUSH	19087.61	23764.26	+20
LRANGE_100	15288.18	17882.69	+15
LRANGE_300	9067.00	10004.00	+10
LRANGE_500	6878.53	7496.25	+8
LRANGE_600	5379.24	6102.77	+12

Test	TCP (requests/s)	Socket (requests/s)	Gain (%)
MSET (10 keys)	19297.57	18178.51	-6

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],
],
```

Configure Transactional File Locking

[Transactional File Locking](#) prevents simultaneous file saving. It is enabled by default and uses the database to store the locking data. This places a significant load on your database. It is recommended to use a cache backend instead. You have to configure it in `config.php` as in the following example, which uses Redis TCP as the cache backend:

```
'filelocking.enabled' => true,
'memcache.locking' => '\OC\Memcache\Redis',
'redis' => [
    'host' => 'localhost',
    'port' => 6379,
    'timeout' => 0,
    'password' => '', // Optional, if not defined no password will be used.
],
```



For enhanced security, it is recommended to configure Redis to require a password. See <https://redis.io/topics/security> for more information.

Configuration Recommendations Based on Type of Deployment

The examples give you an overview, adapt them to your environment and your needs.

Private Home Server With Low Access Rates

Use APCu for local caching, file locking is not mandatory.

```
'memcache.local' => '\OC\Memcache\APCu',
```

Small Server

Use APCu for local caching and Redis for file locking.

```
'filelocking.enabled' => true,
'memcache.local' => '\OC\Memcache\APCu',
'memcache.locking' => '\OC\Memcache\Redis',
'redis' => [
    'host' => 'localhost',
    'port' => 6379,
],
```

Small Organization, Single-server Setup

Use Redis Socket for local caching and for file locking.

```
'filelocking.enabled' => true,
'memcache.local' => '\OC\Memcache\Redis',
'memcache.locking' => '\OC\Memcache\Redis',
'redis' => [
    'host' => '/var/run/redis/redis.sock',
    'port' => 0,
],
```

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:

```
'filelocking.enabled' => true,
'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,
],
```

See [Define Redis Cluster connection details](#) when using a Redis clustered setup.

Caching Exceptions

If ownCloud is configured to use either Memcached or Redis as a memory cache, 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 <code>local</code> and <code>distributed</code> , 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

Config.php Parameters

Introduction

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`.



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.

Unique identifier for your ownCloud installation

This unique identifier is 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. Needs to start with a letter.

```
'instanceid' => 'd3c944a9a',
```

Code Sample

```
'instanceid' => '',
```

Auto-generated salt used to hash all passwords

The salt used to hash all passwords and is 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.

Code Sample

```
'passwordsalt' => '',
```

Define 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.

Code Sample

```
'trusted_domains' => [  
    'demo.example.org',  
    'otherdomain.example.org',  
],
```

Define global list of CORS domains

All users can use tools running CORS (Cross-Origin Resource Sharing) requests from the listed domains.

Code Sample

```
'cors.allowed-domains' => [  
    'https://foo.example.org',  
],
```

Define the directory 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)

Code Sample

```
'datadirectory' => '/var/www/owncloud/data',
```

Define the directory where the crash logs will be stored

By default, this will be the same as the one configured as "datadirectory".

The directory MUST EXIST and be WRITABLE by the web server. Note that crashes are extremely rare (although they can come in burst due to multiple requests), so the default location is usually fine. Also note that the log can contain sensitive information, but it should be useful to pinpoint where is the problem.

Code Sample

```
'crashdirectory' => '/var/www/owncloud/data',
```

Current version number of your ownCloud installation

This is set up during installation and update, so you shouldn't need to change it.

Code Sample

```
'version' => '',
```

Show or hide the ownCloud version information in `status.php`

This hardens an ownCloud instance by hiding the version information in `status.php`.

This can be a legitimate step. Please consult the documentation before enabling this.

Code Sample

```
'version.hide' => false,
```

Show or hide the server hostname in `status.php`

Optional config option, defaults to hidden.

Code Sample

```
'show_server_hostname' => false,
```

Show the short hostname in `status.php`

Optional config option, defaults to use the `gethostname()` return value.

Code Sample

```
'use_relative_domain_name' => false,
```

Identify 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)

Code Sample

```
'dbtype' => 'mysql',
```

Define the database server host 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`.

Code Sample

```
'dbhost' => '',
```

Define the ownCloud database name

The name of the ownCloud database which is set during installation.

You should not need to change this.

Code Sample

```
'dbname' => 'owncloud',
```

Define the ownCloud database user

This must be unique across ownCloud instances using the same SQL database.

This is setup during installation, so you shouldn't need to change it.

Code Sample

```
'dbuser' => '',
```

Define the password for the database user

This is set up during installation, so you shouldn't need to change it.

Code Sample

```
'dbpassword' => '',
```

Define the prefix for the ownCloud tables in the database

Code Sample

```
'dbtableprefix' => '',
```

Indicate whether the ownCloud instance was installed successfully

`true` indicates a successful installation, `false` indicates an unsuccessful installation.

Code Sample

```
'installed' => false,
```

User Experience

These optional parameters control some aspects of the user interface. Default values, where present, are shown.

Define the default language of your ownCloud instance

Using ISO_639-1 language codes such as `en` for English, `de` for German, and `fr` for French.

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.

Code Sample

```
'default_language' => 'en_GB',
```

Define the default app to open on user login

Use the app names as they appear in the URL after clicking them in the Apps menu, such as `files`,

documents or calendar etc. 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.

Code Sample

```
'defaultapp' => 'files',
```

Enable or disable avatars or user profile photos

`true` enables avatars, or user profile photos, `false` disables them.

These appear on the User page, on user's Personal pages and are used by some apps (contacts, mail, etc).

Code Sample

```
'enable_avatars' => true,
```

Allow or disallow users to change their display names

`true` allows users to change their display names (on their Personal pages), `false` prevents them from changing their display names.

Code Sample

```
'allow_user_to_change_display_name' => true,
```

Allow or disallow users to change their email addresses

`true` allows users to change their email address (on their Personal pages), `false` prevents them from changing their email address.

Code Sample

```
'allow_user_to_change_mail_address' => true,
```

Define the lifetime of the remember-login cookie

The remember-login cookie is set when the user clicks the `remember` checkbox on the login screen. The default is 15 days, expressed in seconds.

Code Sample

```
'remember_login_cookie_lifetime' => 60*60*24*15,
```

Define the lifetime of a session after inactivity

The web UI might send a "heartbeat" based on the activity happening in order to extend the session lifetime and keeping it from timing out prematurely. If there is no activity happening and the lifetime is reached, you'll have to login again.

The default is 20 minutes, expressed in seconds.

Code Sample

```
'session_lifetime' => 60 * 20,
```

Enable 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 regardless of any activity happening. This heartbeat will keep extending the session over again, so the user won't be logged out even if he isn't active in the web UI.

Code Sample

```
'session_keepalive' => true,
```

Enforce token only authentication for apps and clients connecting to ownCloud

If enabled, all access requests using the user's 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.

Code Sample

```
'token_auth_enforced' => false,
```

Enforce strict login check with user backend

If enabled, strict login check for password in user backend will be enforced, meaning only the login name typed by the user would be validated. With this configuration enabled, e.g. an additional check for email will not be performed.

Code Sample

```
'strict_login_enforced' => false,
```

Define additional login buttons on the logon screen

Provides the ability to create additional login buttons on the logon screen, for e.g., SSO integration

```
'logon.alternatives' => [ [ 'label', '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'], ]
```

Code Sample

```
'login.alternatives' => [],
```

Enable or 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.



leave this as is if you're not sure what it does.

Code Sample

```
'csrf.disabled' => false,
```

Define how to relax same site cookie settings

Possible values: *Strict*, *Lax* or *None*.

Setting the same site cookie to *None* is necessary in case of OpenID Connect. For more information about the impact of the values see: <https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Set-Cookie/SameSite#values> and <https://web.dev/schemeful-samesite/>

- Use 'strict' whenever possible
- If necessary relax to 'lax'
- Use 'none' if it needs to be relaxed even further

Code Sample

```
'http.cookie.samesite' => 'Strict',
```

Define the directory where the skeleton files are located

These files will be copied to the data directory of new users.

Set this to the empty string if you do not want to copy any skeleton files. A valid path must be given for this key otherwise errors will be generated in owncloud.log.

Code Sample

```
'skeletondirectory' => '/path/to/owncloud/core/skeleton',
```

Define the `user_backends` app

Those need to be enabled first and allow you to configure alternate authentication backends.

Supported backends are: IMAP (OC_User_IMAP), SMB (OC_User_SMB), and FTP (OC_User_FTP).

Code Sample

```
'user_backends' => [  
  [  
    'class' => 'OC_User_IMAP',  
    'arguments' => ['{imap.gmail.com:993/imap/ssl}INBOX']  
  ]  
],
```

Define a custom link to reset passwords

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.

If you do not want to provide any link, replace the URL with 'disabled'.

Code Sample

```
'lost_password_link' => 'https://example.org/link/to/password/reset',
```

Allow medial search on user account properties

These account properties can be 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.

Code Sample

```
'accounts.enable_medial_search' => true,
```

Allow medial search on the group id

Allows finding 'test' in groups when searching for 'es'.

This is only used in the DB group backend (local groups). This won't be used against LDAP,

Shibboleth or any other group backend.

Code Sample

```
'groups.enable_medial_search' => true,
```

Define minimum characters entered before a search returns results

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. For example, entering "tom" will always return "Tom" if there is an exact match.

Code Sample

```
'user.search_min_length' => 2,
```

Mail Parameters

These configure the email settings for ownCloud notifications and password resets.

Define the email RETURN address

The return address that you want to appear on emails sent by the ownCloud server.

Example: `oc-admin@example.com`, substituting your own domain, of course.

Code Sample

```
'mail_domain' => 'example.com',
```

Define the email FROM address

The FROM address that overrides the built-in `sharing-noreply` and `lostpassword-noreply` FROM addresses.

Code Sample

```
'mail_from_address' => 'owncloud',
```

Enable or disable SMTP class debugging

Code Sample

```
'mail_smtpdebug' => false,
```

Define the mode for sending an email

Modes 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.

Code Sample

```
'mail_smtpmode' => 'sendmail',
```

Define the IP address of your mail server host

Depends on `mail_smtpmode`. 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`.

Code Sample

```
'mail_smtphost' => '127.0.0.1',
```

Define the port for sending an email

Depends on `mail_smtpmode`.

Code Sample

```
'mail_smtpport' => 25,
```

Define the SMTP server timeout

Depends on `mail_smtpmode`. Sets the SMTP server timeout in seconds.

You may need to increase this if you are running an anti-malware or spam scanner.

Code Sample

```
'mail_smtptimeout' => 10,
```

Define the SMTP security style

Depends on `mail_smtpmode`. Specify when you are using `ssl` or `tls`.

Leave empty for no encryption.

Code Sample

```
'mail_smtpsecure' => '',
```

Define the SMTP authentication

Depends on `mail_smtpmode`. Change this to `true` if your mail server requires authentication.

Code Sample

```
'mail_smtpauth' => false,
```

Define the SMTP authentication type

Depends on `mail_smtpmode`. If SMTP authentication is required, choose the authentication type as `LOGIN` (default) or `PLAIN`.

Code Sample

```
'mail_smtpauthtype' => 'LOGIN',
```

Define the SMTP authentication username

Depends on `mail_smtpauth`. Specify the username for authenticating to the SMTP server.

Code Sample

```
'mail_smtpname' => '',
```

Define the SMTP authentication password

Depends on `mail_smtpauth`. Specify the password for authenticating to the SMTP server.

Code Sample

```
'mail_smtppassword' => '',
```

Proxy Configurations

Override automatic proxy detection

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`.

Code Sample

```
'overwritehost' => '',
```

Override protocol (http/https) usage

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`.

Code Sample

```
'overwriteprotocol' => '',
```

Override ownClouds webroot

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.

Code Sample

```
'overwritewebroot' => '',
```

Override condition for the remote IP address with a regular expression

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]$`

Code Sample

```
'overwritecondaddr' => '',
```

Override 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, they will be redirected to that URL and must logon again.

Code Sample

```
'overwrite.cli.url' => '',
```

Define the Web base URL

This key is necessary for the navigation item to the new ownCloud Web UI and for redirecting public and private links.

Code Sample

```
'web.baseUrl' => '',
```

Define rewrite private and public links

Rewrite private and public links to the new ownCloud Web UI (if available).

If `web.rewriteLinks` is set to 'true', public and private links will be redirected to this url. The Web UI will handle these links accordingly.

As an example, in case `'web.baseUrl'` is set to `'http://web.example.com'`, the shared link `'http://ocx.example.com/index.php/s/THoQjwYYMJvXMdW'` will be redirected by ownCloud to `'http://web.example.com/index.html#/s/THoQjwYYMJvXMdW'`.

Code Sample

```
'web.rewriteLinks' => false,
```

Define clean URLs without `/index.php`

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 `sudo -u www-data ./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

Code Sample

```
'htaccess.RewriteBase' => '/',
```

Define the URL of your proxy server

Example: `proxy.example.com:8081`.

Code Sample

```
'proxy' => '',
```

Define proxy authentication

The optional authentication for the proxy to use to connect to the internet.

The format is: `username:password`.

The username and the password need to be urlencoded to avoid breaking the delimiter syntax "username:password@hostname:port"

Example: `usern@me` needs to be encoded as `usern%40ame`.

Code Sample

```
'proxyuserpwd' => '',
```

Deleted Items (trash bin)

These parameters control the Deleted files app.

Define the trashbin retention obligation

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

Code Sample

```
'trashbin_retention_obligation' => 'auto',
```

Define the trashbin purge limit

This setting defines the percentage of free space occupied by deleted files that triggers auto purging of deleted files for this user

Code Sample

```
'trashbin_purge_limit' => 50,
```

Define trashbin directory skip list

Define a list of directories that will skip the trashbin and therefore be deleted immediately.

Only defined directories and only in the root of a mount will skip the trashbin. Consider not to use

reserved directory names when using snapshot capable storage systems. The setting expects folder names with or without trailing slash. All the content of such directories including their subdirectories will also skip the trashbin.

Code Sample

```
'trashbin_skip_directories' => [  
    'temp',  
],
```

Define trashbin file extension skip list

Define a list of file extensions to determine files that will skip the trashbin and therefore be deleted immediately.

Extension names are valid for all mount points, take care when selecting the names.

Values must not have a leading ".", otherwise corresponding files won't be detected. Values are case-insensitive

Code Sample

```
'trashbin_skip_extensions' => [  
    'iso',  
    'mkv',  
],
```

Define trashbin threshold size

Define a threshold for files to skip the trashbin and delete immediately. Once the size of a resource is greater than or equal the given value, the trashbin will be skipped.

File sizes are valid for all mount points, take care when defining the threshold.

All positive numbers and zero is allowed. Append one of the following options directly and without space: B, K, KB, MB, M, GB, G, TB, T, PB, P

Code Sample

```
'trashbin_skip_size_threshold' => "1GB",
```

File versions

These parameters control the Versions app.

Define the files versions retention obligation

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 https://doc.owncloud.com/server/latest/admin_manual/configuration/files/file_versioning.html 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

Code Sample

```
'versions_retention_obligation' => 'auto',
```

ownCloud Verifications

ownCloud performs several verification checks. There are two options, **true** and **false**.

Enable or disable updatechecker

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.

Code Sample

```
'updatechecker' => true,
```

Define the updatechecker URL

The URL that ownCloud should use to look for updates

Code Sample

```
'updater.server.url' => 'https://updates.owncloud.com/server/',
```

Check for an internet connection

Is ownCloud connected to the Internet or running in a closed network?

Code Sample

```
'has_internet_connection' => true,
```

Check for a .well-known setup

Allows ownCloud to verify a working .well-known URL redirect.

This is done by attempting to make a request from JS to <https://your-domain.com/.well-known/caldav/>

Code Sample

```
'check_for_working_wellknown_setup' => true,
```

Define if config.php is read only

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.

Code Sample

```
'config_is_read_only' => false,
```

Define ownCloud operation modes

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 impacts on the behavior of ownCloud.

The primary impact is, that clustered instances won't download apps from the marketplace and install in one server. Instead the admin has to ensure that this happens manually on all servers. The same applies to config.php configuration settings done via `occ`.

Code Sample

```
'operation.mode' => 'single-instance',
```

Logging

These parameters configure the logging options. For additional information or advanced configuration, please see the logging section in the documentation.

Define the log type

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.

Code Sample

```
'log_type' => 'owncloud',
```

Define the log path

Log file path for the ownCloud logging type.

Defaults to `[datadirectory]/owncloud.log`

Code Sample

```
'logfile' => '/var/log/owncloud.log',
```

Define the log level

Loglevel to start logging at. Valid values are: 0 = Debug, 1 = Info, 2 = Warning, 3 = Error, and 4 = Fatal. The default value is Warning.

Code Sample

```
'loglevel' => 2,
```

Define the syslog tag

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`.

Code Sample

```
'syslog_tag' => 'ownCloud',
```

Define the syslog format

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.

Code Sample

```
'log.syslog.format' => "[%reqId%][%remoteAddr%][%user%][%app%][%method%][%url%]  
%message%",
```

Define log conditions

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

Code Sample

```
'log.conditions' => [  
  [  
    'shared_secret' => '57b58edb6637fe3059b3595cf9c41b9',  
    'users' => ['user1'],  
    'apps' => ['files_texteditor'],  
    'logfile' => '/tmp/test.log'  
  ],  
  [  
    'shared_secret' => '57b58edb6637fe3059b3595cf9c41b9',  
    'users' => ['user1'],  
    'apps' => ['files_mediaviewer'],  
    'logfile' => '/tmp/mediaviewer.log'  
  ],  
],
```

Define the log date format

This uses PHP.date formatting; see <http://php.net/manual/en/function.date.php>

Code Sample

```
'logdateformat' => 'F d, Y H:i:s',
```

Define the log timezone

The default timezone for logfiles is UTC. You may change this; see <http://php.net/manual/en/timezones.php>

Code Sample

```
'logtimezone' => 'Europe/Berlin',
```

Define logging if Cron ran successfully

Log successful cron runs.

Code Sample

```
'cron_log' => true,
```

Define the maximum log rotation file size

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.

Code Sample

```
'log_rotate_size' => false,
```

Alternate Code Locations

Some of the ownCloud code may be stored in alternate locations.

Define alternative app directories

If you want to store apps in a custom directory instead of ownCloud's default `/apps`, 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.

Code Sample

```
'apps_paths' => [
  0 =>
    [
      'path' => OC::$SERVERROOT.'/apps',
      'url' => '/apps',
      'writable' => false,
    ],
  1 =>
    [
      'path' => OC::$SERVERROOT.'/apps-external',
      'url' => '/apps-external',
      'writable' => true,
    ],
],
```

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 preview generation

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

Code Sample

```
'enable_previews' => true,
```

Define the preview path

Location of the thumbnails folder, defaults to `data/$user/thumbnails` where `$user` is the current user. When specified, the format will change to `$previews_path/$user` where `$previews_path` is the configured previews base directory and `$user` will be substituted with the user id automatically.

For example if `previews_path` is `/var/cache/owncloud/thumbnails` then for a logged-in user `user1` the thumbnail path will be `/var/cache/owncloud/thumbnails/user1`.

Code Sample

```
'previews_path' => '',
```

Define the maximum x-axis width for previews

The maximum width, in pixels, of a preview.

A value of `null` means there is no limit.

Code Sample

```
'preview_max_x' => 2048,
```

Define the maximum y-axis width for previews

The maximum height, in pixels, of a preview. A value of `null` means there is no limit.

Code Sample

```
'preview_max_y' => 2048,
```

Define the maximum preview 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. A value of `1` or `null` disables scaling.

Code Sample

```
'preview_max_scale_factor' => 10,
```

Define the maximum preview filesize limit

Max file size for generating image previews with `imagegd` (default behaviour) If the image is bigger, it will 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.

Code Sample

```
'preview_max_filesize_image' => 50,
```

Define the custom path for the LibreOffice / OpenOffice binary

Code Sample

```
'preview_libreoffice_path' => '/usr/bin/libreoffice',
```

Define additional arguments for LibreOffice / OpenOffice

Use this setting if LibreOffice/OpenOffice requires additional arguments.

Code Sample

```
'preview_office_cl_parameters' =>  
  '--headless --nologo --nofirststartwizard --invisible --norestore ',  
  '--convert-to pdf --outdir ',
```

Define preview providers

Show thumbnails for register providers that have been explicitly enabled.

The following providers are enabled by default if no other providers are selected:

- OC\Preview\PNG
- OC\Preview\JPEG
- OC\Preview\WEBP
- OC\Preview\GIF
- OC\Preview\BMP
- OC\Preview\XBitmap
- OC\Preview\Markdown
- OC\Preview\MP3
- OC\Preview\TXT

See the Previews Configuration documentation for more details.

Code Sample

```
'enabledPreviewProviders' => [  
  'OC\Preview\PDF',  
  'OC\Preview\SGI',  
  'OC\Preview\Heic',
```

```
'OC\Preview\PNG',  
'OC\Preview\JPEG',  
'OC\Preview\WEBP',  
'OC\Preview\GIF',  
'OC\Preview\BMP',  
'OC\Preview\XBitmap',  
'OC\Preview\MP3',  
'OC\Preview\TXT',  
'OC\Preview\Markdown'  
],
```

Define the jpeg preview quality

This setting defines the JP(E)G image quality in [%] for displaying thumbnails and image previews for apps like 'files_mediaviewer'. Note that this setting is for displaying only and has no impact on the stored thumbnail / preview quality or size.

The scale ranges from 1 to 100, where 1 is the lowest and 100 the highest. It defaults to -1 which is equivalent to approximately 75% of the original image quality.

Note that any value over 80 may result in an unnecessary increase of the displayed image and has larger responses sizes when requesting images, without much increase of the image quality.

For more information see: <https://www.php.net/manual/en/function.imagejpeg.php>

Code Sample

```
'previewJpegImageDisplayQuality' => -1,
```

Comments

Global settings for the Comments infrastructure

Define an alternative Comments Manager

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.

Code Sample

```
'comments.managerFactory' => '\OC\Comments\ManagerFactory',
```

Define an alternative System Tags Manager

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.

Code Sample

```
'systemtags.managerFactory' => '\\0C\SystemTag\ManagerFactory',
```

Maintenance

These options are for halting user activity when you are performing server maintenance.

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.

Code Sample

```
'maintenance' => false,
```

Enable or disable single user mode

When set to true, the ownCloud instance will be unavailable for all users who are not in the admin group.

Code Sample

```
'singleuser' => false,
```

SSL

Extra SSL options to be used for configuration

Code Sample

```
'openssl' => [  
  'config' => '/absolute/location/of/openssl.cnf',  
],
```

Allow the configuration of system-wide trusted certificates

Code Sample

```
'enable_certificate_management' => false,
```

Memory caching backend configuration

Available cache backends:

- `\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

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.

Memory caching backend for locally stored data

- Used for host-specific data, e.g. file paths

Code Sample

```
'memcache.local' => '\OC\Memcache\APCu',
```

Memory caching backend for distributed data

- Used for installation-specific data, e.g. database caching
- If unset, defaults to the value of `memcache.local`

Code Sample

```
'memcache.distributed' => '\OC\Memcache\Memcached',
```

Define Redis connection details

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.

Code Sample

```
'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 Index. Out of the box, every Redis instance supports 16 databases
so '<dbIndex>' has to be set between 0 and 15.
// Optional config option
// In order to use connection_parameters php-redis extension >= 5.3.0 is required
// In order to use SSL/TLS redis server >= 6.0 is required
// In a single-server configuration, prefix the host with tls:// like
tls://localhost
// In a single-server configuration the SSL/TLS data **must** be in the stream
section
'connection_parameters' => [
    'stream' => [
        'local_cert' => '/file/path/to/redis.crt',
        'local_pk' => '/file/path/to/redis.key',
        'cafile' => '/file/path/to/ca.crt',
        'verify_peer_name' => true
    ],
],
],

```

Define Redis Cluster connection details

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 primary nodes (default) - \RedisCluster::FAILOVER_ERROR - failover to replicas for read commands if primary is unavailable - \RedisCluster::FAILOVER_DISTRIBUTE - randomly distribute read commands across primary and replica nodes

Code Sample

```

'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,
    'password' => '', // Optional, if not defined no password will be used.
// Optional config option
// In order to use connection_parameters php-redis extension >= 5.3.0 is required
// In order to use SSL/TLS redis server >= 6.0 is required
// In a cluster configuration, prefix the seeds with tls:// like
tls://localhost:7000

```

```

    // In a cluster configuration the SSL/TLS data **must not** be in the stream
    section
    'connection_parameters' => [
        'local_cert' => '/file/path/to/redis.crt',
        'local_pk' => '/file/path/to/redis.key',
        'cafile' => '/file/path/to/ca.crt',
        'verify_peer_name' => true
    ],
],

```

Define server details for memcached servers to use for memory caching

Server details for one or more memcached servers to use for memory caching

Code Sample

```

'memcached_servers' => [
    // 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
    ['localhost', 11211],
    //[other.host.local', 11211],
],

```

Define connection options for memcached

For more details please see <http://apprize.info/php/scaling/15.html>

Code Sample

```

'memcached_options' => [
    // 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,

```

```
],
```

Define the location of the cache folder

The 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.

Code Sample

```
'cache_path' => '',
```

Define the TTL for garbage collection

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.

Code Sample

```
'cache_chunk_gc_ttl' => 86400, // 60*60*24 = 1 day
```

Define the DAV chunk base directory

Location of the chunk folder, defaults to `<datadirectory>/$user/uploads` where `$user` is the current user and `datadirectory` is the datadirectory described here.

When specified, the format will change to `$dav.chunk_base_dir/$user` where `$dav.chunk_base_dir` is the configured cache directory here and `$user` is the user.

Code Sample

```
'dav.chunk_base_dir' => '',
```

Sharing

Global settings for Sharing

Define an alternative Share Provider

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.

Code Sample

```
'sharing.managerFactory' => '\0C\Share20\ProviderFactory',
```

Allow schema fallback for federated sharing servers

When talking with federated sharing server, allow falling back to HTTP instead of hard forcing HTTPS

Code Sample

```
'sharing.federation.allowHttpFallback' => false,
```

Show a quick action for the public link creation

Set this to true to display a quick action for creating public links in the filelist. A public link created this way will be read-only per default.

Note: if enforced password protection for read-only links is enabled, the quick action will not be displayed!

Code Sample

```
'sharing.showPublicLinkQuickAction' => false,
```

Save and display the author of each version of uploaded and edited files.



This does not work for S3 storage backends.

Code Sample

```
'file_storage.save_version_author' => false,
```

All other configuration options

Define additional database driver options

Additional driver options for the database connection, e.g. to enable SSL encryption in MySQL or specify a custom wait timeout on a cheap hoster.

Code Sample

```
'dbdriveroptions' => [  
  PDO::MYSQL_ATTR_SSL_CA => '/file/path/to/ca_cert.pem',  
  PDO::MYSQL_ATTR_INIT_COMMAND => 'SET wait_timeout = 28800'  
],
```


Define sqlite3 journal mode

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>

Code Sample

```
'sqlite.journal_mode' => 'DELETE',
```

Define MySQL 3/4 byte character handling

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: `sudo -u www-data ./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/benchmarking-innodb-page-compression-performance.html> <https://titanwolf.org/Network/Articles/Article?AID=58c487d4-7e0f-4fbe-9262-4285553ef443> (Using innodb_large_prefix to avoid ERROR 1071)

Code Sample

```
'mysql.utf8mb4' => false,
```

Force a specific database platform class

False means that autodetection will take place.

E.g. to fix MariaDB 1.2.7+ taken for MySQL 'db.platform' ⇒ `\Doctrine\DBAL\Platforms\MariaDb1027Platform'`

See: <https://docs.microsoft.com/en-us/azure/mariadb/concepts-limits#current-known-issues>

Code Sample

```
'db.platform' => false,
```

Define supported database types

Database types that are supported for installation.

Available: - sqlite (SQLite3 - Not in Enterprise Edition) - mysql (MySQL) - pgsq (PostgreSQL) - oci (Oracle - Enterprise Edition Only)

Code Sample

```
'supportedDatabases' => [  
  'sqlite',  
  'mysql',  
  'pgsq',  
  'oci',  
],
```

Define the location for temporary files

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.

Code Sample

```
'tempdirectory' => '/tmp/owncloudtemp',
```

Define the hashing cost

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.

Code Sample

```
'hashingCost' => 10,
```

Define blacklisted files

Blacklist a specific file or files and disallow the upload of files with this name. `.htaccess` is blocked by default.



USE THIS ONLY IF YOU KNOW WHAT YOU ARE DOING.

Code Sample

```
'blacklisted_files' => [  
  '.htaccess'  
],
```

Define blacklisted files regular expression(s)

Blacklist files that match any of the given regular expressions and disallow the upload of those files. The matching is case-insensitive.



USE THIS ONLY IF YOU KNOW WHAT YOU ARE DOING.

Code Sample

```
'blacklisted_files_regex' => [  
  '.*\.ext',  
  '^somefilename.*'  
],
```

Define excluded directories

Exclude specific directory names and disallow scanning, creating and renaming using these names. The matching is 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, e.g. snapshot directories to be excluded.



USE THIS ONLY IF YOU KNOW WHAT YOU ARE DOING.

Code Sample

```
'excluded_directories' => [  
  '.snapshot',  
  '~snapshot',  
],
```

Define excluded directories regular expression(s)

Exclude directory names that match any of the given regular expressions and disallow scanning, creating and renaming using these names. The matching is 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, e.g. snapshot directories to be excluded.



USE THIS ONLY IF YOU KNOW WHAT YOU ARE DOING.

Code Sample

```
'excluded_directories_regex' => [  
  '^backup.*',  
  '.*backup$',  
],
```

Define files that are excluded from integrity checking

Exclude files from the integrity checker command

Code Sample

```
'integrity.excluded.files' => [  
  '.DS_Store',  
  'Thumbs.db',  
  '.directory',  
  '.webapp',  
  '.htaccess',  
  '.user.ini',  
],
```

Define apps or themes that are excluded from integrity checking

The list of apps that are allowed and must not have a signature.json file present.

Besides ownCloud apps, this is particularly useful when creating ownCloud themes, because themes are treated as apps. The app is identified with its app-id. The app-id can be identified by the foldername of the app in your apps directory. The following example allows app-1 and theme-2 to have no signature.json file.

Code Sample

```
'integrity.ignore.missing.app.signature' => [  
  'app-id of app-1',  
  'app-id of theme-2',  
],
```

```
],
```

Define a default folder for shared files and folders other than root

Code Sample

```
'share_folder' => '/',
```

Define the default cipher for encrypting files

Currently AES-128-CFB and AES-256-CFB are supported.

Code Sample

```
'cipher' => 'AES-256-CFB',
```

Define the file format for encrypting files

Define if encrypted files will be written in the old format (**true**) or the new binary format (**false**) which has a significant reduced filesize. Defaults to **false**.

With binary, only new files are written in the binary format, existing encrypted files in the old format stay readable. This guarantees a smooth transition.

Code Sample

```
'encryption.use_legacy_encoding' => false,
```

Define the minimum supported ownCloud desktop client version

Define the minimum ownCloud desktop client version that is allowed to sync with this server instance. All connections made from earlier clients will be denied by the server.

As shipped, the value here is the oldest desktop client that is technically compatible with the server. The version number seen here does not imply official support or test coverage on behalf of ownCloud.



Lowering this value may lead to unexpected behaviour, and can include data loss.

Code Sample

```
'minimum.supported.desktop.version' => '2.3.3',
```

Define whether to include external storage in quota calculation

EXPERIMENTAL: option whether to include external storage in quota calculation, defaults to false.

Code Sample

```
'quota_include_external_storage' => false,
```

Define how often filesystem changes are detected

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.

→ Never check the filesystem for outside changes, provides a performance increase when it's certain that no changes are made directly to the filesystem

→ Check each file or folder at most once per request, recommended for general use if outside changes might happen.

Code Sample

```
'filesystem_check_changes' => 0,
```

Define unsuccessful mountpoint rename attempts

This config value avoids infinite loops for seldom cases where a file renaming conflict between different share backends could occur.

The value defines how many unsuccessful mountpoint rename attempts are allowed. e.g. target mountpoint name could be claimed as unused by the filesystem but renaming to this target name will fail due to some other reasons like database constraints. Change this value only under supervision of ownCloud support.

Code Sample

```
'filesystem.max_mountpoint_move_attempts' => 10,
```

Define where part files are located

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 user's folder which might be required to work with certain external storage setups that have limited rename capabilities.

Note that setting this to false causes issues with the following apps: Encryption, Document classification, Anti-Virus and Ransomware Protection.

Code Sample

```
'part_file_in_storage' => true,
```

Prevent cache changes due to changes in the filesystem

When `true`, prevent ownCloud from changing the cache due to changes in the filesystem for all storage.

Code Sample

```
'filesystem_cache_readonly' => false,
```

Define ownClouds internal secret

Secret used by ownCloud for various purposes, e.g. to encrypt data.

If you lose this string there will be data corruption.

Code Sample

```
'secret' => '',
```

Define 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).

Code Sample

```
'trusted_proxies' => [  
  '203.0.113.45',  
  '198.51.100.128'  
],
```

Define `forwarded_for_headers`

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!

If not set, defaults to 'HTTP_X_FORWARDED_FOR'.

Code Sample

```
'forwarded_for_headers' => [  
    'HTTP_X_FORWARDED',  
    'HTTP_FORWARDED_FOR'  
],
```

Define the maximum filesize for animated GIF's

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.

Code Sample

```
'max_filesize_animated_gifs_public_sharing' => 10,
```

Enable transactional file locking

Transactional file locking 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.

Code Sample

```
'filelocking.enabled' => true,
```

Define the TTL for file locking

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.

Code Sample

```
'filelocking.ttl' => 3600,
```

Define the memory caching backend for file locking

Because most memcache backends can clean values without warning, using redis is highly recommended to **avoid data loss**.

Code Sample

```
'memcache.locking' => '\\OC\Memcache\Redis',
```

Disable the web based updater

The web based updater is enabled by default.

Code Sample

```
'upgrade.disable-web' => false,
```

Define whether or not to enable automatic update of market apps

Set to `false` to disable.

Code Sample

```
'upgrade.automatic-app-update' => true,
```

Enable debugging mode for this ownCloud instance

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!**. Furthermore the content-disposition header will be lost and thus files will be displayed in the browser rather than downloaded. We strongly encourage you never to use it in production.

Code Sample

```
'debug' => false,
```

Define 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 `sudo -u www-data ./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.

Code Sample

```
'data-fingerprint' => '',
```

Define if you have copied the sample configuration

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.

Code Sample

```
'copied_sample_config' => true,
```

Enable or disable the files_external local mount option

Set this property to true if you want to enable the files_external local mount option.

Default: false

Code Sample

```
'files_external_allow_create_new_local' => false,
```

Enable or disable debug logging for SMB access

Set this property to true if you want to enable debug logging for SMB access.

Code Sample

```
'smb.logging.enable' => false,
```

Enable or disable async DAV extensions

Code Sample

```
'dav.enable.async' => false,
```

Enable propfind depth infinity requests

Tell the clients whether `depth=infinity` is allowed for propfind requests.

Streamed infinite depth propfind requests can reduce memory usage with large responses. For details see: <https://datatracker.ietf.org/doc/html/rfc4918#section-10.2>

Code Sample

```
'dav.propfind.depth_infinity' => true,
```

Show the grace period popup

Decide whether show or not the grace period popup. There is no change in the behaviour of the grace period.

Code Sample

```
'grace_period.demo_key.show_popup' => true,
```

Link to get a demo key during active grace period

The admin will be directed to that web page when they click on the "get a demo key" link in the grace period popup. It's expected that the web page contains instructions on how to get a valid demo key to be used in the ownCloud server.

If this key isn't present, ownCloud's default will be used.

Code Sample

```
'grace_period.demo_key.link' => 'https://owncloud.com/try-enterprise/',
```

Apps Config.php Parameters

Introduction

This document describes parameters for apps maintained by ownCloud that are not part of the core system. All keys are only valid if the corresponding app is installed and enabled. You must copy the keys needed to the active `config.php` file.

Multiple configuration files

ownCloud supports loading configuration parameters from multiple files. You can add arbitrary files ending with `.config.php` in the `config/` directory.

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`.

ownCloud may write configurations into `config.php`. These configurations may conflict with identical keys already set in additional config files. Be careful when using this capability!

App: Activity

Possible keys: `activity_expire_days` DAYS

Define the retention for activities of the activity app

Code Sample

```
'activity_expire_days' => 365,
```

App: Admin Audit

Possible keys: `log.conditions` ARRAY

Possible keys: `admin_audit.groups` ARRAY

Configure the path to the log file

Code Sample

```
'log.conditions' => [  
  [  
    'apps' => ['admin_audit'],  
    // Adjust the path below, to match your setup  
    'logfile' => '/var/www/owncloud/data/admin_audit.log'  
  ],  
],
```

Filter the groups that messages are logged for

Code Sample

```
'admin_audit.groups' => ['group1', 'group2'],
```

App: Files Antivirus

Possible keys: `files_antivirus.av_path` STRING

Possible keys: `files_antivirus.av_cmd_options` STRING

Default path to the *clamscan* command line anti-virus scanner.

This setting only applies when the operating mode of the `files_antivirus` app is set to executable mode. See the documentation for more details.

Code Sample

```
'files_antivirus.av_path' => '/usr/bin/clamscan',
```

Command line options for the *clamscan* command line anti-virus scanner.

This setting only applies when the operating mode of the `files_antivirus` app is set to executable mode. See the documentation for more details.

Code Sample

```
'files_antivirus.av_cmd_options' => '',
```

App: Files Versions

Possible keys: `versions_retention_obligation` STRING

Use following values to configure the retention behaviour. Replace **D** with the number of days.

auto

Default value if nothing is set

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.

Pattern to define the expiration date for each backup version created.

Code Sample

```
'versions_retention_obligation' => 'auto',
```

App: Firstrunwizard

Possible keys: `customclient_desktop` URL

Possible keys: `customclient_android` URL

Possible keys: `customclient_ios` URL

Define the download links for ownCloud clients

Configuring the download links for ownCloud clients, as seen in the first-run wizard and on Personal pages

Code Sample

```
'customclient_desktop' =>
  'https://owncloud.com/desktop-app/' ,
'customclient_android' =>
  'https://play.google.com/store/apps/details?id=com.owncloud.android' ,
'customclient_ios' =>
  'https://apps.apple.com/app/id1359583808' ,
```

App: LDAP

Possible keys: `ldapIgnoreNamingRules doSet` or `false`

Possible keys: `user_ldap.enable_medial_search` `BOOL`

Define parameters for the LDAP app

Code Sample

```
'ldapIgnoreNamingRules' => false,
'user_ldap.enable_medial_search' => false,
```

App: Market

Possible keys: `appstoreurl` `URL`

Define the download URL for apps

Code Sample

```
'appstoreurl' => 'https://marketplace.owncloud.com' ,
```

App: Metrics

Note: This app is for Enterprise customers only.

Possible keys: `metrics_shared_secret` `STRING`

Secret to use the Metrics dashboard

You have to set a Metrics secret to use the dashboard. You cannot use the dashboard without defining a secret. You can use any secret you like. In case you want to generate a random secret, use the following example command: `echo $(tr -dc 'a-z0-9' < /dev/urandom | head -c 20)` It is also

possible to set this secret via an occ command which writes key and data to the config.php file. Please see the occ command documentation for more information.

Code Sample

```
'metrics_shared_secret' => 'replace-with-your-own-random-string',
```

App: Microsoft Office Online (WOPI)

Note: This app is for Enterprise customers only.

Possible keys: `wopi.token.key` STRING

Possible keys: `wopi.office-online.server` URL

Possible keys: `wopi_group` STRING

Possible keys: `wopi.proxy.url` URL

Possible keys: `wopi.business-flow.enabled` STRING

Random key created by the ownCloud admin

This is a random key created by the ownCloud admin. This key is used by ownCloud to create encrypted JWT tokens for the communication with your Microsoft Office Online instance.

You can use the following example command to generate a random key: `echo $(tr -dc 'a-z0-9' < /dev/urandom | head -c 20)`

Code Sample

```
'wopi.token.key' => 'replace-with-your-own-random-string',
```

Microsoft Office Online instance URL

This is the URL of the Microsoft Office Online instance ownCloud communicates with. Keep in mind that you need to grant communication access at your Microsoft Office Online instance with this ownCloud instance. For further information, read the ownCloud documentation.

Code Sample

```
'wopi.office-online.server' => 'https://your.office.online.server.tld',
```

Define the group name for users allowed to use Microsoft Office Online

Restrict access to Microsoft Office Online to a defined group. Please note, only one group can be defined. Default = empty = no restriction.

Code Sample

```
'wopi_group' => '',
```

Define the Proxy URL

This global option defines the proxy URL if you are a Microsoft Business user.

Note that you will get a working URL from ownCloud Support after you provide a written declaration that your company has an eligible Microsoft Business contract.

Code Sample

```
'wopi.proxy.url' => 'https://o365.example.com',
```

Define if Business Flow Is Enabled

This global option defines if Office users are business users.

In that case, Office Online will check if the user logged in has an Office 365 business account. If not, the user must sign in and Office Online will check if the subscription is valid. Use yes to enable it and no to disable it or remove the key completely. To use this option, you need at least ownCloud's Microsoft Office Online app version 1.6.0.

Code Sample

```
'wopi.business-flow.enabled' => 'no',
```

App: Microsoft Teams Bridge

Possible keys: `msteamsbridge` ARRAY

Sub key: `loginButtonName` STRING

Login Button Label

This key is necessary for security reasons. Users will be asked to click a login button each time when accessing the ownCloud app after a fresh start of their Microsoft Teams app or after idle time. This behavior is by design. The button name can be freely set based on your requirements.

Code Sample

```
'msteamsbridge' => [  
  "loginButtonName" => "Login to ownCloud with Azure AD",  
],
```


App: OpenID Connect (OIDC)

Possible keys: `openid-connect` ARRAY

Configure OpenID Connect - all possible sub-keys

You have to use the main key together with sub keys listed below, see code samples.

allowed-user-backends

Limit the users which are allowed to login to a specific user backend - e.g. LDAP (`'allowed-user-backends' ⇒ ['LDAP']`)

auth-params

Additional parameters which are sent to the IdP during the auth requests

autoRedirectOnLoginPage

If `true`, the ownCloud login page will redirect directly to the Identity Provider login without requiring the user to click a button. The default is `false`.

auto-provision

If auto-provision is setup, an ownCloud user will be created if not exists, after successful login using openid connect. The config parameters `mode` and `search-attribute` will be used to create a unique user so that the lookup mechanism can find the user again. This is where an LDAP setup is usually required. If auto-provision is not setup or required, it is expected that the user exists and you MUST declare this with `['enabled' ⇒ false]` like shown in the Easy Setup example. `auto-provision` holds several sub keys, see the example setup with the explanations below.

auto-update

When using the provisioning mode `auto-update`, user account info will update with the current information provided by the OpenID Connect provider upon each user log in.

insecure

Boolean value (`true/false`), no SSL verification will take place when talking to the IdP - **DO NOT use in production!**

loginButtonName

The name as displayed on the login screen which is used to redirect to the IdP. By default, the OpenID Connect App will add a button on the login page that will redirect the user to the Identity Provider and allow authentication via OIDC. This parameter allows the button text to be modified.

mode

This is the attribute in the owncloud accounts table to search for users. The default value is `email`. The alternative value is: `userid`.

post_logout_redirect_uri

A given URL where the IdP should redirect to after logout.

provider-params

Additional config array depending on the IdP to be entered here - usually only necessary if the IdP does not support service discovery.

provider-url, client-id and client-secret

Variables are to be taken from the OpenID Connect Provider's setup. For the `provider-url`, the URL where the IdP is living. In some cases (KeyCloak, Azure AD) this holds more than just a domain but also a path.

redirect-url

The full URL under which the ownCloud OpenId Connect redirect URL is reachable - only needed in special setups.

scopes

Enter the list of required scopes depending on the IdP setup.

search-attribute

The attribute which is taken from the access token JWT or user info endpoint to identify the user. This is the claim from the OpenID Connect user information which shall be used for searching in the accounts table. The default value is `email`. For more information about the claim, see https://openid.net/specs/openid-connect-core-1_0.html#Claims.

token-introspection-endpoint-client-id

Client ID to be used with the token introspection endpoint.

token-introspection-endpoint-client-secret

Client secret to be used with the token introspection endpoint.

use-access-token-payload-for-user-info

If set to `true` any user information will be read from the access token. If set to `false` the userinfo endpoint is used (starting app version 1.1.0).

use-token-introspection-endpoint

If set to `true`, the token introspection endpoint is used to verify a given access token - only needed if the access token is not a JWT. If set to `false`, the userinfo endpoint is used (requires version $\geq 1.1.0$) Tokens which are not JSON WebToken (JWT) may not have information like the expiry. In these cases, the OpenID Connect Provider needs to call on the token introspection endpoint to get this information. The default value is `false`. See <https://datatracker.ietf.org/doc/html/rfc7662> for more information on token introspection.

Easy setup

Code Sample

```
'openid-connect' => [  
    // it is expected that the user already exists in ownCloud  
    'auto-provision' => ['enabled' => false],  
    'provider-url' => 'https://idp.example.net',
```

```

    'client-id' => 'fc9b5c78-ec73-47bf-befc-59d4fe780f6f',
    'client-secret' => 'e3e5b04a-3c3c-4f4d-b16c-2a6e9fdd3cd1',
    'loginButtonName' => 'OpenId Connect'
  ],

```

Setup auto provisioning mode

Code Sample

```

'openid-connect' => [
  // explicit enable the auto provisioning mode,
  // if not exists, the user will be created in ownCloud
  'auto-provision' => [
    'enabled' => true,
    // documentation about standard claims:
    // https://openid.net/specs/openid-connect-core-1_0.html#StandardClaims
    // only relevant in userid mode, defines the claim which holds the email of
the user
    'email-claim' => 'email',
    // defines the claim which holds the display name of the user
    'display-name-claim' => 'given_name',
    // defines the claim which holds the picture of the user - must be a URL
    'picture-claim' => 'picture',
    // defines a list of groups to which the newly created user will be added
automatically
    'groups' => ['admin', 'guests', 'employees'],
    // sets a claim which is defined at the IDP.
    // the IDP will return a single value or an array like:
    // "allowed_applications": ["erp", "owncloud"],
    'provisioning-claim' => 'allowed_applications',
    // defines the matching case for the provisioning. the attribute can only be
a
    // single value in case no match is found against the IDP response,
    // no provisioning will be made, "User not found" will be returned
    'provisioning-attribute' => 'owncloud',
    // auto-update user account info with current information provided by the
    // OpenID Connect provider account attributes, that will be updated,
    // can be specified in `attributes` config option
    'auto-provision' => [
      'update' => [
        // enable the user info auto-update mode
        'enabled' => true,
      ],
    ],
  ],
],
// `mode` and `search-attribute` will be used to create a unique user in
ownCloud
'mode' => 'email',
'search-attribute' => 'email',

```

```
],
```

Manual setup

Code Sample

```
'openid-connect' => [  
  // it is expected that the user already exists in ownCloud  
  'auto-provision' => ['enabled' => false],  
  'autoRedirectOnLoginPage' => false,  
  'client-id' => 'fc9b5c78-ec73-47bf-befc-59d4fe780f6f',  
  'client-secret' => 'e3e5b04a-3c3c-4f4d-b16c-2a6e9fdd3cd1',  
  'loginButtonName' => 'OpenId Connect',  
  'mode' => 'userid',  
  'search-attribute' => 'sub',  
  // only required if the OpenID Connect Provider does not support service  
  discovery  
  // replace the dots with your values  
  'provider-params' => [  
    'authorization_endpoint' => '...',  
    'end_session_endpoint' => '...',  
    'jwks_uri' => '...',  
    'registration_endpoint' => '...',  
    'token_endpoint' => '',  
    'token_endpoint_auth_methods_supported' => '...',  
    'userinfo_endpoint' => '...' ]  
  ],  
  'provider-url' => '...',  
  'use-token-introspection-endpoint' => true  
],
```

Test setup

Code Sample

```
'openid-connect' => [  
  // it is expected that the user already exists in ownCloud  
  'auto-provision' => ['enabled' => false],  
  'provider-url' => 'http://localhost:3000',  
  'client-id' => 'ownCloud',  
  'client-secret' => 'ownCloud',  
  'loginButtonName' => 'node-oidc-provider',  
  'mode' => 'userid',  
  'search-attribute' => 'sub',  
  'use-token-introspection-endpoint' => true,  
  // do not verify tls host or peer  
  'insecure' => true  
],
```

App: Richdocuments

Possible keys: `collabora_group` STRING

Define the group name for users allowed to use Collabora

Please note, only one group can be defined. Default = empty = no restriction.

Code Sample

```
'collabora_group' => '',
```

App: Windows Network Drive (WND)

Note: This app is for Enterprise customers only.

Possible keys: `wnd.listen.reconnectAfterTime` INTEGER

Possible keys: `wnd.logging.enable` BOOL

Possible keys: `wnd.fileInfo.parseAttrs.mode` STRING

Possible keys: `wnd.in_memory_notifier.enable` BOOL

Possible keys: `wnd.permissionmanager.cache.size` INTEGER

Possible keys: `wnd2.cachewrapper.ttl` INTEGER

Possible keys: `wnd.activity.registerExtension` BOOL

Possible keys: `wnd.activity.sendToSharees` BOOL

Possible keys: `wnd.groupmembership.checkUserFirst` BOOL

Possible keys: `wnd.connector.opts.timeout` INTEGER

Note With WND 2.1.0, key `wnd.storage.testForHiddenMount` is obsolete and has been removed completely.

Mandatory Listener Reconnect to the Database

The listener will reconnect to the DB after given seconds. This will prevent the listener to crash if the connection to the DB is closed after being idle for a long time.

Code Sample

```
'wnd.listen.reconnectAfterTime' => 28800,
```

Enable Additional Debug Logging for the WND App

Code Sample

```
'wnd.logging.enable' => false,
```

The Way File Attributes for Folders and Files will be Handled

There are 3 possible values: "none", "stat" and "getxattr":

- "stat". This is the default if the option is missing or has an invalid value. This means that the file attributes will be evaluated only for files, NOT for folders. Folders will be shown even if the "hidden" file attribute is set.
- "none". This means that the file attributes won't be evaluated in any case. Both hidden files and folders will be shown, and you can write on read-only files (the action is available in ownCloud, but it will fail in the SMB server).
- "getxattr". This means that file attributes will always be evaluated. However, due to problems in recent libsmbclient versions (4.11+, it might be earlier) it will cause malfunctions in ownCloud; permissions are wrongly evaluated. So far, this mode works with libsmbclient 4.7 but not with 4.11+ (not tested with any version in between).

Note that the ACLs (if active) will be evaluated and applied on top of this mechanism.

Code Sample

```
'wnd.fileInfo.parseAttrs.mode' => 'stat',
```

Enable or Disable the WND In-Memory Notifier for Password Changes

Having this feature enabled implies that whenever a WND process detects a wrong password in the storage - maybe the password has changed in the backend - all WND storages that are in-memory will be notified in order to reset their passwords if applicable and not to requery again.

The intention is to prevent a potential password lockout for the user in the backend. As with PHP lower than 7.4, this feature can take a lot of memory resources. This is because WND keeps the storage access and its caches in-memory. With PHP 7.4 or above, the memory usage has been reduced significantly. Alternatively, you can disable this feature completely.

Code Sample

```
'wnd.in_memory_notifier.enable' => true,
```

Maximum Number of Items for the Cache Used by the WND Permission Managers

A higher number implies that more items are allowed, increasing the memory usage.

Real memory usage per item varies because it depends on the path being cached. Note that this is

an in-memory cache used per request. Multiple mounts using the same permission manager will share the same cache, limiting the maximum memory that will be used.

Code Sample

```
'wnd.permissionmanager.cache.size' => 512,
```

TTL for the WND2 Caching Wrapper

Time to Live (TTL) in seconds to be used to cache information for the WND2 (collaborative) cache wrapper implementation. The value will be used by all WND2 storages. Although the cache isn't exactly per user but per storage id, consider the cache to be per user, because it will be like that for common use cases. Data will remain in the cache and won't be removed by ownCloud. Aim for a low TTL value in order to not fill the memcache completely. In order to properly disable caching, use -1 or any negative value. 0 (zero) isn't considered a valid TTL value and will also disable caching.

Code Sample

```
'wnd2.cachewrapper.ttl' => 1800, // 30 minutes
```

Enable to Push WND Events to the Activity App

Register WND as extension into the Activity app in order to send information about what the `wnd:process-queue` command is doing. The activity sent will be based on what the `wnd:process-queue` detects, and the activity will be sent to each affected user. There won't be any activity being sent outside of the `wnd:process-queue` command. `wnd:listen` `wnd:process-queue` + `activity` app are required for this to work properly. See `wnd.activity.sendToSharees` below for information on how to send activities for shared resources. Please consider that this can have a performance impact when changes are sent to many users.

Code Sample

```
'wnd.activity.registerExtension' => false,
```

Enable to Send WND Activity Notifications to Sharees

The `wnd:process-queue` command will also send activity notifications to the sharees if a WND file or folder is shared (or accessible via a share). It's REQUIRED that the `wnd.activity.registerExtension` flag is set to true (see above), otherwise this flag will be ignored. This flag depends on the `wnd.activity.registerExtension` and has the same restrictions.

Code Sample

```
'wnd.activity.sendToSharees' => false,
```

Make the Group Membership Component Assume that the ACL Contains a User

The WND app doesn't know about the users or groups associated with ACLs. This means that an ACL containing "admin" might refer to a user called "admin" or a group called "admin". By default, the group membership component considers the ACLs to target groups, and as such, it will try to get the information for such a group. This works fine if the majority of the ACLs target groups. If the majority of the ACLs contain users, this might be problematic. The cost of getting information on a group is usually higher than getting information on a user. This option makes the group membership component assume the ACL contains a user and checks whether there is a user in ownCloud with such a name first. If the name doesn't refer to a user, it will get the group information. Note that this will have performance implications if the group membership component can't discard users in a large number of cases. It is recommended to enable this option only if there are a high number of ACLs targeting users.

Code Sample

```
'wnd.groupmembership.checkUserFirst' => false,
```

The timeout (in ms) for all the operations against the backend.

The same timeout will be applied for all the connections.

Increase it if requests to the server sometimes time out. This can happen when SMB3 encryption is selected and smbclient is overwhelming the server with requests.

Code Sample

```
'wnd.connector.opts.timeout' => 20000, // 20 seconds
```

App: Workflow / Tagging

Note: This app is for Enterprise customers only.

Possible keys: `workflow.retention_engine` STRING

Provide Advanced Management of File Tagging

Enables admins to specify rules and conditions (file size, file mimetype, group membership and more) to automatically assign tags to uploaded files. Values: `tagbased` (default) or `userbased`.

Code Sample

```
'workflow.retention_engine' => 'tagbased',
```

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.com/desktop-app/",
"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
```

Email Configuration

Introduction

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.



To be able to send emails, a functioning mail server must be available, whether locally in your network, or remotely.

The Graphical Email Configuration Wizard

The wizard supports two mail server types: *SMTP* and *PHP*. Use SMTP for a remote email server, and PHP when your mail server is on the same machine as ownCloud.

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 ownCloud's email server

configuration.

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.

You need the following information from your email 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.

Email server *i*

This is used for sending out notifications.

Send mode: smtp | Encryption: SSL/TLS

From address: mail @ example.com

Authentication method: Login (selected) | Authentication required

Server address: 0

Credentials: NT LAN Manager | SMTP Password: |

Test receiver email: admin@example.com

Test email settings

Your changes are saved immediately.

You must enter a valid email address to which a test email will be sent. This field is mandatory and will be prefilled with the logged-in admin's email if set, but can be changed to any other valid email address. Note that this test recipient address can't be set via a config value in `config.php`. Click the **[Send Email]** button to test your configuration. This sends a test message to the email address you configured. The test message says:

If you received this email, the settings seem to be correct.

```
--
ownCloud
web services under your control
```

Configuring PHP for sending Emails

To configure PHP select it and enter your desired return address.

Email server

This is used for sending out notifications.

Send mode

From address @

Test receiver email

Test email settings

Same as with the SMTP configuration above, you must enter an email address to which a test email will be sent when testing the configuration. For details see the section above.



PHP mode uses your local `sendmail` binary and any drop-in Sendmail replacement such as Postfix, Exim, or Courier. All of these include a `sendmail` binary, and are freely interchangeable. 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 depending on which server you are using, so consult your server's documentation to see what your options are.

Setting Mail Server Parameters via `config.php`

If you prefer, you may set your email server parameters directly in `config/config.php`.

Supported SMTP sending modes

- SMTP
- PHP Mail



Compatibility of *sending modes* might depend on the installation environment. In case of problems with a *sending mode*, it is recommended to try other mode configurations.

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 and 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:

```
'mail_smtpmode' => 'smtp',
```

```
'mail_smtpost' => 'smtp-1.server.dom;smtp-2.server.dom:425',  
'mail_smtpport' => 25,
```

Or:

```
'mail_smtpmode' => 'smtp',  
'mail_smtpost' => '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:

```
'mail_smtptimeout' => 30,
```

If the SMTP server accepts insecure connections, the default setting can be used:

```
'mail_smtpsecure' => '',
```

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**:

```
'mail_smtpost' => 'smtp.server.dom:465',  
'mail_smtpsecure' => 'ssl',
```

STARTTLS

A secure connection will be initiated using STARTTLS via SMTP on the default port **25/tcp**:

```
'mail_smtpost' => 'smtp.server.dom',  
'mail_smtpsecure' => 'tls',
```

An alternative is the port **587/tcp** (recommended):

```
'mail_smtpost' => 'smtp.server.dom:587',  
'mail_smtpsecure' => '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.

```
'mail_smtpath' => 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**.

```
'mail_smtpath' => true,  
'mail_smtpathtype' => '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.

```
'mail_smtpmode' => 'php',  
'mail_smtphost' => '127.0.0.1',  
'mail_smtport' => 25,  
'mail_smtptimeout' => 10,  
'mail_smtsecure' => '',  
'mail_smtpath' => false,  
'mail_smtpathtype' => '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_smtdebug` parameter in `config/config.php`.

```
'mail_smtpdebug' => true;
```



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:

```
'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.



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:

```
'mail_smtpdebug' => true,
```



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



You have to install and enable a custom theme in order to use and customize email templates. Additionally you need to have the [Mail Template Editor](#) app installed and enabled.

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.	<code>core/templates/mail.php</code>
Lost password mail	HTML	Password reset email for users who lose their passwords.	<code>core/templates/lostpassword/email.php</code>
New user email	HTML		<code>settings/templates/email.new_user.php</code>
	plain text		<code>settings/templates/email.new_user_plain_text.php</code>
Public link share email	HTML	Notify users of new public link shares.	<code>core/templates/mail.php</code>
	plain text		<code>core/templates/altmail.php</code>
New file share email	HTML	Notify users of new file shares.	<code>core/templates/internalmail.php</code>
	plain text		<code>core/templates/internalaltmail.php</code>

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. Log in as the admin user.
2. Navigate to **Settings › Admin › General › Mail Templates**.
3. Select a template from the drop-down menu.



If you don't see the drop down menu but instead *You need to activate own theme to edit email templates*, you haven't installed and configured a custom theme yet.

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.



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.

Excluding Directories and Blacklisting Files

Introduction

This document describes how to manage blacklisted files and excluded directories.

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 directories on 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 manager. Even when a filepath is entered manually via a file explorer, the path cannot be accessed.

For example configurations please see the [config.sample.php](#) file.



Many filesystems do not allow the coexistence of a file and folder with exactly the same name on the same directory level. Therefore no differentiation is made in processing files and folders for blacklisting or excluding, as it would just return a deny at a later stage. With the implementation made, you get an immediate error message.

Example: The storage backend has a reserved directory name ".snapshot" which is excluded by configuration. If you try to add a file or folder via the browser or sync a file or folder from the client named ".snapshot", you will get an immediate ownCloud triggered deny.

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. You can also prevent uploading, e.g., Outlook `.pst` files, with this mechanism to avoid massive backend space allocation.

Excluded Directories

Reasons 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
 - a. Snapshot directories are read-only
 - b. There is no common naming convention for these directories, and there most likely will never be. For example, NetApp uses `.snapshot` and `~snapshot`, EMC e.g., `.ckpt`, HDS e.g., `.latest` and `~latest`, and the ZFS filesystem uses `.zfs`
 - c. It does not make sense for these directories to be visible to users as they are used to ease backup, restoration, and cloning
2. Directories which are part of the mounted filesystem, but must not be user accessible/visible

3. Manual managed but user invisible backup directories

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` can 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
```

Reasons for Blacklisting Files

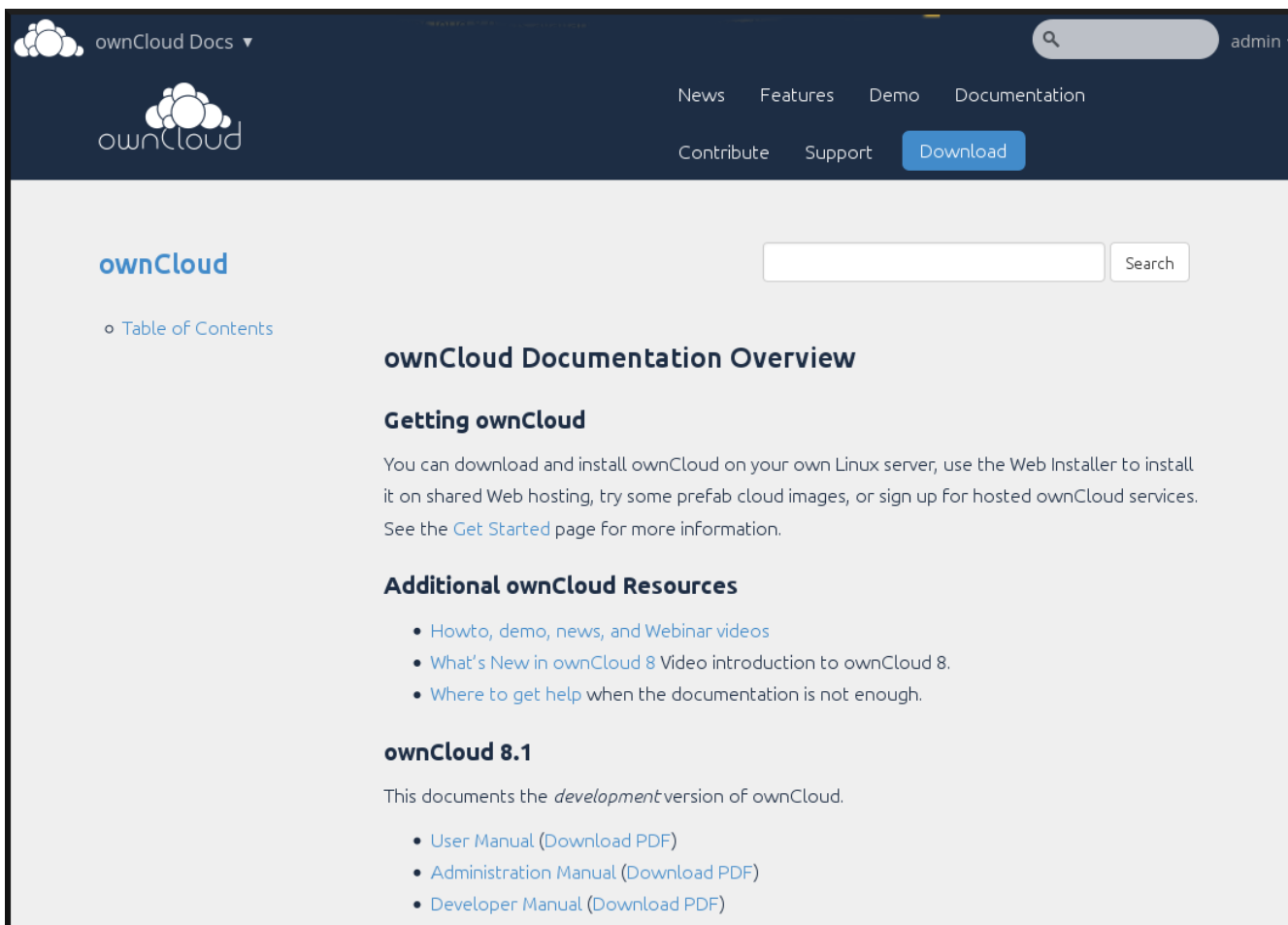
The reason for blacklisting files can be explained based on the example of a `.htaccess` file. Such a file can lead to a unwanted behaviour of your webserver when visible to ownCloud in a directory.

Example `blacklisted_files` entries in `config.php` can look like this:

```
'blacklisted_files' => [  
    'hosts',  
    'evil_script.sh',  
],
```

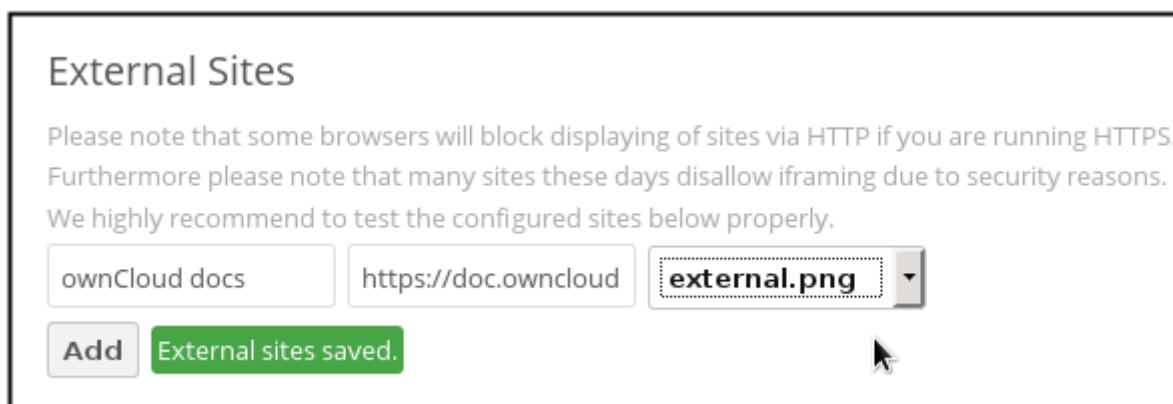
Linking External Sites

You can embed external Web sites inside your ownCloud pages with the External Sites app, as this screenshot shows.

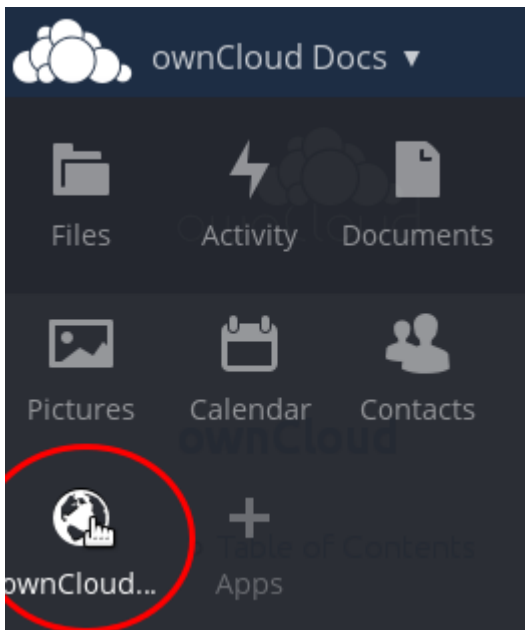


This is useful for quick access to important Web pages such as the ownCloud manuals and informational pages for your company, and for presenting external pages inside your custom ownCloud branding, if you use your own custom themes.

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.

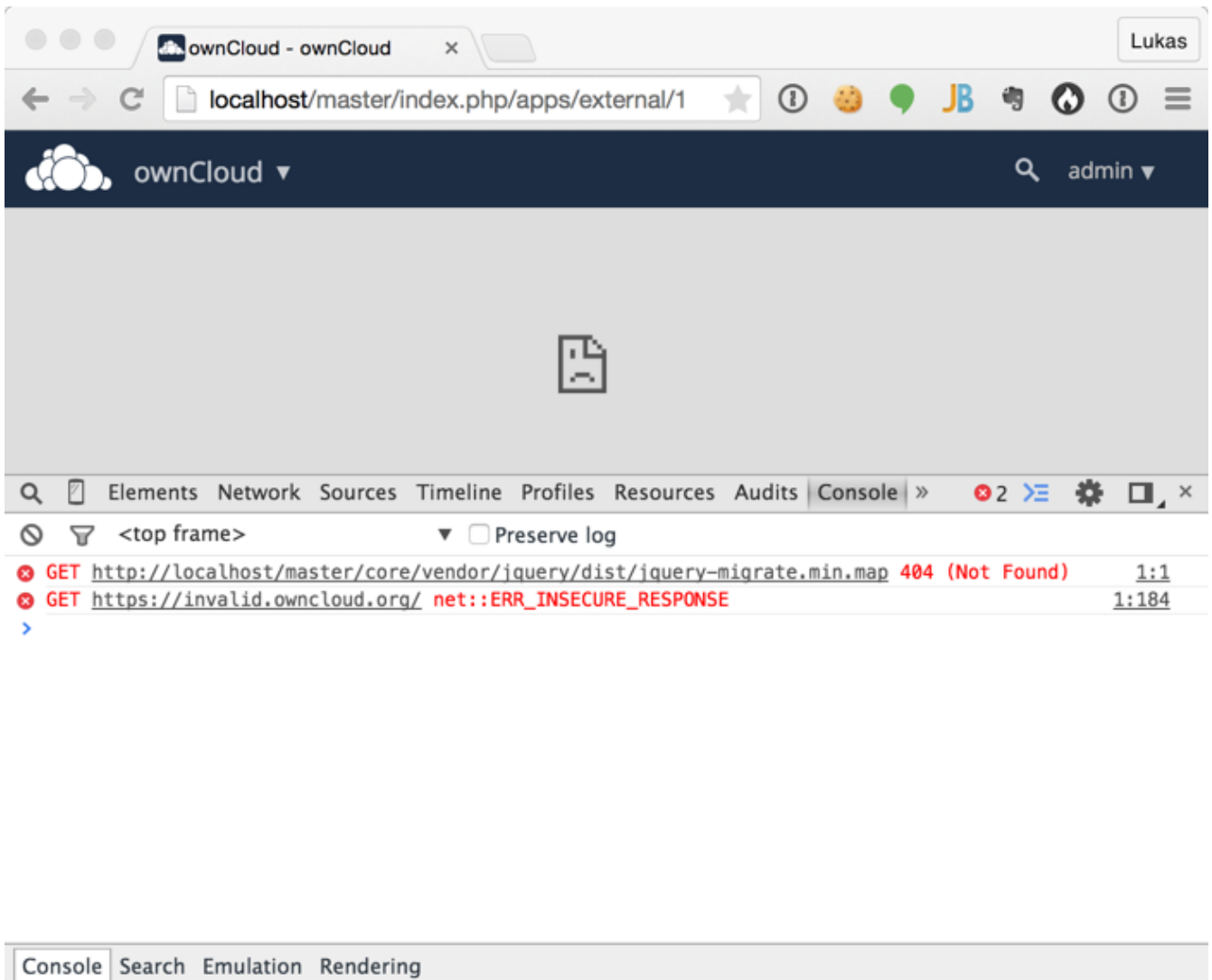


The links appear in the ownCloud dropdown menu on the top left after refreshing your page, and have globe icons.

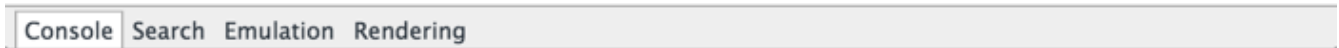
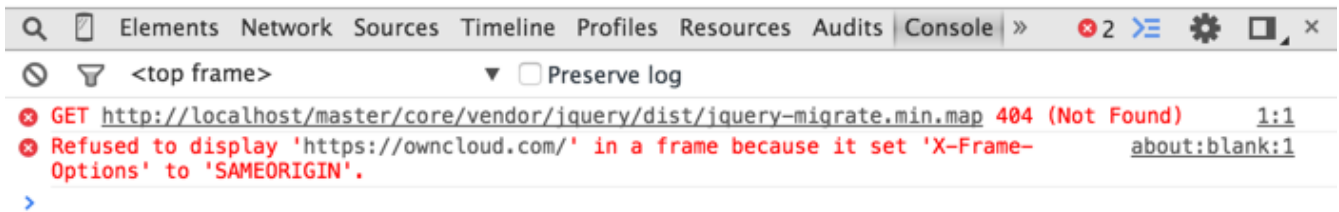
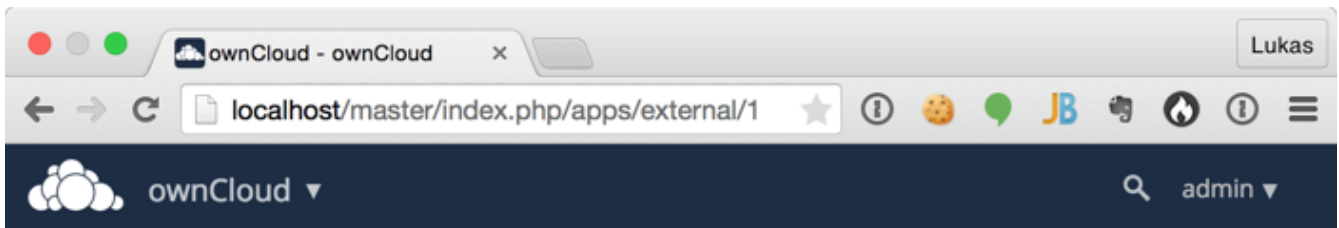


Your links may or may not work correctly due to the various ways that Web browsers and Web sites handle HTTP and HTTPS URLs, and because the External Sites app embeds external links in IFrames. Modern Web browsers try very hard to protect Web surfers from dangerous links, and safety apps like [Privacy 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. "Clickjacking"). 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.

Hardening and Security Guidance

Introduction

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.



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. It only verifies the first 72 characters of passwords. This applies to all passwords you use in ownCloud: user passwords, passwords on link shares and passwords on external shares.

Rate Limiting

Currently ownCloud deliberately does not provide any form of rate-limiting (though it does provide [brute-force protection](#)). This is because ownCloud needs to integrate in to a diverse range of environments and infrastructure, which often already provide specialized rate-limiting solutions, e.g., *Apache*, *HAProxy*, and *F5*.

If you are yet to implement a rate-limiting solution for your ownCloud instance, start by retrieving a list of all active routes. This information is obtained by running `occ's security:routes` command, as in the following example.

```
sudo -u www-data ./occ security:routes
```

It should print a list of all the routes as in the following truncated example.

```
+-----+-----+
| Path                                     | Methods |
+-----+-----+
| /apps/encryption/ajax/adminRecovery     | POST    |
| /apps/encryption/ajax/changeRecoveryPassword | POST    |
| /apps/encryption/ajax/getStatus         | GET     |
| /apps/encryption/ajax/setEncryptHomeStorage | POST    |
| /apps/encryption/ajax/updatePrivateKeyPassword | POST    |
| /apps/encryption/ajax/userSetRecovery    | POST    |
| /apps/federatedfilessharing/            | GET     |
| /apps/federatedfilessharing/notifications | POST    |
+-----+-----+
```

With this information, you can begin customizing a rate-limiting solution specific to your ownCloud installation.

Further Reading

- Rate limiting with Apache
 - [mod_evasive](#)
 - [mod_ratelimit](#)
 - [mod_security](#)
 - Rate limiting with [Fail2Ban](#)
 - [Fail2Ban Behind A Proxy/Load Balancer](#)
- [Rate limiting with HAProxy](#)
- [Rate limiting with F5](#)

Operating system

Enable hardening modules such as SELinux

We also recommend 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

A simple but efficient way to increase the security of your data is to place your `data` directory outside of the Web root (i.e. outside of `/var/www`), ideally at the time of installation.

Disable preview image generation

ownCloud is able to generate preview images of common file types such as images or text files. By default, the preview generation for some file types that we consider secure enough for deployment is enabled. 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 administrator you are also able to manage which preview providers are enabled by modifying the `enabledPreviewProviders` option switch.

Use HTTPS

Using ownCloud without 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.

For information on how to setup HTTPS, consult the documentation of your Web server. The following examples apply to 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. 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. Therefore we recommend setting 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 adding the following settings in 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`.



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. The available SSL ciphers and options depend completely on your environment, therefore we can't provide a general recommendation.

However, We do recommend using the [Mozilla SSL Configuration Generator](#) to generate a configuration suitable 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 benefit from 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) a threat. 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 installed in a segregated network and proper firewall rules are in place.

Use of Security-Related Headers on the Web server

Basic security headers are provided by ownCloud already in a default environment. These include:

X-Content-Type-Options: nosniff

Instructs some browsers to not sniff the MIME type of files. This is used for example to prevent browsers from interpreting text files as JavaScript.

X-XSS-Protection: 0

The cross-site scripting filter is deprecated and not used in modern browsers anymore.

X-Robots-Tag: none

Instructs search engines to not index these pages.

X-Frame-Options: SAMEORIGIN

Prevents embedding of the ownCloud instance within an iframe on other domains to prevent clickjacking and 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 let the Web server deliver these HTTP headers. To do this, configure Apache to use the `.htaccess` file and enable the following Apache modules:

- `mod_headers`
- `mod_env`

Verify this security change by accessing a static resource and check the above mentioned security headers are delivered.

Use Fail2ban

Another approach to hardening ownCloud server is to use an intrusion detection system. An excellent one is [Fail2ban](#). Fail2ban is designed to protect servers from brute force attacks. It works by scanning 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 originate. This makes the process more difficult and prevents DDOS-style attacks. However, after a predefined time period, the banned IP is usually unbanned again.

This helps if the login attempts were genuine, so that users don't lock themselves out permanently. An example of such an action is users attempting to brute force log in 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=ssh ruser= rhost=221.194.44.231 user=root
Mar 15 11:14:57 yourhost sshd[10837]: pam_unix(sshd:auth): authentication failure;
logname= uid=0 euid=0 tty=ssh ruser= rhost=221.194.44.231 user=root
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 221.194.44.231 port 46838 ssh2]
```

```
Mar 15 11:15:04 yourhost sshd[10837]: Received disconnect from 221.194.44.231: 11:
[preauth]
```



If you're not familiar with what's going on, this snippet highlights a number of failed login attempts.

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* 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',
```



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, then
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



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: \
```

```
Date template hits:
|- [# of hits] date format
| [40252] ISO 8601
| `-
```

Lines: 40252 lines, 0 ignored, 1 matched, 40251 missed

The `Failregex` counter increases in increments of 1 for every failed login attempt. To unban an IP 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
```

Importing System-wide and Personal SSL Certificates

Introduction

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.

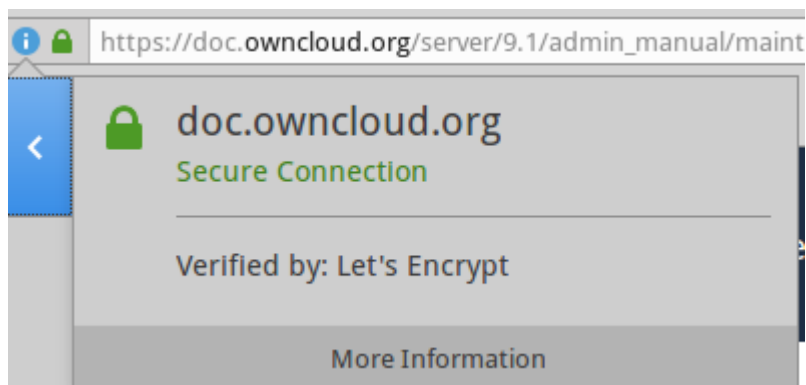
Importing Personal SSL Certificates

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

Import root certificate

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.

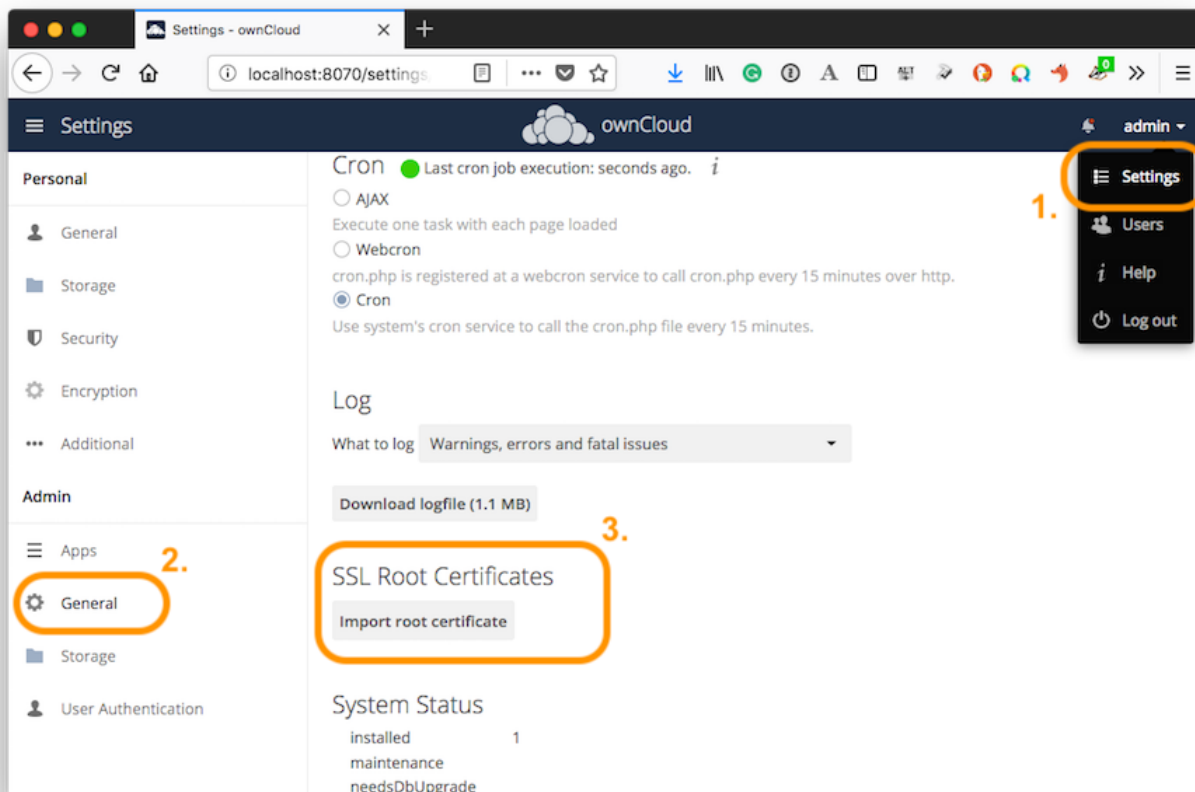


Site-wide SSL Import

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,
```

Then you'll have an **[Import root certificate]** button on your admin page, just like the one on your personal page. Navigate to it by clicking **Settings > General > SSL Root Certificates** which is located almost at the bottom.



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 the occ Command](#) to learn about how to use `occ`.

Enable index.php-less URLs

Introduction

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 Correct 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 `config_sample_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 `occ_command`)

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.

Using the `occ` Command

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, app settings, and more.

Running occ

Check if occ Is Set to Executable

Note that this step is not necessary when using a docker installation.

To check if the `occ` command is set to executable, change to your ownCloud directory first, then enter the command:

```
ls -lhF occ
```

This should give an output similar to this:

```
-rwxr-x--x 1 root www-data 283 May 18 17:44 occ*
```

In case it does not, set the `occ` command to executable with:

```
sudo chmod +x occ
```

As Your HTTP User

On a regular ownCloud installation, `occ` is in the `owncloud/` directory, this is on Ubuntu Linux for example `/var/www/owncloud`. `occ` itself 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. The default HTTP user is different on the various Linux distributions.

- 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`.



Use the following command to find your HTTP user:

```
ps -ef | egrep '(apache|apache2)' | grep -v `whoami` | grep -v root |  
head -n1 | awk '{print $1}'
```

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 with SCL-PHP74 installed, the command looks like this:

```
sudo -u apache /opt/rh/php74/root/usr/bin/php /var/www/html/owncloud/occ
```

occ Command Structure

The `occ` command has *options*, *commands*, and *arguments*.

1. Options are optional.
2. Commands are required.
3. Arguments can be required *or* optional.

The generic syntax is:

```
occ [options] command [arguments]
```

Listing 9. Example command running occ in Ubuntu

```
sudo -u www-data /var/www/owncloud/occ
```

If your web server is configured to use a different PHP version than the default (`/usr/bin/php`), the `occ` command should be run with the same version.

With a Docker Container

If your ownCloud instance is set up in a docker container, you need a user in the group `docker` to perform `occ` commands. An example command looks like this:

```
docker exec --user www-data <owncloud-container-name> occ <your-command>
```

For more information on docker, refer to section [Installing with Docker](#).

With the ownCloud Appliance

The ownCloud Appliance offers two possibilities to perform `occ` commands:

1. Log in to the ownCloud instance as root user with the command `univention-app shell owncloud`. Then use `occ` commands without a preceding `sudo -u www-data`.
2. Alternatively, you can use `occ` on the host system with the command `univention-app shell owncloud occ` followed by the desired options, commands and arguments.

If you want to find out more about the Appliance, click [here](#).

Example Commands

Running `occ` with no options lists all commands and options, like this example on Ubuntu:

```
sudo -u www-data ./occ
ownCloud version 10.8.0

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 ./occ list`. Run it with the `-h` option for syntax help:

```
sudo -u www-data ./occ -h
```

Display your ownCloud version:

```
sudo -u www-data ./occ -V
ownCloud version 10.8.0
```

Query your ownCloud server status:

```
sudo -u www-data ./occ status
- installed: true
- version: 10.8.0.4
- versionstring: 10.8.0
- edition: Community
```

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 ./occ status --output=json
{"installed":true,"version":"10.8.0.4","versionstring":"10.8.0","edition":""}
```

or `json_pretty`:

```
sudo -u www-data ./occ status --output=json_pretty
{
  "installed": true,
  "version": "10.8.0.4",
  "versionstring": "10.8.0",
  "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`.

Get detailed information on individual commands with the `help` command, like in this example for the `maintenance:mode` command:

```
sudo -u www-data ./occ help maintenance:mode --help
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
```

Core Commands

This command reference covers the ownCloud core commands, which are always available.

App Commands

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 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 ./occ app:list [--] [<search-pattern>]
```

Arguments

<code>search-pattern</code>	Show only those apps whose names match the given search pattern (regular expression).
-----------------------------	---

Options

<code>--enabled</code>	Only display enabled apps. When used, the output will contain the app's version number as well
<code>--disabled</code>	Only display disabled apps. If the app was previously enabled, the app version is also displayed. When used, the output will contain the app's version number as well, <i>if</i> it was previously enabled
<code>--shipped=<SHIPPED></code>	If <code>SHIPPED</code> is set to <code>true</code> , only shipped apps will be listed. If <code>SHIPPED</code> is set to <code>false</code> , only non-shipped apps will be listed
<code>-m</code> <code>--minimal</code>	Minimal view - only display apps with version. When used, the output will contain the app's version number as well.
<code>--output[=OUTPUT]</code>	The output format to use (<code>plain</code> , <code>json</code> or <code>json_pretty</code>). [default: "plain"]

Enable an App

Enable an app, for example the Market app.

```
sudo -u www-data ./occ app:enable market
market enabled
```

Disable an App

```
sudo -u www-data ./occ app:disable market
market disabled
```



Be aware that the following apps cannot be disabled: *DAV*, *FederatedFileSharing*, *Files* and *Files_External*.

Check App Code

`app:check-code` has multiple checks:

- It checks if an app uses ownCloud's public API (OCP) or private API (OC_),
- 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 ./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 ./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
```

Get the App Installation Path

You can get the full file path to an app.

```
sudo -u www-data ./occ app:getpath notifications
/var/www/owncloud/apps/notifications
```

Background Jobs Selector

Use the `background` command to select which scheduler you want to use for controlling [background jobs](#). 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
```

Examples

```
# Set the background scheduler to Ajax
sudo -u www-data ./occ background:ajax

# Set the background scheduler to Cron
sudo -u www-data ./occ background:cron
```



```
# Set the background scheduler to Webcron
sudo -u www-data ./occ background:webcron
```



See [background jobs configuration](#) to learn more.

Config Commands

The `config` commands are used to configure the ownCloud server.



- In general, key names are not checked for validity, they are used as written.
- Whenever you use the **app** parameter, a config is read or written from or to the database.
- Whenever you use the **system** parameter, a config is read or written from or to the `config.php` file.

```
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
```

config:app References

The following apps, core functions or documents use/refer to `config:app` settings:

Standard

- [Configuring Federation Sharing](#)
- [Custom Groups](#)
- [File Sharing](#)
- [The HSM \(Hardware Security Module\) Daemon \(hsmdaemon\)](#)
- [Legal Settings Configuration](#)
- [LDAP Integration](#)
- [Manual File Locking](#)
- [Manually Move a Data Directory](#)
- [Virus Scanner Support](#)
- [OpenID Connect \(OIDC\)](#)
- [UI Configuration](#)

Enterprise

- [Shibboleth Integration](#)
- [Auditing](#)
- [File Lifecycle Management](#)

occ Commands

- [occ Anti-Virus](#)
- [occ Auditing](#)
- [occ Brute Force Protection](#)
- [occ Custom Groups](#)
- [occ Collabora Online / Secure View](#)
- [occ Encryption](#)
- [occ File Lifecycle Management](#)
- [occ Full Text Search](#)
- [occ LDAP Integration](#)

config:system References

The following apps, core functions or documents use/refer to `config:system` settings:

Standard

- [Quick Install on Ubuntu 20.04](#)
- [Quick Install on Ubuntu 22.04](#)

occ Commands

- [occ Metrics](#)

Enterprise

- [Metrics](#)

Config App Commands

These commands manage the configurations of apps. Keys and values are stored in the database.

config:app:delete

```
sudo -u www-data ./occ config:app:delete [options] [--] <app> <name>
```

Arguments

<code>app</code>	Name of the app.
<code>name</code>	Name of the config to delete.

Options

<code>--error-if-not-exists</code>	Checks whether the config exists before deleting it.
<code>--output=[OUTPUT]</code>	The output format to use (<code>plain</code> , <code>json</code> or <code>json_pretty</code> , default is <code>plain</code>).

Examples:

```
sudo -u www-data ./occ config:app:delete myappname provisioning_api
Config value provisioning_api of app myappname 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 ./occ config:app:delete doesnotexist --error-if-not-exists
Config provisioning_api of app appname could not be deleted because it did not exist
```

config:app:get

```
sudo -u www-data ./occ config:app:get [options] [--] <app> <name>
```

Arguments

<code>app</code>	Name of the app.
<code>name</code>	Name of the config to get.

Options

<code>--default-value=[DEFAULT-VALUE]</code>	If no default value is set and the config does not exist, the command will exit with 1.
<code>--output=[OUTPUT]</code>	The output format to use (<code>plain</code> , <code>json</code> or <code>json_pretty</code> , default is <code>plain</code>).

Examples

```
sudo -u www-data ./occ config:app:get activity installed_version
2.2.1
```

config:app:set

```
sudo -u www-data ./occ config:app:set [options] [--] <app> <name>
```

Arguments

<code>app</code>	Name of the app. Must not be an empty string.
<code>name</code>	Name of the config to set. Must not be an empty string.

Options

<code>--value=[VALUE]</code>	The new value of the config.
<code>--update-only</code>	Only updates the value. If it is not set before, it is not being added.
<code>--output=[OUTPUT]</code>	The output format to use (<code>plain</code> , <code>json</code> or <code>json_pretty</code> , default is <code>plain</code>).

Examples

```
sudo -u www-data ./occ config:app:set \  
  files_sharing \  
  incoming_server2server_share_enabled \  
  --value=true \  
  --type=boolean \  
Config value incoming_server2server_share_enabled for app files_sharing set to yes
```

The `config:app:set` command creates the value, if it does not already exist. To update an existing value, set `--update-only`:

```
sudo -u www-data ./occ config:app:set \  
  doesnotexist \  
  --value=true \  
  --type=boolean \  
  --update-only \  
Value not updated, as it has not been set before.
```

General Config Commands

These commands manage listing and importing configurations.

`config:import`

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 ./occ config:import filename.json
```

It is also possible to import remote files, by piping the input:

```
sudo -u www-data ./occ config:import < local-backup.json
```



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.

config:list

The `config:list` command lists all configuration values for your ownCloud setup as well as for any apps.

```
sudo -u www-data ./occ config:list [options] [--] [<app>]
```

Arguments

<code>app</code>	Name of the app. You can use "system" to get the config.php values, or "all" (the default) for all apps and system.
------------------	---

Options

<code>--private</code>	Use this option when you want to include sensitive configs, like passwords and salts.
------------------------	---

By default, passwords and other sensitive data are omitted from the report so that the output can be posted publicly (e.g., as part of a bug report). You can see a sample output in the example below.

```
Unresolved directive in
modules/admin_manual/pages/configuration/server/occ_commands/core_commands/_config_commands.adoc - include::partial$configuration/server/occ_command/config-list-report.json[]
```

Displaying Sensitive Information

To generate a full report which includes sensitive values, such as passwords and salts, use the `--private` option, as in the following example.

```
sudo -u www-data ./occ config:list --private
```

Filtering Information Reported

The output can be filtered to just the core information, core and apps, or one specific app. In the example below, you can see how to filter for each of these categories.

```
# List only system configuration details
```

```

sudo -u www-data ./occ config:list -- system

# List system and app configuration details
# This is the default, so doesn't need to be explicitly specified
sudo -u www-data ./occ config:list -- all

# List configuration details of the dav app
sudo -u www-data ./occ config:list -- dav

```

Below is an example of listing the config details for a single app.

```

{
  "apps": {
    "files_versions": {
      "enabled": "yes",
      "installed_version": "1.3.0",
      "types": "filesystem"
    }
  }
}

```

Config System Commands

These commands manage system configurations.

config:system:delete

```

sudo -u www-data ./occ config:system:delete [options] [--] <name> (<name>)...

```

Arguments

name	Name of the config to delete, specify multiple for array parameter.
------	---

Options

--error-if-not-exists	Checks whether the config exists before deleting it.
--output=[OUTPUT]	The output format to use (plain, json or json_pretty, default is plain).

Examples:

```

sudo -u www-data ./occ config:system:delete maintenance:mode
System config value maintenance:mode deleted

```

config:system:get

```
sudo -u www-data ./occ config:system:get [options] [--] <name> (<name>)...
```

Arguments

name	Name of the config to get. Specify multiple for array parameter.
------	--

Options

--default-value[=DEFAULT-VALUE]	If no default value is set and the config does not exist, the command will exit with 1.
--output=[OUTPUT]	The output format to use (plain, json or json_pretty, default is plain).

Examples:

```
sudo -u www-data ./occ config:system:get version
10.7.0.4
```

config:system:set

```
sudo -u www-data ./occ config:system:set [options] [--] <name> (<name>)...
```

Arguments

name	Name of the config parameter, specify multiple for array parameter. Must not be an empty string.
------	--

Options

--type=[TYPE]	Value type to use (string, integer, double, boolean, json, default is string). Note: you must use json to write multi array values.
--value=[VALUE]	The new value of the config.
--update-only	Only updates the value. If it is not set before, it is not being added.
--output=[OUTPUT]	The output format to use (plain, json or json_pretty, default is plain).



In order to write a boolean, float, JSON, or integer value to the configuration file, you need to specify the type of your command. This applies only to the `config:system:set` command. See table above for available types.

Examples

Disable the maintenance mode:

```
sudo -u www-data ./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 because of multi array values):

```
sudo -u www-data ./occ config:system:set apps_paths \  
  --type=json \  
  --value='[  
    {  
      "path":"/var/www/owncloud/apps",  
      "url":"/apps",  
      "writable": false  
    },  
    {  
      "path":"/var/www/owncloud/apps-external",  
      "url":"/apps-external",  
      "writable": true  
    }  
  ]'
```

Adding Redis to the configuration:

```
sudo -u www-data ./occ config:system:set \  
  redis \  
  --value '{"host": "127.0.0.1", "port": "6379"}' \  
  --type json  
  
System config value redis set to json {"host": "127.0.0.1", "port": "6379"}
```

Some configurations (e.g., the trusted domain setting) are an array of data. The array starts counting with 0. 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 ./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 ./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 ./occ config:system:get trusted_domains
localhost
owncloud.local
example.com
```

Config 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 will generate 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
```



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.



These instructions assume that you have a fully working and configured webserver. If not, please refer to the documentation on configuring [Configure the](#)

[Web Server](#) for detailed instructions.

Apply the [correct permissions](#) to your ownCloud directories. Then choose your `occ` options. This lists your available options:

```
sudo -u www-data ./occ 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
```


Command Description

Display your `maintenance:install` options.

```
sudo -u www-data ./occ help maintenance:install
ownCloud is not installed - only a limited number of commands are available
Usage:
```

```
maintenance:install [--database=["..."]] [--database-connection-string=["..."]] \  
                   [--database-name=["..."]] [--database-host=["..."]] \  
                   [--database-user=["..."]] [--database-pass=["..."]] \  
                   [--database-table-prefix=["..."]] [--admin-user=["..."]] \  
                   [--admin-pass=["..."]] [--data-dir=["..."]]
```

Options

<code>--database</code>	Supported database type (default: <code>sqlite</code>). The supported values are: <ul style="list-style-type: none">• <code>mysql</code>: MySQL/MariaDB• <code>oci</code>: Oracle (<i>ownCloud Enterprise edition only</i>)• <code>pgsql</code>: PostgreSQL• <code>sqlite</code>: SQLite3 (<i>ownCloud Community edition only</i>)
<code>--database-connection-string</code>	An Oracle-specific connection string.  As soon as this parameter is provided, other parameters like <code>database-host</code> and <code>database-name</code> are not used and do not need to be provided. For example: Example <pre>sales= (DESCRIPTION= (AADDRESS= (PROTOCOL=tcp)(HOST=sales-server)(PORT=1521)) (CONNECT_DATA= (SERVICE_NAME=sales.us.acme.com)))</pre>
<code>--database-name</code>	Name of the database.
<code>--database-host</code>	Hostname of the database (default: <code>localhost</code>).
<code>--database-user</code>	User name to connect to the database.
<code>--database-pass</code>	Password of the database user.
<code>--database-table-prefix</code>	Prefix for all tables (default: <code>oc_</code>).
<code>--admin-user</code>	Password of the admin account.
<code>--data-dir</code>	Path to data directory (default: <code>/var/www/owncloud/data</code>).

Example

This example completes the installation:

```
cd /var/www/owncloud/
sudo -u www-data ./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

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:

Command Description

```
sudo -u www-data ./occ upgrade --help
Usage:
upgrade [options]
```

Options

<code>--major</code>	Automatically update apps to new major versions during minor updates of ownCloud Server.
<code>--no-app-disable</code>	Skip disabling of third party apps.

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 [the maintenance upgrade documentation](#)) use this command to upgrade your databases, like this example on CentOS Linux:

```
sudo -u www-data ./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 <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 ./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
```

DAV Commands

A set of commands to create and sync address books and calendars:

```
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
```



These commands are not available in [single-user \(maintenance\) mode](#).

Cleanup Chunks

`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.

```
sudo -u www-data ./occ dav:cleanup-chunks [options] [--] [<minimum-age-in-days>]
```

Arguments

<code>minimum-age-in-days</code>	Minimum age of uploads to cleanup (in days - minimum 2 days - maximum 100) [default: 2]
----------------------------------	---

Options

<code>-l</code> <code>--local</code>	Only delete chunks that exist on the local filesystem. This applies to setups with multiple servers connected to the same database and chunk folder is not shared among them.
---	---

Example

In the example below, chunks older than 10 days will be removed.

```
sudo -u www-data ./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 [>-----]
```

Create Addressbook

Create a dav address book.

```
sudo -u www-data ./occ dav:create-addressbook <user> <name>
```

Arguments

<code>user</code>	User for whom the address book will be created
<code>name</code>	Name of the addressbook

Example

This example creates the address book `mollybook` for the user `molly`:

```
sudo -u www-data ./occ dav:create-addressbook molly mollybook
```

Molly will immediately see her address book.

Create Calendar

Create a dav calendar.

```
sudo -u www-data ./occ dav:create-calendar <user> <name>
```

Arguments

<code>user</code>	User for whom the calendar will be created
-------------------	--

<code>name</code>	Name of the calendar
-------------------	----------------------

Example

This example creates a new calendar `mollycal` for user `molly`:

```
sudo -u www-data ./occ dav:create-calendar molly mollycal
```

Molly will immediately see her calendar.

Sync Birthday Calendar

Synchronizes the birthday calendar. It adds all birthdays to your calendar from address books shared with you.

```
sudo -u www-data ./occ dav:sync-birthday-calendar [<user>]
```

Arguments

<code>user</code>	User for whom the birthday calendar will be synchronized
-------------------	--

Example

This example syncs to your calendar from user `bernie`:

```
sudo -u www-data ./occ dav:sync-birthday-calendar bernie
```

Sync System Addressbook

Synchronizes all users to the system addressbook.

```
sudo -u www-data ./occ dav:sync-system-addressbook
```

Database Commands

Database Conversion Commands

Convert the Database Type

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
```

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 ./occ db:convert-type mysql oc_dbuser 127.0.0.1 oc_database
```



For a more detailed explanation see [converting database types](#).

Convert the MySQL Charset

Convert charset of MySQL/MariaDB to use utf8mb4. If you are using an older ownCloud installation, the database may not be setup to use the 4-byte unicode charset. This command changes the database charset to use **utf8mb4**. Check your database charset before you use this command.

```
sudo -u www-data ./occ db:convert-mysql-charset
```

Restore the Table Format

This command sets the default row format of MySQL/MariaDB tables. This is only necessary once before you are going to e.g. install MariaDB 10.6 or higher because the COMPRESSED row format is now read-only by default. As a prerequisite, ownCloud 10.9 needs to be installed first. See the [Database Upgrade](#) guide for details.

```
sudo -u www-data ./occ db:restore-default-row-format
```

Encryption

occ includes a complete set of commands for managing encryption. When using a HSM (Hardware Security Module, can also be emulated by software), additional occ encryption-related commands can be used.

```
encryption
config:app:set encryption encryptHomeStorage Encrypt the users home storage

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
```


<code>encryption:encrypt-all</code>	Encrypt all files for all users
<code>encryption:fix-encrypted-version</code>	Fix the encrypted version if the encrypted file(s) are not downloadable.
<code>encryption:list-modules</code>	List all available encryption modules
<code>encryption:migrate</code>	Initial migration to encryption 2.0
<code>encryption:recreate-master-key</code>	Replace existing master key with new one. Encrypt the file system with newly created master key
<code>encryption:select-encryption-type</code>	Select the encryption type. The encryption types available are: <code>masterkey</code> and <code>user-keys</code> . There is also no way to disable it again.
<code>encryption:set-default-module</code>	Set the encryption default module
<code>encryption:show-key-storage-root</code>	Show current key storage root
<code>encryption:status</code>	Lists the current status of encryption

When using a HSM (Hardware Security Module, additional `occ` encryption-related commands can be used, see the HSM `occ` documentation below. The `occ` commands can also be used when HSM is initiated via software emulation like `SoftHSM2`.

<code>encryption</code>	
<code>encryption:hsmdaemon</code>	Export or Import the Masterkey
<code>encryption:hsmdaemon:decrypt</code>	Decrypt a String
<code>config:app:set encryption</code>	Various encryption configuration commands for HSM

Status

`occ 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 `occ encryption:enable`:

```
sudo -u www-data ./occ app:enable encryption
sudo -u www-data ./occ encryption:enable
sudo -u www-data ./occ encryption:status
- enabled: true
- defaultModule: OC_DEFAULT_MODULE
```

Encrypt the Users Home Storage

Server-side encryption for local storage like the users home and remote storages like Google Drive can operate independently of each other. By doing so, you can encrypt a remote storage without also having to encrypt the users home storage on your ownCloud server. Possible values are `0` and `1`

```
config:app:set encryption encryptHomeStorage --value '1'
```

Change Key Storage Root

`encryption:change-key-storage-root` is for moving your encryption keys to a different folder within your data directory. It takes one argument, which defines your new root folder. The folder must exist and the path is relative to your data directory.

```
sudo -u www-data ./occ encryption:change-key-storage-root ../data/security/oc-keys
```

You can see the current location of your keys folder:

```
sudo -u www-data ./occ encryption:show-key-storage-root
Current key storage root: default storage location (data/)
```

List Modules

`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.

Encrypt All

`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.

Arguments

<code>-y</code>	Answer yes to all questions.
<code>--yes</code>	This argument automatically answers, potential, questions with "yes", which is particularly important for automated deployments with Ansible or similar tools.

Decrypt All

`encryption:decrypt-all` decrypts all user data files, or optionally a single user:

```
sudo -u www-data ./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, using [the maintenance commands](#), to prevent any user activity until decryption is completed.

Arguments

-m=[METHOD]	Accepts the methods: <i>recovery</i> or <i>password</i> If the <i>recovery</i> method is chosen, then the recovery password will be used to decrypt files. If the <i>password</i> method is chosen, then individual user passwords will be used to decrypt files.
-c=[COMMAND]	Accepts the commands: <i>yes</i> or <i>no</i> This lets the command know whether to ask for permission to continue or not.

Method Descriptions

Recovery method

This method reads the value from the environment variable `OC_RECOVERY_PASSWORD`. This variable bounds the value of recovery password set in the encryption page. If this variable is not set the recovery process will be halted. This has to be used for decrypting all users. While opting recovery method user should not forget to set `OC_RECOVERY_PASSWORD` in the shell.

Password method

This method reads the value from the environment variable `OC_PASSWORD`. This variable bounds the value of user password. The password which user uses to login to oC account. When password method is opted the user needs to set this variable in the shell.

Continue Option Description

The continue option can be used to bypass the permissions asked like *yes* or *no* while decrypting the file system. If the user is sure about what he/she is doing with the command and would like to proceed, then `-c yes` when provided to the command would not ask permissions. If `-c no` is passed to the command, then permissions would be asked to the user. It becomes interactive.

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.

Fix Encrypted Version

```
sudo -u www-data ./occ encryption:fix-encrypted-version [options] [--] <user>
```

`encryption:fix-encrypted-version` fixes the encrypted version of files if the encrypted file(s) are not downloadable for a given user. You only need this command if you get an "Invalid Signature" message in the browser or the clients.

Background: the `oc_filecache` database table contains the integer columns "version" and "encryptedVersion" which start with 1 and are incremented on every file modification. When using encryption, those values are used together with the ciphertext to generate a cryptographic signature for the file. The version value is required to verify the signature. In some very rare cases like timeouts or bugs etc., the value might not get updated accordingly or get lost. The brute-force approach is to use the `fix:encrypted:version` command until the file can be decrypted. Starting with ownCloud 10.8, the behavior of the command got improved so that the encryptedVersion value is reset to its original value if no correct version was found. Before that fix, the last tried value was stored in the database thus modifying the state of the system and making further rescue attempts non-deterministic.

Arguments

<code>user</code>	The id of the user whose files need fixing.
-------------------	---

Options

<code>-p</code> <code>--path=PATH</code>	Limit files to fix with path, e.g., <code>--path="/Music/Artist"</code> . If path indicates a directory, all the files inside directory will be fixed.
<code>-i</code> <code>--increment-range=INCREMENT</code> <code>-RANGE</code>	Find the correct version of the file to verify the signature. Searches in increments from -n to +n. [default: "5"]

HSM Related Commands

Export or Import the Masterkey

```
sudo -u www-data ./occ encryption:hsmdaemon [options]
```

Options

<code>--export-masterkey</code>	Export the private master key in base64
<code>--import-masterkey=IMPORT-MASTERKEY</code>	Import a base64 encoded private masterkey.

`--export-masterkey` prints the `base64_encode` of the file `data/files_encryption/OC_DEFAULT_MODULE/master_*.privateKey`.

The private key file in the directory may be named like `master_08ea43b7.privateKey`.

Test to Decrypt a String

Allows to test the `hsmdaemon` setup by providing an encrypted string to ownCloud and test if it can be decrypted.

```
sudo -u www-data ./occ encryption:hsmdaemon:decrypt [options] [--] <decrypt>
```

Arguments

<code>decrypt</code>	The string to decrypt
----------------------	-----------------------

Options

<code>--username[=USERNAME]</code>	The name of the user who is able to decrypt the provided string
<code>--keyId[=KEYID]</code>	The keyId which was used to encrypt the provided string

Set the HSM URL

Set the url on which the `hsmdaemon` REST-API is reachable.

```
sudo -u www-data ./occ config:app:set encryption hsm.url --value 'http://127.0.0.1:8513'
```

Set the JSON Web Token Secret

To access the `hsmdaemon` API, ownCloud must authenticate with a JWT (JSON Web Token). The given secret is shared between the `hsmdaemon` (see the `hsmdaemon.toml` configuration file) and ownCloud to sign the JWT. See the [HSM documentation](#) for an example how to generate a secret.

```
sudo -u www-data ./occ config:app:set encryption hsm.jwt.secret --value '7a7d1826-b514-4d9f-afc7-a7485084e8de'
```

Set the JWT Clockskew

The JWT described above has an expiry timestamp. In case the time clocks on ownCloud and `hsmdaemon` system drift or skew apart, additional time is added to the expiry time to counteract this situation. Set or change the clockskew only if ownCloud advises to do so. Defaults to 120, value is in seconds.

```
sudo -u www-data ./occ config:app:set encryption hsm.jwt.clockskew --value '120'
```

Federation Sync

Synchronize the address books of all federated ownCloud servers.

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 ./occ federation:sync-addressbooks
```



This command is only available when the "Federation" app ([federation](#)) is enabled.

File Operations

`occ` has the following commands for managing files in ownCloud.

```
files
files:check-cache          Check if the target file exists in the primary storage
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).
files:troubleshoot-transfer-ownership Scan for problems that might have occurred while running
ownership transfer
```



These commands are not available in [single-user \(maintenance\) mode](#).

The `files:check-cache` command

The main purpose of this command is to clear the cache for objectstores (`objectstore` and `files_primary_S3` apps) as primary storage, but it is not limited to this type of storage. It can be used for any other type as long it is the primary storage.

Files in the primary storage could be deleted outside of ownCloud, leaving information in ownCloud's file cache. This command intends to check if the target file can be read from the primary backend storage and, if not, allows you to remove the information cached.



Removing files directly from the primary storage is not supported and should not happen. As such, the cases where you need to run this command should be extremely rare. This is why this command is only provided to check for one file instead of scanning the whole of ownCloud's filesystem.

```
sudo -u www-data ./occ files:check-cache --help
Usage:
files:check-cache [options] [--] <uid> <target-file>
```

Arguments

<code>uid</code>	The user (user id) who owns the file
<code>target-file</code>	The file we want to check

Options

<code>--remove</code>	Remove the file from the cache if it's missing in the backend
-----------------------	---

Examples of checking files for user maria:

```
sudo -u www-data ./occ files:check-cache maria welcome.txt
```

```
welcome.txt has been accessed properly
```

```
sudo -u www-data ./occ files:check-cache maria maria@smbhome/myfile.txt
```

```
Ignoring maria@smbhome/myfile.txt because it is shared or not inside the primary storage
```

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`).



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.

```
sudo -u www-data ./occ files:checksums:verify
```

```
This operation might take very long.
```

```
Mismatch for files/welcome.txt:
```

```
Filecache:  SHA1:eeb2c08011374d8ad4e483a4938e1aa1007c089d
```

```
MD5:368e3a6cb99f88c3543123931d786e21  ADLER32:c5ad3a63
```

```
Actual:  SHA1:da39a3ee5e6b4b0d3255bfef95601890afd80709
```

```
MD5:d41d8cd98f00b204e9800998ecf8427e  ADLER32:00000001
```

```
Mismatch for thumbnails/9/2048-2048-max.png:
```

```
Filecache:  SHA1:2634fed078d1978f24f71892bf4ee0e4bd0c3c99
```

```
MD5:dd249372f7a68c551f7e6b2615d49463 ADLER32:821230d4
Actual: SHA1:da39a3ee5e6b4b0d3255bfef95601890afd80709
MD5:d41d8cd98f00b204e9800998ecf8427e ADLER32:00000001
```

Options

<code>-r, --repair</code>	Repair filecache-entry with mismatched checksums.
<code>-u, --user=USER</code>	Specific user to check.
<code>-p, --path=PATH</code>	Path to check relative to user folder. [default: ""]. For example, if the user's id was "john" and the <code>--path</code> value was "tree/apple", the command would check the ownCloud directory <code>/john/files/tree/apple</code> .

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 ./occ files:scan --help
Usage:
  files:scan [options] [--] [<user_id>]...
```

Arguments

<code>user_id</code>	Will rescan all files of the given user(s).
----------------------	---

Options

<code>--output=[OUTPUT]</code>	The output format to use (<code>plain</code> , <code>json</code> or <code>json_pretty</code> , default is <code>plain</code>).
<code>-p --path=[PATH]</code>	Limit rescan to this path, e.g. <code>--path="/alice/files/Music"</code> , the <code>user_id</code> is determined by the path and the <code>user_id</code> parameter and <code>--all</code> are ignored.
<code>--group=[GROUP]</code>	Scan user(s) under the group(s). This option can be used as <code>--group=foo --group=bar</code> to scan groups <code>foo</code> and <code>bar</code> (multiple values allowed)

<code>-g --groups=[GROUP]</code>	Scan user(s) under the group(s). This option can be used as <code>--groups=foo,bar</code> to scan groups foo and bar (multiple values allowed separated by commas)
<code>-q --quiet</code>	Do not output any message.
<code>--all</code>	Will rescan all files of all known users.
<code>--repair</code>	Will repair detached filecache entries (slow).
<code>--unscanned</code>	Only scan files which are marked as not fully scanned.



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 the following command:

```
sudo -u www-data ./occ files_external:list user_id
```



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.



Mounts based on session credentials can not be scanned as the users credentials are not available to the occ command set.

The `--path`, `--all`, `--group`, `--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.



We strongly suggest that you backup the database before running this command.

The `--repair` option can be run within two different scenarios:

- Requiring a downtime when used on all affected storages at once.
- Without downtime, filtering by a specified User Id.

The following commands show how to enable single user mode, run a repair file scan in bulk on all storages, and then disable single user mode. This way is much faster than running the command for every user separately, but it requires single user mode.

```
sudo -u www-data ./occ maintenance:singleuser --on
sudo -u www-data ./occ files:scan --all --repair
sudo -u www-data ./occ maintenance:singleuser --off
```

The following command filters by the storage of the specified user.

```
sudo -u www-data ./occ files:scan USERID --repair
```



If many users are affected, it could be convenient to create a shell script, which iterates over a list of User ID's.

The `files:transfer-ownership` command

You may transfer all files and **outgoing** shares from one user to another.

Incoming shares are not transferred.

If the target users don't exist, they will be created.

This command is useful before removing users.

```
sudo -u www-data ./occ files:transfer-ownership --help
Usage:
files:transfer-ownership [options] [--] <source-user> <destination-user>
```

Arguments

<code>source-user</code>	owner of files which shall be moved
<code>destination-user</code>	user who will be the new owner of the files

Options

<code>--path=[PATH]</code>	selectively provide the path to transfer. For example <code>--path="folder_name"</code>
<code>-S,</code> <code>--accept-skipped-shares</code>	always confirm to continue in case of skipped shares.
<code>--destination-use-user-folder</code>	transfer directly to top-level user folder, operation only possible if destination user never logged in and command aborts otherwise.

For example, to move all files from `<source-user>` to `<destination-user>` transfer folder, use the following command:

```
sudo -u www-data ./occ files:transfer-ownership \  
  <source-user> \  
  <destination-user>
```

You can also move a limited set of files from `<source-user>` to `<destination-user>` transfer folder by making use of the `--path` switch, as in the example below. Ownership of `folder/to/move` and all files and folders which it contains will be transferred to `<destination-user>` transfer folder.

```
sudo -u www-data ./occ files:transfer-ownership \  
  --path="folder/to/move" \  
  <source-user> \  
  <destination-user>
```

If the entire user folder of `<source-user>` needs to be migrated to `<destination-user>` user folder, use the `--destination-use-user-folder` switch, as in the example below. The destination user needs to be created but never log in, we recommend using owncloud maintenance mode for this operation.

```
sudo -u www-data ./occ files:transfer-ownership \  
  --destination-use-user-folder \  
  <source-user> \  
  <destination-user>
```

Please keep the following in mind when using this command:

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 will be moved into the destination user's `files` directory, into a directory name 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.

The `files:troubleshoot-transfer-ownership` command

This command is used to scan for problems, that might have occurred during a run of ownership transfer using the above command `files:transfer-ownership`. It can also be used to automatically attempt to fix problems. For example, transferred shares that may now have an invalid share owner.



By default, the command performs a dry run and displays the problems found to the console output.

```
sudo -u www-data ./occ files:troubleshoot-transfer-ownership --help
Usage:
files:troubleshoot-transfer-ownership [options] [--] [<type>]
```

Arguments

<code>type</code>	"all", "invalid-owner", "invalid-initiator", [default: ""]
-------------------	---

Options

<code>-f, --fix</code>	perform auto-fix for found problems
<code>-u, --uid=UID</code>	scope for particular user

Run the command with one of the type arguments:

```
sudo -u www-data ./occ files:troubleshoot-transfer-ownership \  
<all|invalid-owner|invalid-initiator>
```

The command can attempt to fix the issues with the `--fix` flag, or execute for a single user using `--uid <uid>`

```
sudo -u www-data ./occ files:troubleshoot-transfer-ownership all \  
--fix \  
--uid=UID
```

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
```

<code>files_external:create</code>	Create a new mount configuration
<code>files_external:delete</code>	Delete an external mount
<code>files_external:export</code>	Export mount configurations
<code>files_external:import</code>	Import mount configurations
<code>files_external:list</code>	List configured mounts
<code>files_external:option</code>	Manage mount options for a mount
<code>files_external:verify</code>	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.



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] [-s|--short] [--]
[<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.
----------------------	--

Options

<code>--show-password</code>	Show passwords and secrets
<code>--mount-options</code>	Show all mount options independent if they are set to their default value or not
<code>--full</code>	Don't truncate long values in table output
<code>-a, --all</code>	Show both system-wide mounts and all personal mounts.
<code>-s, --short</code>	Show only a reduced mount info.
<code>-i, --importable</code> <code>-format</code>	Provide output values in a format compatible with <code>files_external:import</code>
<code>--output=[OUTPUT]</code>	The output format to use (<code>plain</code> , <code>json</code> or <code>json_pretty</code> , default is <code>plain</code>).

Example

```
sudo -u www-data ./occ files_external:list user_1 --short
+-----+-----+-----+
| Mount ID | Mount Point      | Type      |
+-----+-----+-----+
| 1        | /mount_1         | Personal  |
| 2        | /mount_2         | Personal  |
+-----+-----+-----+
```



The `--importable-format` option helps to make the technical mount settings visible. To see all settings you still need to use the other options such as `--show-password`, `--full` and `--all`. When you want to export the mount settings for later import, use the `files_external:export` command. `files_external:export` ensures that all the necessary settings are included in the output.

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>	Can be obtained using <code>occ files_external:list</code> .
-----------------------	--

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=[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

<code>type</code>	Only show backends of a certain type. Possible values are <code>authentication</code> or <code>storage</code> .
<code>backend</code>	Only show information of a specific backend.

Options

<code>--output=[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

<code>mount_id</code>	The ID of the mount to edit.
<code>key</code>	Key of the config option to set/get.
<code>value</code>	Value to set the config option to, when no value is provided the existing value will be printed.

Options

<code>--output=[OUTPUT]</code>	The output format to use (<i>plain</i> , <i>json</i> or <i>json_pretty</i> . The default is plain).
--------------------------------	--

files_external:create

Create a new mount configuration.

Usage

[source,plaintext

```
files_external:create [options]
  [--]
  <mount_point>
  <storage_backend>
  <authentication_backend>
```

Arguments

<code>mount_point</code>	Mount point for the new mount.
<code>storage_backend</code>	Storage backend identifier for the new mount, see <code>occ files_external:backends</code> for possible values.
<code>authentication_backend</code>	Authentication backend identifier for the new mount, see <code>occ files_external:backends</code> for possible values.

Options

<code>--user=[USER]</code>	User to add the mount configurations for, if not set the mount will be added as system mount.
<code>-c,</code> <code>--config=[CONFIG]</code>	Mount configuration option in <code>key=value</code> format (multiple values allowed).
<code>--dry</code>	Don't save the imported mounts, only list the new mounts.
<code>--output=[OUTPUT]</code>	The output format to use (<code>plain</code> , <code>json</code> or <code>json`pretty</code>). The default is <code>plain</code> .

Storage Backend Details

Storage Backend	Identifier
Windows Network Drive	<code>windows_network_drive</code>
WebDav	<code>dav</code>
Local	<code>local</code>
ownCloud	<code>owncloud</code>
SFTP	<code>sftp</code>
Amazon S3	<code>amazons3</code>
Dropbox	<code>dropbox</code>
Google Drive	<code>googledrive</code>

Storage Backend	Identifier
SMB / CIFS	<code>smb</code>

Authentication Details

Authentication method	Identifier, name, configuration
Log-in credentials, save in session	<code>password::sessioncredentials</code>
Log-in credentials, save in database	<code>password::logincredentials</code>
User entered, store in database	<code>password::userprovided (*)</code>
Global Credentials	<code>password::global</code>
None	<code>null::null</code>
Builtin	<code>builtin::builtin</code>
Username and password	<code>password::password</code>
OAuth1	<code>oauth1::oauth1 (*)</code>
OAuth2	<code>oauth2::oauth2 (*)</code>
RSA public key	<code>publickey::rsa (*)</code>
OpenStack	<code>openstack::openstack (*)</code>
Rackspace	<code>openstack::rackspace (*)</code>
Access key (Amazon S3)	<code>amazons3::accesskey (*)</code>

(*) - Authentication methods require additional configuration.



Each Storage Backend needs its corresponding authentication methods.

`files_external:delete`

Delete an external mount.

Usage

```
files_external:delete [options] [--] <mount_id>
```

Arguments

<code>mount_id</code>	The ID of the mount to edit.
-----------------------	------------------------------

Options

<code>-y, --yes</code>	Skip confirmation.
<code>--output=[OUTPUT]</code>	The output format to use (plain, json or json_pretty, default is plain).

files_external:export

Usage

```
files_external:export [options] [--] [<user_id>]
```

Arguments

<code>user_id</code>	User ID to export the personal mounts for, if no user is provided admin mounts will be exported.
----------------------	--

Options

<code>-a, --all</code>	Show both system-wide mounts and all personal mounts.
------------------------	---

files_external:import

Import mount configurations.

Usage

[source,plaintext

```
files_external:import [options] [--] <path>
```

Arguments

<code>path</code>	Path to a json file containing the mounts to import, use - to read from stdin.
-------------------	--

Options

<code>--user=[USER]</code>	User to add the mount configurations for, if not set the mount will be added as system mount.
<code>--dry</code>	Don't save the imported mounts, only list the new mounts.
<code>--output=[OUTPUT]</code>	The output format to use (<i>plain</i> , <i>json</i> or <i>json_pretty</i> , default is <i>plain</i>).

files_external:option

Manage mount options for a mount.

Usage

```
files_external:option <mount_id> <key> [<value>]
```

Arguments

<code>mount_id</code>	The ID of the mount to edit.
<code>key</code>	Key of the mount option to set/get.
<code>value</code>	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

<code>mount_id</code>	The ID of the mount to check.
-----------------------	-------------------------------

Options

<code>-c,</code> <code>--config=[CONFIG]</code>	Additional config option to set before checking in <code>key=value</code> pairs, required for certain auth backends such as login credentials (multiple values allowed).
<code>--output=[OUTPUT]</code>	The output format to use (<i>plain</i> , <i>json</i> or <i>json_pretty</i> , default is <i>plain</i>).

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 ./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

<code>--output=[OUTPUT]</code>	Output format (plain, json or json_pretty, default is plain) [default: "plain"].
--------------------------------	--

This example lists groups containing the string "finance".

```
sudo -u www-data ./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 ./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

<code>--output=[OUTPUT]</code>	Output format (plain, json or json_pretty, default is plain) [default: "plain"].
--------------------------------	--

This example lists members of the "Finance" group.

```
sudo -u www-data ./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 ./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 ./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 ./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 ./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 ./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 ./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.

<code>integrity</code>	
<code>integrity:check-app</code>	Check app integrity using a signature.
<code>integrity:check-core</code>	Check core integrity using a signature.
<code>integrity:sign-app</code>	Signs an app using a private key.
<code>integrity:sign-core</code>	Sign core using a private key

After creating your signing key, sign your app like this example:

```
sudo -u www-data ./occ integrity:sign-app \  
  --privateKey=/Users/karlmay/contacts.key \  
  --certificate=/Users/karlmay/CA/contacts.crt \  
  --path=/Users/karlmay/Programming/contacts
```

Verify your app:

```
sudo -u www-data ./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.

`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.



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:createjvs          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 Comments app.



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/comments/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 ./occ l10n:createjs comments de_AT
```

This will generate two translation files, `de_AT.js` and `de_AT.json`, in `/var/www/owncloud/apps/comments/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 ./occ l10n:createjs comments 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
```

Command Description

Run `log:owncloud` to see your current logging status:

```
sudo -u www-data ./occ log:owncloud
Log backend ownCloud: enabled
Log file: /opt/owncloud/data/owncloud.log
Rotate at: disabled
```

Options

<code>--enable</code>	Enable this logging backend.
<code>--file=[FILE]</code>	Set the log file path.
<code>--rotate-size=[ROTATE-SIZE]</code>	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`:

<code>--backend=[BACKEND]</code>	Set the logging backend [owncloud, syslog, errorlog].
<code>--level=[LEVEL]</code>	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 ./occ log:manage --level 4
sudo -u www-data ./occ log:manage --level error
```



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.

Managing Background Jobs

Use the `background:queue` command to manage background jobs.

```
background:queue
background:queue:delete    Delete a job from the queue
background:queue:execute  Run a single background job from the queue
background:queue:status   List queue status
```

Deleting a Background Job

The command `background:queue:delete` deletes a queued background job. It requires the job id of the job to be deleted.

```
background:queue:delete <Job ID>
```

Arguments

<code>Job ID</code>	ID of the job to be deleted
---------------------	-----------------------------



Deleting a job cannot be undone. Be sure that you want to delete the job before doing so.

This example deletes queued background job #12.

```
sudo -u www-data ./occ background:queue:delete 12

Job has been deleted.
```

Executing a Background Job

The command `background:queue:execute` executes a queued background job. It requires the job id of the job to be executed.

```
background:queue:execute [options] [--] <Job ID>
```

Arguments

Job ID	ID of the job to be deleted
--------	-----------------------------

Options

-f --force	Force run the job even if within timing interval
--accept-warning	No warning about the usage of this command will be displayed

This example executes queued background job #12.

```
sudo -u www-data ./occ background:queue:execute 12
```

```
This command is for maintenance and support purposes.
This will run the specified background job now. Regular scheduled runs of the job will
continue to happen at their scheduled times.
If you still want to use this command please confirm the usage by entering: yes
yes
Found job: OCA\UpdateNotification\Notification\BackgroundJob with ID 12
Running job...
Finished in 0 seconds
```

List Queued Backgroundjobs

The command `background:queue:status` will list queued background jobs, including details when it last ran.

```
background:queue:status
```

This example lists the queue status:

```
sudo -u www-data ./occ background:queue:status
```

```
+----+-----+-----+-----+
+-----+
| Id | Job                               | Last run           |
Job Arguments |
+----+-----+-----+-----+
+-----+
| 1  | OCA\Files\BackgroundJob\ScanFiles | 2018-06-13T15:15:04+00:00 |
|   |                                     |                         |
| 2  | OCA\Files\BackgroundJob\DeleteOrphanedItems | 2018-06-13T15:15:04+00:00 |
|   |                                     |                         |
+-----+
```

3	OCA\Files\BackgroundJob\CleanupFileLocks	2018-06-13T15:15:04+00:00
4	OCA\DAV\CardDAV\SyncJob	2018-06-12T19:15:02+00:00
5	OCA\Federation\SyncJob	2018-06-12T19:15:02+00:00
6	OCA\Files_Sharing\DeleteOrphanedSharesJob	2018-06-13T15:15:04+00:00
7	OCA\Files_Sharing\ExpireSharesJob	2018-06-12T19:15:02+00:00
8	OCA\Files_Trashbin\BackgroundJob\ExpireTrash	2018-06-13T15:15:04+00:00
9	OCA\Files_Versions\BackgroundJob\ExpireVersions	2018-06-13T15:15:04+00:00
10	OCA\UpdateNotification\Notification\BackgroundJob	2018-06-12T19:15:03+00:00
11	OC\Authentication\Token\DefaultTokenCleanupJob	2018-06-13T15:15:04+00:00

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.

<code>maintenance</code>	
<code>maintenance:data-fingerprint</code>	Update the systems data-fingerprint after a backup is restored
<code>maintenance:install</code>	Install ownCloud
<code>maintenance:mimetype:update-db</code>	Update database mimetypes and update filecache
<code>maintenance:mimetype:update-js</code>	Update mimetypeelist.js
<code>maintenance:mode</code>	Set maintenance mode
<code>maintenance:repair</code>	Repair this installation
<code>maintenance:singleuser</code>	Set single user mode
<code>maintenance:update:htaccess</code>	Updates the .htaccess file

Update the Systems Data-Fingerprint

When a backup has been restored, the ETag information, which is necessary when accessing ownCloud with clients, has been changed. Run the following command to tell desktop and mobile clients that a server backup has been restored.

```
sudo -u www-data ./occ maintenance:data-fingerprint
```

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.

Install ownCloud



This command is only available if the following key in your `config.php` is not present or set to `false`. This is the case when the installation has not been made or not finalized. This key automatically turns to `true` after a successful installation. This results in the command no longer being available.

```
'installed' => false,
```

```
sudo -u www-data ./occ maintenance:install [options]
```

The `maintenance:install` command supports the following options:

Option	Description
<code>--database=DATABASE</code>	Supported database type. [default: <code>sqlite</code>] Possible values: <code>sqlite</code> , <code>mysql</code> , <code>pgsql</code> , <code>oci</code> Note that <code>oci</code> (Oracle) is only available with the Enterprise license.
<code>--database-connection-string=DATABASE-CONNECTION-STRING</code>	Oracle specific connection string. As soon as this parameter is provided, other parameters like <code>database-host</code> and <code>database-name</code> are not used and do not need to be provided.
<code>--database-name=DATABASE-NAME</code>	Name of the database.
<code>--database-host=DATABASE-HOST</code>	Hostname of the database. [default: <code>"localhost"</code>]
<code>--database-user=DATABASE-USER</code>	User name to connect to the database.
<code>--database-pass=DATABASE-PASS</code>	Password of the database user.
<code>--database-table-prefix=DATABASE-TABLE-PREFIX</code>	Prefix for all tables (default: <code>oc_</code>).
<code>--admin-user=ADMIN-USER</code>	User name of the admin account. [default: <code>"admin"</code>]
<code>--admin-pass=ADMIN-PASS</code>	Password of the admin account.
<code>--data-dir=DATA-DIR</code>	Path to the data directory. [default: <code>"/var/www/owncloud/data"</code>]

Update Database Mimetypes

Update database mimetypes and file cache.

Usage:

```
sudo -u www-data ./occ maintenance:mimetype:update-db [options]
```

The `maintenance:mimetype:update-db` command supports the following options:

Option	Description
<code>--repair-filecache</code>	Repair the file cache for all mimetypes, not just the new ones.

Update the `mimetyplist.js` File

This command updates the `mimetyplist.js` file.

Usage:

```
sudo -u www-data ./occ maintenance:update-js
```

Enable or Disable Maintenance Mode

`maintenance:mode` command 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. Once you take the server out of maintenance mode, logged-in users must refresh their Web browsers to continue working.

Usage:

```
sudo -u www-data ./occ maintenance:mode [options]
```

The `maintenance:repair` command supports the following options:

Option	Description
<code>--on</code>	Enable maintenance mode.
<code>--off</code>	Disable maintenance mode.

Turn on maintenance mode:

```
sudo -u www-data ./occ maintenance:mode --on
```

Turn it off when you're finished with the maintenance tasks:

```
sudo -u www-data ./occ maintenance:mode --off
```

Installation Repair Commands

The `maintenance:repair` command helps administrators repair an installation. The command runs

automatically during upgrades to clean up the database. So, while you can run it manually, there usually isn't a need to.



Your ownCloud installation needs to be in maintenance mode to use the `maintenance:repair` command.

Usage:

```
sudo -u www-data ./occ maintenance:repair [options]
```

Repair Command Options

The `maintenance:repair` command supports the following options:

Option	Description
<code>--list</code>	Lists all possible repair steps.
<code>-s --single=SINGLE</code>	Run just one repair step given its class name.
<code>--include-expensive</code>	Use this option when you want to include resource and load expensive tasks.

Running All Repair Steps

Here is an example of running the command:

```
sudo -u www-data ./occ maintenance:repair
```

To list all off the possible repair steps, use the `--list` option. It should output the following list to the console:

```
Found 16 repair steps

OC\Repair\RepairMimeType -> Repair mime types
OC\Repair\RepairMismatchFileCachePath -> Detect file cache entries with path that does
not match parent-child relationships
OC\Repair\FillETags -> Generate ETags for file where no ETag is present.
OC\Repair\CleanTags -> Clean tags and favorites
OC\Repair\DropOldTables -> Drop old database tables
OC\Repair\DropOldJobs -> Drop old background jobs
OC\Repair\RemoveGetETagEntries -> Remove getetag entries in properties table
OC\Repair\RepairInvalidShares -> Repair invalid shares
OC\Repair\RepairSubShares -> Repair sub shares
OC\Repair\SharePropagation -> Remove old share propagation app entries
OC\Repair\MoveAvatarOutsideHome -> Move user avatars outside the homes to the new
location
OC\Repair\RemoveRootShares -> Remove shares of a users root folder
OC\Repair\RepairUnmergedShares -> Repair unmerged shares
```

```
OC\Repair\DisableExtraThemes -> Disable extra themes
OC\Repair\OldGroupMembershipShares -> Remove shares of old group memberships
OCA\DAV\Repair\RemoveInvalidShares -> Remove invalid calendar and addressbook shares
```

Running a Single Repair Step

To run a single repair step, use either the `-s` or `--single` options, as in the following example.

Usage:

```
sudo -u www-data ./occ maintenance:repair \
  --single="OCA\DAV\Repair\RemoveInvalidShares"
```



The step's name must be quoted, otherwise you will see the following warning message appear, and the command will fail: *"Repair step not found. Use --list to show available steps."*

Single User Mode

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.

Usage:

```
sudo -u www-data ./occ maintenance:singleuser --on
```

Turn it off when you're finished:

```
sudo -u www-data ./occ maintenance:singleuser --off
```

Update the .htaccess File

This command updates the `.htaccess` file.

Usage:

```
sudo -u www-data ./occ maintenance:update:htaccess
```

Migration Steps Command

You can run migration steps with the `migrations` command.

```
sudo -u www-data ./occ migrations:execute <app> <version>
```

Arguments

<code>app</code>	Name of the app this migration command shall work on.
<code>version</code>	The version to execute.

Example

This example executes the migration step for the core app:

```
sudo -u www-data ./occ migrations:execute core 20181220085457
```

Mimetype Update Commands

`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.

Notifications

If you want to send notifications to users or groups use the following command.

```
1 notifications
2 notifications:generate Generates a notification.
```

Command Description

```
sudo -u www-data ./occ notifications:generate [-u|--user USER] [-g|--group GROUP] [-l|--link <linktext>] [--] <subject> [<message>]
```

Arguments:

<code>subject</code>	The notification subject - maximum 255 characters.
<code>message</code>	A more extended message - maximum 4000 characters.
<code>linktext</code>	A link to an HTML page.

Options

<code>-u [USER]</code> <code>--user=[USER]</code>	User id to whom the notification shall be sent.
<code>-g [GROUP]</code> <code>--group=[GROUP]</code>	Group id to whom the notification shall be sent.
<code>-l [LINK]</code> <code>--link=[LINK]</code>	A link associated with the notification.

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 ./occ notifications:generate -g Office "Emergency Alert" "Rebooting in 5min"
```

Poll Incoming Federated Shares For Updates

This command must be used if received federated shares are being referenced by desktop clients but not regularly accessed via the webUI. This is because, for performance reasons, federated shares do not update automatically. Instead, federated share directories are only updated when users browse them using the [webUI](#).

ownCloud and system administrators can use the `incoming-shares:poll` command to poll federated shares for updates.



The command polls all received federated shares, so does not require a path.

```
sudo -u www-data ./occ incoming-shares:poll
```

When using federation, it is recommended to execute `occ incoming-shares:poll` regularly [using Cron jobs](#). The time interval between executions is a trade-off between the availability of changes in federated shares and resource consumption; which naturally depends a lot on the number of federated shares and the frequency of changes within those shares.



Executing the command once every 12 hours *should* be safe enough for most instances. However, the interval can be reduced to once every 2 hours, for instances with a small number of federated shares.

Depending on the desired resource consumption, this value should be lowered or increased based on individual expectations. To find a value that fits a specific setup, it is recommended to execute the command once, measure the execution time and set the interval, so that the background job can finish before the next execution is triggered.

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 load balancers etc.

Command Description

```
security:routes [options]
```

Options

<code>--output=[OUTPUT]</code>	Output format (plain, json or json-pretty, default is plain).
<code>--with-details</code>	Adds more details to the output.

Example 1:

```
sudo -u www-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 -u www-data ./occ security:routes --output=json-pretty
```

```
[
  {
    "path": "\\apps\\federation\\auto-add-servers",
    "methods": [
      "POST"
    ]
  },

```

Example 3:

```
sudo -u www-data ./occ security:routes --with-details
```

```
+-----+-----+
+-----+-----+
+-----+
| Path                                     | Methods | Controller
| Annotations                            |         |
+-----+-----+
+-----+
+-----+
| /apps/files/api/v1/sorting              | POST    |

```

```
OCA\Files\Controller\ApiController::updateFileSorting | NoAdminRequired
|
| /apps/files/api/v1/thumbnail/{x}/{y}/{file} | GET |
OCA\Files\Controller\ApiController::getThumbnail | NoAdminRequired,NoCSRFRequired
|
...
```

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 ./occ security:certificates
```

Import a new certificate:

```
sudo -u www-data ./occ security:certificates:import /path/to/certificate
```

Remove a certificate:

```
sudo -u www-data ./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 ./occ sharing:cleanup-remote-storages
```

You can also set it up to run as [a background job](#).



These commands are not available in [single-user \(maintenance\) mode](#).

System Commands

```
system
system:cron          Execute background jobs as cron
```

```
sudo -u www-data ./occ -h system:cron
```

-Usage:

```
system:cron [options]
```

Options

<code>-p, --progress</code>	Shows a progress bar - for use in manual execution. Do not use when executing from crontab
-----------------------------	--

To execute [background jobs](#) using [cron](#), you can use the `system:cron` command, as in the following example:

```
sudo -u www-data ./occ system:cron
```

If the `--progress` or `-p` argument is specified, then progress output will be displayed in the console, as in the example below.

```
Executing: 12 - OCA\UpdateNotification\Notification\BackgroundJob
          13 [----->-----]
```

If neither of these arguments is provided, no output will be displayed by the command.



Displaying progress information is useful when you want visual confirmation that background jobs have been executed. However, in a non-interactive environment, such as crontab, it should not be used.

Updating an Existing System Cron Configuration

If you have already automated background jobs via Cron, you must update the relevant `crontab` entry using the example below as a guide.

Instead of the following configuration



```
/usr/bin/php -f /path/to/your/owncloud/cron.php
```

Use the following one instead

```
sudo -u www-data ./occ system:cron
```

This command does not work if:



- [Maintenance or Admin-only \(single user\) modes](#) are enabled
- Background jobs are disabled

Trashbin



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 ./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 ./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 documentation](#)). The default is to delete expired files for all users, or you may list users in a space-delimited list.

Two-Factor Authentication

The following commands only enable or disable the two-factor authentication for a particular user. See the [Two-Factor TOTP](#) section for managing the two-factor app provided by ownCloud.

If a two-factor provider app is enabled, it is enabled for all users by default but a user has to opt-in,

though the provider can decide whether or not the user has to pass the challenge. In case a user is losing access to the second factor like a lost or defect phone with two-factor SMS/app verification, the user would now be locked out. To give the user access to his account, an admin can temporarily disable the two-factor check for that user via the occ command. After the issue has been fixed, the admin can reenable two-factor authentication for that user.

The following commands are available for the two-factor authentication:

```
twofactorauth
twofactorauth:disable  Disable two-factor authentication for a user.
twofactorauth:enable  Enable two-factor authentication for a user.
```

Disable

Disable two-factor authentication for a user:

```
sudo -u www-data ./occ twofactorauth:disable [options] [--] <uid>
```

Arguments

<code>uid</code>	The user (user id) to be disabled for two-factor authentication.
------------------	--

Enable

Enable two-factor authentication for a user:

```
sudo -u www-data ./occ twofactorauth:enable [options] [--] <uid>
```

Arguments

<code>uid</code>	The user (user id) to be (re)enabled for twofactor authentication.
------------------	--

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:home         List home directories and users in a particular
home
user:inactive      Reports users who are known to owncloud,
```

days	but have not logged in for a certain number of
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:move-home	Move a user's home folder to a new location
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.

```
sudo -u www-data ./occ user:add \
  [--password-from-env] \
  [--display-name [DISPLAY-NAME]] \
  [--email [EMAIL]] \
  [-g|--group [GROUP]] \
  [--] \
  <uid>
```

Arguments

<code>uid</code>	User ID used to login (must only contain a-z, A-Z, 0-9, -, _ and @).
<code>--password-from-env</code>	Read the password from the <code>OC_PASS</code> environment variable. A password is not required , if an email address is provided. If a password is not provided, a temporary one will be generated. It cannot be set to <code>0</code> .
<code>--display-name=[DISPLAY-NAME]</code>	This corresponds to the Full Name on the Users page in your ownCloud Web UI.
<code>--email=[EMAIL]</code>	Email address for the user (optional). The user will be emailed a link to set their password, if email is configured correctly.
<code>-g [GROUP]</code> <code>--group=[GROUP]</code>	The groups the user should be added to. The group will be created if it does not exist. Multiple values are allowed.

Command Examples

This example adds new user, Layla Smith, and adds her to the `users` and `db-admins` groups. If either group does not exist, it is created.

Listing 10. Create a user with a password, email address, and display name, and add them to two groups

```
sudo -u www-data ./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"
```

Listing 11. Create a user with a temporary password (the user will receive a link to set their password).

```
sudo -u www-data ./occ user:add \  
--display-name "Layla Smith" \  
--email "*****" \  
--group "users" \  
--group "db-admins" layla  
  
The user "layla" was created successfully  
Display name set to "Layla Smith"  
Email address set to "*****"  
User layla added to group users  
User layla added to group db-admins
```

Deleting A User

To delete a user, you use the `user:delete` command.

```
sudo -u www-data ./occ user:delete [options] [--] <uid>
```

Arguments

<code>uid</code>	The username.
------------------	---------------

Options

<code>-f</code> <code>--force</code>	Try to force the deletion of the user data even if the user is missing.
---	---

```
sudo -u www-data ./occ user:delete fred
```

Disable Users

Admins can disable users via the `occ` command too:


```
sudo -u www-data ./occ user:disable <uid>
```

Arguments

uid	The user name.
-----	----------------



Once users are disabled, their connected browsers will be disconnected. Use the following command to enable the user again:

Enable Users

```
sudo -u www-data ./occ user:enable <uid>
```

Arguments

uid	The user name.
-----	----------------

List User Home Directories

List all available root directories for user homes that are currently in use. For details see [Moving the User Home](#) documentation.

This command is complementary when using `user:move-home`.

```
sudo -u www-data ./occ user:home:list-dirs [options]
```

Options

<code>--output=[OUTPUT]</code>	Output format (plain, json or json_pretty, default is plain) [default: "plain"].
--------------------------------	--

Examples

```
sudo -u www-data ./occ user:home:list-dirs  
- /var/www/owncloud/data
```

List all Users For a Given Home Directory

List all users that have their home in a given path. For details see [Moving the User Home](#) documentation.

This command is complementary when using `user:move-home`.

```
sudo -u www-data ./occ user:home:list-users [options] [--] [<path>]
```

Arguments

<code>path</code>	Path where the user home must be located
-------------------	--

Options

<code>--all</code>	List all users for every home path.
<code>--output=[OUTPUT]</code>	Output format (plain, json or json_pretty, default is plain) [default: "plain"].

Examples

Note for the example below, some user accounts originated from LDAP.

```
sudo -u www-data ./occ user:home:list-users /var/www/owncloud/data
- admin
- aca4c3ec-691d-103b-8380-55a4da3d3a76
- 9918b614-6a2e-103b-89a7-f5edf5d332f5
- c298ae18-6a2e-103b-89a8-f5edf5d332f5
- dbcca7b4-7306-103b-813a-19652cf0a9d2
```

Run the following command to list all users from all available home directories. The example shows, that user `lisa` has been moved to a different home directory with `user:move-home`.

```
sudo -u www-data ./occ user:home:list-users --all
- /mnt/newhome_1
- lisa
- /var/www/owncloud/data
- admin
- user01
```

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.

```
sudo -u www-data ./occ user:inactive [options] [--] <days>
```

Arguments

<code><days></code>	The number of days (integer) that the user has not logged in since.
---------------------------	---

Options

<code>--output=[OUTPUT]</code>	Output format (plain, json or json_pretty, default is plain) [default: "plain"].
--------------------------------	--

The example below searches for users inactive for five days or more:

```
sudo -u www-data ./occ user:inactive 5
```

By default, this will generate output in the following format:

```
- 0:  
  - uid: admin  
  - displayName: admin  
  - inactiveSinceDays: 5
```

You can see a counting number starting with `0`, 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  
  }  
]
```

Finding the User's Last Login

To view a user's most recent login, use the `user:lastseen` command:

```
sudo -u www-data ./occ user:lastseen <uid>
```

Arguments

<code>uid</code>	The user name.
------------------	----------------

Example

```
sudo -u www-data ./occ user:lastseen layla  
layla's last login: 09.01.2015 18:46
```

Listing Users

You can list existing users with the `user:list` command.

```
sudo -u www-data ./occ 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

<code>--output=[OUTPUT]</code>	Output format (plain, json or json-pretty, default is plain).
<code>-a [ATTRIBUTES]</code> <code>--attributes=[ATTRIBUTES]</code>	Adds more details to the output. Allowed attributes, multiple values possible: <code>uid, displayName, email, quota, enabled, lastLogin, home, backend, cloudId, searchTerms</code> [default: <code>[displayName]</code>]
<code>-s</code> <code>--show-all-attributes</code>	All attributes to include from <code>uid, displayName, email, quota, enabled, lastLogin, home, backend, cloudId, searchTerms</code>

This example lists user IDs containing the string `ron`

```
sudo -u www-data ./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 ./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 ./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.

```
sudo -u www-data ./occ user:list-groups [options] [--] <uid>
```

Arguments

<code>uid</code>	User ID.
------------------	----------

Options

<code>--output=[OUTPUT]</code>	Output format (plain, json or json-pretty, default is plain).
--------------------------------	---

Examples

This example lists group membership of user `julie`:

```
sudo -u www-data ./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 ./occ user:list-groups --output=json_pretty julie
[
  "Executive",
  "Finance"
]
```

Modify User Details

This command modifies either the users username or email address.

```
sudo -u www-data ./occ 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> and <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 ./occ user:modify carla email foobar@foo.com
```

The email address of `carla` is updated to `foobar@foo.com`.

Move a Users Home Folder

This command moves a user's home folder to a new location. For details see [Moving the User Home](#) documentation. Note that moving a users home is only possible for POSIX file systems. Also see the `user:home` commands for additional support.

```
sudo -u www-data ./occ user:move-home <user_id> <new_location>
```

Arguments

<code>user_id</code>	ID of the user whose home folder is to be moved.
<code>new_location</code>	Absolute path to the parent folder of the new location of the home folder.



You must not use temp directories like `/tmp` and `/var/tmp` as target directory.

- Any data located in one of the two directories will not survive a reboot
- For systemd services, they are private sub-directories of the host's real `/tmp/` and `/var/tmp/`, and thus not system-wide locations anymore, but service-specific ones. For more details see [Using /tmp/ and /var/tmp/ Safely](#)

Example:

```
sudo -u www-data ./occ user:move-home lisa /mnt/newhome_1
```

This command moves the home directory of user `lisa` to the new location `/mnt/newhome_1`

Generating a User Count Report

Generate a simple report that counts all users including users on external user authentication servers such as LDAP, and guest users which are created by the guests app.

```
sudo -u www-data ./occ user:report
```

There are no arguments and no options beside the default once to parametrize the output.

```
sudo -u www-data ./occ user:report
+-----+-----+
| User Report          |      |
+-----+-----+
| OCA\User_LDAP\User_Proxy | 23 |
| OC\User\Database      | 100 |
| guest users           | 20 |
| total users           | 143 |
```

user directories	4
------------------	---



A user directory is created, when a local user has logged on the first time after creation. Therefore the difference between `OC\User\Database` and `user directories` equals all users which have been created locally, but have not logged on at least once.

Setting a User's Password

Resets the password of the named user.

```
sudo -u www-data ./occ user:resetpassword [options] [--] <user>
```

Unresolved directive in modules/admin_manual/pages/configuration/server/occ_commands/core_commands/_user_commands.adoc - include::partial\$configuration/user/update-password-note.adoc[]

Arguments

<code>uid</code>	The user's name.
------------------	------------------

Options

<code>--password-from-env</code>	Read the password from the <code>OC_PASS</code> environment variable.
<code>--send-email</code>	The email ID set while creating the user, will be used to send. link for password reset. This option will also display the link sent to user.
<code>--output-link</code>	The link to reset the password will be displayed.

`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.



To use `send-email`, the ownCloud instance must have email access fully configured.

Examples

Add a new user, called Fred Jones:

```
export OC_PASS=newpassword
```

```
su -s /bin/sh www-data -c '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 [Reset Admin Password](#)):

```
sudo -u www-data ./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
su -s /bin/sh www-data -c 'occ user:resetpassword \
--password-from-env \
layla'
Successfully reset password for layla
```

This example emails a password reset link to the user. Additionally, when the command completes, it outputs the password reset link to the console:

```
sudo -u www-data ./occ user:resetpassword \
--send-email \
--output-link \
layla
The password reset link is:
http://localhost:8080/index.php/lostpassword/reset/form/rQA1CjNeQf3aphA6Hraq2/layla
```

If the specified user does not have a valid email address set, then the following error will be output to the console, and the email will not be sent:

```
Email address is not set for the user layla
```

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

```
sudo -u www-data ./occ user:setting [options] [--] <uid> [[<app> [<key>]]
```

Arguments

<code>uid</code>	User ID used to login.
<code>app</code>	Restrict listing the settings for a given app. [default: ""].
<code>key</code>	Setting key to set, get or delete [default: ""].

Options

<code>--output=[OUTPUT]</code>	Output format (plain, json or json-pretty, default is plain).
<code>--ignore-missing-user</code>	Use this option to ignore errors when the user does not exist.
<code>--default-value=[DEFAULT -VALUE]</code>	If no default value is set and the config does not exist, the command will exit with 1. Only applicable on get.
<code>--value=[VALUE]</code>	The new value of the setting.
<code>--update-only</code>	Only updates the value, if it is not set before, it is not being added.
<code>--delete</code>	Specify this option to delete the config.
<code>--error-if-not-exists</code>	Checks whether the setting exists before deleting it.

The descriptions for the `app` and `key` arguments may not be completely transparent. Here's a description of both.

Argument	Description
<code>app</code>	When a 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 <code>core</code> , <code>files_trashbin</code> , and <code>user_ldap</code> . A complete list cannot be supplied as it is impossible to know the entire list of applications 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 settings for a user, you need to call the `user:setting` command and supply at least the user's user name. You can drill down restricting results to a particular app and a key in the app.

```
sudo -u www-data ./occ user:setting <uid> [<app>] [<key>]
```

Arguments

<code>uid</code>	User ID used to log in.
<code>app</code>	Restrict listing the settings for a given app. [default: ""].
<code>key</code>	Setting key to set, get or delete [default: ""].

Examples:

1. Retrieve all settings set for a given user:

```
sudo -u www-data ./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.

2. Retrieve all settings set restricted to application `core` for a given user:

```
sudo -u www-data ./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`.

3. Retrieve all settings set restricted to application `core`, key `lang` for a given user

```
sudo -u www-data ./occ user:setting layla core lang
```

This will display the value for that setting, such as `en`.

Setting and Deleting a Setting

```
sudo -u www-data ./occ user:setting [options] [--] <uid> [<app>] [<key>]
```



In case you want to change the email address, use [the `user:modify` command](#).

Here's an example of how you would set the language of the user `layla`.

```
sudo -u www-data ./occ user:setting layla core lang --value=en
```

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 ./occ user:setting layla core lang --delete
```

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.



It's also [one of the commands](#) that you should run on a regular basis to ensure that your ownCloud installation is running optimally.



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>]
```

Synchronize users from a given backend to the accounts table.

Arguments:

<code>backend-class</code>	The quoted PHP class name for the backend, e.g., - LDAP: <code>"OCA\User_LDAP\User_Proxy"</code> - Samba: <code>"OCA\User\SMB"</code> - Shibboleth: <code>"OCA\User_Shibboleth\UserBackend"</code>
----------------------------	---

Options

<code>-l</code> <code>--list</code>	List all enabled backend classes.
<code>-u [UID]</code> <code>--uid=[UID]</code>	Sync only the user with the given user id.
<code>-s</code> <code>--seenOnly</code>	Sync only seen users.
<code>-c</code> <code>--showCount</code>	Calculate user count before syncing.

<pre>-m [MISSING-ACCOUNT-ACTION] --missing-account -action[=MISSING-ACCOUNT -ACTION]</pre>	<p>Action to take if the account isn't connected to a backend any longer.</p> <p>Options are disable and remove.</p> <p>Note that removing the account will also remove the stored data and files for that account</p>
<pre>-r --re-enable</pre>	<p>When syncing multiple accounts re-enable accounts that are disabled in ownCloud but available in the synced backend.</p>

Below are examples of how to use the command with an *LDAP*, *Samba*, and *Shibboleth* backend.

LDAP

```
sudo -u www-data ./occ user:sync "OCA\User_LDAP\User_Proxy"
```

Samba

```
sudo -u www-data ./occ user:sync "OCA\User\SMB" -vvv
```

Below are examples of how to use the command with the **LDAP** backend along with example console output.

Example 1

```
sudo -u www-data ./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 -u www-data ./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 -u www-data ./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 -u www-data ./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 [=====]
```

Example 5

```
sudo -u www-data ./occ user:sync "OCA\User_LDAP\User_Proxy" -m remove
```

Example 6

```
sudo -u www-data ./occ user:sync "OCA\User_LDAP\User_Proxy"
```

If unknown `users` are found, what `do` you want to `do` with their accounts? (removing the account will also remove its data)

```
[0] disable
[1] remove
[2] ask later
```

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 "OCA\User_LDAP\User_Proxy"
```

Versions



These commands are only available when the "Versions" app (`files_versions`) is enabled. These commands are not available in [single-user \(maintenance\) mode](#).

versions:cleanup

`versions:cleanup` can delete all versioned files, as well as the `files_versions` folder, for either specific users, or for all users.

```
sudo -u www-data ./occ versions:cleanup [<user_id>]...
```

Options

<code>user_id</code>	Delete versions of the given user(s), if no user is given all versions will be deleted.
----------------------	---

The example below deletes all versioned files for all users:

```
sudo -u www-data ./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 ./occ versions:cleanup freda molly
Delete versions of   freda
Delete versions of   molly
```

versions:expire

`versions:expire` deletes only expired files according to the `versions_retention_obligation` setting in `config.php` (see the File versions section in `config_sample_php_parameters`). The default is to delete expired files for all users, or you may list users in a space-delimited list.

```
sudo -u www-data ./occ versions:expire [<user_id>]...
```

Options

<code>user_id</code>	Expire file versions of the given user(s), if no user is given file versions for all users will be expired.
----------------------	---

Apps Commands

This command reference covers the ownCloud maintained apps commands, which are only available if the respective app is installed and enabled.

Activity

The `activity` command is used for sending automated activity email notifications in ownCloud server.

```
activity
activity:send-emails  Send all pending activity emails now
```

Send Emails Now

The `activity:send-emails` command sends all pending activity emails immediately, regardless of the time they are scheduled.

```
sudo -u www-data ./occ activity:send-emails
```

Manage Rename and Move Action Notifications

Starting with Activity app version 2.7.0, rename and move action notifications can be sent. This feature is disabled by default and must be enabled manually.

Enable Rename and Move Action Notifications

```
sudo -u www-data ./occ config:app:set activity enable_move_and_rename_activities
--value "yes"
```

Disable Rename and Move Action Notifications

```
sudo -u www-data ./occ config:app:set activity enable_move_and_rename_activities
--value "no"
```

or

```
sudo -u www-data ./occ config:app:delete activity enable_move_and_rename_activities
```

Anti-Virus

Marketplace URL: [Anti-Virus](#)

Use these commands to configure the Anti-Virus app. Parametrisation must be done with the `occ config` command set.

List the Current Settings

```
sudo -u www-data ./occ config:list files_antivirus
```

Set the Setting

To set a new value, use the command below and replace `<Key>` and value `<Value>` accordingly.

```
sudo -u www-data ./occ config:app:set files_antivirus <Key> --value=<Value> --update
-only
```

Antivirus Mode [string]

Antivirus Configuration.

Key	<code>av_mode</code>
Default	'executable'
Possible Values	'executable' 'daemon' 'socket'

Antivirus Socket [string]

Antivirus Socket.

Key	av_socket
Default	'/var/run/clamav/clamd.ctl'

Antivirus Host [string]

Hostname or IP address of Antivirus Host.

Key	av_host
Default	

Antivirus Port [integer]

Port number of Antivirus Host, 1-65535.

Key	av_port
Default	
Possible Values	1-65535

Antivirus Command Line Options [string]

Extra command line options (comma-separated).

Key	av_cmd_options
Default	

Antivirus Path to Executable [string]

Path to clamscan executable.

Key	av_path
Default	'/usr/bin/clamscan'

Antivirus Maximum Filesize [integer]

File size limit, -1 means no limit.

Key	av_max_file_size
Default	'-1'
Possible Values	'-1' integer number

Antivirus Maximum Stream Length [integer]

Max Stream Length.

Key	<code>av_stream_max_length</code>
Default	'26214400'

Antivirus Action [string]

When infected files were found during a background scan.

Key	<code>av_infected_action</code>
Default	'only_log'
Possible Values	'only_log' 'delete'

Antivirus Scan Process [string]

Define scan process.

Key	<code>av_scan_background</code>
Default	'true'
Possible Values	'true' 'false'

Auditing

Marketplace URL: [Auditing](#)

Tracks various activities and actions of your users and admins. For details, please see the [Auditing](#) documentation.

Ignore all CLI triggered events.

Set or Change Ignore CLI Events

To ignore all CLI triggered events, you can set the following option, defaults to track cli events:

```
sudo -u www-data ./occ config:app:set \  
  "admin_audit ignore_cli_events" \  
  --value "yes"
```

Get Value of Ignore CLI Events

This command reads the value of `admin_audit ignore_cli_events`:

```
sudo -u www-data ./occ config:app:get "admin_audit ignore_cli_events"
```

```
yes
```

Delete Ignore CLI Events

This command completely removes the key and the value:

```
sudo -u www-data ./occ config:app:delete "admin_audit ignore_cli_events"
```

Brute Force Protection

Marketplace URL: [Brute-Force Protection](#)

Use these commands to configure the Brute Force Protection app. Parametrisation must be done with the `occ config` command set. The combination of `uid` and `IP address` is used to trigger the ban.

List the Current Settings

```
sudo -u www-data ./occ config:list brute_force_protection
```

Set the Setting

To set a new value, use the command below and replace `<Key>` and value `<Value>` accordingly.

```
sudo -u www-data ./occ config:app:set brute_force_protection <Key> --value=<Value>
--update-only
```

Fail Tolerance [attempts]

Number of wrong attempts to trigger the ban.

Key	<code>brute_force_protection_fail_tolerance</code>
Default	3

Time Threshold [seconds]

Time in which the number of wrong attempts must occur to trigger the ban.

Key	<code>brute_force_protection_time_threshold</code>
Default	60

Ban Period [seconds]

Time how long the ban will be active if triggered.

Key	<code>brute_force_protection_ban_period</code>
Default	300

Calendar

Marketplace URL: [Calendar](#)

For commands for managing the calendar, please see the DAV Command section in the occ core command set.

Contacts

Marketplace URL: [Contacts](#)

For commands for managing contacts, please see the DAV Command section in the occ core command set.

Custom Groups

Marketplace URL: [Custom Groups](#)

Use these commands to configure the Custom Groups app.

Parameterization should be done with the `occ config` command set, though some but not all settings result in an entry in `config.php` which also can be set manually.

Get a Current Setting

You can get the value of a current setting. For details how to do so see the [Config Command Set](#).

Disallow Admin Access

By default, administrators can administrate custom groups of an instance. When changed, only group admins can administrate custom groups. You can change this behaviour with the following command:

```
sudo -u www-data ./occ config:system:set \  
  customgroups.disallow-admin-access-all \  
  --type boolean --value true
```

This occ command will create a key-value pair in your `config.php` which must be writable for the webserver user. You can also do this manually by adding the following key in `config.php`:

```
'customgroups.disallow-admin-access-all' => true,
```

Disallow Members of Defined Groups

You can hide custom groups from a user's personal settings page based on a user's group membership. This makes it easier to collect users you want to exclude into defined groups which will be further used for this setting:

```
sudo -u www-data ./occ config:system:set \  
  customgroups.disallowed-groups \  
  --type json \  
  --value '["no_guest_app_users", "project5"]'
```

This occ command will create a key-value pair in your config.php which must be writable for the webserver user to be set. You can also set this manually by adding the following key in config.php:

```
'customgroups.disallowed-groups' =>  
array (  
  0 => 'no_guest_app_users',  
  1 => 'project5',  
)
```

Restrict Group Creation

This setting defines if ordinary users are allowed to create custom groups. By default, all users can create custom groups, but this can be restricted to admins (if allowed as above) and group-admins. Values to be set can be 'true' and 'false', defaults to 'false'.

```
sudo -u www-data ./occ config:app:set \  
  customgroups \  
  only_subadmin_can_create \  
  --value 'true'
```

Restrict Add or Remove Group Members

This setting defines if an existing ordinary group member is allowed to add other users to the target group or remove them. By default, all users can add members to groups, but this can be restricted to admins (if allowed as above) and group-admins. Values to be set can be 'yes' and 'no', defaults to 'no'.

```
sudo -u www-data ./occ config:app:set \  
  core \  
  shareapi_only_share_with_group_members \  
  --value 'yes'
```

Allow Duplicate Group Display Names

This setting allows the creation of multiple groups with the same display name. By default, group

display names must be unique, but it can be allowed to have multiple identical group display names. Values to be set can be 'true' and 'false', defaults to 'false'.

```
sudo -u www-data ./occ config:app:set \  
  customgroups \  
  allow_duplicate_names \  
  --value 'false'
```

Data Exporter

This app is only available as a [git clone](#). See the [Data Exporter](#) description for more information how to install this app. Import and export users from one ownCloud instance in to another. The export contains all user-settings, files and shares.

Export User Data

```
instance:export:user <userId> <exportDirectory>
```

Arguments

<code>userId</code>	User to export.
<code>exportDirectory</code>	Path to the directory to export data to.

Import User Data

```
instance:import:user [options] [--] <importDirectory>
```

Arguments

<code>userId</code>	User to export.
<code>importDirectory</code>	Path to the directory to import data from.

Options

<code>-a [UID]</code> <code>--as=[UID]</code>	Import the user under a different user id.
--	--

Migrate Shares

```
instance:export:migrate:share <userId> <remoteServer>
```

Arguments

<code>userId</code>	The exported <code>userId</code> whose shares we want to migrate.
<code>remoteServer</code>	The remote ownCloud server where the exported user is now, for example "https://myown.server:8080/owncloud".

File Lifecycle Management

Marketplace URL: [File Lifecycle Management](#)

The File Lifecycle Management extension allows service providers to manage the lifecycle of files within ownCloud. For details please see the [File Lifecycle Management](#) documentation.

The `lifecycle` commands configure the File Lifecycle Management app.

Listing 12. App Configuration

```
lifecycle
lifecycle:archive      Archive files which have reached a certain age
lifecycle:expire      Expire files from Archive which have reached a certain age
lifecycle:restore      Restore files from Archive to the original location
lifecycle:restore-all Restore all archived files in the system back to their
                        original locations
lifecycle:set-upload-time Set upload time for files which do not have one
```

`config:app` commands configure the Policies for the File Lifecycle Management app.

Listing 13. Policy Configuration

```
config:app:get|set
files_lifecycle archive_period  Number of days since upload (or restore)
                                after which files will be archived
files_lifecycle expire_period   Number of days since archiving after which files
will                             be permanently deleted
files_lifecycle excluded_groups Define groups of users that are exempt from the
                                lifecycle policies
files_lifecycle policy          Restoration policies for users
files_lifecycle disable_ui      Enable/Disable the user interface components
```

App Configuration

Archive Aged Files

Archive files which have reached a certain age.

```
sudo -u www-data ./occ lifecycle:archive [options]
```

Options

`-d,`
`--dryrun[=DRYRUN]`

Don't apply changes to the system [default: false]

Expire Files From Archive

Expire files from archive which have reached a certain age.

```
sudo -u www-data ./occ lifecycle:expire [options]
```

Options

`-d,`
`--dryrun[=DRYRUN]`

Don't apply changes to the system [default: false]

Restore Files From Archive

Restore files from archive to the original location. Note that the location for archived files always follows the pattern `$userid/archive/files/...`

```
sudo -u www-data ./occ lifecycle:restore <path>
```

Arguments

`path`

Enter path to a folder or to a single file

Example

Restore all files in folder `project1` for user `alice` with path `/work/projects/project1`

```
sudo -u www-data ./occ lifecycle:restore /alice/archive/files/work/projects/project1
```

Restore All Files From Archive

Restore all archived files for all users in the system back to their original locations. This command has no additional arguments or options.

```
sudo -u www-data ./occ lifecycle:restore-all
```

Set Default Upload Time

Set upload time for files which do not have one.



Files without upload time are silently skipped by `occ lifecycle:archive`. This can happen with files that were uploaded before the `files_lifecycle` app was configured.

or when it was temporarily disabled and therefore do not have an upload time set.

```
sudo -u www-data ./occ lifecycle:set-upload-time [options] [--] <date>
```

Arguments

<code>date</code>	Date in format y-m-d. Example: 2018-07-23
-------------------	---

Options

<code>-d,</code> <code>--dryrun[=DRYRUN]</code>	Don't apply changes to the system [default: false]
--	--

Policy Configuration

All policy configurations are set and queried with the `config:app` command set. The examples below set a value. To query a value use `config:app:get` and the corresponding key without any options or attributes.

Set the Archive Period

The number of days since upload (or restore) after which files will be archived.

The following example command sets the time passed since upload (or restore) for archiving files to 90 days.

```
sudo -u www-data ./occ config:app:set files_lifecycle archive_period --value='90'
```

Set the Expire Period

The number of days since archiving after which files will be permanently deleted.

The following example command sets the time passed to delete files to 180 days.

```
sudo -u www-data ./occ config:app:set files_lifecycle expire_period --value='180'
```

Set Groups to be Excluded

Define groups of users that are exempt from the lifecycle policies (comma-separated group ids).

The following example command specifies groups whose members will not be part of the lifecycle management.

```
sudo -u www-data ./occ config:app:set files_lifecycle excluded_groups --value  
='group1,group2'
```

Restoration Policy for Users

Set a policy who can restore files. Use the value `soft` for self-service and `hard` for admin/groupadmin-service.

The following example command sets the restoration policy for users to `soft` (default).

```
sudo -u www-data ./occ config:app:set files_lifecycle policy --value='soft'
```

Disable User Interface

Disable the whole user interface for the File Lifecycle Management app.

The following example command disables the user interface for the File Lifecycle Management app.

```
sudo -u www-data ./occ config:app:set files_lifecycle disable_ui --value='yes'
```

You can reenable it by deleting the key:

```
sudo -u www-data ./occ config:app:delete files_lifecycle disable_ui
```

Full Text Search

Use these commands when you manage full text search related tasks.

Command Description

```
search
  search:index:create  Create initial Search Index for one or all users.
                       This command could not update the search index correctly
                       after the initial indexing.
  search:index:rebuild Rebuild the search index for a given User.
                       If you want to rebuild the whole index, run
                       `search:index:reset` and then `search:index:create --all`
  search:index:reset   Reset the index
  search:index:update  Update the search index by running all pending background
  jobs.
```

In addition to the settings provided by the Full Text Search app, you can set/read additional options via the `occ config:app` commands. These are [Set App Modes](#), [Index Metadata Only](#) and [Limit Metadata Search for Groups](#).

Create the Full Text Search Index

The command `search:index:create` creates the initial full text search index for one or all users.

```
sudo -u www-data ./occ search:index:create <user_id> (<user_id>)...
```

Arguments

<code><user_id></code>	The ID of the user (or space-separated list of user IDs) to create a full text search index for. A full text search index is created for all users, if this value is omitted.
------------------------------	---

Options

<code>--all</code>	Will create index for all files of all known users.
--------------------	---

Example 1

This example creates a full text search index for the user with user id `testuser`.

```
sudo -u www-data ./occ search:index:create testuser
```

```
Indexing user testuser
```

Example 2

This example creates a full text search index for the users with user ids `admin` and `testuser`.

```
sudo -u www-data ./occ search:index:create admin testuser
```

```
Indexing user admin  
Indexing user testuser
```

Rebuild the Full Text Search Index

Rebuild the search index for a given user.

If you want to rebuild the whole index, run `search:index:reset` and then `search:index:create --all`.

```
sudo -u www-data ./occ search:index:rebuild <user_id> (<user_id>)...
```

Arguments

<code><user_id></code>	Provide a user ID. This argument is required.
------------------------------	---

Options

<code>-q --quiet</code>	Do not output any message.
<code>-f --force</code>	Use this option to reset the index without further questions.

Example 1

This example rebuilds the full text search index for the user with user ID `testuser`.

Listing 14. Rebuild the index for a single user

```
sudo -u www-data ./occ search:index:rebuild testuser

Indexing user testuser

This will delete all full text search index data for testuser! Do you want to proceed?
[0] no
[1] yes
> 1
Rebuilding full text search Index for testuser
```

Example 2

This example rebuilds the full text search index for the users with user IDs `admin` and `testuser`.

Listing 15. Rebuild the index for multiple users

```
sudo -u www-data ./occ search:index:rebuild admin testuser

This will delete all search index data for admin, testuser! Do you want to proceed?
[0] no
[1] yes
> 1
Rebuilding Search Index for admin
Rebuilding Search Index for testuser
```

Rebuild the Entire Index

The entire index can be rebuilt by running the following two commands:

```
sudo -u www-data ./occ search:index:reset
sudo -u www-data ./occ search:index:create --all
```

Reset the Full Text Search Index

The command `search:index:reset` resets (recreates and clears) the full text search index for all users.

```
sudo -u www-data ./occ search:index:reset
```

Arguments

<code>-f --force</code>	Use this option to reset the index without further questions.
-------------------------	---

Example

```
sudo -u www-data ./occ search:index:reset
This will delete the whole search index! Do you want to proceed?
[0] no
[1] yes
> 1
Search index has been reset.
```

Update the Full Text Search Index

Updates to the search index due to changed content or changed metadata are happening via background jobs that are added to a queue. These background jobs are normally run by the ownCloud cronjob. The command `search:index:update` updates the full text search index by running all pending background jobs.

```
sudo -u www-data ./occ search:index:update
```

Arguments

<code>-q --quiet</code>	Suppress all output from the command.
-------------------------	---------------------------------------

Example

This example updates the full text search index for all users.

```
sudo -u www-data ./occ search:index:update
Start Updating the Elastic search index:
No pending jobs found.
```

Set App Modes

To do an initial full indexing without the Full Text Search app interfering, it can be put in passive mode. See the [App Modes](#) section in the Full Text Search description for details.

```
sudo -u www-data ./occ config:app:set \
  search_elastic mode --value passive
```

Switching back to active mode can be done by running the following command:

```
sudo -u www-data ./occ config:app:set \
```

```
search_elastic mode --value active
```

Restrict Search Results

Search results can be restricted in different ways, see the [Restrict Search Results](#) section in the Full Text Search description for details.

Index Metadata Only

```
sudo -u www-data ./occ config:app:set \  
search_elastic nocontent --value true
```

Switching back to provide all content search results can be done by running the following command:

```
sudo -u www-data ./occ config:app:set \  
search_elastic nocontent --value false
```

Limit Metadata Search for Groups

```
sudo -u www-data ./occ config:app:set \  
search_elastic group.nocontent \  
--value group1,group2,"group with blank"
```

LDAP Integration

Marketplace URL: [LDAP Integration](#)

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:invalidate-cache	Invalidates the LDAP cache
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

Search for a User

Search for an LDAP user, using this syntax:

```
sudo -u www-data ./occ ldap:search [options] [--] <search>
```

Arguments

<code>search</code>	The search string (can be empty)
---------------------	----------------------------------

Options

<code>--group</code>	Searches groups instead of users
<code>--offset=OFFSET</code>	The offset of the result set. Needs to be a multiple of limit. [default: 0]
<code>--limit=LIMIT</code>	Limit the results. 0 means no limit. [default: 15]

Note that the search string can be empty to list all users, or groups when the `--group` option is set. In this case, the search string must be declared with `'`. It is by default a prefix search. Start the string with `*` to change to infix (substring) search.

Search Configuration and Rules

Search attributes are configurable in the LDAP wizard (**Settings › Admin › User Authentication › LDAP**) or via an occ command `ldap:set-config` as described below:

General rule

1. If *User/Group Search Attributes* are **NOT** defined (empty), the entry defined in the *User/Group Display Name Field* is used as the search attribute, for details see below.
2. Important when having multiple search attributes, results are unique as long hits correspond to a unique user or group entry.

Rules for users

1. If **User Search Attributes** are defined (not empty) in:

Settings › Admin › User Authentication › LDAP › Advanced › User Search Attributes

`LdapAttributesForUserSearch`

a. Example

If your search attributes would be `givenName` and `sn` you can find users by first name + last name very quickly. You will find "Terri Hanson" by searching for `te ha`. Trailing whitespace is ignored.

2. Else use the **User Display Name Field** which usually defaults to the default `displayname` attribute "displayname"

Settings › Admin › User Authentication › LDAP › Advanced › User Display Name Field

`LdapUserDisplayName`

Rules for groups

1. If **Group Search Attributes** are defined (not empty) in:

Settings › Admin › User Authentication › LDAP › Advanced › Group Search Attributes

LdapAttributesForGroupSearch

2. Else use the **Group Display Name Field** which usually defaults to the default displayname attribute "cn"

Settings › Admin › User Authentication › LDAP › Advanced › Group Display Name Field

LdapGroupDisplayName

Offset and Limit

The best way understanding `offset` and `limit` is the following table when using `occ ldap:search '[options]`

Options	Result Set
<code>--offset 0</code> <code>--limit 5</code>	"A", "B", "C", "D" and "E"
<code>--offset 5</code> <code>--limit 5</code>	"F", "G", "H", "I" and "J"
<code>--offset 1</code> <code>--limit 3</code>	"B", "C" and "D"

Examples

Searches match at the beginning of the attribute value only. This example searches for `givenNames` that start with 'rob':

```
sudo -u www-data ./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 ./occ ldap:search "*rob"
```

The following examples use `offset` and `limit` options:

```
sudo -u www-data ./occ ldap:search "re"  
Rebecca OShea (Rebecca.OShea)  
Rebecca Vintin (Rebecca.Vintin)  
Rebekka Da-Cahuna (Rebekka.Da-Cahuna)  
Rekha Cox (Rekha.Cox)  
Rekha Craft (Rekha.Craft)
```

```
sudo -u www-data ./occ ldap:search "re" --offset 0 --limit 3  
Rebecca OShea (Rebecca.OShea)  
Rebecca Vintin (Rebecca.Vintin)
```



```
Rebekka Da-Cahuna (Rebekka.Da-Cahuna)
```

```
sudo -u www-data ./occ ldap:search "re" --offset 3 --limit 3  
Rekha Cox (Rekha.Cox)  
Rekha Craft (Rekha.Craft)
```

Check if an LDAP User Exists

This only works if the ownCloud server is connected to an LDAP server.

```
ldap:check-user [options] [--] <ocName>
```

Arguments

<code>ocName</code>	The user name as used in ownCloud (see e.g. the user's Federated Cloud ID).
---------------------	---

Options

<code>--force</code>	Ignores disabled LDAP configuration
----------------------	-------------------------------------

Example:

```
sudo -u www-data ./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 a check of all active LDAP connections.

```
sudo -u www-data ./occ ldap:check-user --force robert
```

Create an Empty LDAP Configuration

Create an empty LDAP configuration.

```
ldap:create-empty-config [<configID>]
```

Arguments

<code>configID</code>	Create a configuration with the specified id
-----------------------	--

Configurations that you create without assigning a `<configID>` are automatically assigned IDs.

```
sudo -u www-data ./occ ldap:create-empty-config
Created new configuration with configID 's01'
```

List and View Your Configurations

You can list and view your configurations:

```
sudo -u www-data ./occ ldap:show-config [options] [--] [<configID>]
```

Arguments

<code>configID</code>	Will show the configuration of the specified id
-----------------------	---

Options

<code>--show-password</code>	Show LDAP bind password
<code>--output[=OUTPUT]</code>	The output format to use (plain, json or json_pretty). [default: "plain"]

Examples

If you omit the `configID`, all configuration ID's with their settings are listed:

```
sudo -u www-data ./occ ldap:show-config
```

View the configuration for a single `configID`:

```
sudo -u www-data ./occ ldap:show-config s01
```

Delete an Existing LDAP Configuration

Deletes an existing LDAP configuration.

```
ldap:delete-config <configID>
```

Arguments

<code>configID</code>	The configuration ID
-----------------------	----------------------

```
sudo -u www-data ./occ ldap:delete s01
Deleted configuration with configID 's01'
```

Invalidate LDAP Cache

This command invalidates the LDAP cache for all users:

```
sudo -u www-data ./occ ldap:invalidate-cache
```

Manipulate LDAP Configurations

This command manipulates LDAP configurations.

```
sudo -u www-data ./occ ldap:set-config <configID> <configKey> <configValue>
```

Arguments

<code>configID</code>	The configuration ID
<code>configKey</code>	The configuration key
<code>configValue</code>	The new configuration value

If a `configKey` allows multiple entries like the key `ldapAttributesForUserSearch`, use semicolons without a whitespace to separate them.

This example sets search attributes:

```
sudo -u www-data ./occ ldap:set-config s01 ldapAttributesForUserSearch  
"cn;givenname;sn;displayname;mail"
```

Available keys, along with default values for `configValue`, are listed in the table below.

Configuration	Setting
hasMemberOfFilterSupport	
hasPagedResultSupport	
homeFolderNamingRule	
lastJpegPhotoLookup	0
ldapAgentName	cn=admin,dc=owncloudqa,dc=com
ldapAgentPassword	*
ldapAttributesForGroupSearch	
ldapAttributesForUserSearch	
ldapBackupHost	
ldapBackupPort	
ldapBase	dc=owncloudqa,dc=com

Configuration	Setting
ldapBaseGroups	dc=owncloudqa,dc=com
ldapBaseUsers	dc=owncloudqa,dc=com
ldapCacheTTL	600
ldapConfigurationActive	1
ldapDynamicGroupMemberURL	
ldapEmailAttribute	
ldapExperiencedAdmin	0
ldapExpertUUIDGroupAttr	
ldapExpertUUIDUserAttr	
ldapExpertUsernameAttr	
ldapGroupDisplayName	cn
ldapGroupFilter	
ldapGroupFilterMode	0
ldapGroupFilterObjectclass	
ldapGroupMemberAssocAttr	uniqueMember
ldapHost	ldap://host
ldapIgnoreNamingRules	
ldapLoginFilter	(&objectclass=inetOrgPerson(uid=%uid))
ldapLoginFilterAttributes	
ldapLoginFilterEmail	0
ldapLoginFilterMode	0
ldapLoginFilterUsername	1
ldapNestedGroups	0
ldapOverrideMainServer	
ldapPagingSize	500
ldapPort	389
ldapQuotaAttribute	
ldapQuotaDefault	
ldapTLS	0
ldapUserDisplayName	displayName
ldapUserDisplayName2	
ldapUserFilter	objectclass=inetOrgPerson
ldapUserFilterGroups	

Configuration	Setting
ldapUserFilterMode	0
ldapUserFilterObjectclass	inetOrgPerson
ldapUuidGroupAttribute	auto
ldapUuidUserAttribute	auto
turnOffCertCheck	0
useMemberOfToDetectMembersh ip	1

Test Your Configuration

Tests whether your configuration is correct and can bind to the server.

```
sudo -u www-data ./occ ldap:test-config <configID>
```

Arguments

<code>configID</code>	The configuration ID
-----------------------	----------------------

Example:

```
sudo -u www-data ./occ ldap:test-config s01
The configuration is valid and the connection could be established!
```

Set and Unset LDAP App Configurations

```
sudo -u www-data ./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 ./occ config:app:delete user_ldap updateAttributesInterval
```

Reuse Existing LDAP Accounts if Available

If you want to allow new LDAP logins to attempt to reuse existing `oc_accounts` entries that match the resolved username attribute, and have backend set to `User_Proxy`, then set the `reuse_accounts`

config setting to **yes**.

Below is an example of how to do so.

```
sudo -u www-data ./occ config:app:set user_ldap reuse_accounts --value="yes"
```

This functionality is valuable for several reasons; these are:

- It handles the situation of when admins mistakenly delete one or more user mappings, and subsequent logins then create new accounts.
- It allows auto-provisioned users with Shibboleth to be moved over to an LDAP server, but be able to continue using ownCloud.



This functionality will not work in the following situations:

1. No user or group account exists with the supplied username.
2. A user or group account exists, but it uses a different backend.

Market

Marketplace URL: [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
```



The user running the update command, which will likely be your webserver user, requires write permission for the `/apps` respectively `apps-external` folder.



If they don't have write permission, the command may report that the update was successful, but it may silently fail.

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`.

```
sudo -u www-data ./occ market:install <ids> [option]
```

Arguments

<code>ids</code>	Ids of the apps
------------------	-----------------

Options

<code>-l [LOCAL]</code> <code>--local=[LOCAL]</code>	Optional path to a local app package.
---	---------------------------------------

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
```



The target directory has to be **accessible to the webserver user** and you have to **enable** the app afterwards with the `occ app:enable` command.

Uninstall an Application

To uninstall an application use the following commands:

```
sudo -u www-data ./occ market:uninstall <ids>
```

Arguments

<code>ids</code>	Ids of the apps
------------------	-----------------

List Apps From The Marketplace

This command lists apps available on the marketplace. It returns the ids of the apps.

```
sudo -u www-data ./occ market:list
```

Upgrade an Application

Install new app versions if available on the marketplace by using following commands:

```
sudo -u www-data ./occ market:upgrade <ids> [options]
```

Arguments

<code>ids</code>	Ids of the apps
------------------	-----------------

Options

<code>-l [LOCAL]</code> <code>--local=[LOCAL]</code>	Optional path to a local app package.
<code>--major</code>	Allow update to a new major version.

Metrics

Marketplace URL: [Metrics](#)

Monitoring and reporting of ownCloud Server. For details please see the [Metrics](#) documentation.

Set a secret for authenticating requests at the endpoint.

In case you want to generate a random secret, use the following example command:

```
echo $(tr -dc 'a-z0-9' < /dev/urandom | head -c 20)
```

Set or change the Secret

Writes the key `metrics_shared_secret` and the secret to `config.php`. The name must not be changed and be exactly as written.

Note: You can also set the config key/value manually into your `config.php` file.

```
sudo -u www-data ./occ config:system:set \  
  "metrics_shared_secret" \  
  --value "your-metrics-secret"
```

The above command adds the following at the end of `config.php`:


```
'metrics_shared_secret' => 'your-metrics-secret',
```

Get the Secret

This command reads the value of the `metrics_shared_secret` key from `config.php`:

```
sudo -u www-data ./occ config:system:get "metrics_shared_secret"
```

```
your-metrics-secret
```

Delete the Secret

This command completely removes the key and the value from `config.php`:

```
sudo -u www-data ./occ config:system:delete "metrics_shared_secret"
```

Password Policy

Marketplace URL: [Password Policy](#)

Command to expire a user or group of users' passwords.

Command Description

```
sudo -u www-data ./occ user:expire-password <uid> [<expiredate>]
```

Arguments

<code>uid</code>	User ID.
<code>expiredate</code>	The date and time when a password expires, e.g. <code>2019-01-01 14:00:00 CET</code> or <code>-1 days</code> .



The expiry date can be provided using any of [PHP's supported date and time formats](#).

Options

<code>-a, --all</code>	Will add password expiry to all known users. <code>uid</code> and <code>group</code> option are discarded if the option is provided by user.
<code>-u [UID]</code> <code>--uid=[UID]</code>	The <code>uid</code> of the user to expire the password for. To expire the password of multiple users, pass the <code>-u</code> or <code>--uid</code> option multiple times, as in this example: <code>--uid "Alice" --uid "Bob"</code> .

<code>-g [GROUP]</code> <code>--group=[GROUP]</code>	Add password expiry to user(s) in one or more groups. This option can be used as <code>--group foo --group bar</code> to add expiry passwords for users in multiple groups.
---	--

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 ./occ user:expire-password -u frank

# Expire the user "frank"'s password in 2 days time.
sudo -u www-data ./occ user:expire-password -u 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 ./occ user:expire-password --uid 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 ./occ user:expire-password --uid 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.

Ransomware Protection (Enterprise Edition only)

Marketplace URL: [Ransomware Protection](#)

Use these commands to help users recover from a Ransomware attack. You can find more information about the application in the [Ransomware Protection documentation](#).

Command Description

```
sudo -u www-data ./occ ransomguard:scan <timestamp> <user>
```

Arguments

<code><timestamp></code> <code><user></code>	Report all changes in a user's account, starting from timestamp.
---	--

```
sudo -u www-data ./occ ransomguard:restore <timestamp> <user>
```

Arguments

<code><timestamp></code> <code><user></code>	Revert all operations in a user account after a point in time.
---	--

```
sudo -u www-data ./occ ransomguard:lock <user>
```

Arguments

<code><user></code>	Set a user account as read-only for ownCloud and other WebDAV clients when malicious activity is suspected.
---------------------------	---

```
sudo -u www-data ./occ ransomguard:unlock <user>
```

Arguments

<code><user></code>	Unlock a user account after ransomware issues have been resolved.
---------------------------	---

Collabora Online / Secure View

Marketplace URL: [Collabora Online](#)

Collabora Online allows you to work with all kinds of collabora office documents inside ownCloud

for improved productivity. For details, see the [Collabora Online / Secure View](#) documentation.

`config:app` commands to configure the Collabora Online app.

```
config:app:get|set
richdocuments wopi_url          WOPI Server URL
richdocuments secure_view_option Enable Secure View
richdocuments watermark_text    Watermark pattern displayed in the document
richdocuments open_in_new_tab   Open documents in a new tab
richdocuments secure_view_can_print_default Define if documents can be printed or
exported
richdocuments secure_view_open_action_default Enforce displaying the watermark by
default
```

App Configuration

All app configurations are set and queried with the `config:app` command set. The examples below set a value. To query a value use `config:app:get` and the corresponding key without any options or attributes. Note that values have to be set in single quotes.

Define the WOPI Server URL

WOPI Server URL

This command sets the WOPI Server to `[IP/URL]:port`

`[IP/URL]:port` can be any IP/URL plus the port on which the WOPI server can be accessed like:

- `a.b.c.d`
- `http://a.b.c.d:8098`
- `https://rd.yourdomain.com`
- ...

Adding the port is only necessary when not using standard ports.

```
sudo -u www-data ./occ config:app:set richdocuments wopi_url --value='[IP/URL]:port'
```

Enable Secure View

Enable Secure View (possible values: true/false, default: false).

The following example command enables secure view globally on the system:

```
sudo -u www-data ./occ config:app:set richdocuments secure_view_option --value='true'
```

Define the Watermark Pattern Displayed

A watermark pattern is displayed in the document when it is viewed. It can be an arbitrary string. The keyword {viewer-email} will be replaced with the current user's email address in the document watermark. If an email address is not set, then the user's display name will be used.

The following example command sets the watermark pattern displayed in the document:

```
sudo -u www-data ./occ config:app:set richdocuments watermark_text --value='Restricted to {viewer-email}'
```

Open Documents in a New Tab

By default, documents will open in a new tab if not otherwise defined. You can change this behaviour with a command (possible values: true/false, default: false).

The following example command makes documents open in the same tab:

```
sudo -u www-data ./occ config:app:set richdocuments open_in_new_tab --value='false'
```

Define the Print and Exporting Option

Enable documents in secure view mode to be printed and exported (possible values: true/false, default: false).

The following example command enables the option to globally print and export documents although secure view is enabled:

```
sudo -u www-data ./occ config:app:set secure_view_can_print_default --value='true'
```

Enforce Displaying the Watermark

Open documents in secure view with watermark by default (possible values: true/false, default: false).

The following example command enables the option to globally enforce displaying the watermark when documents are viewed:

```
sudo -u www-data ./occ config:app:set richdocuments secure_view_open_action_default --value='true'
```

Delete a Key or Change a Key

You can delete a key with the following example command:

```
sudo -u www-data ./occ config:app:delete richdocuments secure_view_open_action_default
```

You can change a key with the following example command:

```
sudo -u www-data ./occ config:app:set richdocuments secure_view_option --value='false'
```

OAuth2

Marketplace URL: [OAuth2](#)

Use these commands to configure OAuth2 clients via the OAuth2 app:

```
oauth2
  oauth2:add-client    Adds an OAuth2 client
  oauth2:list-clients Lists OAuth2 clients
  oauth2:remove-client Removes an OAuth2 client
  oauth2:modify-client Modify OAuth2 client details
```

Add a Client

Usage

```
oauth2:add-client <name> <client-id> <client-secret> <redirect-url> [<allow-sub-
domains> [<trusted> [<force-trust>]]]
```

Arguments

<code>name</code>	Name of the client - will be displayed in the authorization page to the user
<code>client-id</code>	Identifier of the client - used by the client during the implicit and authorization code flow
<code>client-secret</code>	Secret of the client - used by the client during the authorization code flow
<code>redirect-url</code>	Redirect URL - used in the OAuth flows to post back tokens and authorization codes to the client
<code>allow-sub-domains</code>	Defines if the redirect url is allowed to use sub-domains. Enter true or false [default: "false"]
<code>trusted</code>	Defines if the client is trusted. Enter true or false [default: "false"]
<code>force-trust</code>	Trust the client even if the redirect-url is localhost. [default: "false"]

List Clients

Usage

```
oauth2:list-clients [options]
```

Options

<code>--output[=OUTPUT]</code>	The output format to use (plain, json or json_pretty). [default: "plain"]
--------------------------------	---

Listing 16. Example Output

```
- Desktop Client:
  - name: Desktop Client
  - redirect-url: http://localhost:*
  - client-id: xdX0t13JKxym1B1QcEncf2XDkLAexMBFwiT9j6EfhHFJhs2KM9jbjTmf8JBXE69
  - client-secret: UBntmLjC2yYCeHwsyj73Uwo9TAaecAetRwMw0xYcvNL9yRdLSUi0hUAHfvCHFeFh
  - allow-sub-domains: false
  - trusted: false
- Android:
  - name: Android
  - redirect-url: oc://android.owncloud.com
  - client-id: e4rAsNUSIU01F4nbv9FmCeUkTlV9GdgTLDH1b5uie7syb90SzEVrbN7HIpmWJeD
  - client-secret: dInFYGV33xKzhbRmpqQ1tYNdfLdJIifJ9L5ISoKhNoT9qZftpdWSP71VrpGR9pmoD
  - allow-sub-domains: false
  - trusted: false
- iOS:
  - name: iOS
  - redirect-url: oc://ios.owncloud.com
  - client-id: mxd50QDk6es5LzOzRvidJNfXLUZS2oN3oUFeXPP8LpPrhx3UroJFduGEYIB0xkY1
  - client-secret: KFeFWWEZ09TkisIQzR3fo7hfiMXl0paqP8CFuTbSHzV1TUuGECg1PxpivKJfOXIx
  - allow-sub-domains: false
  - trusted: false
```

Modify Client Details

Usage

```
oauth2:modify-client <name> <key> <value>
```

Arguments

<code>name</code>	Name of client
<code>key</code>	Key to be changed. Valid keys are: <code>name</code> , <code>client-id</code> , <code>client-secret</code> , <code>redirect-url</code> , <code>allow-sub-domains</code> , <code>trusted</code>
<code>value</code>	The new value of the key.

Remove a Client

Usage

```
oauth2:remove-client <client-id>
```

Arguments

<code>client-id</code>	Identifier of the client - used by the client during the implicit and authorization code flow
------------------------	---

S3 Primary Objectstore

Commands to configure Amazon S3 compatible object storages as the primary ownCloud storage location.

Marketplace URL: [S3 Primary Object Storage](#)

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

<code>update-configuration</code>	If the bucket exists, the configuration will be updated.
<code>accept-warning</code>	No warning about the usage of this command will be displayed.

SAML/SSO Shibboleth Integration (Enterprise Edition only)

Marketplace URL: [SAML/SSO Integration](#)

`shibboleth:mode` sets your Shibboleth mode to `notactive`, `autoprovision`, or `ssonly`

```
sudo -u www-data ./occ shibboleth:mode [mode]
```

Two-Factor TOTP

Marketplace URL: [2-Factor Authentication](#)

The following commands manage the *2-Factor Authentication App*. TOTP stands for *time-based one-time password*. There is also a core component independent of the *2-Factor Authentication App* with which a particular user can be enabled or disabled for the two-factor authentication. For details see section [Two-Factor Authentication](#).

The following commands are available for the 2-Factor Authentication app:

```
twofactor_totp
twofactor_totp:delete-redundant-secret      Delete the redundant secret of non-
existing users
twofactor_totp:set-secret-verification-status  Set secret verification status of
specified users or all users
```

Delete Redundant Secrets

Delete the redundant secrets of non-existing users:

```
sudo -u www-data ./occ twofactor_totp:delete-redundant-secret
```

Set Secret Verification Status

Set secret verification status of specified users or all users:

```
sudo -u www-data ./occ twofactor_totp:set-secret-verification-status [options] [--]
<set-verified>
```

Arguments

<code>set-verified</code>	Secret verification status to set. (true or false)
---------------------------	--

Options

<code>--all</code>	Will affect all users that use TOTP
<code>-u, --uid=UID</code>	The user's uid is used. This option can be used as <code>--uid="Alice" --uid="Bob"</code> (multiple values allowed)

Windows Network Drive (WND)

Marketplace URL: [External Storage: Windows Network Drives](#)

Integrate Windows and Samba/CIFS shared network drives as external storages. For details please see the [Windows Network Drive \(WND\)](#) documentation.

The `wnd` commands configure the WND app.

```
wnd
  wnd:listen                Listen to smb changes and store notifications for later
  processing
  wnd:process-queue        Process the notifications stored by the wnd:listen command
  wnd:set-service-account  Sets the service account for the target mount point
  (deprecated)
```

Please see the [Windows Network Drive Notifications](#) for how to properly setup `wnd:listen` and `wnd:process-queue`.

Configure the Listener

Listen to smb changes and store notifications for later processing in the database

```
sudo -u www-data ./occ wnd:listen [options] [--] <host> <share> <username>
[<password>]
```

Arguments

<code>host</code>	The hostname or IP address of the server to listen to
<code>share</code>	The share inside the host to listen to for changes
<code>username</code>	The username that will be used to connect to the share
<code>password</code>	The user's password (will be asked for if it isn't provided)

Options

<code>-p,</code> <code>--path=PATH</code>	The path inside the share to watch for changes [default: ""]
<code>--password-file=PASSWORD</code> <code>-FILE</code>	The file containing the password for the account to be used to listen
<code>--password-from-service</code> <code>-account</code>	Use the password from the matching service account. This works only for collaborative WND mounts
<code>--password-trim</code>	Trim blank characters from the password
<code>--unbuffering</code> <code>-option=UNBUFFERING-OPTION</code>	Force the usage of that unbuffering option for the underlying smbclient command. Possible options are either "auto", "pty" or "stdbuf" [default: "auto"]

<code>--output[=OUTPUT]</code>	The output format to use (plain, json or json_pretty). [default: "plain"]
--------------------------------	--



1. To enter the password of the service account via the console, the `password` option, the `password-file` option and the `password-from-service-account` option must not be set.
2. To use the password for the service account from the mount point settings, use the `password-from-service-account` option.
3. If you use the `password` option together with the `password-file` option, the `password-file` option takes precedence over the `password` argument.

Process Notifications

Process the notifications stored by the `wnd:listen` command

```
sudo -u www-data ./occ wnd:process-queue [options] [--] <host> <share>
```

Arguments

<code>host</code>	The server whose notifications will be processed
<code>share</code>	The share whose notifications will be processed

Options

<code>--output[=OUTPUT]</code>	The output format to use (plain, json or json_pretty). [default: "plain"]
--------------------------------	--

Set the Service Account



This command is deprecated starting with ownCloud 10.8. All mount options marked as *password* are now encrypted by default. Existing old settings are migrated automatically.

Sets the service account for the target mount point. You'll be asked for the password of the service account.

```
sudo -u www-data ./occ wnd:set-service-account [options] [--] <mount-id>
```

Please see the occ documentation of [files_external:list](#) to get the required mount-id.

Arguments

<code>mount-id</code>	ID of the mount point. Use "occ files_external:list --short" to find it
-----------------------	---

Options

```
--output[=OUTPUT]
```

The output format to use (plain, json or json_pretty).
[default: "plain"]

Language Configuration

In normal cases, ownCloud will automatically detect the language of the Web UI. If this does not work as expected, or you want to make sure that ownCloud always starts with a given language, you can use the **default_language** configuration parameter.

This parameter can be set in *config/config.php*

Parameters

```
'default_language' => 'en',
```

Keep in mind that this will not affect the language preferences of users, which can be configured under **Settings** › **Personal** › **General** › **Language** once they have logged in.

More supported languages can be found in directory *<ownCloud_root>/settings/l10n*. List all files with *ls *js*. The language code to be used is the filename without extension.

Example:

```
en_GB.js --> en_GB
```

Refer to [Wikipedia](#) for a match of language code to country.

Legal Settings Configuration

Introduction

Because of one or more legal frameworks around the world, some ownCloud instances may need to display links to both an Imprint as well as a Privacy Policy on all pages (both in the Web UI and within email templates). An Imprint document is a legally mandated statement of the ownership and authorship of the ownCloud installation. You can think of an Imprint as a rather fancy "**About Us**" page or an enhanced "**Terms and Conditions**" page; in Germany, this is known as an "**Impressum**".



Imprint and Privacy Policy links are shown on all **public** pages and in e-mail footers. Authenticated pages, such as files app or settings, do not show them.

Some of the more global legal frameworks prominent are:

- The [GDPR General Data Protection Regulation](#)
- 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 \(COPPA\)](#)

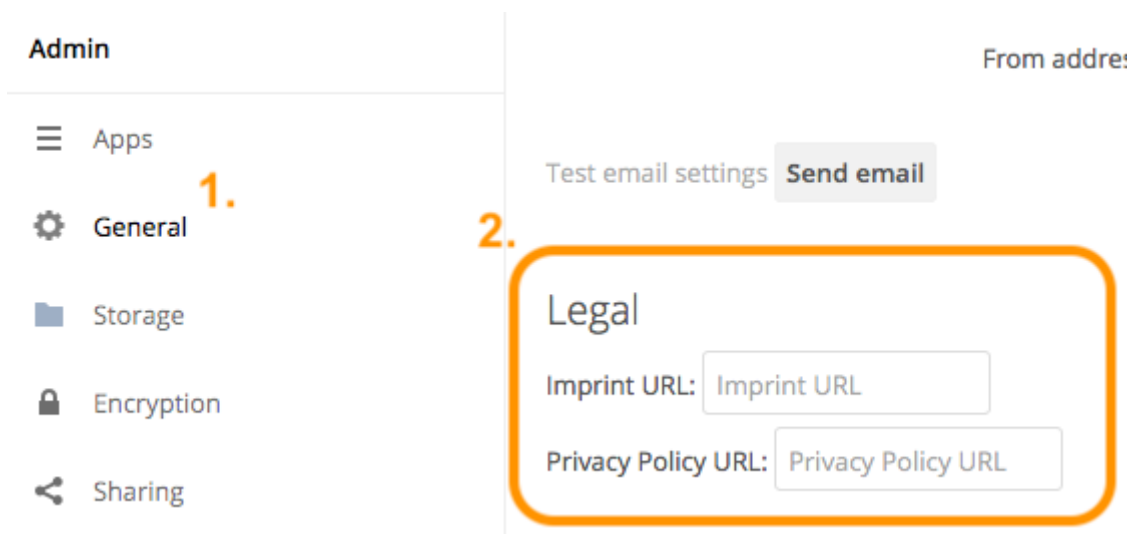
If you're required to link to either one of these, you can specify the link to them in two ways:

- [Using the Web UI](#)
- [Using the Command Line](#)

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.

Configuring Imprint and Privacy Policy URLs in the ownCloud Web UI.



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:

```
sudo -u www-data ./occ config:app:get core legal.imprint_url
sudo -u www-data ./occ config:app:get core legal.privacy_policy_url
```

Set the Imprint and Privacy Policy URLs:

```
sudo -u www-data ./occ config:app:set core legal.imprint_url --value=new_value
sudo -u www-data ./occ config:app:set core legal.privacy_policy_url --value=new_value
```

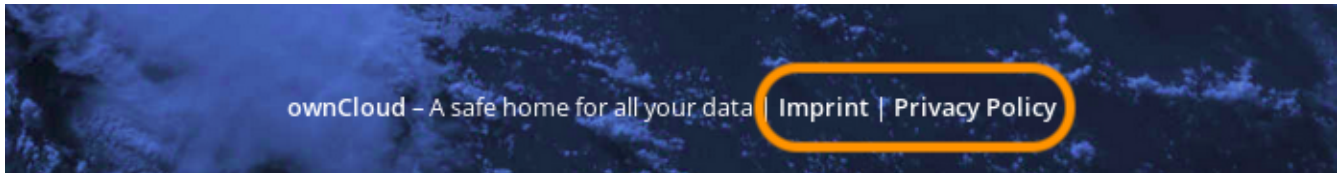
For more information about these commands, refer to [the config command reference in the occ commands documentation](#).

Viewing the URLs



Customized email templates and themes that were built prior to ownCloud version 10.0.9 [need to be updated](#).

Once the settings have been updated, you will see two links appear at the bottom the ownCloud login page, one for each option, as in the screenshot below.



Logging Configuration

Introduction

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 using the default syslog daemon.

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`. As an example see:

```
'datadirectory' => '/var/www/owncloud/data',
```

When not using the default location for the logfile, it can be [specified](#) via:

```
'logfile' => '<your-path>/owncloud.log',
```

Note that the web server user must have write rights to that directory.

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" => "3",  
"logdateformat" => "F d, Y H:i:s",
```

syslog

The log type can be set to [syslog](#) and all log information will be sent to your default syslog daemon.

```
"log_type" => "syslog",  
"logfile" => "",  
"loglevel" => "3",
```

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

[Log conditions](#) for log level increase based on conditions can be set. This will increase the logging level automatically 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' => ['comments'],
    'logfile' => '/tmp/test2.log'
  ]
],
```

Based on the conditional log settings above, the following logs are written to the same logfile:

- 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 **comments** gets debug logged.

Request Tracing

ownCloud logs the **X-REQUEST-ID** header from desktop and mobile clients in the ownCloud log when sent with client requests.

The header helps when clients have a problem communicating with an ownCloud server, because:

1. The user can include the value in bug reports; and
2. System administrators can filter log files for the header value.

Storing this information makes searching more efficient, as system administrators don't have to

rely solely on normal log entry elements, such as timestamps and IP addresses.

The Header's Value

The header's value is a [UUID \(version 4\)](#). These are generated from truly random (or pseudo-random) numbers by the client and do not contain *any* sensitive information. As a result it will not violate the user's privacy nor allow users to be tracked.

Required Server Configuration

Before the value can be stored in your web server's log files, your system administrator(s) need to configure two areas:

1. **The web server:** The web server's logging configuration needs to be adjusted, e.g., Apache's access and error log format, so that the value is stored in request log entries. An example of configuring Apache's CustomLog format [is provided below](#).
2. **Load balancers:** All load balancers sitting in-between clients and your ownCloud instance(s), e.g., [Traefik](#), [Big-IP](#), need to be configured to pass the header through. This way it is possible to track ("trace") requests through larger environments. Please refer to your load balancer's configuration for details on how to adjust their configuration.

Web Server Configuration Example

Listing 17. Example for Apache

```
CustomLog /var/log/apache2/access.log "%h %l %u %t \"%r\" %>s %0 \"%{Referer}i\"  
\"%{User-Agent}i\" \"%{X-Request-ID}i\""
```



The exact log format chosen is entirely up to your system administrator(s).

Reverse Proxy Configuration

Introduction

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 `overritewebroot` 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`.

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"
```



If you want to use the SSL proxy during installation you have to create `config/config.php` manually, otherwise you have to extend the existing `$CONFIG` array.

Unresolved directive in modules/admin_manual/pages/configuration/server/security/index.adoc - include::partial\$section_page.adoc[]

- [OAuth2](#)
- [Password Policy](#)
- [Brute-Force Protection](#)
- [Hardware Security Module Daemon](#)

- [jQuery Warnings](#)

Brute-Force Protection

The Brute-Force Protection extension allows administrators to specify a maximum number of unsuccessful user account login attempts. On reaching the unsuccessful login limit, ownCloud temporarily bans further login attempts to those user accounts from the originating IP address. The time frame of the ban is configurable by ownCloud administrators.

To configure this app in the web interface, navigate to [admin](#) → [settings](#) → [admin/security](#).

Brute Force Protection

Count failed login attempts over how many seconds?

Ban after how many failed login attempts?

Ban for how many seconds?

Save settings

To configure this app on the command line you can use [occ commands](#).

Open Authentication (OAuth2)

Introduction

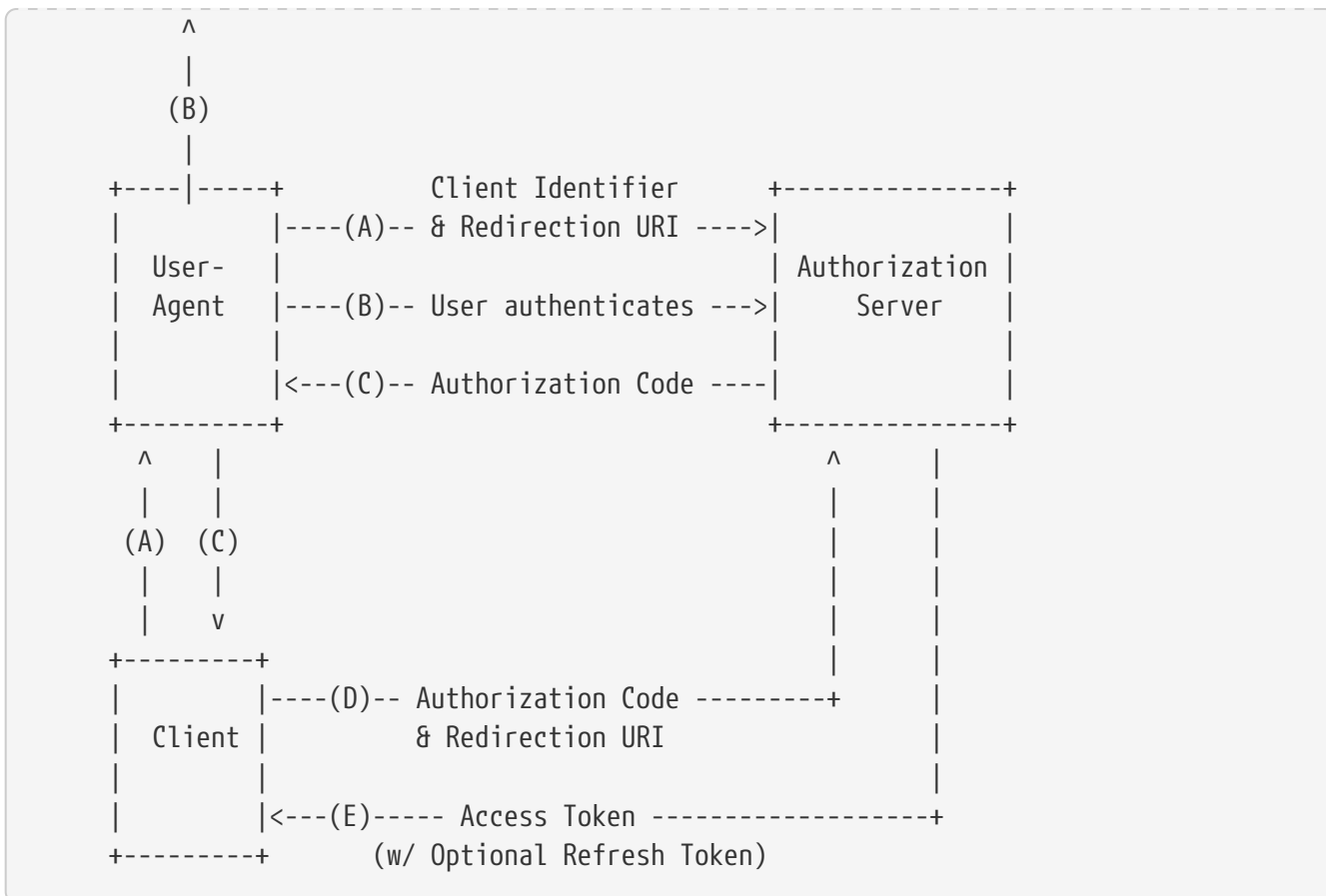
OAuth2 (OpenAuthentication) is summarized in [RFC 6749](#) as follows:

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.

— OAuth2 Overview

Here is an overview of how the process works:

```
+-----+
| Resource |
|  Owner  |
|         |
+-----+
```



The OAuth2 App

OAuth2 support is available in ownCloud via the [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.

Requirements

To use the OAuth2 app, your ownCloud installation will need to meet the following dependencies:

- **Apache:** If you are hosting your ownCloud installation using the Apache web server, then [mod_rewrite](#) and [mod_headers](#) modules must be installed and enabled.
- **Redis:** You will need to have a Redis server available, ideally the latest, stable version.
- **PHP-Redis:** Your PHP installation must have the [php-redis](#) extension (≥ 4.2) installed and enabled.

See the [Detailed Installation Guide](#) for how to install Redis and PHP-Redis.

Installation

To install the application, download the [OAuth2 app](#) from the marketplace to the ownCloud `app` directory or use the Market app.

Basic Configuration

To enable token-only based app or client logins in `config/config.php`, set `token_auth_enforced` to `true`. See [config sample file](#) for more details.



The OAuth2 app comes with a set of `occ` commands to configure clients. For more information on usage of `occ` for OAuth2, see section [OAuth2 Commands](#).

Trusting Clients

Since version 0.5.0 of the OAuth2 app, you can mark clients as trusted. This will have the effect that the consent step in the authentication process will be skipped for this client.



Only mark trustworthy clients and web apps under your control as trusted. Apps which cannot keep the `Client Identifier (ID)` secret or have `redirect URIs` which can not be fully controlled should not be marked as trusted.

Refer to the [official OAuth2 RFC sections 10.1 and 10.2](#) for further information about the risks.

OAuth 2.0

Registered clients

Name	Redirection URI	Client identifier	Secret	Subdomains allowed	Trusted client
Desktop Client	http://localhost:*	xdX0t133Kxym1B1QcEncf2XDkLAexMBFw1T9j6EfhHFJhs2KM9jBjTmf8JBXE69	UBntmLjC2yYCeHwsyJ73Uwo9TAaecAetRwMw0xycvNL9yRdLSU10HUAHvCHFeFh		<input type="checkbox"/>
Android	oc://android.owncloud.com	e47rASnUSIU0LF4nbv9FmCeUKTLV9GdgTLDH1b5u1e7syb9052EVrbN7HIpmWJeD	dInFYGV33xKzhhRmpQ0LTYMfLdJJI79L51SoKNoT9qZfTpdwSP71VrpG9pnoD		<input type="checkbox"/>
iOS	oc://ios.owncloud.com	mx0500K6es5Lz0zRv1dJNfXLUZ52oN3oUFEXPP8lpPrhx3UroJFduGEYIB0xkY1	KFeFWEZ09TK1sIQzR3f07h7f1MXL0paqP8CFuTbSH2V1TUuGECgLPxp1VKJf0XIX		<input type="checkbox"/>

Add client

Allow subdomains Trusted client

If you want to mark an existing client as trusted, you have to:

- Copy the `Client Identifier (ID)` and the `Client Secret`.
- Then delete the existing entry either in the UI or via the [occ oauth2 remove command](#).
- And finally add it again with the [occ oauth2 add command](#) with the trusted setting enabled. When deleting in the web UI, you might need to scroll horizontally to see the delete buttons. Follow this link regarding [Client IDs, Secrets and Redirect URIs](#) for ownCloud clients.

Restricting Usage

- Enterprise installations can limit the access of authorized clients, preventing unwanted clients from connecting.

Endpoints

Description	URI
Authorization URL	/index.php/apps/oauth2/authorize
Access Token URL	/index.php/apps/oauth2/api/v1/token

Protocol Flow

Client Registration

Clients first have to be registered in the web-UI **Settings > Admin > 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.

Refer to the [official client registration RFC from the IETF](#) for further information about client registration.

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 <code>code</code> 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.

Refer to the [official authorization request RFC from the IETF](#) for further information about client registration.

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.

Refer to the [official authorization response RFC from the IETF](#) for further information about client registration.

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> .

Parameter	Required	Description
<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.	

Refer to the [official access token request RFC from the IETF](#) for further information about client registration.

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/owncld/index.php/apps/oauth2/authorization-successful"
}
```

Refer to the [official access token response RFC from the IETF](#) for further information about client registration.



For a succinct explanation of the differences between access tokens and authorization codes, check out this [answer on StackOverflow](#).

Limitations

- Since the app does not handle 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.
- It is not possible to explicitly end user sessions when using OAuth2. Have a read through [User Authentication with OAuth 2.0](#) to find out more.

Further Reading

- [User Authentication with OAuth 2.0](#)

- [The problem with OAuth for Authentication.](#)
- [Session Authentication vs Token Authentication](#)
- [OAuth 2.0 Token Revocation](#)

Password Policy

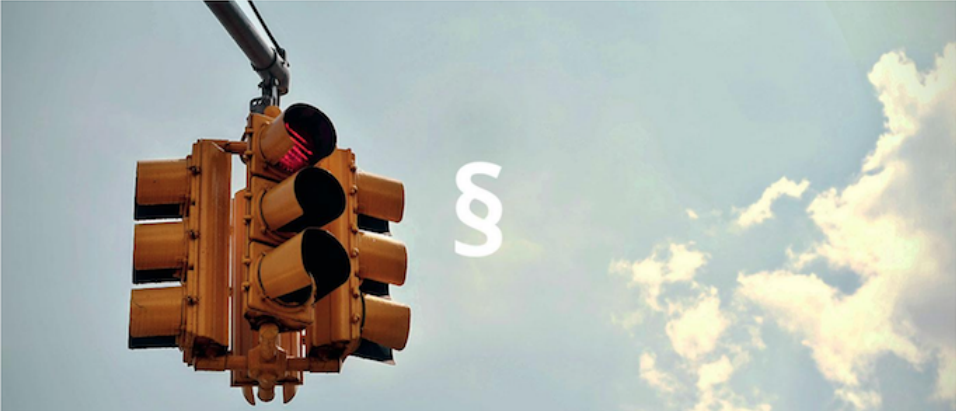
The Password Policy App


Password Policy

Define password policies for user and public link passwords

ENTERPRISE

made by [ownCloud](#)





This app is part of ownCloud Enterprise Edition. Take your ownCloud to the next level and start an ownCloud Enterprise Trial today!

[START ENTERPRISE TRIAL >](#)

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 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.

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.	*	

Setting	User Passwords	Public Links
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 not set		*

Here is an example of what an administrator will see:

Password and public link expiration policies

Minimum password requirements for user accounts and public links:

- minimum characters
- lowercase letters
- uppercase letters
- numbers
- special characters
- Restrict to these special characters:

User password policies:

- last passwords should not be used
- 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



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.



Installing and enabling the application also extends the occ command to support [password policy](#) management.



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.

Warnings on Admin Page

Introduction

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

- Transactional file locking should be configured to use memory-based locking, not the default slow database-based locking. See the [documentation](#) for more information.
- We recommend to enable system cron as any other cron method has possible performance and reliability implications.
- You are accessing this site via HTTP. We strongly suggest you configure your server to require using HTTPS instead as described in our [security tips](#).
- No memory cache has been configured. To enhance your performance please configure a memcache if available. Further information can be found in our [documentation](#).

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 [caching_configuration](#).

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.

Background Jobs

We recommend to enable system cron as any other cron method has possible performance and reliability implications.

Further Information can be found in the docs article on [Background Jobs](#)

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 webserver.

- [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 tips](#) 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.

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 with Binary Logging Enabled](#)) how to configure your database for this requirement.

The HSM (Hardware Security Module) Daemon (`hsmdaemon`)

Introduction

The `hsmdaemon` is a daemon provided by ownCloud to delegate encryption to an [HSM \(Hardware Security Module\)](#). This can be necessary as PHP cannot directly interface with a [PKCS11 stack](#), neither with an API wrapper because none exists, nor via the OpenSSL bindings. Therefore a separate process is needed to decrypt anything with the private key stored in an HSM.



When using `hsmdaemon` with an HSM, the keys *may* still be stored on the same physical machine as ownCloud.



For `hsmdaemon` support, you need ownCloud Enterprise Edition ≥ 10.2 . We recommend consulting with us when deploying storage encryption with an HSM.



Starting with the Encryption App version 1.5.1, HSM can now work with both **binary** and **base64** encoding/decoding. If not otherwise configured, **binary** is the default.

Running `exec()` to decrypt the key with a command line command to do the encryption might leak the HSM credentials if the admin lists the currently running processes. To prevent that, an HSM daemon will be used that can open a session to the HSM upon startup.

This daemon will be used by ownCloud to decrypt the current master key upon request. The communication happens via **UNIX sockets** or **TCP sockets** and is authorized by a shared token that the daemon stores in the ownCloud database via a REST/JSON route.

ownCloud internally uses OpenSSL to encrypt and decrypt keys and that is extended to support **en-/decrypt** operations via the new daemon. The current solution encrypts the ownCloud master key with a key from the HSM.



From the technical point of view the **Crypt** class is extended to handle the key generation in the HSM device and also to get the key from HSM. For the read/write operation on a file, the request goes to the HSM and then, based on the keys fetched from HSM, the files are encrypted or decrypted. The keys are not replaced.

How The HSM Daemon Interacts with ownCloud

Upon startup, the daemon will generate a token and send it to ownCloud via a new REST/JSON route. After connecting with the HSM daemon, an unsophisticated, line-based, protocol is used (every line ends with CRLF):

1. ownCloud sends the token read from database.
2. The daemon compares the received token with its token and returns an **OK** line.
3. ownCloud then sends the data it wants to decrypt as a **Base64-encoded**, one-line string.
4. The daemon returns the decrypted data as a Base64-encoded one-line string.

Doing so ensures that an evil admin will need to wiretap the communication between either the database or the HSM daemon and ownCloud.

Quick Overview

HSM support consists of two core parts:

1. An actual HSM PKCS11 module.
2. A **hsmdaemon** that provides a **JWT** - protected web API for the PKCS11 stack to generate key pairs and decrypt data.

Deployment Recommendation

We recommend running **hsmdaemon** on every web server to reduce latency.

Installation

Integrating the `hsmdaemon` with ownCloud requires 3 steps; these are:

1. [Install a PKCS11 Module](#)
2. [Install and Configure the hsmdaemon](#)
3. [Configure ownCloud](#)



The installation instructions in this guide have been designed to work with ownCloud's [supported operating systems](#). If you are using a different operating system or distribution, please adjust the instructions to suit your environment.

Install a PKCS11 Module

Install Using a Preconfigured PKCS11 Module

At least one PKCS11 library is necessary. This is typically provided by an HSM vendor. If a PKCS11 library is not available, you can [use the software HSM - SoftHSM2](#).

Initialise the Token

Now we can initialize the token:

```
sudo softhsm2-util --init-token --slot 0 --label "My token 1"
```

It will ask for two PINs, an SO and a User pin. See [opendnssec](#) for more information. The SO PIN can e.g. be used to re-initialize the token and the user PIN is handed out to the application so it can interact with the token.

Install PKCS11 CLI tools (optional)

To use the PKCS11 API on the CLI, we need to install [OpenSC](#).

- [Debian and Ubuntu](#)
- [openSUSE and SUSE Linux Enterprise Server](#)
- [Fedora and Red Hat Enterprise Linux and Centos](#)

Initialise on Debian and Ubuntu

To install OpenSC on Debian and Ubuntu, run the following command:

```
sudo apt install -y opensc
```

Initialise on openSUSE and SUSE Linux Enterprise Server

To install OpenSC on openSUSE and SUSE Linux Enterprise Server, run the following command:

```
sudo zypper install -y --auto-agree-with-licenses opensc
```

Initialise on Fedora and Red Hat Enterprise Linux and Centos

To install OpenSC on Fedora and Red Hat Enterprise Linux and Centos, run the following command:

```
sudo yum install --assumeyes opensc
```

List Tokens

You can list available tokens using the [pkcs11-tool](#) by running the following command:

```
sudo pkcs11-tool --module </path/to/libsofthsm2.so> -l --pin <user-pin> -0
```

The Module Parameter

The module parameter is either the library provided by the HSM vendor or `libsofthsm2` which was installed with SoftHSM 2. If you are using `libsofthsm2`, the path to `libsofthsm2.so` for each of the supported distributions is available below.

Distribution	Path
Debian and Ubuntu	<code>/usr/lib/softhsm/libsofthsm2.so</code>
openSUSE and SUSE Linux Enterprise Server	<code>/usr/lib64/pkcs11/libsofthsm2.so</code>
Fedora and Red Hat Enterprise Linux and Centos	<code>/usr/lib64/pkcs11/libsofthsm2.so</code>



See the [OpenSC Wiki](#) for more information.

Install and Configure the hsmdaemon

Installing `hsmdaemon` requires several steps. These are:

1. [Install the hsmdaemon Binary](#)
2. [Copy the Config File](#)
3. [Install the System Service](#)
4. [Configure the PKCS 11 Module Path](#)
5. [Configure Slot and Pin](#)
6. [Test the hsmdaemon](#)
7. [Configure Other Options](#)

Install the hsmdaemon Binary

After you have obtained the `hsmdaemon` from ownCloud, you need to move the `hsmdaemon` binary to a

directory located in your system path and make the binary executable:

```
sudo install -m 755 ./hsmdaemon /usr/local/bin/hsmdaemon
```

Copy the Config File

The default location where `hsmdaemon` looks for its config file is `/etc/hsmdaemon/hsmdaemon.toml`. To create it from the example config file available in the provided package, run the following commands:

Create the `hsmdaemon` configuration directory:

```
sudo mkdir /etc/hsmdaemon
```

Copy the example config file, allow only root and users in the root group to read & write the configuration file:

```
sudo install -m 640 ./hsmdaemon.toml /etc/hsmdaemon/hsmdaemon.toml
```

Install the System Service

Now that the binary is available and the configuration file is in place, `hsmdaemon` must be installed as a system service. To do so, run it with the `install` option as in the example below.

```
sudo /usr/local/bin/hsmdaemon install
sudo service hsmdaemon start
```

If it installs successfully, you should see the following console output:

```
Install HSM Daemon:          [ OK ]
```

It should now be running and set to start automatically at boot time.



The daemon is managed using the following three commands:

- `sudo service hsmdaemon start`
- `sudo service hsmdaemon stop` and
- `sudo service hsmdaemon status`

Configure the PKCS11 Module Path

To set the path to the PKCS11 module, update the line below in `/etc/hsmdaemon/hsmdaemon.toml`, with the appropriate path on your system.


```
[pkcs11]
```

```
# softhsm v2
```

```
module = "/usr/lib/x86_64-linux-gnu/softhsm/libsofthsm2.so"
```

List Available Slots

This command lists the available slots.

```
sudo hsmdaemon listslots
```

```
{"level":"debug","ts":"2019-02-14T09:27:02.068+0100","caller":"hsmdaemon/keymanager.go:27","msg":"initialize pkcs11 module","module":"/usr/lib/softhsm/libsofthsm2.so"}
```

```
{"level":"info","ts":"2019-02-14T09:27:02.087+0100","caller":"hsmdaemon/keymanager.go:65","msg":"Slots found","slotIds":[550099622,1989683358,2]}
```

Available slots:

Slot: 550099622,

Slot info:

Description: SoftHSM slot ID 0x20c9daa6

Manufacturer ID: SoftHSM project

Hardware version: 2.2

Firmware version: 2.2

Token present: yes

Flags:

Token info:

Manufacturer ID: SoftHSM project

Model: SoftHSM v2

Hardware version: 2.2

Firmware version: 2.2

Serial number: e8ba06bca0c9daa6

Initialized: yes

User PIN init.: yes

Label: oc token without pin

MaxSessionCount: 0

SessionCount: 18446744073709551615

MaxRwSessionCount: 0

RwSessionCount: 18446744073709551615

MaxPinLen: 255

MinPinLen: 4

TotalPublicMemory: 18446744073709551615

FreePublicMemory: 18446744073709551615

TotalPrivateMemory: 18446744073709551615

FreePrivateMemory: 18446744073709551615

UTCTime: 2019021408270200

Flags: CKF_RNG CKF_LOGIN_REQUIRED CKF_RESTORE_KEY_NOT_NEEDED

CKF_USER_PIN_COUNT_LOW

Slot: 1989683358,

Slot info:

Description: SoftHSM slot ID 0x7698289e
Manufacturer ID: SoftHSM project
Hardware version: 2.2
Firmware version: 2.2



See the [OpenSC Wiki](#) for more information.

Configure the Slot and Pin

Define which slot to use and if a PIN is needed. Update `/etc/hsmdaemon/hsmdaemon.toml` with the information gathered in the `pkcs11` section as in the example below.

```
[pkcs11]
# softhsm v2
module = "/usr/lib/x86_64-linux-gnu/softhsm/libsofthsm2.so"
# The user pin supplied when running softhsm2-util --init-token, comment it out
# or leave empty if no pin is necessary
pin = "1234"
# Find your slot id with `sudo hsmdaemon listslots`
slot = 550099622
```

Test the hsmdaemon

Test Key Generation



If no PIN is supplied, generating a new key might be protected by an operator card that has to be inserted in the HSM. In this case, coordinate testing and final master key generation with your HSM team.

For testing the key generation, run the following example command:

```
sudo hsmdaemon genkey test
```

```
Id: 9bac3719-2b8d-11e9-aeab-0242b5ece4c3, label: test
```

```
-----BEGIN PUBLIC KEY-----
```

```
MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAl1B04vsI+xDk+x0nccL7
HQhMR/hwfa0+N8fyYNI8yzTTmYDqz9aaF20qG48+mjC0AUEt2kfKo94xM3UeEw4c
st4j1dpRJtmAJThcuN80H3sa+3MeXWgGuWxjB1lxEE0qax2A6Xz1LD1bDsogwkOL
hSkUU9AaMRBtF8fASJGtJDP+iXwdb70sFg78PS1wBAISYSUwk06xY7LwWIxge+hY
4oU+5x4itusd06rz6kbcJtmUyDUb8DhKnN60dkhniFUZLBG9HQyTa50M+BAabbFZ
mTM2gZ1UnGKXN7c4kaBPFt1IfjjVYu7pvj3B2uxUf4GywuSuWGwNAy89FqeXteRV
jwIDAQAB
```

```
-----END PUBLIC KEY-----
```

Test Showing Keys

To show an existing key, use the `hsmdaemon showkey` command with the key's id as in the following example.

```
sudo hsmdaemon showkey 9bac3719-2b8d-11e9-aeab-0242b5ece4c3
```

Test Data Encryption

For testing data encryption, run the following example commands:

The first argument is the `Id`: value from running the `genkey` command above. The second is the `base64-encoded data` to be encrypted.

```
sudo hsmdaemon encrypt 9bac3719-2b8d-11e9-aeab-0242b5ece4c3 Zm9vYmFy
```

If successful, you should see output similar to the example below:

```
{"level":"debug","ts":"2019-03-20T12:43:40.540+0100","caller":"hsmdaemon/keymanager.go:27","msg":"initialize pkcs11 module","module":"/usr/lib/softhsm/libsofthsm2.so"}
{"level":"debug","ts":"2019-03-20T12:43:40.545+0100","caller":"hsmdaemon/keymanager.go:205","msg":"openHSMSession","slotID":"858597139"}
{"level":"info","ts":"2019-03-20T12:43:40.549+0100","caller":"hsmdaemon/keymanager.go:621","msg":"Fetching private key","keyID":"9bac3719-2b8d-11e9-aeab-0242b5ece4c3"}
{"level":"debug","ts":"2019-03-20T12:43:40.549+0100","caller":"hsmdaemon/keymanager.go:641","msg":"Got uuid","string":"13d34146-4b02-11e9-adbd-0023ae27c404"}
WcezVb2N6bF8wLDooKZcmFn3tZgoIpoFGx6wQetx9sp1nK7JW2Y40Kt7P+0VKK1F07yXaffVDD2Q6jZZCQukQV
RV1zJrwbI9xU3Y10AwJFPP+WM/dZ1vdUwi7L05wq8UpL13LJWlMkvd1eIqKJS7apMnFk2hbnxXP6UKZmI++1tX
vqbAc6fwhcB5J+JG6lms4RwnD+eJC3dq5t00zzdI6vuIM/y3UT7ESklmHl5bKl+N+d6yk6qLxnFnIjweL+M3Tf
13+XPNAh5JxZpheJPvN3oL28uX76aizy4BCLnRgQ/ryUQeDF+a4zNF22sMwBh4Pt46KrYGNdZAnQpVzmkRZQ==
```

Test Data Decryption

For testing data decryption, run the following example commands:

```
sudo grep "generated keypair" /var/log/hsm.log
```

You should see output similar to the example below:

```
{"level":"debug","ts":"2021-06-19T03:10:01.562+0200","msg":"generated keypair","tokenId":"1262668f-d09b-11eb-b283-960000c05f34"}
{"level":"debug","ts":"2021-06-19T03:10:03.043+0200","msg":"generated
```

```
keypair", "tokenID": "1374447f-d09b-11eb-83c8-960000c05f34"}
{"level": "debug", "ts": "2021-06-19T03:10:03.710+0200", "msg": "generated
keypair", "tokenID": "13cd3f95-d09b-11eb-83c8-960000c05f34"}
```

```
key_id=$(sudo grep "generated keypair" /var/log/hsm.log | head -1 | jq .tokenID -r)
```

```
hello="Hello, world!"
```

```
echo "$hello" | base64
```

```
SGVsbG8sIHdvcmxkIQo=
```

```
test_enc=$(sudo ./hsmdaemon encrypt $key_id $(echo "$hello" | base64) | tee
/dev/stderr)
```

```
ep6Y1aAVAYpAesZ1+sQzzUepj082o34kjm63Drnz+6KED4oIBARQkXeW/OoxgUg6kQhQK1thA/3Ww33aaRxIE
SzVQF598qjXhhEXQ/0GL6BC+3tPcLC7ujUZaA7CG1NDkMneLFDd2+Tbax4OM+/w0zhfTMPgT0I1NrH/03owVgI
bWHjgLZmN/vxpPZKm/lyAV9tI2HW36UjVLEMD2qtPFXqjLU4YjZOVnMdETxQNSCWIVauFw0+VQQ/RiAqiXzRXE
g06YKx0Bk0n9IMT6XEh4MkMQTgb9pB12jrNSa9aMHbCvCneEmhd0CHBxPX499EkxxwtoEnXe6PATXs0g3VRA==
```

```
sudo -u www-data ./occ encryption:hsmdaemon:decrypt --keyId $key_id "$test_enc"
```

```
decrypted string (base64 encoded): 'SGVsbG8sIHdvcmxkIQo='
```

```
sudo tail -5 /var/log/hsm.log
```

```
{"level": "debug", "ts": "2021-06-20T23:46:11.958+0200", "msg": "openHSMSession", "slotID": 757826573}
{"level": "debug", "ts": "2021-06-20T23:46:11.960+0200", "msg": "created new session"}
{"level": "debug", "ts": "2021-06-20T23:46:11.960+0200", "msg": "Got
uuid", "string": "1262668f-d09b-11eb-b283-960000c05f34"}
{"level": "debug", "ts": "2021-06-20T23:46:11.962+0200", "msg": "found
object", "id": "\u0012bf\u00fffd\u0011\u00fffd\u0000\u0000\u00fffd_4"}
{"level": "debug", "ts": "2021-06-20T23:46:11.963+0200", "msg": "Decrypted"}
```

Results

- ☑ The base64 encoded string matches before encryption and after decryption.
- ☑ The key-id seen in the log with "generated keypair" causes no errors during encryption.

- ☑ The key-id re-appears in the log during decryption ("Got uuid")

Configure Other Options (optional)

For more options see the self-documented default config file `hsmdaemon.toml`.



During ownCloud config, you might want to run the `hsmdaemon` service in the foreground to see what is going on. You can do so using the following command (which also shows example console output, formatted for readability):

```
sudo hsmdaemon
```

```
{
  "level": "info",
  "ts": "2019-02-14T09:32:59.081+0100",
  "caller": "hsmdaemon/hsmdaemon.go:146",
  "msg": "Server listening",
  "host": "localhost",
  "port": 8513,
  "version": "0.0.7",
  "build": "2019-02-08T10:47:55+00:00"
}
```

Configure ownCloud



If anyone accesses ownCloud while encryption is enabled, it will automatically generate the keys. To prevent this shut down the web server until encryption is appropriately configured.

Configuring ownCloud to work with the `hsmdaemon` requires the following steps:

- [Generate a Secret for the hsmdaemon REST API](#)
- [Configure HSM-based Encryption](#)
- [Initialize and Check Generated Keys](#)

Generate a Secret for the hsmdaemon REST API

Generate a shared secret to use for the `hsmdaemon`.

```
cat /proc/sys/kernel/random/uuid
```

```
7a7d1826-b514-4d9f-afc7-a7485084e8de
```

Use this generated secret for `hsmdaemon` in `/etc/hsmdaemon/hsmdaemon.toml`

```
[jwt]  
secret = "7a7d1826-b514-4d9f-afc7-a7485084e8de"
```

Set the generated secret for ownCloud:

```
sudo -u www-data ./occ config:app:set encryption hsm.jwt.secret --value '7a7d1826-  
b514-4d9f-afc7-a7485084e8de'
```

If the command succeeds, you should see the following console output:

```
Config value hsm.jwt.secret for app encryption set to 7a7d1826-b514-4d9f-afc7-  
a7485084e8de
```

Configure HSM-based Encryption

Enable the HSM mode and enable encryption by running the commands in the following example:

```
sudo -u www-data ./occ app:enable encryption  
sudo -u www-data ./occ config:app:set encryption hsm.url --value  
'http://localhost:8513'  
sudo -u www-data ./occ encryption:select-encryption-type masterkey  
sudo -u www-data ./occ encryption:enable
```

If the commands are successful, you should see the following console output:

```
encryption enabled  
  
Config value hsm.url for app encryption set to http://localhost:8513  
  
Master key successfully enabled.  
  
Encryption enabled  
Default module: OC_DEFAULT_MODULE
```

Initialize and Check Generated Keys

Now start your web server and log in with any user to initialize the keys, have a look at the output of the `hsmdaemon` to see key generation and decryption requests. Check that the private key `/path/to/data/files_encryption/OC_DEFAULT_MODULE/` is less than **1000 bytes**. If it is not, then something is not configured correctly. You have to wipe all keys and reset the database flags for encryption to get a clean start for the ownCloud setup.

jQuery Warnings

:toc:right

Introduction

While ownCloud is using an older version of jQuery, we have fixed the known vulnerabilities in the patches listed below. We closely follow any security related news regarding the library for any new issues.



The jQuery version shipped inside ownCloud is secure.

Note that automatic scanners may still report false positives even if the CVE's have been addressed as the scanners just look at the jQuery version shipped.

Fixed Issues

- jQuery
 - CVE-2020-11022 and CVE-2020-11023
[patched in 10.5.0](#)
 - CVE-2015-9251
[patched in 10.0.9 RC3](#)
 - CVE-2019-11358
[patched in 10.8.0](#)
 - CVE-2016-7103
[patched in 10.9.0](#)
- jQuery-ui
 - CVE-2021-41182, CVE-2021-41183 and CVE-2021-41184
[patched in 10.9.0](#)

If you know about any issues which were not patched yet or which are not included in this list please notify us at security@owncloud.com.

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 set to the lower value of..
```

If so, please consider that newer versions of Redis have their own TCP-backlog value set to **511**, and that you have to increase if you have many connections. In high requests-per-second environments, you need a significant backlog to avoid slow clients connection issues.



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 latency and memory usage issues with Redis.
```

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 [Linux 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 [database conversion](#).

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 process 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 e.g. 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 >= 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 e.g. 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%. We recommend to keep the `KeepAliveTimeout` between 3 and 5. Higher numbers can block the Server with inactive connections. In combination with the periodic checks of the sync client the following settings are recommended:

```
KeepAlive On
KeepAliveTimeout 3
MaxKeepAliveRequests 200
```

Hostname Lookups

```
cat /etc/httpd/conf/httpd.conf
```

```
...
```

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.

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",
```

Virus Scanner Support

Introduction

When sharing files, security is a key aspect. The ownCloud Anti-Virus extension helps by protecting against malicious software like trojans or viruses.

You can get the [Anti-Virus](#) extension from the marketplace. It forwards files that are being uploaded to the ownCloud server to a malware scanning engine before they are written to the storage. When a file is recognized as malicious, it can be logged and prevented from being uploaded to the server to ensure that files in ownCloud are free of malware. More sophisticated rules may be specified as admin in the ownCloud Web interface **Admin** › **Settings** › **Security**.

General Info

Out of the box, the ownCloud Anti-Virus extension works with [Clam AntiVirus \(ClamAV\)](#) as the directly supported virus scanner. It detects all forms of malware including trojans, viruses and worms and scans compressed files, executables, image files, PDF, as well as many other file types. The ownCloud Anti-Virus application relies on the underlying ClamAV virus scanning engine, to

which the admin points ownCloud when configuring the application. The ClamAV virus definitions need to be kept up to date in order to provide effective protection.

Starting with Anti-Virus version 1.0.0, the app also offers an ICAP integration for Enterprise installations. Admins can integrate their favorite enterprise-grade antivirus scanners through the open standard [Internet Content Adaptation Protocol \(ICAP\)](#). With this set up, ownCloud can delegate the scanning of uploaded files to another machine, the ICAP server. The ICAP server then checks them and either greenlights them or, if malicious code is found, treats the offending file(s) as specified in the settings and notifies the ownCloud server. ownCloud can then act accordingly and based on the settings made reject the upload. Offloading the anti-virus scans to another dedicated server can greatly improve performance compared to running the ClamAV virus scanner on the same machine as ownCloud.

Starting with Anti-Virus version 1.1.0, additional scanners like the FortiSandbox and McAfee Web Gateway have been added as selectable ICAP scanners.

ClamAV In Native Mode

ClamAV Feature List

- Operates on all major operating systems, including *Windows*, *Linux*, and *macOS*.
- 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.

ClamAV Integration Into ownCloud

ownCloud integrates with antivirus tools by connecting to them via:

- A URL
- A host name and port
- A socket
- Streaming the data from the command line via a pipe with a configured executable

In case of ClamAV, ownCloud's antivirus extension sends files either through a unix-domain socket (which requires clamd running on the same host) or through a pipe to stdin/stdout of the clamscan executable (installed on the same host) or through the network using a host name and port pair (which allows running the clamd daemon on another server).



Individual chunks are **not** scanned. The whole file is scanned when it is moved or saved 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. In case of an infected upload, the appropriate action is always to delete the file(s). The choice "delete" or "log" for the infected condition only applies to the special case of background scans.



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 only.

Scanning Notes for ClamAV

1. Files are checked when they are uploaded or updated but *not* when they are downloaded.
2. ownCloud does not maintain 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 scans and to file uploads.
6. After installing ClamAV and the related tools, you will have two configuration files: `/etc/freshclam.conf` and `/etc/clamd.d/scan.conf`.
7. We recommend that you enable verbose logging in both `clamd.conf` and `freshclam.conf` initially, to verify correct operation of both.

Installing ClamAV

Install ClamAV on Ubuntu with the following command:

```
sudo apt install clamav clamav-daemon
```

This automatically creates the default configuration files and launches the `clamd` and `freshclam` daemons.

Enabling and Running ClamAV

Enable and start the `clamd` service with following commands.

```
sudo systemctl daemon-reload
sudo systemctl enable clamav-daemon.service
sudo systemctl start clamav-daemon.service
```

When successful, an output similar to the following should appear on the terminal:

```
Synchronizing state of clamav-daemon.service with SysV service script with
/lib/systemd/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable clamav-daemon
```

ClamAV Virus Database Updates

1. You can manually start the updating process with this command:

```
sudo freshclam
```

You should update manually at least once before using ClamAV within ownCloud. The initial update can take several minutes. In case of persisting issues running `freshclam`, you can gently end the process with the following command:

```
sudo pkill -15 -x freshclam
```

and retry manually updating again.

2. To automate the update process, run this cron entry for example.

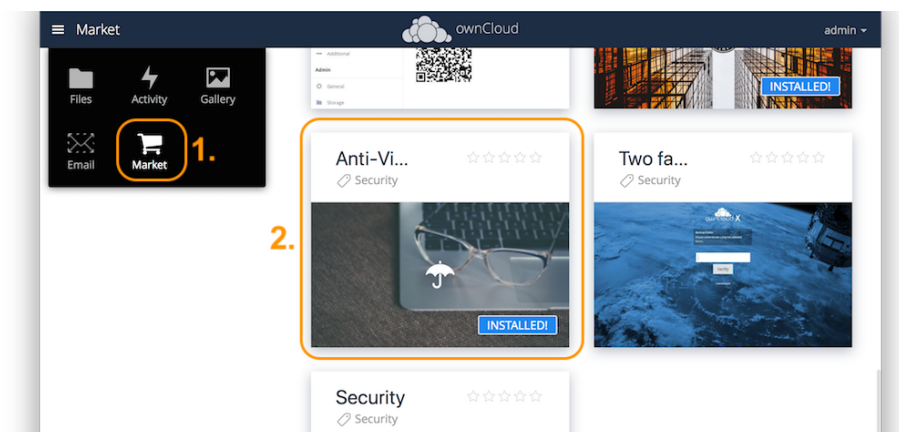
```
# m h dom mon dow command
47 * * * * /usr/bin/freshclam --quiet
```



Avoid any multiples of 10 to better distribute the load on the ClamAV virus pattern servers. This can reduce the load on the servers and therefore update times.

Install the ownCloud Anti-Virus App

The Anti-Virus app needs to be installed from the ownCloud Market (it's available in the "Security" category).



To install the App directly via the `occ` command, execute:

```
sudo -u www-data ./occ market:install files_antivirus
```

Configuring ClamAV within ownCloud



If the app is enabled but either not or incorrectly configured, it will **strictly reject all uploads** for the whole instance!

ClamAV can be configured in the following two ways:

1. [By using the Antivirus Configuration panel](#)

2. By using the `occ config:app` command set.

Change Log Level Temporarily

Once ClamAV is installed, select **Settings > General (Admin)** and, in the "Log" section, temporarily set [**Log level**] to "Everything (fatal issues, errors, warnings, info, debug)".

Log

Log level **Everything (fatal issues, errors, warnings, info, debug)** ▼

Configure ClamAV Using the AV Configuration Panel

Navigate to **Settings > Security (Admin)**, where you'll find the "Antivirus Configuration" panel as you can see in the example screenshot below.

Antivirus Configuration

Mode	<input type="text" value="Daemon"/>	▼
Host	<input type="text"/>	
Port	<input type="text"/>	
Stream Length	<input type="text" value="26214400"/>	bytes
File size limit, -1 means no limit	<input type="text" value="-1"/>	bytes
When infected files were found during a background scan	<input type="text" value="Only log"/>	▼

Configure ClamAV Using occ

All of the configuration settings for ClamAV are configurable by passing the relevant key and value to the `occ config:app:set files_antivirus` command. For example:

```
sudo -u www-data ./occ config:app:set files_antivirus \  
av_socket --value="/var/run/clamav/clamdctl"
```

To get a current option run for example:

```
sudo -u www-data ./occ config:app:get files_antivirus \  
av_socket
```

Available Configuration Settings

Setting	Description	Default
<code>av_cmd_options</code>	Extra command line options (comma-separated) to pass to ClamAV.	
<code>av_host</code>	The host name or IP address of the antivirus server.	
<code>av_infected_action</code>	The action to take when infected files were found during a background scan. It can be set to one of <code>only_log</code> and <code>delete</code> .	<code>only_log</code>
<code>av_max_file_size</code>	The maximum file size limit; <code>-1</code> means no limit.	<code>-1</code>
<code>av_mode</code>	The Anti Virus binary operating mode. It can be set to one of <code>executable</code> , <code>daemon</code> , and <code>socket</code> .	<code>executable</code>
<code>av_path</code>	The path to the <code>clamscan</code> executable.	<code>/usr/bin/clamscan</code>
<code>av_port</code>	The port number of the antivirus server. Allowed values are <code>1 - 65535</code> .	
<code>av_scan_background</code>	Should scans run in the background?	<code>true</code>
<code>av_socket</code>	The name of ClamAV's UNIX socket file.	<code>/var/run/clamav/clamdctl</code>
<code>av_stream_max_length</code>	The maximum stream length that ClamAV will accept in bytes (*).	<code>26214400</code>

(*) The `Stream Length` value sets the number of bytes to read in one pass and defaults to 26214400 bytes (twenty-six megabytes). This value should be no larger than the PHP `memory_limit` settings or physical memory if `memory_limit` is set to `-1` (no limit).

Configuration Modes

ClamAV runs in one of three modes:

- [Daemon \(Socket\)](#)
- [Daemon](#)
- [Executable](#)



In both daemon modes, background scans are enabled by default. If you want to disable them, run the command:

```
sudo -u www-data ./occ config:app:set files_antivirus
av_scan_background --value 'false'
```

Daemon (Socket, Same Server)

In *Daemon (Socket)* mode, ClamAV runs in the background on the same server as the ownCloud installation, or the socket can be made available via a share mount. When there is no activity, `clamd`

places a minimal load on your system. Consider that high CPU usage can occur when users upload large volumes of files.



You must run `freshclam` at least once for ClamAV to generate the socket.

Antivirus Configuration

Mode	<input type="text" value="Daemon (Socket)"/>	
Socket	<input type="text" value="/var/run/clamav/clam"/>	
Stream Length	<input type="text" value="26214400"/>	bytes
File size limit, -1 means no limit	<input type="text" value="-1"/>	bytes
When infected files were found during a background scan	<input type="text" value="Only log"/>	

1. Set [**Mode**] to "**Daemon (Socket)**". ownCloud should detect your `clamd` socket and fill in the "**Socket**" field. This is the `LocalSocket` option in `clamd.conf`.

You can run `ss` (a utility to investigate sockets) to verify it, as in the example below:

```
sudo ss -a | grep -iq clamav && echo "ClamAV is running"
```



If you don't have `ss` installed, you may have `netstat` installed. If so, you can run the following to check if ClamAV is running:

```
netstat -a | grep -q clam && echo "ClamAV is running"
```

2. When infected files were found during a background scan, you have the choice of either:
 - Logging any alerts without deleting the files
 - Immediately deleting infected files

Daemon (Different Server)

In *Daemon* mode, ClamAV runs on a different server. This is a good option to reduce load on the ownCloud servers when high network bandwidth is available and many concurrent uploads happen.

Antivirus Configuration

Mode

Host

Port

Stream Length bytes

File size limit, -1 means no limit bytes

When infected files were found during a background scan

1. Set [**Mode**] to "**Daemon**".
2. Set [**Host**] to the host name or IP address of the remote server running ClamAV, and set [**Port**] to the server's port number.



The port number is the value of `TCPsocket` in `/etc/clamav/clamd.conf`.

Executable

In *Executable* mode, ClamAV runs on the same server as the ownCloud installation, with the `clamscan` command running only when a file is uploaded.



`clamscan` can respond slower and may not always be reliable for on-demand usage; it is better to use one of the daemon modes.

Antivirus Configuration

Mode

Path to clamscan You can change this value in the system configuration ↗

Extra command line options (comma-separated) You can change this value in the system configuration ↗

Stream Length bytes

File size limit, -1 means no limit bytes

When infected files were found during a background scan

The image shows a command line option `--allmatch=yes` (continue scanning within the file after finding a match) which is not necessary to be set and just used here for demonstration purposes of the field.



Starting with ownCloud Anti-Virus version 1.0.0, the path to `clamscan` and the command line options are set via a `config.php` entry and are read-only in the user

interface. Refer to the [config.php parameters for apps](#) for more details.



If you had configured the path and command line options before via the user interface, the values are being migrated from the database to config.php automatically. Check the settings in config.php for their presence after upgrading.

1. Set [**Mode**] to "Executable".
2. Set [**Path to clamscan**] to the path of `clamscan`, which is the interactive ClamAV scanning command, on your server. To find the exact path, run

```
which clamscan
```

Set Back Log Level

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.

Configuration Warnings

The Anti-Virus App shows one of three warnings if it is misconfigured or ClamAV is not available. You can see an example of all three below.

```
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/clamscan"
```

```
Antivirus app is misconfigured or antivirus inaccessible. Could not connect to socket "/var/run/clamav/cslamd-socket": No such file or directory (code 2)
```

Manage Infected Files Found

During an upload these actions are taken:

- The upload is blocked.
- The event is logged in the owncloud server log.
- The event is reported and/or logged by the client / Web UI.

During a background scan the app can take one of two actions:

- **Log Only:** Log the event.
- **Delete file:** Delete the detected file.

Set [**When infected files were found during a background scan**] to the value that suits your needs.

Response Rule Configuration

ownCloud provides the ability to customize how it reacts to the response given by an antivirus scan. To do so, under **Admin > Security (Admin)** click [**Advanced**], which you can see in the screenshot below, you can view and change the existing rules. You can also add new ones.

The screenshot shows a table of response rules with the following columns: Match by, Scanner exit status or signature to search, Description, and Mark as. Annotations point to various parts of the interface:

- "Whether to match on the exit status or scanner output" points to the "Match by" column.
- "The exit status code returned by ClamAV to match against" points to the "Scanner exit status or signature to search" column.
- "A human-readable description of what the status code means" points to the "Description" column.
- "The action to take when that status is returned" points to the "Mark as" column.
- "Delete an existing rule" points to the trash icon in the "Mark as" column.
- "Confirm the new rule or existing rule changes" points to the checkmarks in the "Match by" column.
- "A regular expression to match against the search response text returned by ClamAV" points to the "Scanner exit status or signature to search" column.

Match by	Scanner exit status or signature to search	Description	Mark as
✓ Scanner exit status	0		Clean
✓ Scanner exit status	1		Infected
✓ Scanner exit status	40	Unknown option passed.	Unchecked
✓ Scanner exit status	50	Database initialization error.	Unchecked
✓ Scanner output	/.* OK\$/	Scanned successfully	Clean
✓ Scanner output	/.* (.* FOUND\$/	FOUND virus	Infected
✓ Scanner output	/.* (.* ERROR\$/	Error scanning file	Unchecked

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
- 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 Rule Set

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

Exit Status or Signature	Description	Marks File As
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

1. You can change the rules to either match an exit status or the scanner's output.
 - 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.
2. 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 [] on the left-hand 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.

ICAP

[ICAP](#) is an open standard supported by many antivirus products. With the release of the *Anti-Virus* app 1.0.0, other virus scanners beside ClamAV can be used via ICAP if you are running it on an ownCloud Enterprise Edition.

Currently the only tested and supported virus scanners, besides ClamAV, are *Kaspersky ScanEngine*, *McAfee Web Gateway* and *FortiSandbox* although far more products might simply work. The use of ICAP requires an enterprise license. The functionality can be tested without a license with a grace period of 24 hours.

Installation

1. If you haven't done so already, install the [Anti-Virus app](#) from the ownCloud marketplace. Alternatively, use this occ command:

```
sudo -u www-data ./occ market:install files_antivirus
```

2. Enable the app as admin in ownCloud under **Settings > Apps** in the category **Security** or with the following occ command:

```
sudo -u www-data ./occ app:enable files_antivirus
```

General Configuration

ICAP can be configured via the Web interface as admin user or via [occ config:app commands](#).

Antivirus Configuration Panel

Log in to ownCloud as admin via the Web interface and go to **Admin** > **Settings** > **Security** and you'll see the Antivirus Configuration dialog.

Enter the desired values:

Mode

Set to **Daemon (ICAP)**.

Host

Enter the IP address of your ICAP server.

Port

Specify the port number (default 1344).

Stream Length

Set the length of streams sent to the ICAP server in bytes.

File size limit

If you want to limit the file size, enter the maximum value in bytes. Default is no limit (-1).

ICAP request service

Select the antivirus software you want to use: **avscan** for ClamAV, **req** for Kaspersky ScanEngine or **wwreqmod** for McAfee.

ICAP response header holding the virus information

Use **X-Infection-Found** for ClamAV (**avscan**) and **X-Virus-ID** for KAV (**req**). McAfee doesn't offer response headers.

When infected files were found during a background scan

Specify what to do with the flagged files. Possible values: **Delete file** or **Only log**.



Do not change the rules hidden under **[Advanced]** unless you know exactly what you're doing. The defaults should work best. If you have special requirements, contact us at consulting@owncloud.com.

ICAP Configuration

You can configure the ownCloud Anti-Virus app either via the Web interface or the command line. The Web interface fields can be easily matched to the command line field names. On the command line, change into your ownCloud directory, usually `/var/www/owncloud`, and enter the following occ commands with an IP address and port based on your environment:

1. Set the IP address of your anti-virus server:

```
sudo -u www-data ./occ config:app:set files_antivirus \
```

```
av_host --value="172.17.0.3"
```

2. Specify the port of the anti-virus server:

```
sudo -u www-data ./occ config:app:set files_antivirus \  
av_port --value="1344"
```

3. Set the mode to ICAP:

```
sudo -u www-data ./occ config:app:set files_antivirus \  
av_mode --value="icap"
```



The setting `icap` triggers a grace period of 24 hours if you don't have an Enterprise license but want to test ICAP.

4. Specify what to do with the offending file:

```
sudo -u www-data ./occ config:app:set files_antivirus \  
av_infected_action --value="delete"
```

Possible values are `delete` and `only_log`.

Depending on your ICAP server, select one of the following example configurations.

Run ClamAV in ICAP Mode

`c-icap` can be configured to use ClamAV. For more information see: [c-icap on sourceforge](#) (for selecting ClamAV see their section: Selecting virus scan engine to use).

1. Install ClamAV based on the instructions at the beginning of this document and `c-icap` as referenced above.
2. Select **[c-icap with ClamAV]** from the dropdown in the Anti Virus app or use the command line:

```
sudo -u www-data ./occ config:app:set files_antivirus \  
av_request_service --value="avscan"
```

3. Set the respective response header:

```
sudo -u www-data ./occ config:app:set files_antivirus \  
av_response_header --value="X-Infection-Found"
```


Run with Kaspersky Anti-Virus in ICAP Mode

1. Install the Kaspersky ScanEngine (KAV) based on their [instructions](#) and prepare KAV for running in ICAP mode.
2. Select **[req]** from the dropdown in the Anti Virus app or use the command line:

```
sudo -u www-data ./occ config:app:set files_antivirus \  
av_request_service --value="req"
```

3. Set the respective response header:

```
sudo -u www-data ./occ config:app:set files_antivirus \  
av_response_header --value="X-Virus-ID"
```



The older versions of Kaspersky's KAV did not send back the virus/infection name in an ICAP header. Starting with KAV v2.0.0, the header to transport the virus can be configured. Default: No header is sent. For more configuration details see [Using Kaspersky Scan Engine in ICAP mode](#).

Run with McAfee Web Gateway in ICAP Mode

Follow this procedure to configure ownCloud for the McAfee Web Gateway 10.x and higher in ICAP Mode.

1. Install McAfee Web Gateway based on their instructions.
2. Select **[McAfee Web Gateway 10.x and higher]** from the dropdown in the Anti Virus app.
3. To use McAfee Web Gateway, set the mode to **respmod** either from the Web interface or via command line:

```
sudo -u www-data ./occ config:app:set files_antivirus \  
av_request_service --value="respmod"
```

4. Set the response header to **X-Virus-Name**

```
sudo -u www-data ./occ config:app:set files_antivirus \  
av_response_header --value="X-Virus-Name"
```



McAfee provides demo versions with limited runtime for evaluation purposes. Have a look at the [McAfee Web page](#) for the Web Gateway.

Run with FortiSandbox in ICAP Mode

1. Install FortiSandbox based on their instructions.
2. Select **[Fortinet]** from the dropdown in the Anti-Virus app.

3. To use FortiSandbox, set the mode to `respmod` either from the Web interface or via command line:

```
sudo -u www-data ./occ config:app:set files_antivirus \
  av_request_service --value="respmod"
```

4. Set the response header to `X-Virus-Name`

```
sudo -u www-data ./occ config:app:set files_antivirus \
  av_response_header --value="X-Virus-Name"
```



Fortinet provides some demo versions of the FortiSandbox. Have a look at their [product page](#) for more information.

UI Configuration

Introduction

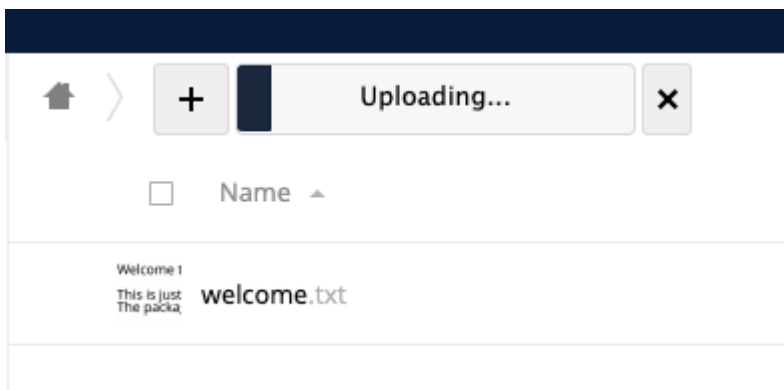
The web UI can be configured for optimal user experience.

Configuration Options

Hide the Upload Estimation

Note that this setting is available for ownCloud Server only.

When uploading a document, an upload estimation (progress bar) is shown like in the example below:



This progress bar can be hidden with the following command:

```
sudo -u www-data ./occ config:app:set files hide_upload_estimation --value="yes"
```

To show the progress bar again, type one of the following commands:

```
sudo -u www-data ./occ config:app:set files hide_upload_estimation --value="no"
```

or





```
sudo -u www-data ./occ config:app:delete files hide_upload_estimation
```

The current value can be queried with the `config:app:get` or the `config:list` command. For details see the [occ Config Commands](#)

User Management

Default View

The **default view** displays basic information about your users.

	Username	E-Mail	Groups	Create		
Everyone 4	Username	Full Name	Password	Groups	Group Admin for	Quota
Admins 2	 admin	admin	••••••	admin	users, artists	Unlimited
users 3	 holger	holger	••••••	admin, users	users	10 GB
artists 1	 john	john	••••••	users	no group	5 GB
	 mark	mark	••••••	artists, users	no group	1 GB

The **Group filter** on the left sidebar lets you quickly filter users by their group memberships, and create new groups.

Users	
+ Add Group	
Everyone	4
Admins	2
users	3
artists	1

Click the [gear] icon on the lower left sidebar to view the available settings.



Default Quota Unlimited ▾

- Show enabled/disabled option
- Show storage location
- Show last log in
- Show user backend
- Set password for new users
- Show email address
- Show password field
- Show quota field

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.

E-Mail

The admin sets the new user's E-Mail. The user then gets an E-Mail to set the password. Both the user and the admin can change the user's E-Mail at anytime.

Groups

You may create system (non-LDAP) groups and assign system group memberships to users. By default new users are not assigned to any groups.

Group Admin

Group admins are granted administrative privileges on system groups, and can add new users and remove existing users from those groups.

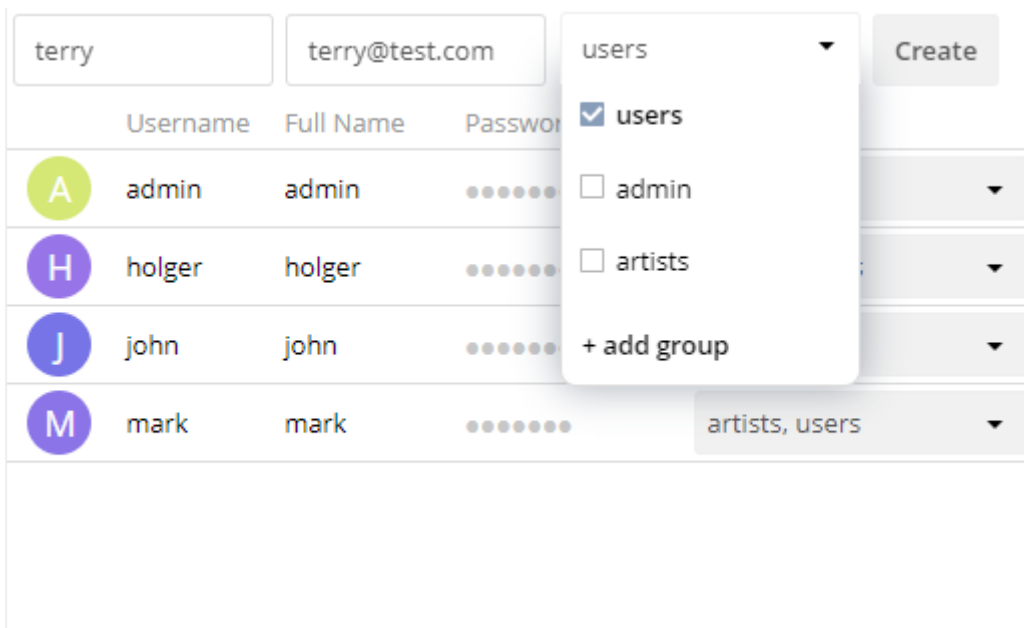
Quota

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 **E-Mail**
- Optionally, assign **Groups** memberships
- Click the [**Create**] button



The screenshot shows a user creation interface. At the top, there are two input fields: 'Username' containing 'terry' and 'Full Name' containing 'terry@test.com'. To the right is a 'Create' button. Below these is a table of existing users with columns for Username, Full Name, and Password. A dropdown menu is open over the table, showing a list of groups: 'users' (checked), 'admin', and 'artists', along with a '+ add group' option. The 'mark' user row shows 'artists, users' selected in its group dropdown.







	Username	Full Name	Password	Groups
	admin	admin	<input checked="" type="checkbox"/> users
	holger	holger	<input type="checkbox"/> admin
	john	john	<input type="checkbox"/> artists
	mark	mark	artists, users

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.

Password Reset

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

	Username	Full Name	Password	Groups
	admin	admin	•	admin
	holger	holger 	••••• 	admin, users
	john	john	•••••	users
	mark	mark	•••••	artists

set new password

If you have encryption enabled, there are special considerations for user password resets.



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

Deleting Users

The screenshot shows the ownCloud user management interface. A dialog box titled "Delete user" is open, warning that the action is permanent and will delete all user data, files, and shares. The dialog has "No" and "Yes" buttons. In the background, a table lists users, with the user "test" highlighted and a trash icon circled in orange next to it.

Username	E-Mail	Groups	Create
admin	admin	admin	no group
test	test	no group	no group

To delete a user, hover your cursor over their name on the **Users** page, and click the trashcan icon that appears at the far right. You'll then see a confirmation dialog appear, asking if you're sure that you want to delete the user.

If you click **[Yes]**, the user is permanently deleted, including all of the files owned by the user, 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).

Alternatively, you can use a sync client to copy them to your local computer. If you click **[No]**, the confirmation dialog will disappear and the user is not deleted.



See [File Sharing Configuration](#) to learn how to create persistent file shares that survive user deletions.

Granting Administrator Privileges

ownCloud has two types of administrators:

- **ownCloud Administrators** have full rights on your ownCloud server, and can access and modify all settings. To assign the ownCloud Administrators role to a user, simply add them to the `admin` group.
- **Group Administrators.** Group administrators have the rights to create, edit and delete users in their assigned system (non-LDAP) groups. Use the dropdown menus in the Group Admin column to assign group admin privileges.

Managing Groups

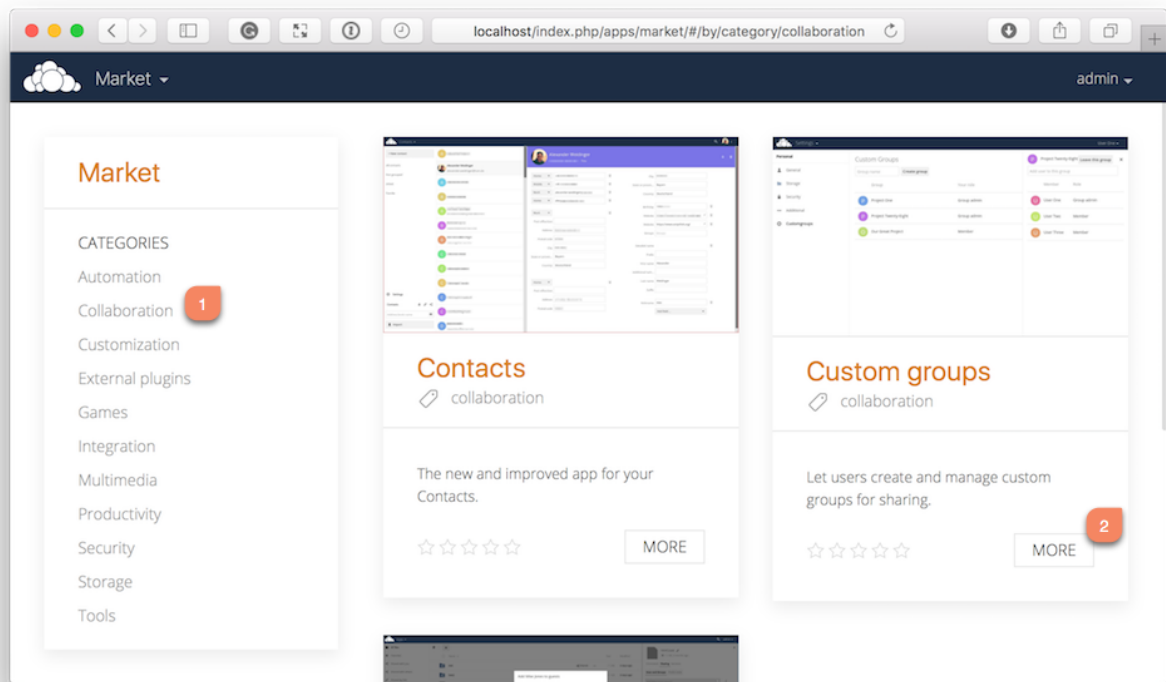
You can assign new users to groups when you create them, and create new groups when you create new users. You may also use the **Add Group** button at the top of the left pane to create new groups. New group members will immediately have access to file shares that belong to their new groups.

Enabling Custom Groups

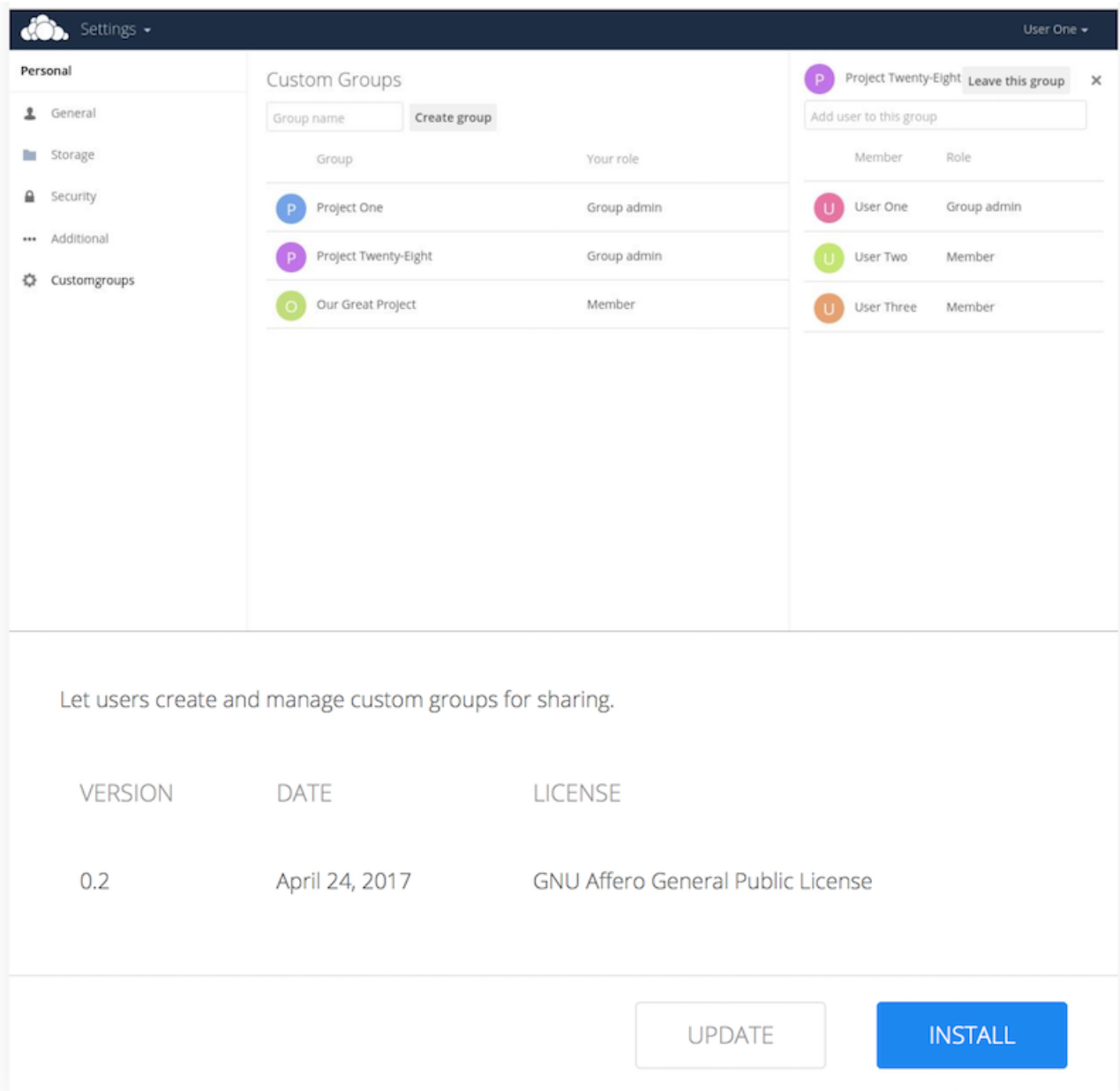
In previous versions of ownCloud, files and folders could only be shared with individual users or groups created by administrators. This wasn't the most efficient way to work. From ownCloud 10.0, users can create groups on-the-fly, through a feature called "Custom Groups", enabling them to share content in a more flexible way.

To enable Custom Groups:

1. From the ownCloud Market, which you can find starting from 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.



With this done, Custom Group functionality will be available in your ownCloud installation.

Overriding Default Behavior

Depending on your Custom Groups and ownCloud's global settings, configured by the ownCloud admin, Custom Groups may behave differently depending on settings made via `occ` commands. See the details in [occ for Custom Groups](#). Note that some settings shown in the examples below can also be set via `config/config.php`. For best practice use the `occ` command where possible.

Disabling Administrators from Administering Custom Groups

- Creating or renaming a Custom Group using an existing name of another Custom Group can be allowed or not depending on administrative settings.
- Custom Group creation can be limited to ownCloud **group admins**.
- Disable administration of Custom Groups by ownCloud administrators:

```
'customgroups.disallow-admin-access-all' => true,
```

Hide Custom Groups App Based On Group Membership

The app can be hidden from the user's personal settings page if the user belongs to one or more disallowed groups, To specify the disallowed groups, list them against the `customgroups.disallowed-groups` key in `config/config.php`, as in the following example.

```
// Hide the Custom Groups app for users in the
// 'no_guest_app_users' and 'project5' group.
'customgroups.disallowed-groups' => ['no_guest_app_users', 'project5'],
```

Set Custom Group Admins

Setting Custom Group admins can only be done via the browser. In case the group admin has left the company and you need to set a different one, you temporarily must allow the [ownCloud instance admins](#) access to groups if disallowed before, set one or more new group admins, and change the instance admin setting back.

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]** icon 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.

External Storage Quota

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,
```

Storage Space Considerations

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%.

Versions

When version control is enabled, the older file versions are not counted against quotas.

Public Links

When a user creates a public link share via URL, and allows uploads, any uploaded files count against that user's quota.

Moving the User Home

Usually, a user's home folder is located in the `data/` directory, the location of which is defined in `config.php` and defaults to `/var/www/owncloud/data`. Usually in smaller installations, the data directory mounts to a physical drive of the server and in bigger installations the data directory is mounted via NFS. This can be less than optimal for very big installations with thousands of users and/or users with very big space consumption. This can result in a high load on a single mount point.

ownCloud offers moving the home folder location of single users from the default location to another path outside the data directory to distribute the load to different mount points. You can

also move back a user's home to the location defined in config.php.



In general, moving a user's home should be the last step after all optimizations of the mount point have been done. Carefully monitor over a period of time the changes made before moving a user's home.



Consider that these new home mount points also need to be part of a [backup](#) and [restore](#) plan.

Steps to Move a User's Home

For details of the occ user commands used below, see the [User Commands](#) section of the occ command reference. The examples use the user ID `lisa` and the mount for the new home is `/mnt/newhome_1`.

1. To report a users home, use the following command:

```
sudo -u www-data ./occ user:list lisa -a home
- lisa: /var/www/owncloud/data/lisa
```

Here you can see, that the home of user `lisa` is located in `/var/www/owncloud/data/lisa`

2. Prepare new mounts **in advance** for one or more users:

Use the OS methods to create one or more new mount points for users home directories not located as defined in config.php. You can create as many new homes as required containing as many new user homes as wanted - there is no ownCloud limitation. The mounts must be fully accessible by the webserver user (usually www-data).

3. Move the users home:



- To move a users home, the target folder **must not contain** a subfolder with the user's ID.
- The target folder **can contain** other user folders.

```
sudo -u www-data ./occ user:move-home lisa /mnt/newhome_1
```

The user gets disconnected and the user's home is now moved which may take a while depending on the load of the server and the bandwidth available on the mount points. When the move operation has finished,

- all data from the user is *copied* to the new home,
- the new path is set in the ownCloud database and
- the user gets enabled again.

After checking, the old user's home location can safely be deleted manually.



If you are using LDAP and the [LDAP Home Connector](#) app, update the user's home mount in the attribute used accordingly.

4. To check the user's new home, use the following command:

```
sudo -u www-data ./occ user:list lisa -a home
- lisa: /mnt/newhome_1/lisa
```

Here you can see that the home of user `lisa` is now located in `/mnt/newhome_1/lisa`.

5. To list the available user home root directories, use the following command:

The following command lists all available user homes. Note a home only gets listed, if it contains at least one user.

```
sudo -u www-data ./occ user:home:list-dirs
- /var/www/owncloud/data
- /mnt/newhome_1/lisa
```

6. To list all users from a users home root directory, use the following command:

The following command lists all users from a given home.

```
{occ-command-example-prefix} user:home:list-users /var/www/owncloud/data
- admin
- user01
```

ownCloud Roles

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

- The [Guests app](#) is available on the ownCloud Marketplace. You must install and enable it first.
- 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).



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 filesystems) 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.

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 ./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 the occ Command](#) to learn more about using the `occ` command.

Unresolved	directive	in
modules/admin_manual/pages/configuration/user/reset_admin_password.adoc		-
include::partial\$configuration/user/update-password-note.adoc[]		

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 that can handle an automatic reset:

```
'lost_password_link' => 'https://example.org/link/to/password/reset',
```

Unresolved	directive	in
modules/admin_manual/pages/configuration/user/reset_user_password.adoc		-
include::partial\$configuration/user/update-password-note.adoc[]		

User Authentication with IMAP, SMB, and FTP

Introduction

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 => ...
        ],
    ],
],
```



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 configuration](#) 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	<code>OC_User_IMAP</code> .
Arguments	A mailbox string as defined in the PHP documentation .
Dependency	PHP's IMAP extension . See Manual Installation on Linux 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'
    ],
  ],
],
],

```



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	<code>OC_User_SMB</code>
Arguments	The samba server to authenticate against.
Dependency	PECL's smbclient extension or smbclient .

Example

```

<?php

"user_backends" => [
  [
    "class"      => "OC_User_SMB",
    "arguments" => [
      'localhost'
    ],
  ],
],
],

```

FTP

Provides authentication against FTP servers.

Option	Value/Description
Class	<code>OC_User_FTP</code>
Arguments	The FTP server to authenticate against.
Dependency	PHP's FTP extension . See Source Installation for instructions on how to install it.

Example

```
<?php
"user_backends" => [
    [
        "class"    => "OC_User_FTP",
        "arguments" => [
            'localhost'
        ],
    ],
],
```

LDAP Integration

Introduction

The LDAP Integration app allows you to integrate your existing LDAP users in ownCloud.

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
- Only read access to your LDAP (edit or delete of users on your LDAP is not supported)

Configuration

First, install the [LDAP Integration](#) app. 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 light appears 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.

LDAPS Configuration

LDAPS encrypts the connection between your LDAP server and ownCloud via SSL/TLS.

1. First you need the Windows Server CA certificate in the `pem` format with `.crt` suffix
2. Import the certificate to `/usr/local/share/ca-certificates/`
3. Execute `update-ca-certificates`

LDAP

The screenshot shows the LDAP configuration page in ownCloud. The 'Server' tab is active, and the configuration is incomplete. The fields are: Host (389), Use StartTLS support (unchecked), User DN, Password (masked with asterisks), One Base DN per line, and Manually enter LDAP filters (unchecked). There are buttons for 'Detect Base DN' and 'Test Base DN'. A 'Continue' button is at the bottom right, and a 'Help' icon is next to it. A 'Configuration incomplete' message is displayed at the bottom left.

Server Configuration

Configure one or more LDAP servers. Click [**Delete Configuration**] to remove the active configuration.

Host

The hostname 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.

Example:

- 389 for unencrypted connection
- 636 for encrypted connection

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. You can either enter this value manually, or click **[Detect Base DN]** to have ownCloud attempt to determine the value.

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 log in to your ownCloud server, use the Login filter. You may bypass the form fields and enter a raw LDAP filter if you prefer.

LDAP

Server
Users
Login Attributes
Groups
Advanced
Expert

ownCloud access is limited 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](#)

LDAP Filter: ((objectclass=inetOrgPerson)(objectclass=posixAccount))

1 user found

Configuration OK ● [Help](#)

Only those Object Classes

ownCloud determines the object classes that are typically available for user objects in your LDAP. ownCloud automatically selects the object class that returns the highest number 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 is selected. You may select multiple groups.



Group membership is configured by adding `memberUid`, `uniqueMember` or `member` attributes to an LDAP group see ([Group Member association](#)) below. 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:

```
Unresolved directive in
modules/admin_manual/pages/configuration/user/user_auth_ldap.adoc -
include::example$configuration/user/user_auth_ldap/group_filter.ldif[]
```

<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.



No matter what search filter is given, the app always adds the value of the `User Display Name Field` (default `(displayName=*)`) to the filter to ensure that your users have this field, otherwise the count will be 0.

Active Directory offers "*Recursive retrieval of all AD group memberships of a user*". This means that you would be able to search the group you enter and all the other child groups from this group for users. Enter this filter to access this feature for a single group:

```
Unresolved directive in
modules/admin_manual/pages/configuration/user/user_auth_ldap.adoc -
```

```
include::example$configuration/user/user_auth_ldap/single_group_search.ldif[]
```

Enter your group name instead of the `<groupname>` placeholder. If you want to search multiple groups with this feature, adjust your filter like this:

```
Unresolved directive in
modules/admin_manual/pages/configuration/user/user_auth_ldap.adoc -
include::example$configuration/user/user_auth_ldap/multi_group_search.ldif[]
```

You can add as many groups to recurse by using the format: `(|(m1)(m2)(m3)...) .` [Here is the description from Microsoft \(point #10\):](#)

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:

- [Active Directory: LDAP Syntax Filters](#)
- [Active Directory Week: Explore Group Membership with PowerShell](#)

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.

Server
Users
Login Attributes
Groups
Advanced
Expert

When logging in, ownCloud will find the user based on the following attributes:

LDAP / AD Username:

LDAP / AD Email Address:

Other Attributes:

[Edit LDAP Query](#)

LDAP Filter: (&((objectclass=inetOrgPerson)(objectclass=posixAccount))
 ((uid=%uid)((mailPrimaryAddress=%uid)(mail=%uid))
 ((givenName=%uid)(uid=%uid))))

Configuration OK ● [Help](#)

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.



Disallowing login with LDAP Email Address requires enabling strict login checking to be effective:

```
sudo -u www-data ./occ config:system:set --type boolean --value true
strict_login_enforced
```

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. Example:

The `%uid` placeholder is replaced with the login name entered by the user upon login.

Examples:

- Only Username:

```
Unresolved directive in
modules/admin_manual/pages/configuration/user/user_auth_ldap.adoc -
```



```
include::example$configuration/user/user_auth_ldap/only_username.ldif[]
```

- Username or Email Address:

```
Unresolved directive in
modules/admin_manual/pages/configuration/user/user_auth_ldap.adoc -
include::example$configuration/user/user_auth_ldap/username_email.ldif[]
```

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.

LDAP

LDAP configuration interface showing the 'Groups' tab. The interface includes tabs for 'Server', 'Users', 'Login Attributes', 'Groups', 'Advanced', and 'Expert'. The 'Groups' tab is active, displaying the following settings:

- Groups meeting these criteria are available in ownCloud:
- Only these object classes: `posixGroup`
- Only from these groups: `owncloudusers`
- [Edit LDAP Query](#)
- LDAP Filter: `(&((objectclass=posixGroup))((cn=owncloudusers)))`
- [Verify settings and count groups](#) 1 group found
- Configuration OK ● [Back](#) [Help](#)

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`

<x> Groups Found

This tells you approximately how many groups will be available in ownCloud. The number updates automatically after any change.



Renaming of LDAP-Groups on the LDAP Server is not supported. Changes like renaming groups in LDAP will not be propagated to ownCloud.

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

LDAP

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.

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 supplied, 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 about 15 seconds or higher, 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

Server	Users	Login Attributes	Groups	Advanced	Expert
<p>▶ Connection Settings</p> <p>▼ Directory Settings</p> <p>User Display Name Field <input type="text" value="cn"/></p> <p>2nd User Display Name Field <input type="text"/></p> <p>Base User Tree <input type="text" value="One User Base DN per line"/></p> <p>User Search Attributes <input type="text" value="Optional; one attribute per line"/></p> <p><small>Each attribute value is truncated to 191 characters</small></p> <p>Group Display Name Field <input type="text" value="cn"/></p> <p>Base Group Tree <input type="text" value="One Group Base DN per line"/></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 Help</p>					

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:

- `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 Active Directory or for objectclass `groupOfNames` groups
- `memberUid` with RDN for objectclass `posixGroup` groups
- `uniqueMember` with FDN for objectclass `groupOfUniqueNames` groups



The Group Member association is used to efficiently query users of a certain group, e.g., 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

Server	Users	Login Attributes	Groups	Advanced	Expert
<p>▶ Connection Settings</p> <p>▶ Directory Settings</p> <p>▼ Special Attributes</p> <p>Quota Field <input type="text"/></p> <p>Quota Default <input type="text"/></p> <p>Email Field <input type="text"/></p> <p>User Home Folder Naming Rule <input type="text"/></p> <p>Test Configuration <i>Help</i></p>					

Quota Field

The name of the LDAP attribute to retrieve the user quota limit from. You have to decide which LDAP attribute you want to use and set a value to it in the Attribute Editor.

Quota Default

Override ownCloud's default quota **for LDAP users** who do not have a quota set in the Quota Field.

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 in the active directory, it will override the LDAP Quota Default value.



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](#)

Quota Priority

If set, this is the current Quota Priority:

1. **Quota Field** overrides **LDAP Quota Default**
2. **LDAP Quota Default** overrides **ownCloud Default Quota**
3. **ownCloud Default Quota** overrides **Unlimited 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 ./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



Please check both the advanced and expert configurations carefully before using in production.

LDAP

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
Usernames 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.

[i Help](#)

In "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 that it is unique. Leave it empty for default behavior. Changes will have effect only on newly mapped LDAP users and groups.

It also will take effect when a user 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 the (see [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 an internal username in ownCloud. This requires a mapping from an ownCloud username to an LDAP user.

The created username is mapped to the UUID of the LDAP user. Additionally, the DN is cached 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.



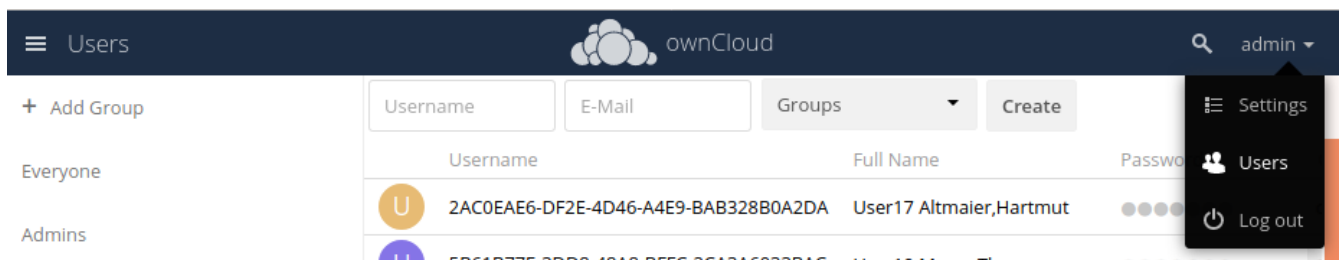
Clearing the mappings is not configuration sensitive, it affects all LDAP configurations!

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 user:sync command](#). Versions of ownCloud before 10.0 imported all users when the users page was loaded, but this is no longer the case.



During initial sync, make sure to check the ownCloud log for errors that could indicate a possible misconfiguration.



We recommend [creating a Cron job](#), to automate regularly syncing LDAP users with your ownCloud database. If you have many users, you do not have to sync all of them to update a small number of users. You can use the [OCS User Sync API](#) to sync individual users. It provides a way to trigger user sync from outside of ownCloud.

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.

Reuse Existing User and Group LDAP Accounts

New LDAP logins can attempt to reuse *existing* user and group accounts if:

- They match the resolved username attribute.

- They have `User_Proxy` set as their backend.

To enable this functionality, the `reuse_accounts` config setting must be set to `yes`. To enable it, run the following command.

```
sudo -u www-data ./occ config:app:set user_ldap reuse_accounts --value=yes
```

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`.

Profile picture



Your avatar is provided by your original account.

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.

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

LDAPS

Use these commands to troubleshoot:

Test encrypted connection:

```
openssl s_client -connect 10.211.55.15:636
```

look for **verify return:1**

Try an ldapsearch query

```
ldapsearch \  
-H ldaps://ad16.oc.local:636 \  
-D "cn=Administrator,cn=users,dc=oc,dc=local" \  
-b "dc=oc,dc=local" \  
-w MyPassword
```

Check:

```
/etc/ldap/ldap.conf /etc/openldap/ldap.conf
```

look for

```
TLS_CACERT /etc/ssl/certs/ca-certificates.crt
```

Turn off certificate validation for testing:

```
TLS_REQCERT ALLOW
```

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 [**Save**]

Now you can modify and enable the configuration.

Filter out Deactivated Users

With this filter you can filter out the deactivated users and show only active users.

```
!(userAccountControl:1.2.840.113556.1.4.803:=2)
```

Here is what the full filter can look like.

```
(&(|(objectclass=organizationalPerson)
!(userAccountControl:1.2.840.113556.1.4.803:=2))
(|(|(memberof=CN=Domain Users,CN=Users,DC=dp,DC=mosreg,DC=ru)(primaryGroupID=513)))
)
```

Caching

Using [caching](#) to speed up lookups. 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 replica 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 of the 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.



Please ensure that you're using the minimum supported PHP version (7.3.0).

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 are 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.

The internal user name and a visible display name are separated. This is not the case for group names yet, as 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.

User Two-Factor Authentication

Introduction

With two-factor authentication (2FA), users can access their ownCloud web accounts only by using a trusted device like their mobile phone. When users want to sign in, they need to provide two pieces of information (factors):

- the password,
- the six-digit verification code that's automatically displayed on the trusted device or sent to the phone number.

Setting Up 2FA

To provide 2FA functionality, an app like the [2-Factor Authentication](#) needs to be installed and enabled.

If a two-factor provider app is enabled, it is enabled for all users by default **but a user has to opt in**, though the provider can decide whether or not the user has to pass the challenge.



For the opt-in function to work, ImageMagick and php-imagick are required to create the QR code. Depending on your operating system, these packages may need to be installed manually.

Troubleshooting

Tasks for the User

Because the user has to opt in, see the [Security section in Personal Settings](#) for tasks on the user side.

Second Factor is Inaccessible

In case a user loses access to the second factor, e.g. by breaking or losing the phone with two-factor SMS/app verification, the user is locked out. To give the user access to the account again, an admin can temporarily disable the two-factor check *for that user* via the [occ commands for Two-Factor Authentication](#). After the issue has been fixed, the admin can reenable two-factor authentication for that user.

Manage Secrets

If owncloud's [2-Factor Authentication](#) is used, the admin can manage the secrets via [occ Two-Factor TOTP commands](#).

User Auth Open Authentication (OAuth2)

Introduction

OAuth2 (Open Authentication) is the open industry-standard protocol for secure authorization of clients. It can be used as a way for users to grant web services or applications access to their data stored in ownCloud. The use of OAuth2 in ownCloud greatly enhances security while facilitating the integration of third party applications or web services:

- Connect ownCloud clients (Desktop, Android, iOS) through a standardized and secure authorization flow.
- Provide a user authorization interface for developers to facilitate the integration of ownCloud in third party applications.

Benefits Provided by the OAuth2 Interface

- No user passwords are being stored in ownCloud clients or third party web applications

Instead of connecting clients with username/password, a user only needs to provide the information once in the browser. The respective client is then provided with a unique access token which is used for future connections to the ownCloud server. ownCloud clients or third party applications never get to know the actual login credentials.

- The use of different access tokens per client provides the ability to selectively revoke user sessions

When using OAuth2 a unique access token is generated for each device or third party application. Users can check their authorized clients in the personal settings and have the ability to selectively invalidate access tokens when e.g. a device is lost. This strengthens control and access security significantly.

The OAuth2 App

OAuth2 functionality is available in ownCloud via the [OAuth2](#) application which is available from the ownCloud Marketplace. For more information on how to set it up, see section [Open Authentication \(OAuth2\)](#)

User Provisioning API

Introduction

The User Provisioning API provides instruction sets to communicate with the user backend. External systems can use this API to create, edit, delete and query user attributes.

Using the User Provisioning API

See [User Provisioning API](#) for available API endpoints and detailed examples.

Guests App

Introduction

Share with external users conveniently just by entering an email address in the sharing dialog. Recipients receive an email containing an activation link. They can log in using their email address as user name and the password they chose during activation. Guests may even use the ownCloud desktop clients and mobile apps to connect to ownCloud and work on shared contents.



Guest users do not have storage space and can only work on content that is shared with them.

Installation

Install and enable the [Guests](#) app if not already installed with your bundle. The Guests app requires the email settings to be configured in your ownCloud setup, because you need to be able to invite your guests by email.

Configuration

Check your Guests app's configuration in **Settings** › **Admin** › **Sharing**. There you can change the Guest's **group name** and add to or exclude apps from the app **whitelist** of the Guests app. Guests cannot access apps that are not on that list.

Guests

Guest users are grouped under a virtual group in the user manager

Group name

Domain blacklist for guest user invitation

The following domains will not be accepted when users try to invite guests.

Limit guest access to an app whitelist

[Reset whitelist](#)

Troubleshooting

If for some reason you don't see all the buttons, try a different browser to exclude a possible script or adblocking add-on as a cause. If for example you as a guest user cannot open a PDF document via your ownCloud but you can download it - check the **whitelist** in the configuration settings described above. You have to explicitly specify that the guest users can access the required app.

OpenID Connect (OIDC)

Introduction

[OpenID Connect](#) is an open standard for single sign-on, identity and access management. With ownCloud it can be used for user authentication and client authorization against an external identity provider(IdP).

Benefits of using ownCloud with OpenID Connect

- Increased security by shifting user authentication to an external identity provider.
- Seamless integration into single sign-on (SSO) environments as well as with third party products.
- Centralized client management within the identity provider.
- Enterprise-grade security through the use of authentication security features (e.g., multi-factor authentication) and policies (e.g., automatic token expiration on certain conditions) provided by identity providers.



ownCloud only supports one configured identity provider which is then valid for all requests.

Click on the [OAuth code flow sequence diagram](#) link to get more details on the flow sequence.

Supported Identity Providers

ownCloud Server can work with identity providers (IdP) that support OpenID Connect. There are many identity providers available and the OpenID Connect implementations vary a lot in terms of supported features as well as configuration needs.

The currently supported products are

- [Microsoft Azure AD](#)
- [Microsoft ADFS](#)
- [PingIdentity PingFederate](#)
- [cidaas](#)
- [Keycloak](#)
- [Kopano Konnect](#)

Please get in touch with ownCloud Consulting if you need help with a specific identity provider product.

Prerequisites

Setting up ownCloud Server to work with OpenID Connect requires a couple of components to work together:

- An external identity provider configured to work with the ownCloud components
- A distributed memcache setup - such as Redis or Memcached - is required to operate this app. Follow the [caching documentation](#) on how to set it up.
- The [OpenID Connect App](#) installed on ownCloud Server
- Configuration settings in `config.php` on ownCloud Server

- `'http.cookie.samesite' => 'None',`

See [config.sample.php](#) and [Schemeeful Same-Site](#) for examples and details.

- Settings for the OpenID Connect App

See [config.apps.sample.php](#) for examples and details or see section [Save Settings in the Database](#) below when running clustered setups.

- Service discovery for the [ownCloud Clients](#)

Save Settings in the Database

If you run a clustered setup, the following method configuring the OpenID Connect app is preferred, because it is stateless. The app checks for settings in the database first. If none are found, it falls back to the settings stored in `config.php`. The settings are stored as a JSON formatted string with the following keys and values:

Key	Value
appid	'openidconnect'
configkey	'openid-connect'
configvalue	<i>JSON-String</i>

If a malformed JSON string is found, an error is logged. The *key* → *value* pairs are the same as when storing them to the `config.php` file. This task has to be done by invoking an `occ` command, see the following example. Use the `occ` commands `config:app:get` to view the current setting or `config:app:delete` to delete it. See the [Config Command Set](#) for more details.

```
sudo -u www-data ./occ config:app:set \
  openidconnect \
  openid-connect \
  --value='{"provider-url":"https://\//idp.example.net","client-id":"fc9b5c78-ec73-47bf-befc-59d4fe780f6f","client-secret":"e3e5b04a-3c3c-4f4d-b16c-2a6e9fdd3cd1","loginButtonName":"Login via OpenId Connect"}'
```



Only set either the database or the `config.php` keys but not both for the OpenID Connect app.

Set Up Service Discovery

1. Webserver Service Discovery Information

In order to allow the ownCloud Clients (Desktop/Android/iOS) to make use of OpenID Connect, the webserver serving ownCloud Server needs to *provide service discovery information* under the following static path:

```
https://cloud.example.com/.well-known/openid-configuration
```

2. App Service Discovery Information

When enabled, the OpenID Connect App provides the service discovery information on the endpoint:

```
https://cloud.example.com/index.php/apps/openidconnect/config
```

3. Webserver Rewrite Rule

To make the endpoint available under the static service discovery path, it is recommended to put a `RewriteRule` in place using in the `VirtualHost` section. The Apache modules `proxy`, `proxy_http` and `proxy_connect` have to be enabled if SSL is used:

```
RewriteEngine on
```

```
RewriteRule "^/\..well-known/openid-configuration"  
"/index.php/apps/openidconnect/config" [P]  
SSLProxyEngine On #This can be omitted if no SSL is used
```



Depending on the respective infrastructure setup there can be other ways to solve this. In any case, please make sure *not to use redirect rules* as this will violate the OpenID Connect specification.



If you use the `.htaccess` file in the ownCloud web root, you have to manually add that rewrite rule again after any ownCloud upgrade.

4. Once service discovery is available as described above, the ownCloud clients will attempt to connect via OpenID Connect.

General Example Setup

All IdPs have their own setup, but often share common ways of configuring things. Although not identical, the [Kopano Konnect](#) example may be a good starting point for the specific configuration of your setup. As Microsoft with Azure is different, it has its own example section.

Example Setup Using Kopano Konnect

Follow this link to see [Example Setup Using Kopano Konnect](#).

Example Setup Using Microsoft Azure

Follow this link to see [Example Setup Using Microsoft Azure](#).

Example Setup Using OneLogin

Follow this link to see [Example Setup Using OneLogin](#).

ownCloud Desktop and Mobile Clients

ownCloud desktop and mobile clients detect whether OIDC is available (service discovery) and use this login method when a new account is created.



The desktop and mobile apps (clients) have a default client ID and secret hard-coded, which are used for ownCloud's oauth2 app. When using Kopano as IdP, it does not pre-define a client ID and secret. You can use the default ones of the client to configure Kopano properly. With some IdPs like MS-Azure, these and other required parameters come from the IdP and must be coded into the client. Note that each IdP has different requirements. Get in touch with ownCloud for a branding subscription to customize the clients according to your needs.

Client Support for OIDC

Following owncloud clients support OIDC

ownCloud Client	Release with OIDC support
Desktop	>= 2.7.0
Android	>= 2.15
iOS	>= 1.2

Client IDs, Secrets and Redirect URIs

All IdPs can use ownCloud's default implemented *Client IDs, Secrets and Redirect URIs* with the exception of Microsoft, which uses a different approach. Here is the data necessary for the configuration.

Client ID

Source	Key
Server/Web	as specified in <code>config.php</code>
Desktop	<code>xdX0t13JKxym1B1QcEncf2XDkLAexMBFwiT9j6EfhHFJhs2KM9jb jTmf8JBXE69</code>
Android	<code>e4rAsNUSIU01F4nbv9FmCeUkTLV9GdgTLDH1b5uie7syb90SzEVr bN7HIpmWJeD</code>
iOS	<code>mxd50QDk6es5Lz0zRvidJNfXLUZS2oN3oUFexPP8LpPrhx3UroJFd uGEYIB0xkY1</code>

Client Secret

Source	Key
Server/Web	as specified in <code>config.php</code>
Desktop	<code>UBntmLjC2yYCeHwsyj73Uwo9TAaecAetRwMw0xYcvNL9yRdLSUi0h UAHfvCHFeFh</code>
Android	<code>dInFYGV33xKzhhRmpqQ1tYNdfLdJIJfJ9L5ISoKhNoT9qZftpdWSP7 1VrpGR9pmoD</code>
iOS	<code>KFeFWWEZ09TkisIQzR3fo7hfiMXL0paqP8CFuTbSHzV1TUuGECg1P xpiVKJfOXIx</code>

Redirect URIs

Source	Redirect URI ¹
Desktop ≤ 2.8	<code>http://localhost</code>
Desktop ≥ 2.9	<code>http://127.0.0.1</code>
Android	<code>oc://android.owncloud.com</code>
iOS	<code>oc://ios.owncloud.com</code>

(1) See the [following note](#) when using Microsoft Azure and 127.0.0.1 as redirect URI.

Migrate Clients from Basic Authentication to OIDC

If your users are logged in to their desktop and mobile clients via basic authentication (username/password) against ownCloud Server and you are not using OAuth2 to authorize the ownCloud clients, a migration to OIDC can be conducted as follows:

1. Make sure you have a working OIDC configuration based on the above sections.
2. Enable the OpenID Connect App.
3. Enable [token-only authentication](#).

Once the OpenID Connect App is enabled, token-only authentication is enforced and service discovery is properly set up, the ownCloud clients will ask the users to re-authenticate. After a successful re-authentication, the migration is done.

To connect legacy clients, users have to generate [special app passwords \(tokens\)](#).

Migrate Clients from OAuth2 to OIDC

If you use OAuth2 for client authorization, a migration to OIDC can be conducted as follows:

1. Make sure you have a working configuration based on the above sections.
2. Enable the OpenID Connect App (while having the OAuth2 App still enabled).
3. Disable the OAuth2 App.

Once the OAuth2 App is disabled and service discovery is properly set up, the ownCloud Clients will ask the users to re-authenticate. After a successful re-authentication, the migration is done.

Migrate Web Login (and Client Login) from SAML to OIDC

If you are using SAML/SSO, a migration to OIDC depends on your identity provider and is not straight forward. Please get in touch with ownCloud Consulting to plan the migration.

How to Upgrade Your ownCloud Server

Introduction

We recommend that you keep your ownCloud server up to date. When an update or upgrade 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.
- Check ownCloud's [mandatory requirements](#) (such as PHP versions and extensions), which can change from one version to the next. Ensure that you review them and update or upgrade your server, if required, before upgrading ownCloud.
- Upgrading is disruptive, as your ownCloud server will be put into [maintenance mode](#).

- Large installations may take several hours to complete the upgrade.
- Review any installed [third-party apps](#) for compatibility with the new ownCloud release.
- 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 attempting this, file a support ticket (if you have paid support) or ask for help in the ownCloud forums to resolve your issue without downgrading.

Unresolved directive in modules/admin_manual/pages/maintenance/upgrading/upgrade.adoc - include::partial\$maintenance/major_release_note.adoc[]

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, enable all those that are compatible with the new release again.



Unsupported apps may disrupt your upgrade.

Upgrade Options

There are two ways to upgrade your ownCloud server:

1. **(Recommended)** Perform a [manual upgrade](#), using the [latest ownCloud release](#).
2. **(Discouraged)** 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. We discourage upgrades with Linux Package Manager because you might encounter unwanted side effects.



Enterprise customers: refer to [Installing & Upgrading ownCloud Enterprise Edition](#) for more information.

Manual ownCloud Upgrade

Introduction

This document describes how to manually upgrade your ownCloud installation. Because installations can vary, this guide can only give an overview of methods and examples. These examples need to be adapted according your needs and your environment.



This guide assumes that you have basic knowledge about Unix terminology, commands and concepts. In case you are not familiar with these, ownCloud highly recommends that you create a playground first to try the steps and/or get in touch with ownCloud support to avoid breaking your system or losing data.



This guide covers the upgrade of the ownCloud instance only. When planning to

update/upgrade your server environment or server packages, read the [Detailed Installation Guide](#) first to match the prerequisites.

After preparing the upgrade, you can decide between two ways of upgrading your instance:

Script-Guided Upgrade

This upgrade automates most of the tasks to be done including setting the correct ownership and permissions.

Manual Step-by-Step Upgrade

Using this type of upgrade, you have to do all the steps manually but you can also handle special setups.



In this description we assume that your ownCloud installation was located in the default directory: `/var/www/owncloud` and the new release will reside there as well. The path might differ, depending on your installation.

General Preparation

There are several steps necessary before you can start with upgrading your ownCloud instance.

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.



In a clustered environment, check that all nodes are in maintenance mode.

Prevent Browser Access

With those steps completed, stop your webserver to prevent users trying to access ownCloud via the web. As an alternative, you can stop serving the virtual host for ownCloud.

Stop the web server:

```
sudo service apache2 stop
```

Backup the Database

First, backup ownCloud and the server database as described in section [Backing up ownCloud](#). This is independent of the next upgrade steps but important in case something goes wrong.

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. Third party apps are all apps that are not distributed by [ownCloud](#) or not listed in [Supported Apps in ownCloud](#).

1. Disable Apps via Command Line

This command lists all apps by <app-id> and app version:

```
sudo -u www-data ./occ app:list
```

This command disables the app with the given <app-id>:

```
sudo -u www-data ./occ app:disable <app-id>
```

2. Disable via Browser

Go to **Settings** › **Admin** › **Apps** and disable all third-party apps.

Backup Manual Changes in `.htaccess`

If you have made changes in `.htaccess` located at the webroot of ownCloud, you must backup these changes. Only backup the changes made but not the complete file as this file will be recreated on upgrades and may contain different settings provided by ownCloud. Manual changes in `.htaccess` can be necessary when you e.g. [Integrate ownCloud into Microsoft Teams](#) or fixing WebDav connection errors as [The network name cannot be found](#) on Windows.

Backup Manual Changes in `.user.ini`

If you have made changes in `.user.ini` located at the webroot of ownCloud, you must backup these changes.

Download the Latest Release

Download the latest [ownCloud server release](#) to the same location where your previous instance is located, in this example the default directory `/var/www/`.

```
cd /var/www/  
sudo wget https://download.owncloud.com/server/stable/owncloud-complete-latest.tar.bz2
```

Script-Guided Upgrade

When using the script-guided upgrade, the script from the [Script-Guided Installation](#) is used. This script can not only **install** a new instance of ownCloud, but also **upgrade** an existing one or can **manage ownership and permissions**. When using the script for upgrading, the script renames the current instance and creates a new instance, copies `config.php` set ownership and permissions etc.

The script [asks questions](#) and beside other parameters, the **upgrade an existing installation** question is selected.

Follow the script documentation for details on how to install and use it.



The script is most convenient if you use links for your `apps-external` and your `data` directory, as it takes care of recreating the links. You will be asked about this when you run the script. If you're using regular directories, these are created, but

content must be moved or copied manually before finalizing the upgrade. If you aren't using the `apps-external` directory, you must manually take care of copying only those apps which are not part of the new source.

When the script has finished, continue with the [Finalize the Upgrade](#) step described below.



When using the script, any manual changes in `.htaccess` or `.user.ini` must be manually transferred from the backup directory the script created to the actual instance directory.

After the upgrade is finished, you can re-run this script to secure the `.htaccess` files.

Manual Step-by-Step Upgrade

Note that this procedure is not an in-place upgrade but an upgrade to a new directory identically named as originally set. This ensures that no code or settings can get orphaned or overwritten.

Move Current ownCloud Directory

Although you have already made a backup, move your current ownCloud directory to a different location for easy later access:

This example assumes Ubuntu Linux and MariaDB, rename the ownCloud directory:

```
sudo mv /var/www/owncloud /var/www/backup_owncloud
```

Extract the New Source

Extract the new server release in the location where your previous ownCloud installation used to be.

```
sudo tar -xf owncloud-complete-latest.tar.bz2
```

Copy the data/ Directory

If you keep your `data/` directory *inside* your `owncloud/` directory and you have not linked it, move it from your old version of ownCloud to your new version:

```
sudo mv /var/www/backup_owncloud/data /var/www/owncloud/data
```

If you have linked the data directory, for ownCloud it is still inside the `owncloud` directory and you have to re-link it.

If you keep your `data` **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.

Copy Relevant config.php Content

With the new source files now in place of where the old ones used to be, copy all `*config.php` and `*.json` files (if any exist) from your old ownCloud directory to your new ownCloud directory:

```
sudo cp /var/www/backup_owncloud/config/*config.php \  
        /var/www/owncloud/config/
```

```
sudo cp /var/www/backup_owncloud/config/*.json \  
        /var/www/owncloud/config/
```

Market and Marketplace App Upgrades

Before getting too far into the upgrade process, consider how the Market app and its configuration options affect the upgrade process. The Market app — and other apps from the Marketplace — will not be updated when you upgrade ownCloud if `upgrade.automatic-app-update` is set to `false` in `config.php`.

In addition, 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 internet connection available, these apps will need to be manually updated once the upgrade is finished.

Copy Old Apps

If you are using third party or enterprise applications, look in your new `/var/www/owncloud/apps/` or `/var/www/owncloud/apps-external/` directory to see if they are present. If not, copy them from your old instance to your new one.



Make sure that all app directories that are defined in the `apps_paths` section of your `config.php` file do exist in your new `/var/www/owncloud/` directory. Also, make sure, that all app directories listed in `apps_path` actually exist. If `occ` complains about missing `apps-external` then try

```
sudo mkdir /var/www/owncloud/apps-external
```

Permissions

To finalize the preparation of the upgrade, you need to set the correct ownership and permissions of the new ownCloud files and folders.

Set correct ownership

Set the ownership for all files and folders to `root:www-data` **except** the `config` and `data` directory:

```
sudo find -L /var/www/owncloud \  
        \(\ -path ./data -o -path ./config \) -prune -o \  
        \
```

```
-type d -print0 | xargs -0 chown root:www-data
```

```
sudo find -L /var/www/owncloud \  
  \(-path ./data -o -path ./config\) -prune -o \  
  -type f -print0 | xargs -0 chown root:www-data
```

Set the ownership for all files and folders to `www-data:www-data` for the `config`, `data` and `apps` directories. Note that it is not mandatory to set the ownership of the `data/` directory as it should already have the correct ownership and it can take a while to finish, depending on the size:

```
sudo chown -R www-data:www-data /var/www/owncloud/config  
sudo chown -R www-data:www-data /var/www/owncloud/data  
sudo chown -R www-data:www-data /var/www/owncloud/apps
```

Set correct permissions

Use `chmod` on files and directories with different permissions:

- For all files use `0640`

```
sudo find -L /var/www/owncloud -type f -print0 | xargs -0 chmod 640
```

- For all directories use `0750`

```
sudo find -L /var/www/owncloud -type d -print0 | xargs -0 chmod 750
```

- Set the `occ` command to executable:

```
sudo chmod +x /var/www/owncloud/occ
```

If you have configured a script for [guided installations](#), you can use it for this step as well as it automates it.

Finalize the Upgrade

Start the Upgrade

With the apps disabled and ownCloud in maintenance mode, start the [upgrade process](#) from the command line. Note that the example is based on Ubuntu Linux. Execute this within the ownCloud root folder.

```
sudo -u www-data ./occ upgrade
```

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 that indicates why the process did not complete successfully.

Reapply Manual Changes

Reapply any manual changes made to `.htaccess` files and the `.user.ini` file located in the owncloud webroot.

The following example command eases to find the differences of two files, which is helpful for reapplying manually added changes to `.htaccess` and `.user.ini`. Replace that paths, directories and files accordingly.

```
diff -y -W 70 --suppress-common-lines owncloud/.user.ini owncloud_2022-02-15-09.18.48/.user.ini
post_max_size=513M | post_max_size=1G
```

Strong Permissions

- Check that `chmod` with `0640` for `.htaccess` and `.user.ini` files has been applied.

If you have configured a script for [guided installations](#), you can use it for this step as well as it automates it.

Disable Maintenance Mode

Assuming your upgrade succeeded, disable maintenance mode using the `occ` command.

```
sudo -u www-data ./occ maintenance:mode --off
```

Enable Browser Access

With all that done, restart your web server, or alternatively re-enable the virtual host serving ownCloud:

```
sudo service apache2 start
```

Check the Upgrade

With maintenance mode disabled and the web server running, log in via the web interface and perform the following steps:

1. Check that the version number reflects the new installation.
It can be reviewed at the bottom of **Settings › Admin › General**.
2. Check that your other settings are correct.
3. Go to the **Settings › Admin › Apps** page and review the core apps to make sure the right ones are enabled.

4. After the upgrade is complete, re-enable any third-party apps that are compatible with the new release. Use `occ app:enable <app-id>` or go to **Settings > Admin > Apps > "Show disabled apps"** and enable all compatible third-party apps.



Install or enable unsupported apps at your own risk.

Rollback

If you need to rollback your upgrade, see the [Restoring ownCloud](#) documentation.

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. InnoDB is limited to row-logging when transaction isolation level
is READ COMMITTED or READ UNCOMMITTED.'
```

Please refer to [MySQL / MariaDB](#) on how to correctly configure your environment.

In the unlikely case that files do not show up in the web-ui after the upgrade, use the [files:scan command](#) to make them visible again. Here is an example of how to do so:

```
sudo -u www-data ./occ files:scan --all
```

See the [Docs & Guides page](#) for further resources for both home and enterprise users.

Sometimes, ownCloud can get *stuck in an upgrade*. This is usually due to the process taking too long and running into a PHP time-out. Stop the upgrade process this way:

```
sudo -u www-data ./occ maintenance:mode --off
```

Then start the manual process:

```
sudo -u www-data ./occ upgrade
```

If this does not work properly, try the repair function:

```
sudo -u www-data ./occ maintenance:repair
```

Database Upgrade

Introduction

Usually, when upgrading a database, follow the guides the vendor provides. You may also take a look at the [Install a Database](#) section for general notes.

This document supports an upgrade in case there are prerequisites and/or special steps to be taken to upgrade to a particular database version.

Upgrading to MariaDB 10.6

ownCloud runs fine when using a MariaDB version lower than 10.6. You can upgrade ownCloud as usual without special considerations regarding the database.

When planning to upgrade to MariaDB 10.6, some prerequisites have to be met and upgrade steps have to be taken.

This is mostly due to the fact that, unlike before, in MariaDB 10.6 *tables of the COMPRESSED row format are read-only by default*. For more information see the [InnoDB COMPRESSED Row Format](#) document.



This process only needs to be carried out once.

Overview

1. You must have upgraded your ownCloud installation to version 10.9 or above. To do so, follow the [Manual ownCloud Upgrade](#) guide.
2. Backup your ownCloud installation, especially the database to rollback in case of issues. To do so, follow the [Backing up ownCloud](#) guide.
3. Prepare the database for the upgrade with an [occ command](#).
4. Follow the respective [Upgrading MariaDB](#) guide to upgrade MariaDB.

Detailed Upgrade Steps

1. If not already done, upgrade the [ownCloud installation](#) to version 10.9 or above.
2. Set ownCloud in maintenance mode

```
sudo -u www-data ./occ maintenance:mode --on
```

3. Prevent browser access

Stop your web server to prevent users from trying to access ownCloud via the web. As an alternative, you can stop serving the virtual host for ownCloud.

Stop the web server:

```
sudo service apache2 stop
```

4. Run an occ command to prepare the database for the upgrade

```
sudo -u www-data ./occ db:restore-default-row-format
```

5. Upgrade MariaDB to version 10.6.x

Follow the instructions in the respective [Upgrading MariaDB](#) guide to upgrade MariaDB.

6. Set ownCloud back to normal operation mode:

```
sudo -u www-data ./occ maintenance:mode --off
```

7. Enable browser access

Start your web server, Alternatively, enable the virtual host serving ownCloud again:

```
sudo service apache2 start
```

Upgrade ownCloud From Packages

Upgrade Steps

The alternative to a manual upgrade is add the [ownCloud package repository](#) to your system's installation sources. Then stay current by using your Linux package manager to install fresh ownCloud packages. However, you should exclude the ownCloud package during system upgrades. For more information, check out the section on [Linux Package Manager Installation](#)



This approach should not be used unattended nor in clustered setups.

In general, we discourage upgrades with a Linux package manager because you might encounter unwanted side effects and you'll have to manage the PHP installation separately. For further information on upgrading PHP, see section [Prepare Your Server](#)

If you want to proceed anyway, read the [release notes](#) for important information first.

Before installing upgraded packages, perform the following steps:

- Disable all [third-party apps](#).
- Make [a fresh backup](#).

Now you can upgrade your ownCloud packages, then run `sudo -u www-data ./occ upgrade`.



The optional parameter to skip migration tests was removed in ownCloud 10.0. See

[Testing a Migration](#) for background information.

After the upgrade is finished, perform the following actions:

- Apply [Set Correct Permissions](#) to your ownCloud directories.
- Take your ownCloud server out of [maintenance mode](#).
- Re-enable third-party apps.

```
Unresolved directive in
modules/admin_manual/pages/maintenance/upgrading/package_upgrade.adoc
include::partial$maintenance/major_release_note.adoc[]
```



When upgrading from oC 9.0 to 9.1 with existing Calendars or Address books please have a look at the [release notes](#) for important information about the needed migration steps during that upgrade.

Upgrading Only ownCloud or the Complete System

Upgrading ownCloud from our [package repositories](#) works like any normal Linux upgrade. For example, on Debian or Ubuntu Linux the standard system upgrade command is:

```
sudo apt-get update && apt-get upgrade
```

Or you can upgrade just ownCloud with this command:

```
sudo apt-get update && apt-get install owncloud-files
```

On Fedora, CentOS, and Red Hat Linux use [yum](#) to see all available updates:

```
sudo yum check-update
```

You can apply all available updates with this command:

```
sudo yum update
```

Or update only ownCloud:

```
sudo 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.



This ownCloud instance is currently in maintenance mode, which may take a while.

This page will refresh itself when the ownCloud instance is available again.

Contact your system administrator if this message persists or appeared unexpectedly.

Thank you for your patience.

Then use `occ` to complete the upgrade. You must run `occ` as your HTTP user. This example is for Debian/Ubuntu as well as CentOS/RHEL/Fedora:

```
sudo -u www-data ./occ upgrade
```

The optional parameter to skip migration tests during this step was removed in ownCloud 10.0.

Setting Strong Directory Permissions

After upgrading, verify that for your ownCloud the [correct permissions](#) are set.

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 should upgrade your ownCloud step by step:

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
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

7. Repeat from step 4 until you reach the last available major release (e.g., 9.1.x)

Upgrading ownCloud with the Updater App

Introduction

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 [manual installations](#).



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.



- 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.

We strongly recommend that you make [regular backups](#), as well as a fresh backup before every upgrade.



The Updater app *does not* backup your database or data directory.

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.



Unsupported apps may disrupt your upgrade.

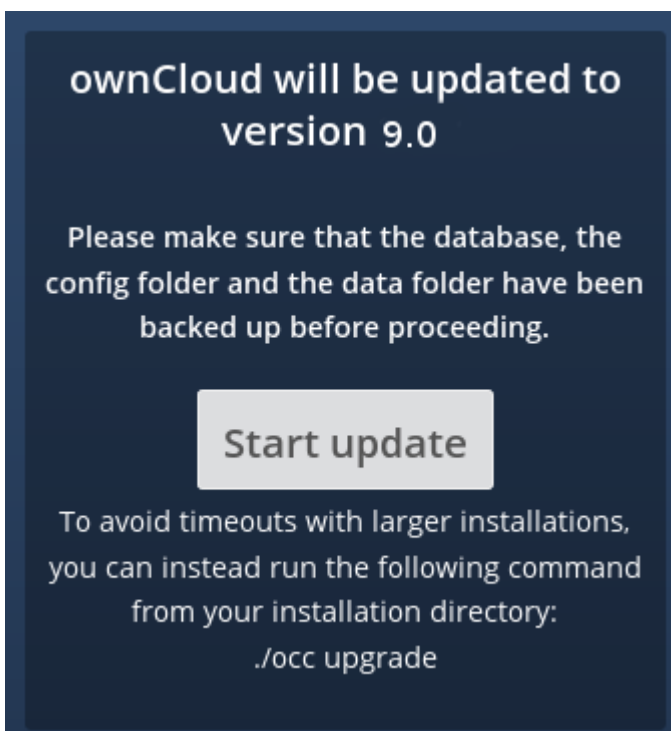
The Updater app performs these operations:

- 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

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 **Settings** › **Admin** › **General** and click the **[Open updater]** button. This takes you to the Updater control panel.
5. Click **[Start]**, 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 Correct 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:



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 ./occ upgrade
```

The optional parameter to skip migration tests during this step was removed in ownCloud 10.0.

1. 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](#).

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.

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 ./occ updater/application.php list
```

See usage for commands, like this example for the `upgrade:checkpoint` command:

```
sudo -u www-data ./occ updater/application.php upgrade:checkpoint -h
```

You can display a help summary:

```
sudo -u www-data ./occ updater/application.php --help
```

When you run it without options it runs a system check:

```
sudo -u www-data ./occ 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 ./occ updater/application.php upgrade:checkpoint --create
Created checkpoint 9.0.0.12-56d5e4e004964
```

List checkpoints:

```
sudo -u www-data ./occ updater/application.php upgrade:checkpoint --list
```

Restore an earlier checkpoint:

```
sudo -u www-data ./occ 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 ./occ /path/to/owncloud/updater/application.php
upgrade:checkpoint --create > /dev/null 2>&1
```

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',
```

Upgrade PHP on RedHat 7 and CentOS 7

Introduction

You should almost always upgrade to the latest version of PHP supported by ownCloud, if and where possible. And if you're on a version of PHP older than 7.3.0 you **must** upgrade. This guide takes you through upgrading your installation of PHP to one of the supported PHP versions (7.3 and 7.4) on Red Hat or CentOS 7.

Unresolved directive in modules/admin_manual/pages/maintenance/upgrading/upgrade_php.adoc - include::partial\$/maintenance/upgrading/upgrade_steps.adoc[leveloffset=+1]

Restart Apache

Finally, you need to restart Apache to make the changes permanent, as in the command below.

```
service httpd restart
```

Upgrade Marketplace Applications

Introduction

To upgrade Marketplace applications, please refer to the documentation below, as applicable for your ownCloud setup.

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.



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.

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 from the [Download Server Packages](#) page.
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.

Backing up ownCloud

Introduction

Depending on how the ownCloud instance has been installed, you may need slightly different steps to do a backup. You may also use different methods as the data directory can be huge. This document is intended as a guideline, but the way you implement it depends on your setup.

In any case, you need the following components to be backed up:

1. The `config/` directory.
2. The `data/` directory.
Note that the `data/` directory may not only contain user files but also keys for encryption.
3. The `apps/` directory.
Note that this is only necessary if you are not using the `apps-external/` directory and have added own apps or themes.
4. The `apps-external/` directory.
Note that this is only necessary if it exists and is in use.
5. The ownCloud database.
6. The custom theme files, if you had any. See [Theming ownCloud](#).
Note that theme files are usually located in either the `apps/` or `apps-external/` directory.



If you have customized user home directories or a custom location for encryption keys, you have to manually take care of backing them up and restoring them to the same location.

Prerequisites

To ensure a consistent backup, stop your web server to prevent users from trying to access ownCloud via the web. As an alternative, you can stop serving the virtual host for ownCloud:


```
sudo service apache2 stop
```

Backup Scenarios

Tarball Installation

1. If you have installed ownCloud from a tarball, you can safely backup the entire installation, with the exception of your ownCloud database. Databases cannot be copied, instead you must use the database tools to make a correct backup.
2. You can also back up only the directories mentioned above and the database. To avoid issues, you have to use the same tarball version as the ownCloud version when restoring.

Package Installation

If you have installed your ownCloud server from our deprecated Open Build Service and not from our new [package repository site](#), **do not back up your ownCloud server files**, which are the other files in your `owncloud/` directory such as `core/`, `3rdparty/`, `lib/`, etc. If you restore these files from backup they may not be in sync with the current package versions and in that case will fail the code integrity check and may also cause other errors.

Backup Directories

If possible, simply copy the directories from your ownCloud installation to your backup location, for example by running the following command from the `owncloud` directory. The following example command copies all directories mentioned above:

```
rsync -Aax config data apps apps-external /oc-backupdir/
```

You can also back up the full ownCloud directory which eases the restore as you do not need to install ownCloud first.

There are many ways to backup normal files. Use whatever method you are accustomed to.

Backup the Database

You can't just copy a database, but must use the database tools to make a correct database dump.

Before backing up the database, set your ownCloud instance into maintenance mode:

```
sudo -u www-data ./occ maintenance:mode --on
```



This guide uses a backup file name like `owncloud-databasebackup_<timestamp>.bak`.

MySQL/MariaDB

Depending on the database version and the setup, username and password may not be necessary. The general command to back up MySQL/MariaDB looks like this:

```
sudo mysqldump \  
  --single-transaction \  
  -h [server] \  
  -u [username] \  
  -p [password] \  
  [db_name] > owncld-dbbbackup_`date +%Y%m%d`.bak
```

Example, replace username and password according your setup:

```
sudo mysqldump \  
  --single-transaction \  
  -h localhost \  
  -u username \  
  -p password \  
  owncld > owncld-dbbbackup_`date +%Y%m%d`.bak
```

SQLite

```
sqlite3 data/owncloud.db .dump > owncld-dbbbackup_`date +%Y%m%d`.bak
```

PostgreSQL

```
PGPASSWORD="password" \  
 pg_dump [db_name] \  
 -h [server] \  
 -U [username] \  
 -f owncld-dbbbackup_`date +%Y%m%d`.bak
```

Backup Cron Jobs

Use this if you want to protect against an accidental deletion of cron entries, plan to restore to a different server like a physical migration or you need to set up a server from scratch.

```
sudo crontab -u www-data -l > www-data_crontab.bak
```

Final Tasks

Reactivate Your Instance

Perform the following tasks to reactivate your ownCloud instance:

Listing 18. Bring back ownCloud into normal operation mode

```
sudo -u www-data ./occ maintenance:mode --off
```

Enable browser access

Start your web server, or alternatively enable the virtual host serving ownCloud:

```
sudo service apache2 start
```

Restoring ownCloud

Introduction

Depending how the ownCloud instance has been installed, you may need slightly different steps to restore it from a backup.

In any case, you need the following components from your backup:

1. The `config/` directory.
2. The `data/` directory.
Note that the `data/` directory may not only contain user files, but also keys for encryption.
3. The `apps/` directory.
Note that this is only necessary if you are not using the `apps-external/` directory and have added own apps or themes.
4. The `apps-external/` directory.
Note that this is only necessary if it exists and is in use.
5. The ownCloud database.
6. The custom theme files, if you had any. See [Theming ownCloud](#).
Note that theme files are usually located in either the `apps/` or `apps-external/` directory.



If you have customized user home directories or a custom location for encryption keys, you have to manually take care of backing them up and restoring them to the same location.

Prerequisites

To ensure a secure restore process, stop your web server to prevent users from accessing ownCloud via the web. As an alternative, you can stop serving the virtual host for ownCloud:

```
sudo service apache2 stop
```

Restore Scenarios

Tarball Installation

1. If you have installed ownCloud from a tarball, you can safely restore the entire installation from the backup, with the exception of your ownCloud database. Databases cannot be copied, instead you must use the database tools to make a correct restoration.
2. You may also install a new instance from a tarball and restore the directories named above

and the database. To avoid issues, use the same tarball version as the ownCloud version from the backup.

Package Installation

If you have installed ownCloud from packages, start with a fresh ownCloud package installation in a new, empty directory. Then restore the above items from your [Backup](#).



Only copy those files and folders from the `apps/` backup directory which are NOT present after the installation. Do not overwrite items of the `apps/` directory in the new installation. This will prevent a failing code integrity check and other errors.

After you have completed restoring files, see how to [Set Correct Permissions](#).

Restore Directories

If possible, simply copy the directories from your backup to your new ownCloud environment, for example by running the following command from the backup directory. The following example command copies all directories mentioned above:

```
sudo rsync -Aax config data apps apps-external /var/www/owncloud/
```

There are many ways to restore normal files from backup. Use whatever method you are accustomed to.

Restore the Database

Before restoring the database, set your ownCloud instance into maintenance mode:

```
sudo -u www-data ./occ maintenance:mode --on
```



This guide assumes that your previous backup is called `owncloud-dbbbackup.bak`, though the file may have a timestamp added in the filename.

MySQL/MariaDB

Depending on the database version and the setup, username and password may not be necessary. To restore MySQL/MariaDB:

```
sudo mysql -h [server] -u [username] -p[password] [db_name] < owncloud-dbbbackup.bak
```

SQLite

```
sudo rm data/owncloud.db
sudo sqlite3 data/owncloud.db < owncloud-dbbbackup.bak
```

```
PGPASSWORD="password" pg_restore -c -d owncloud -h [server] -U [username] owncloud-
dbbackup.bak
```

Restoring Files From a Backup When Encryption Is Enabled

If you need to restore files from a backup during which encryption was enabled, proceed as follows with caution.



This is **not officially supported**. ownCloud officially supports either restoring the full backup or restoring nothing — not restoring individual parts of it.

- Restore the file from backup.
- Restore the file's encryption keys from your backup.
- Run `occ files:scan`, which makes the scanner find it.

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.

- Retrieve the encrypted flag value
- Update the encrypted flag.



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`.

- 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.

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, the `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. The example query 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.

```
SELECT encrypted
FROM oc_filecache
WHERE path = 'path/to/the/file/to/restore'
AND storage = <numeric_id>
```

6. Update the live database instance with the retrieved information, by running the following query, substituting the placeholders with the retrieved values:

```
UPDATE oc_filecache
SET encrypted = <encrypted>
WHERE fileid = <fileid>.
```

Final Tasks

Reactivate Your Instance

Perform the following tasks to reactivate your ownCloud instance:

Update the systems data-fingerprint after a backup is restored

```
sudo -u www-data ./occ maintenance:data-fingerprint
```

Bring back ownCloud into normal operation mode

```
sudo -u www-data ./occ maintenance:mode --off
```

Enable browser access

Start your web server, or alternatively enable the virtual host serving ownCloud:

```
sudo service apache2 start
```

Restore Cron Jobs

This is only necessary if you accidentally deleted the crontab entries, or you're restoring to a different server to carry out a physical migration or you need to set up a server from scratch.

```
sudo crontab -u www-data < www-data_crontab.bak
```

Maintenance Mode Configuration

Introduction

You must put your ownCloud server into maintenance mode before performing upgrades. The same applies to performing troubleshooting and maintenance tasks. See [Using the occ Command](#) to learn how to put your server into the various maintenance modes (`maintenance:mode`, `maintenance:singleuser`, and `maintenance:repair`) with the `occ` command. You can also use the `config.php` file for setting maintenance modes.

`maintenance:mode` locks the sessions of logged-in users and prevents new logins. This is the mode to use for upgrades.

Enable Maintenance Mode

To enable maintenance mode, run the following command:

```
sudo -u www-data ./occ maintenance:mode --on
```

You may also put your server into this mode by editing `config/config.php`.

```
'maintenance' => true,
```

Disable Maintenance Mode

To disable maintenance mode, run the following command:

```
sudo -u www-data ./occ maintenance:mode --off
```

You may also put your server into this mode by editing `config/config.php`.

```
'maintenance' => false,
```

Data Exporter

Important Information



This app is currently in beta stage, the functionality is officially not supported. Please file any issues [here](#).



The app is not available on the marketplace. To use this app, you must [git clone](#) it from the `data_exporter` repository and run `make all` in the apps root directory to install all dependencies.

Introduction

A set of `occ command line` tools to export and import users with their shares from one ownCloud instance in to another. Please see [What is Exported](#) for export details and [Known Limitations](#) for limitation details. Please see the [Data Exporter Commands](#) description for details using the `occ` commands.



To use data exporter, you must install and enable the `data exporter` app on both, the source and the target instance first.

Use Cases

- Manual zero-downtime migration of users and their shares from one instance in to another.
- Migrate from instances with different storages (POSIX to S3).
- Service GDPR-Requests by providing all files and metadata of a user in a single package.
- Merge users from different instances.

Usage Example

Export `user1` from a `source instance` to a `target instance` while preserving all shares with users on the source instance. For this example, both instances must be able to reach each other via federation.



Test if you can create remote-shares before starting this process.

Export the User on the Source Instance

This will create a folder `/tmp/export/user1` which contains all the files and metadata of the user.

```
sudo -u www-data ./occ instance:export:user user1 /tmp/export
```


Copy the Export to the Target Instance

Copy the created export to the target instance, for example using `scp`:

```
scp -rp /tmp/export root@newinstance.com:/tmp/export
```

Import the User on the Target Instance

This imports the user in to the target instance while converting all his outgoing-shares to federated shares pointing to the source instance:

```
sudo -u www-data ./occ instance:import:user /tmp/export/user1
```

Recreate all Shares to Point to the Target Instance

`user1` now lives on a target instance, therefore it is necessary to recreate all shares so that they point to the target instance. To do so run this command on the source instance:

```
sudo -u www-data ./occ instance:export:migrate:share user1 https://newinstance.com
```

Delete the User on the Source Instance

Finally delete `user1` on the source instance:



This can not be undone!



If the user is stored in the ownCloud database, you need to manually reset his password on the target instance. See [Known Limitations](#) for further information.

```
sudo -u www-data ./occ user:delete user1
```

What is Exported

- Files (Local)
- Meta-data (Username, Email, Personal Settings)
- Shares (Local, Link-shares, Group-Shares)
- Versions

Known Limitations

- External storages, comments and tags are not exported
- If a user is stored in the ownCloud database (not-LDAP etc.) the password must be manually reset by the admin as passwords can not be migrated.

- Versions import in to S3 does not preserve the version timestamp.
- Import alias (import using another username) currently does not work and breaks share-import.
- Shares import requires federation to be correctly setup between both servers and share-api to be enabled.
- A share's state will always be "accepted" regardless of the state in the old server.
- Remote shares from both directions need to be manually accepted.
- Federated shares from other servers are not migrated.
- Password protected link-shares are not imported correctly, user needs to reset the password.
- Group shares require the group to be present on the target-system or else the share will be ignored silently.
- If link-shares require a password on the new server but do so on the old the import process will crash.

As this is an early version some limitations might be fixed in the future while others can not be circumvented.

Manually Move a Data Directory

Introduction

If you need to move your ownCloud data directory from its current location to another location — **without** using a symbolic link — this section steps through how to do so.

Assumptions

This guide assumes that:

- The current folder is: `/var/www/owncloud/data`
- The new folder is: `/mnt/owncloud/data`
- You're using Apache as your webserver
- The ownCloud database name is `owncloud`

Please change the paths above to reflect your environment.

Description of Steps

The following steps are necessary to move the data directory.

1. Stop Apache
2. Enable maintenance mode for your instance
3. Use Rsync to sync the files from the current to the new directory
4. Double-check the [directory permissions](#) on the new directory

5. Change the ownCloud configuration to point to the new data directory
6. Disable maintenance mode for your instance
7. Restart Apache

Look at each section below for a detailed description.

Apache and Rsync

To save time, here are the commands which you can copy/paste for Apache and rsync:

```
sudo service apache2 stop

sudo service apache2 start

sudo rsync -avz /var/www/owncloud/data /mnt/owncloud
```



Check your commands for how to start or stop your webserver if you are not on Ubuntu/Debian.

Enable and Disable Maintenance Mode

It is necessary to enable maintenance mode to avoid running cron jobs. To enable maintenance mode, run the following command.

```
sudo -u www-data ./occ maintenance:mode --on
```

To disable maintenance mode of your instance run the following command:

```
sudo -u www-data ./occ maintenance:mode --off
```

Fix Hard-coded Database Path Variables

Open a database command line client to enter database commands and activate your ownCloud database.

```
use owncloud;
```

Update the oc_storages Table

Run the SQL below:

```
UPDATE oc_storages
SET id='local::/mnt/owncloud/data/'
```

```
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/owncloud/data/my_user/files`.

If a user does not have the path already set, you have to identify the users `id` and set the path with the following command, user by user. This example assumes the user name is `my_user` and their `id` is `1`.

Run the SQL below:

```
UPDATE oc_accounts SET home='/mnt/owncloud/data/my_user/files'
WHERE id=1;
```

For all users who already have a path like `/var/www/owncloud/data/` in your database, you can use the `REPLACE` command:

```
UPDATE oc_accounts
SET home = REPLACE(
    home,
    '/var/www/owncloud/data/',
    '/mnt/owncloud/data/'
);
```

For more information follow the complete MySQL [REPLACE](#) command syntax.



Please don't copy and paste this example verbatim — nor any of the others. They are examples only.

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 results are returned, run the SQL below to update them, changing the `id` value as appropriate.

```
UPDATE oc_jobs
SET argument = REPLACE(
    argument,
    '\\var\\www\\owncloud\\data\\',
```

```
'\\mnt\\/owncloud/data\\/'  
)  
WHERE id = <id of the incorrect record>;
```



The old data path will be written with `\\`. Therefore you must add one, additional, backslash, like this: `\\`.

Fix the Application Settings

Individual apps may reference the data directory separately from the core system configuration. For those apps, you have to change the configured path. Run the following command to list app configs.

```
sudo -u www-data ./occ config:list
```

Here is an example of the output which you may see:

```
{  
  "apps": {  
    "fictitious": {  
      "enabled": "yes",  
      "installed_version": "2.3.2",  
      "types": "filesystem",  
      "datadir": "/var/www/owncloud/data"  
    }  
  }  
}
```

In the example above, the app "fictitious" sets the data directory to `/var/www/owncloud/data`. Change this value by using the following command:

```
sudo -u www-data ./occ config:app:set --value /mnt/owncloud/data fictitious datadir
```



You have to repeat this for all apps found defining the data directory as key.

Fix the config.php Settings

To fix the config.php settings:

1. Change the `datadirectory` key in your `config.php` to the new path. To do so, start an editor of your choice and open `/var/www/owncloud/config/config.php`
2. Change the value of the key from `'datadirectory' => '/var/www/owncloud/data'`, to `'datadirectory' => '/mnt/owncloud/data',.`

Migrating User Key Encryption to Master Key Encryption

Introduction

Why should you move away from User Key-based encryption?

While it is a bit more secure than a central encryption approach, User key-based encryption has some disadvantages. It blocks some additional functions such as the integration of an online editor like LibreOffice or OnlyOffice into ownCloud and can cause problems when sharing files with groups. See [Limitations of User-Key Based Encryption](#) for more details. Therefore Master-key-based encryption is now the recommended setup for all new installations.



User key-based encryption is planned to be removed from ownCloud in the near future. As an existing customer, you will be able to continue to use this solution as long as ownCloud 10.x is supported.

Pre-Conditions

The decryption workflow described here will only work with the following pre-conditions:

- The admin recovery key password is activated and available to the ownCloud administrator
- Users have opted-in to enable the admin recovery key password
- The recovery key password has been supplied by the admin on the users page

Please see [How To Enable Users File Recovery Keys](#) for more details.



A notification to the users (e.g. through the [announcement app](#)) prior to the migration process is recommended, as the instance will not be available during this task.

Steps to Migrate from User Key-based to Master Key-based Encryption

There are several steps you need to follow to ensure a smooth and complete transition:

1. [Disable User Key-based encryption](#)
2. [Remove the encryption records from the ownCloud database](#)
3. [Remove the files_encryption directory](#)
4. [Encrypt the filesystem using Master Key-based encryption](#)

Disable User Key-based Encryption

The first part of the migration process is to decrypt all files and to disable encryption in ownCloud, which requires three commands to be executed. These commands are:

1. `occ encryption:decrypt-all,`
2. `occ encryption:disable` and
3. `occ app:disable.`

You can see an example of calling the commands listed below, configured to require no user interaction.

```
sudo -u www-data ./occ encryption:decrypt-all --continue=yes && \  
sudo -u www-data ./occ encryption:disable --no-interaction && \  
sudo -u www-data ./occ app:disable --no-interaction encryption
```



The decryption of the files by the ownCloud administrator requires the current passwords of all users! This only works when users have enabled password recovery and if an admin recovery password is available.

Remove the Encryption Records from the ownCloud Database

Once your ownCloud files are unencrypted, and encryption has been disabled, you need to remove the encryption records from the database. There is, currently, no `occ` command to handle this, so it has to be done manually. Specifically, you need to remove all records from the `oc_appconfig` table where the `appid` column is set to `encryption`.

In the examples below, you can see how to do this using MySQL. If you are not using MySQL, please use the commands specific to your database vendor.

```
SELECT * FROM `oc_appconfig` WHERE `appid` LIKE 'encryption'
```

Remove the `files_encryption` Directory

With the database updated, next, the `files_encryption` directory needs to be removed. Below is an example of how to do so, to save you time.

```
cd <your owncloud root directory>  
find ./data* -name files_encryption -exec rm -rvf {} \;
```

Encrypt the Filesystem Using Master Key-based Encryption

Now, your ownCloud files can be encrypted using Master Key-based encryption. This requires the following steps:

1. The encryption app needs to be enabled
2. Encryption needs to be enabled
3. The encryption type needs to be set to Master Key
4. Re-encryption of the ownCloud filesystem.

The following example shows how to do this on the command line.

```
sudo -u www-data ./occ app:enable encryption && \  
sudo -u www-data ./occ encryption:enable && \  
-----
```

```
sudo -u www-data ./occ encryption:select-encryption-type masterkey -y 88 \
sudo -u www-data ./occ encryption:encrypt-all --yes
```

Verify the Encrypted Files

With the files encrypted using Master Key-based encryption, you should now verify that everything worked properly. To do so, run a `SELECT` query in your database which returns all files from the `oc_appconfig` table where the `appid` column is set to `encryption`. You should see a number of records, as in the output of the example below.

```
select * from `oc_appconfig` where appid='encryption';
encryption|recoveryKeyId|recoveryKey_73facda6
encryption|publicShareKeyId|pubShare_73facda6
encryption|masterKeyId|master_73facda6
encryption|installed_version|1.3.1
encryption|types|filesystem
encryption|enabled|yes
encryption|useMasterKey|1
```

Unresolved directive in modules/admin_manual/pages/maintenance/encryption/migrating-from-user-key-to-master-key.adoc - include::partial\$/configuration/server/disable-single-user-mode.adoc[leveloffset=+1]

Post Note



It is possible, that after migration, some or all users see a re-synchronisation of their data from the server to the desktop client - especially for shared folders.

Migrating to a Different Server

Introduction

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.



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 installation while debugging the problem.

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 6 - 7 minutes for all sync clients to register that the server is in maintenance mode, stop the web server 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.



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.

Managing Trusted Domains

All URLs used to access your ownCloud server must be white-listed 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.



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 white-listed, 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.

Example Migration

The following is an example migration with assumptions to make this migration work:

- Ubuntu 16.04+
- SSH with `PermitRootLogin` set to `yes`
- Database used is MySQL / MariaDB

Preparation

If not already available on the new server, make sure SSH is installed:

```
sudo apt install ssh -y
```

Next, edit `ssh-config` and enable root ssh login.

```
nano /etc/ssh/sshd_config  
PermitRootLogin yes
```

And then restart SSH.

```
sudo 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 ./occ maintenance:mode --on
```

After that's done, then wait a few minutes and stop your web server, in this case Apache:

```
sudo 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 -v 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
```



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`.

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.

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

The following ownCloud directories will be synced to the target instance: `apps`, `config` and `data`.

```
rsync -avt apps config data root@new_server_address:/var/www/owncloud
```



If you have an additional apps directory like `apps-external`, this directory needs to be added to the sync list above.



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](#) 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 ./occ maintenance:mode
```

Next, start up the database and web server on the new machine.

```
sudo service mysql start
sudo 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 ./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:



This is a security measure and improves SSH security.

```
sudo 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.

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.

Some configurations, such as SAML IDPs, or LDAP or AD instances, may need additional configuration to connect.

How to Install the Appliance

Introduction

The installation process is a little involved, but not too much. To keep it succinct, you need to:

- [Download](#) and [Launch](#) the appliance
- Step through the [Configuration Wizard](#)
- [Activate](#) the configured appliance
- After that, you can access the running instance of ownCloud and further [Administrate it](#) to suit your needs.



It's recommended to setup the appliance with a working DHCP Server and access to the internet.



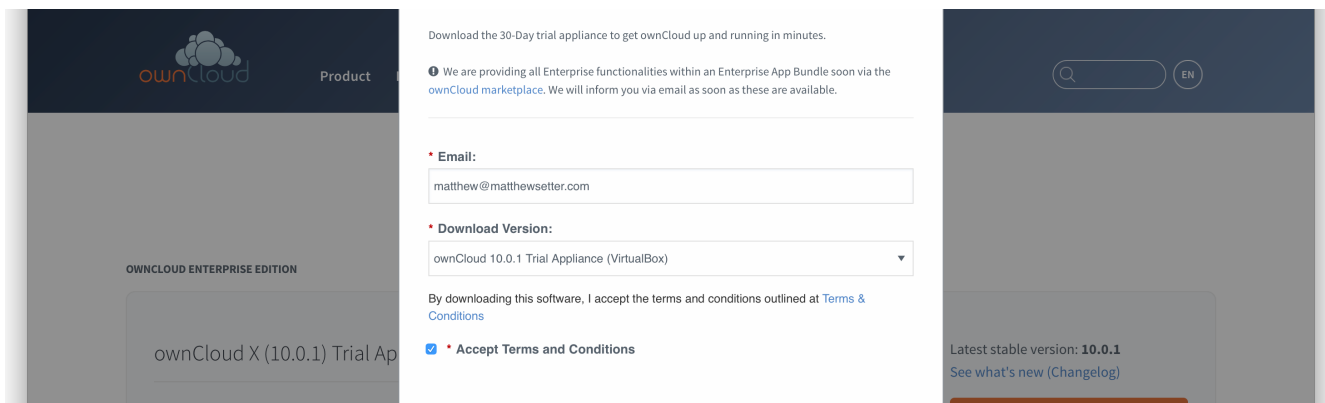
The appliance has to be activated with a license that you will receive from Univenton via email. This license has to be imported into the appliance via the **web interface**.

Download the Appliance

First off, you need to download the ownCloud X Appliance from the [ownCloud Appliance download page](#). You can select various appliance types to download like *ESXi*, *VirtualBox*, *QCOW2 (KVM)* and *VMWARE*.

Fill out the form to download the documentation which will be delivered directly in your inbox.

Alternatively you can view it online.

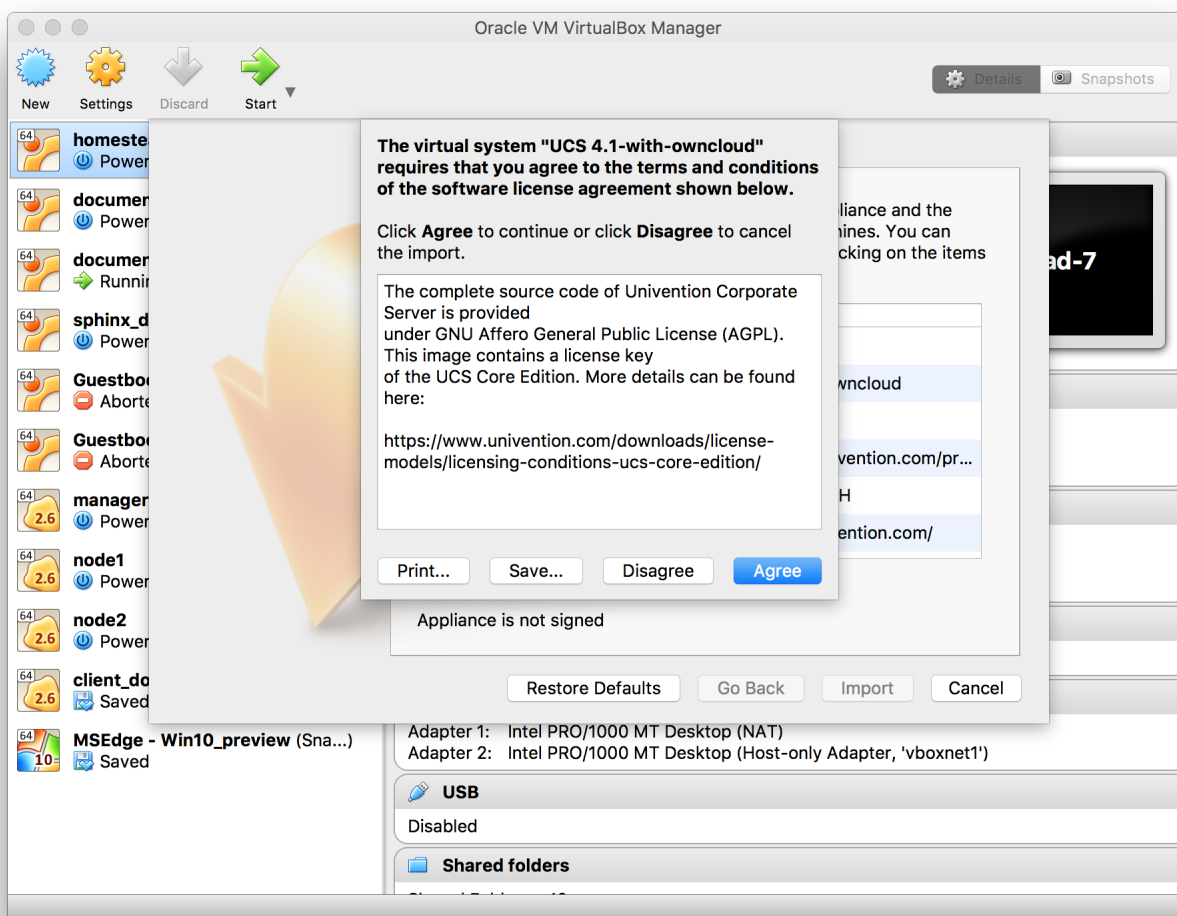


The virtual appliance files are around 1.4GB in size, so may take some time, depending on your network bandwidth.

You can also download it from the [Appliance download page](#).

Launch 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.



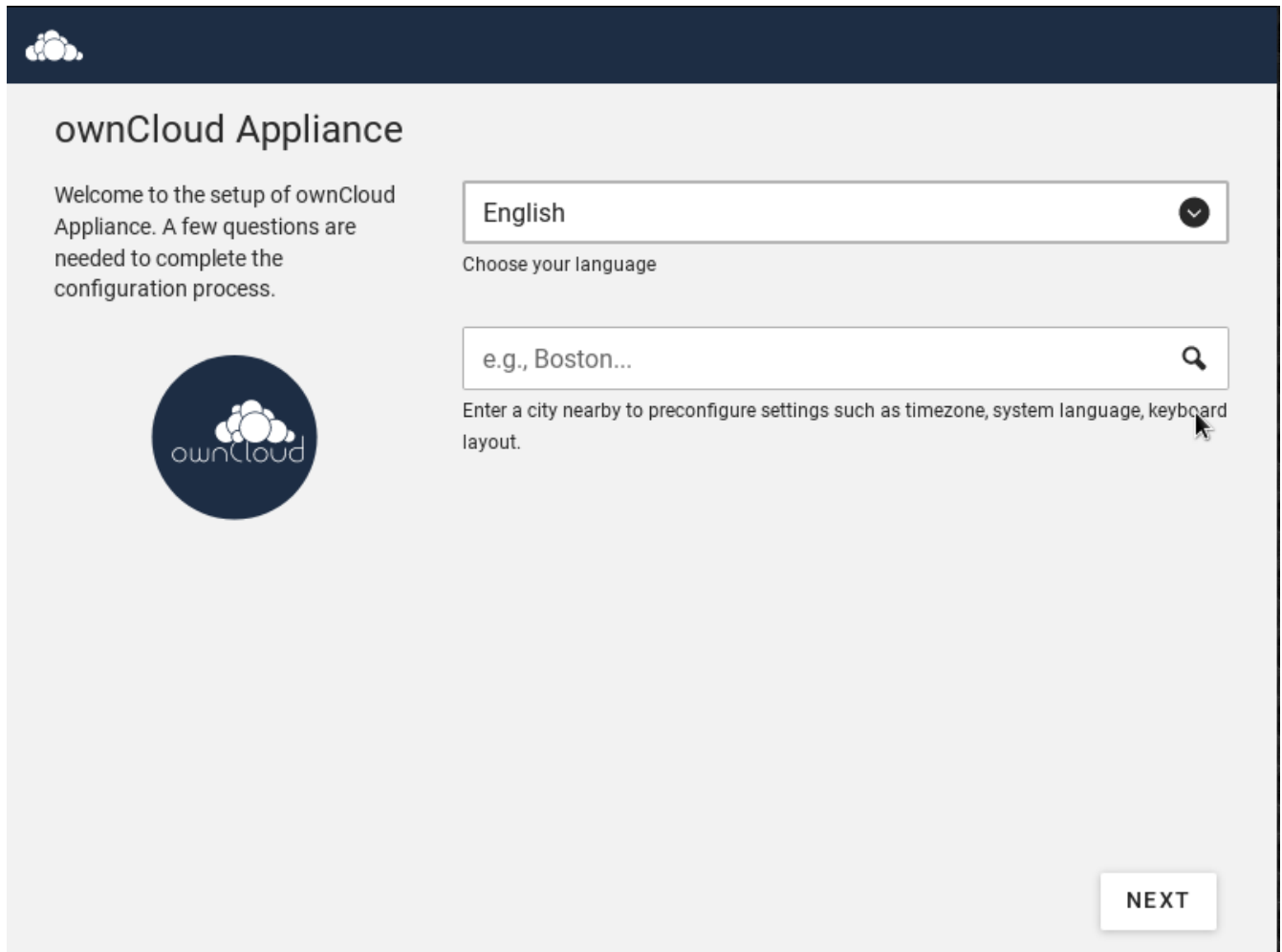
If you try to install an ownCloud appliance in your domain after removing an existing one, please remember to remove the original one from your DNS configuration.

Don't Forget the **IP Address** and the **Administrator Password**. You will need them to use the Appliance.

Configuration Wizard

Once imported, start the appliance. Doing so launches the installer wizard which helps you specify the core configuration.

Follow this screenshot guide to securely and easily configure your appliance.



Here, you can choose your **language**. Currently there are 2 options: English and German. You can set your city, which will then automatically set the localization settings in the next screen.



Localization settings

Choose your system's localization settings.



English (United States)



Default system locale

America/New_York



Time zone

English (US)



Keyboard layout



BACK

NEXT

Here, you can set your default **language**, **time zone** and **keyboard layout**. This will be set automatically if you enter your City in the previous screen.



Domain and network configuration

Specify the network settings for this system.



Obtain IP address automatically (DHCP) [\(Request address again\)](#)

10.42.17.55

IPv4/IPv6 address

255.255.252.0

IPv4 net mask/IPv6 prefix

10.42.18.1

Gateway

10.42.18.1

Preferred DNS server

Alternate DNS server

[\(configure proxy settings\)](#)

BACK

NEXT

Here, you will see the automatically obtained **network configuration** if you have a DHCP server in your network. If not - you will have to set this yourself. You can also enter an alternate DNS server if you need one.



Domain setup

Please select your domain settings.



Manage users and permissions directly on this system

A new domain directory is created on this system. User and management data are stored locally.

Join into an existing UCS domain

Use this option if you already have one or more UCS systems.

Join into an existing Microsoft Active Directory domain

This system will become part of an existing non-UCS Active Directory domain.

If unsure, select *Manage users and permissions directly on this system*.

BACK

NEXT

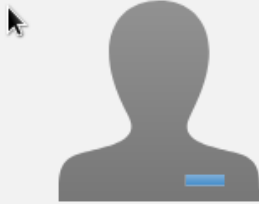
This is an important setting. **Choose the default option** if you don't have deep knowledge about Microsoft Active directory and the univention system.



Account information

Enter the name of your organization, an e-mail address to activate ownCloud Appliance and a password for your *Administrator* account.

The password is mandatory, it will be used for the domain Administrator as well as for the local superuser *root*.



Organization name

E-mail address to activate ownCloud Appliance ([more information](#))

Fill in the password for the system administrator user **root** and the domain administrative user account **Administrator**.

Password *

Password (retype) *

BACK

NEXT

The second important setting during this setup: the **Administrator password**. You will need this to log in to your appliance and administer it. Please **write this password down**. Setting your email address here is optional, since you can set it later on.



Host settings

Specify the name of this system.



Fully qualified domain name *

LDAP base *

BACK

NEXT

Here, you can set or change the **FQDN** to your custom address.



Confirm configuration settings

Please confirm the chosen configuration settings which are summarized in the following.



UCS configuration: A new UCS domain will be created.

Localization settings

- *Default system locale:* English (United States)
- *Time zone:* America/New_York
- *Keyboard layout:* English (US)

Account information

- *Organization name:* owncloud

Domain and host configuration

- *Fully qualified domain name:* ucs-7053.owncloud.intranet
- *LDAP base:* dc=owncloud,dc=intranet
- *Address configuration:* IP address is obtained dynamically via DHCP
- *DNS server:* 10.42.18.1

Software components: No additional software components will be installed.

Update system after setup ([more information](#))

With the activation of UCS you agree to our [privacy statement](#).

BACK

CONFIGURE SYSTEM

Here, you get a finalized confirmation screen of what you have entered / set and you can finish the process. Note that if you let the check box to update your system in - the installation will take **considerably longer**. Keep his in mind. You can apply the updates later on if you choose to skip it during the installation.



Confirm configuration settings

Please confirm the chosen configuration settings which are summarized in the following.



Installing owncloud



UCS configuration: A new UCS domain will be created.

Localization settings

- *Default system locale:* English (United States)
- *Time zone:* America/New_York
- *Keyboard layout:* English (US)

Account information

- *Organization name:* owncloud

90%

- *Fully qualified domain name:* ucs-7053.owncloud.intranet
- *LDAP base:* dc=owncloud,dc=intranet
- *Address configuration:* IP address is obtained dynamically via DHCP
- *DNS server:* 10.42.18.1

Software components: No additional software components will be installed.

Update system after setup ([more information](#))

With the activation of UCS you agree to our [privacy statement](#).

BACK

CONFIGURE SYSTEM

Wait until the setup is finished.



Setup successful



ownCloud Appliance has been successfully set up.

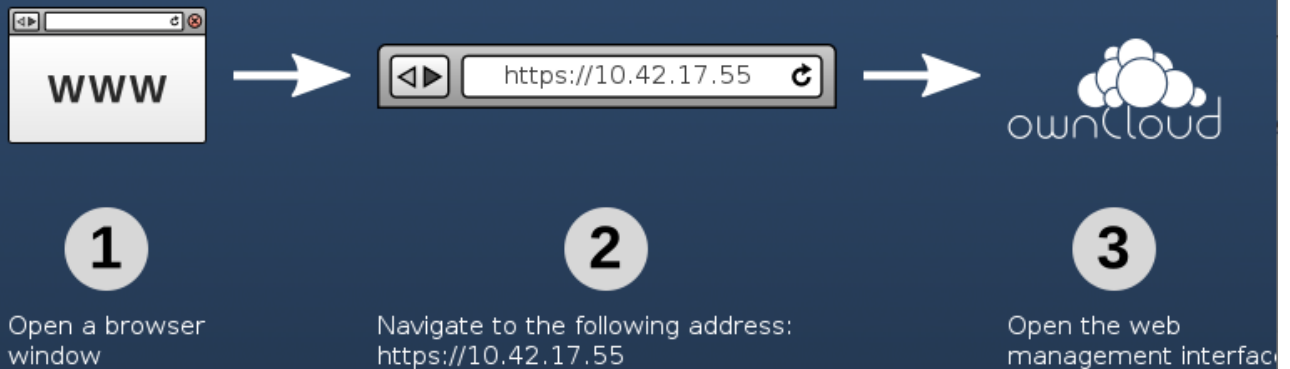
Click on *Finish* for putting this system into operation.

When accessing the system for the first time, you will be asked to request and upload a new license.

FINISH

When the installation is complete, you will see this screen informing you that the installation was successful.

ownCloud Appliance



[Press any key to open text console]

Powered by
univention

Activate the Appliance

The VM will show you this screen, showing the ip **address** you have to navigate to in order to **activate** your appliance

Anforderung einer Lizenz für ownCloud Appliance

Bitte geben Sie eine gültige E-Mail-Adresse ein, um ownCloud Appliance zu aktivieren. Die Aktivierung ist Voraussetzung, um das System in Gebrauch zu nehmen. Im nächsten Schritt können sie die Lizenzdatei hochladen, die an Ihre E-Mail-Adresse gesendet wurde.

E-Mail-Adresse




Weitere Informationen zu der Aktivierung können im [UCS-Handbuch](#) gefunden werden.

Wenn Sie bereits über eine Lizenzdatei verfügen, dann können Sie diesen [Schritt überspringen und die Lizenz einspielen](#).

AKTIVIERUNG ANFORDERN

Enter your email-address to receive a **license** to activate your Appliance. Without activation you **can not login** in to the appliance.

Univention activation  Posteingang 



noreply@univention.de
an mich 

----English----

The installation of various applications and third party apps from the App Center requires the activation of UCS. For this you can find a license key attached to this mail.

To import the license key, first save it locally on your computer. Then upload the license key as specified.

If you need help with the setup and operation of UCS, feel free to visit our user forum 'Help' [<https://help.univention.com/>].

Best regards
Your Univention team

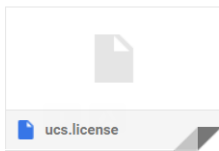
----Deutsch----

Die Installation diverser Anwendungen und 3rd Party Apps aus dem App Center erfordert die Aktivierung von UCS. Dafür finden Sie im Anhang dieser Mail einen Lizenzschlüssel.

Für das Einspielen des Lizenzschlüssels speichern Sie diesen zunächst lokal auf Ihrem Computer. Anschließend laden Sie den Lizenzschlüssel wie angegeben hoch.

Falls Sie Hilfe bei der Inbetriebnahme und dem Betrieb von UCS benötigen, schauen Sie gerne in unserem Nutzer-Forum „Help“ [<https://help.univention.com/>] vorbei.

Viele Grüße
Ihr Univention Team



You will receive the email shortly. **Download** the license and **import** it in to the appliance.

Aktivierung erfolgreich!

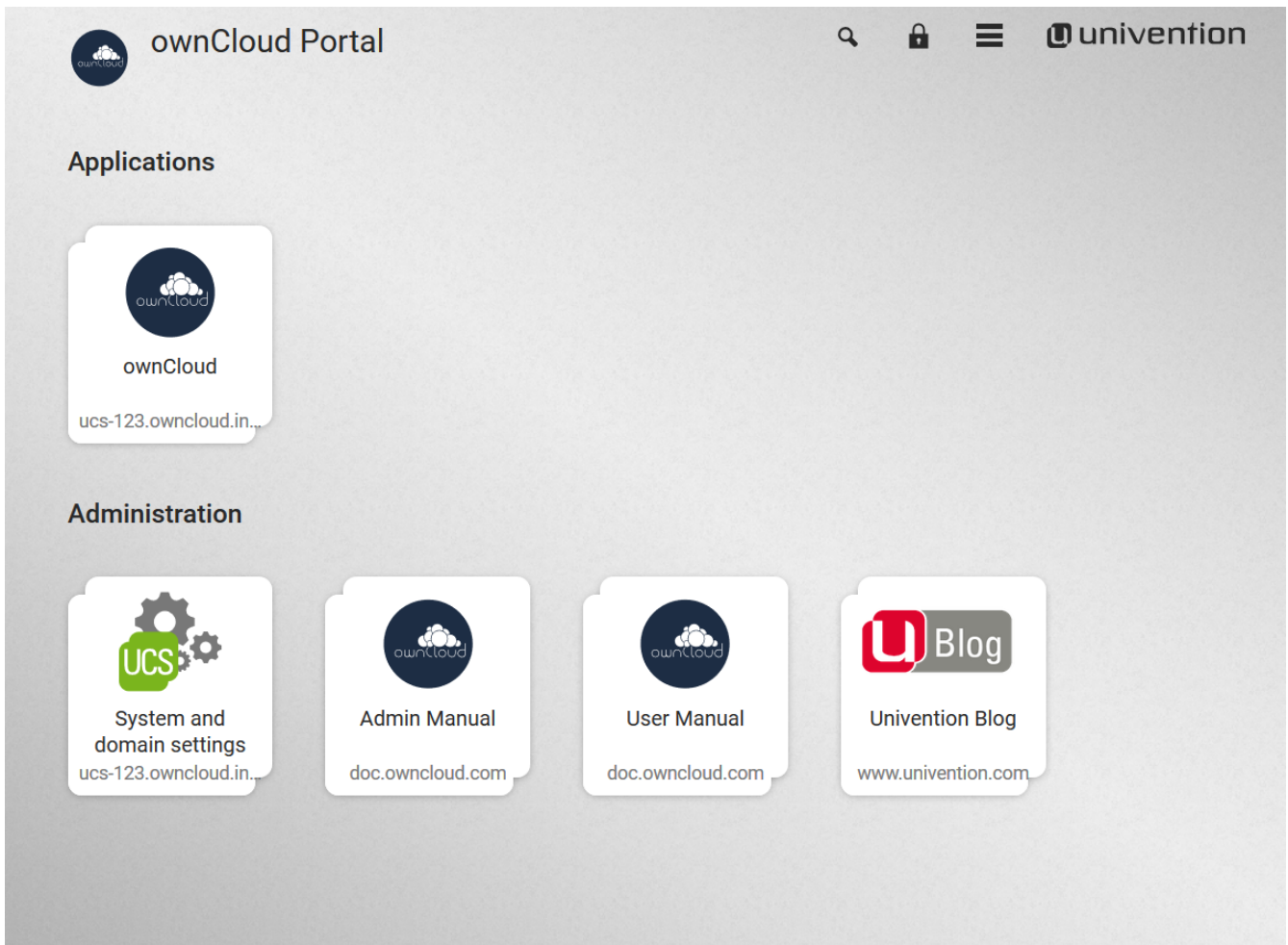
ownCloud Appliance ist nun aktiviert. Klicken sie auf "Weiter", um auf die Verwaltungsoberfläche zuzugreifen. (Das kann einige Zeit benötigen.)

FERTIGSTELLEN

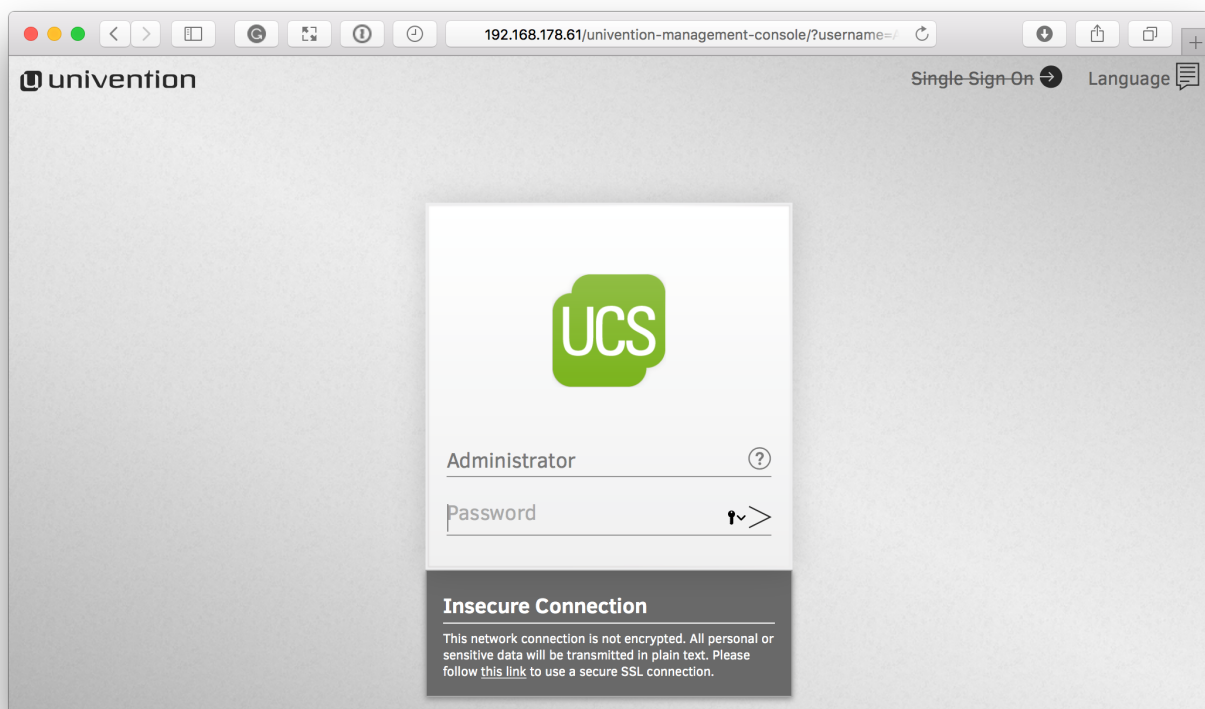
Once activated, you will see this screen, informing you that the appliance was successfully activated.

Administer the Appliance

Once activated, you should be redirected to the portal, which you can see below.

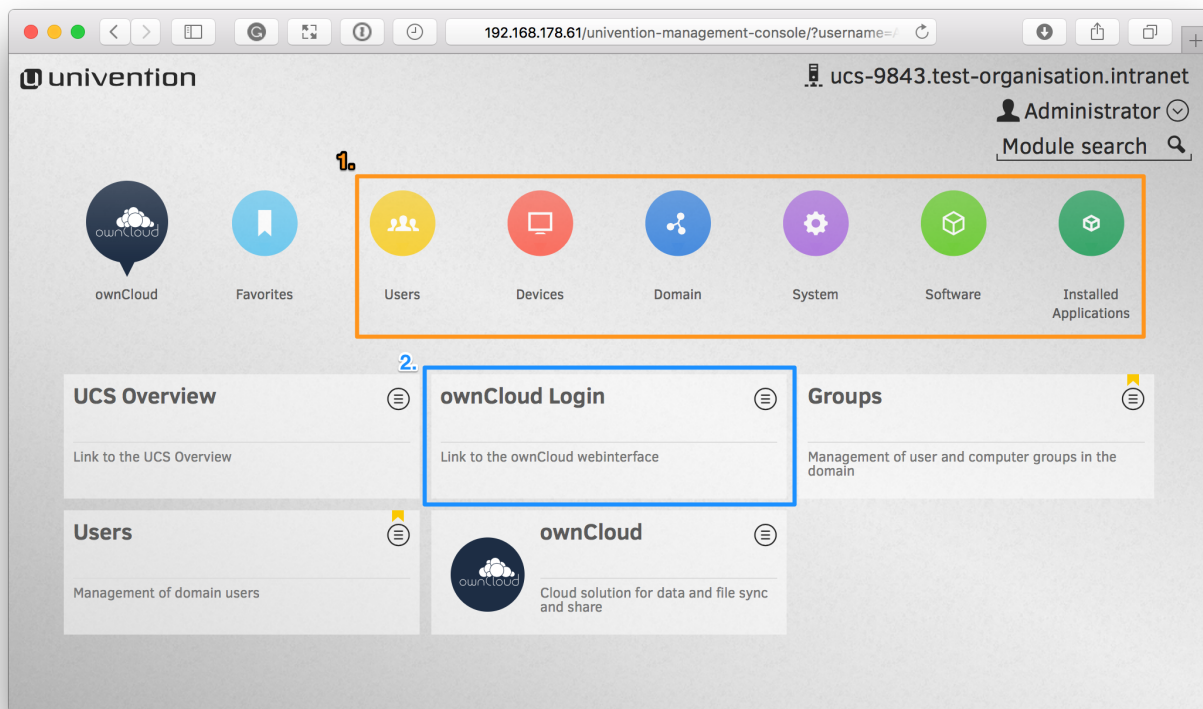


If you want to create new users and groups, or download apps from the Univention appcenter click on the [**System and domain settings**]. Login as the "**Administrator**" using the password that you supplied during the configuration wizard earlier.



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).

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.

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.

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.

```
Unresolved directive in modules/admin_manual/pages/appliance/configuration/index.adoc -
include::partial$section_page.adoc[]
```

Login Information and Custom Paths

Welcome to the ownCloud Appliance. Here are the login credentials.

```
username: owncloud
password: owncloud
```

Log in to the Appliance via command line or SSH with the root account.

```
username: root
password: <Administrator password>
```

Log in to the ownCloud docker container with this Univention command:

```
univention-app shell owncloud
```

Set ownCloud as the default page instead of the Univention Portal

```
ucr set apache2/startsite=/owncloud
service apache2 restart
```

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
```

File extension blacklist for the Ransomware app:

```
/var/lib/univention-
appcenter/apps/owncloud/data/custom/ransomware_protection/blacklist.txt.dist
```



While you are logged in to the Appliance you can also use ownCloud's command-line interface `occ` without a preceding `sudo -u www-data`. For more information on

occ commands, refer to [Using the occ Command](#).

App Settings

Configurable Options

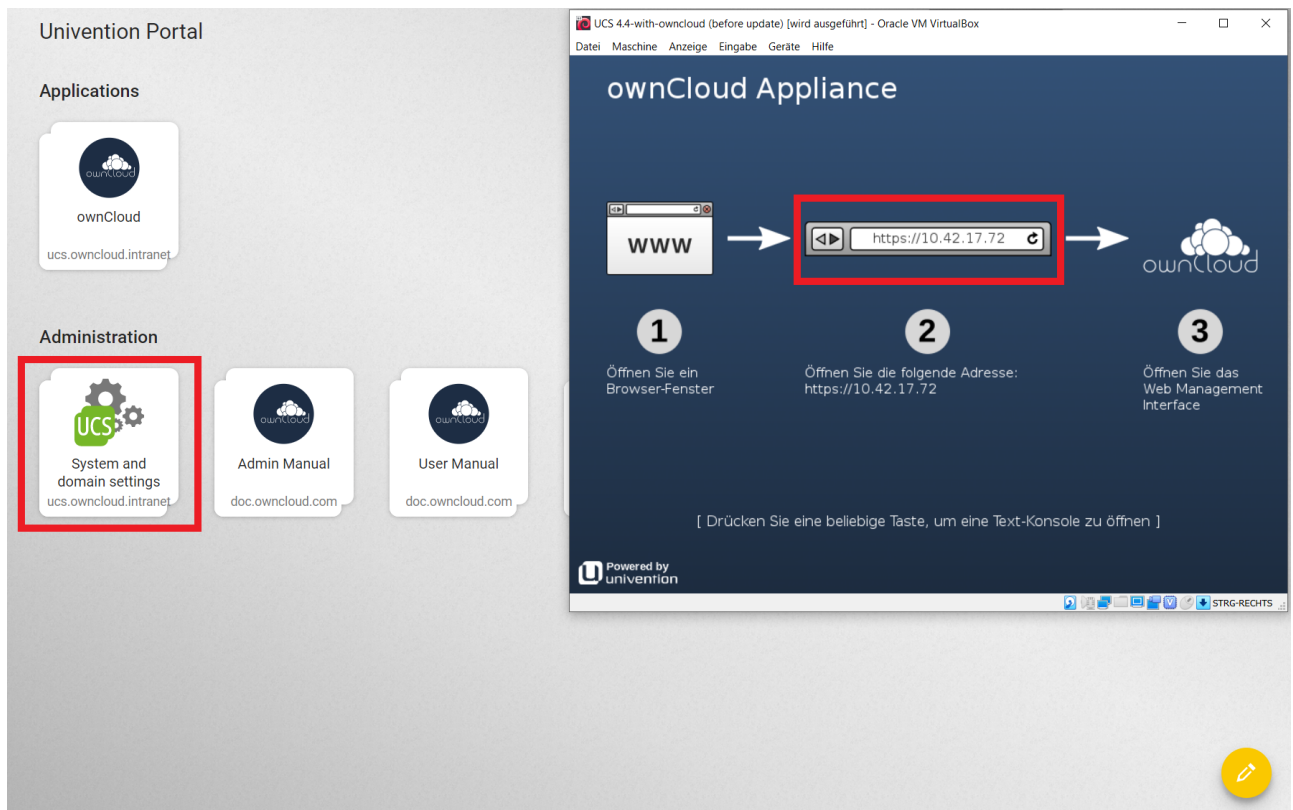
You can configure certain the ownCloud app in the Univention Portal:

- Enterprise License Key
- Marketplace API Key
- Language
- ownCloud Domain
- ownCloud SubURL
- Log Level
- Password Reset

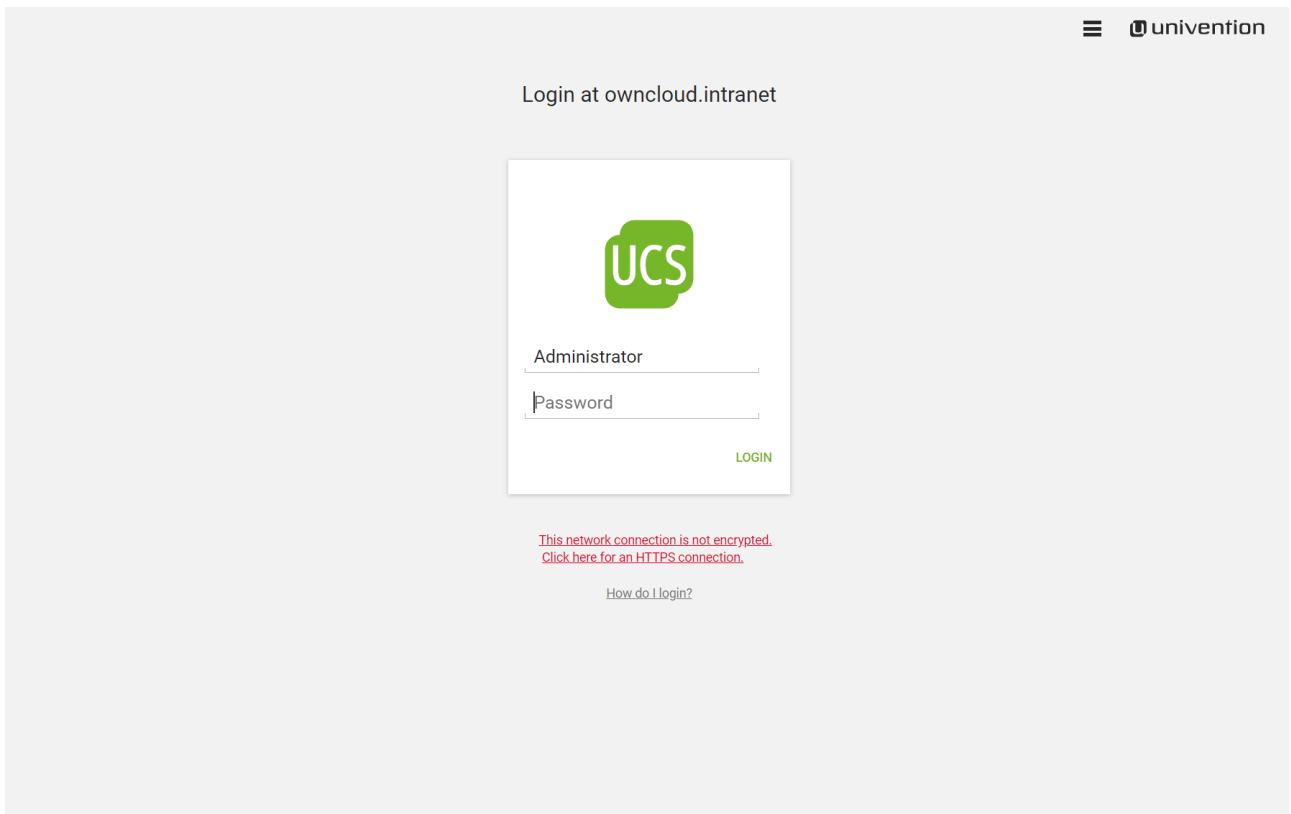
Access the settings:

Here is how you can access these settings:

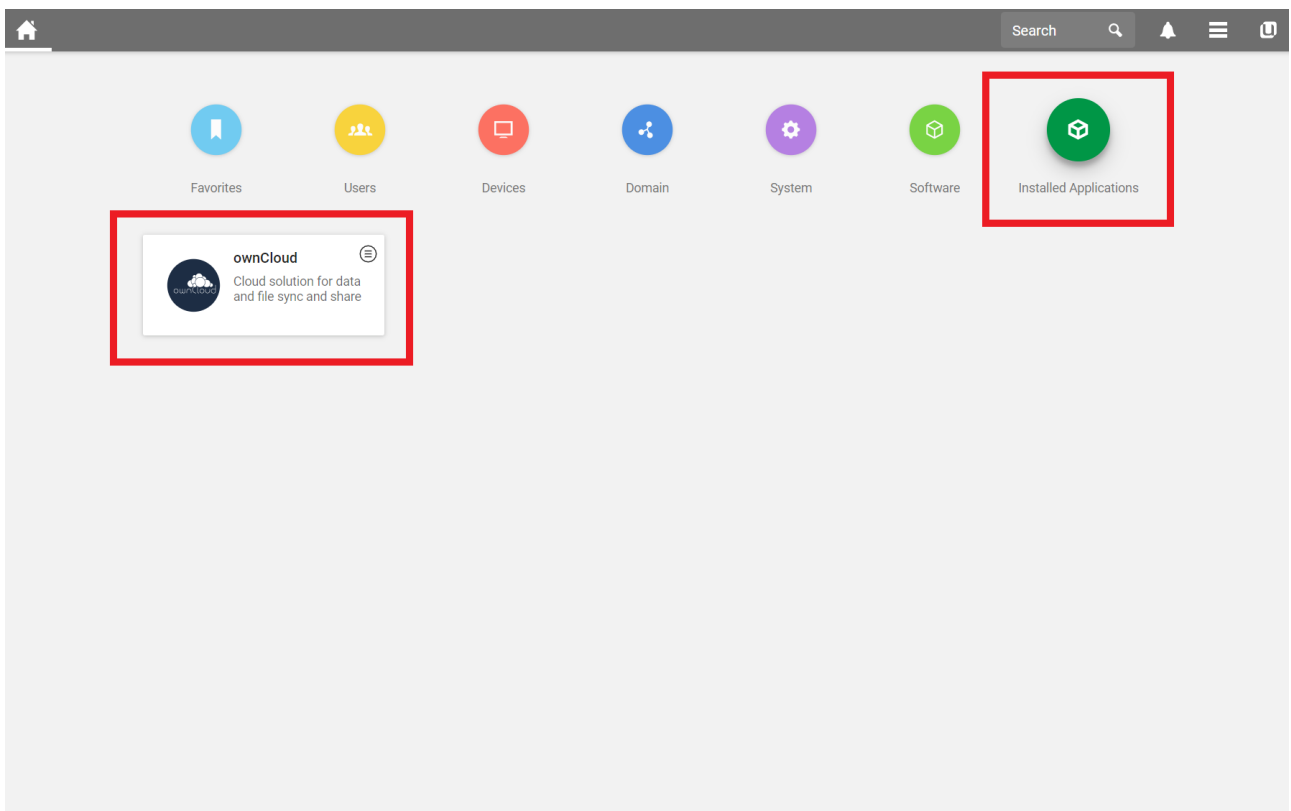
1. Go to the Portal Page of your Appliance and select **System Settings**.



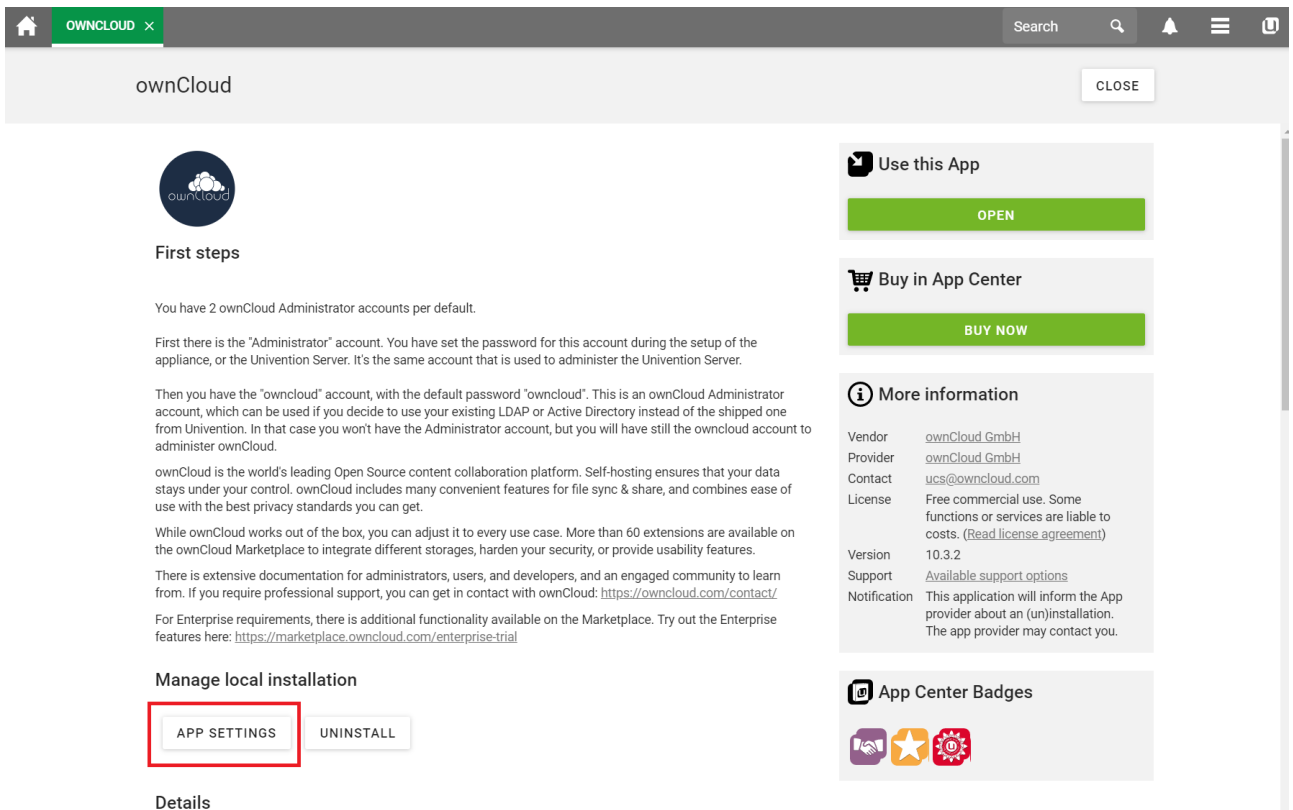
2. Login as the Appliance Administrator.



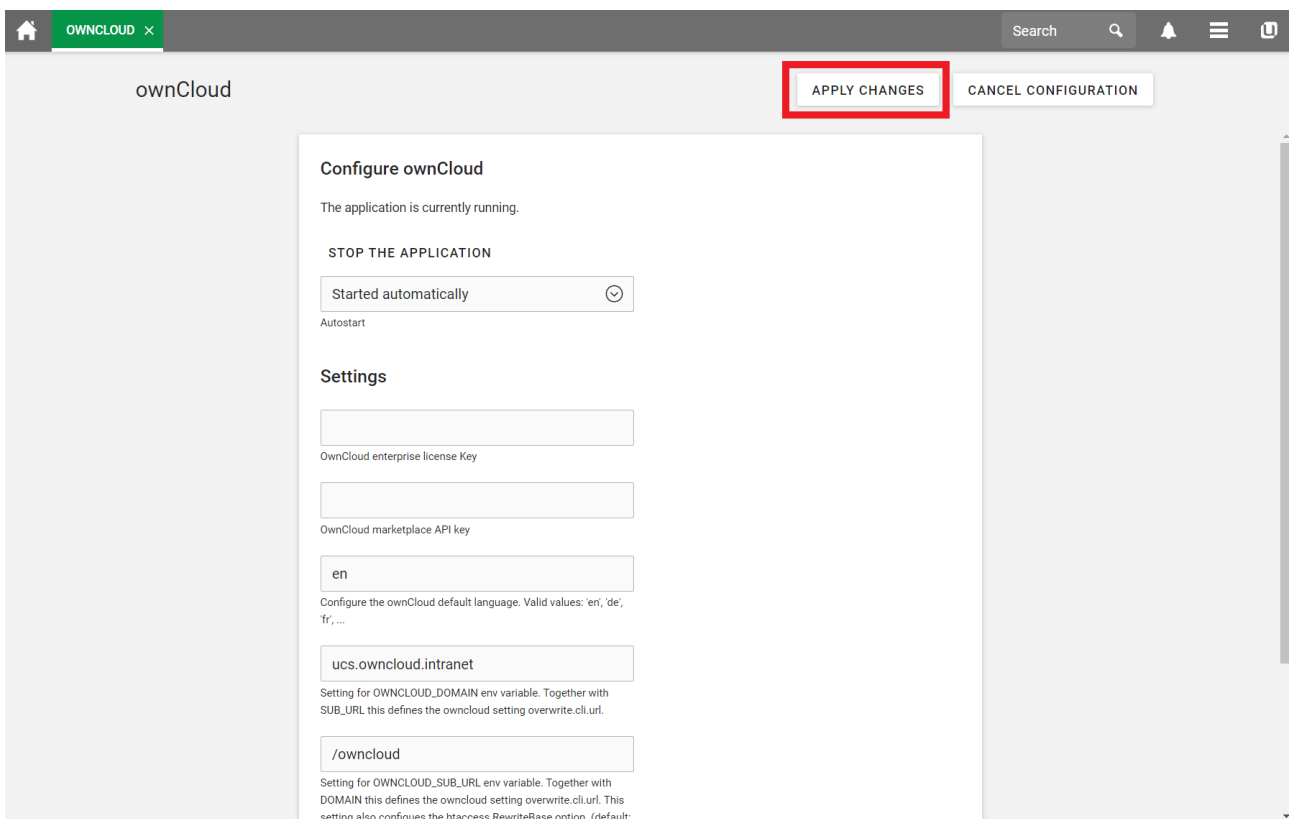
3. Go to **Installed Applications** and select **ownCloud**.



4. Go in to **App Settings**.



5. After changing these Settings, don't forget to **save** them.



How to add 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"
```

Remember to adjust the path and filename to match your certificate.

Once you've completed these steps, restart Apache using the following command:

```
sudo 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:

```
sudo ucr set apache2/force_https=yes
```

For further information please visit our partner site at [Univention](#).

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:

- 176.9.114.147
- 5.9.68.237
- 8.8.8.8
- docker.software-univention.de
- marketplace.owncloud.com
- owncloud.com
- owncloud.org
- software-univention.de

Adding Users and Groups in UCS for ownCloud

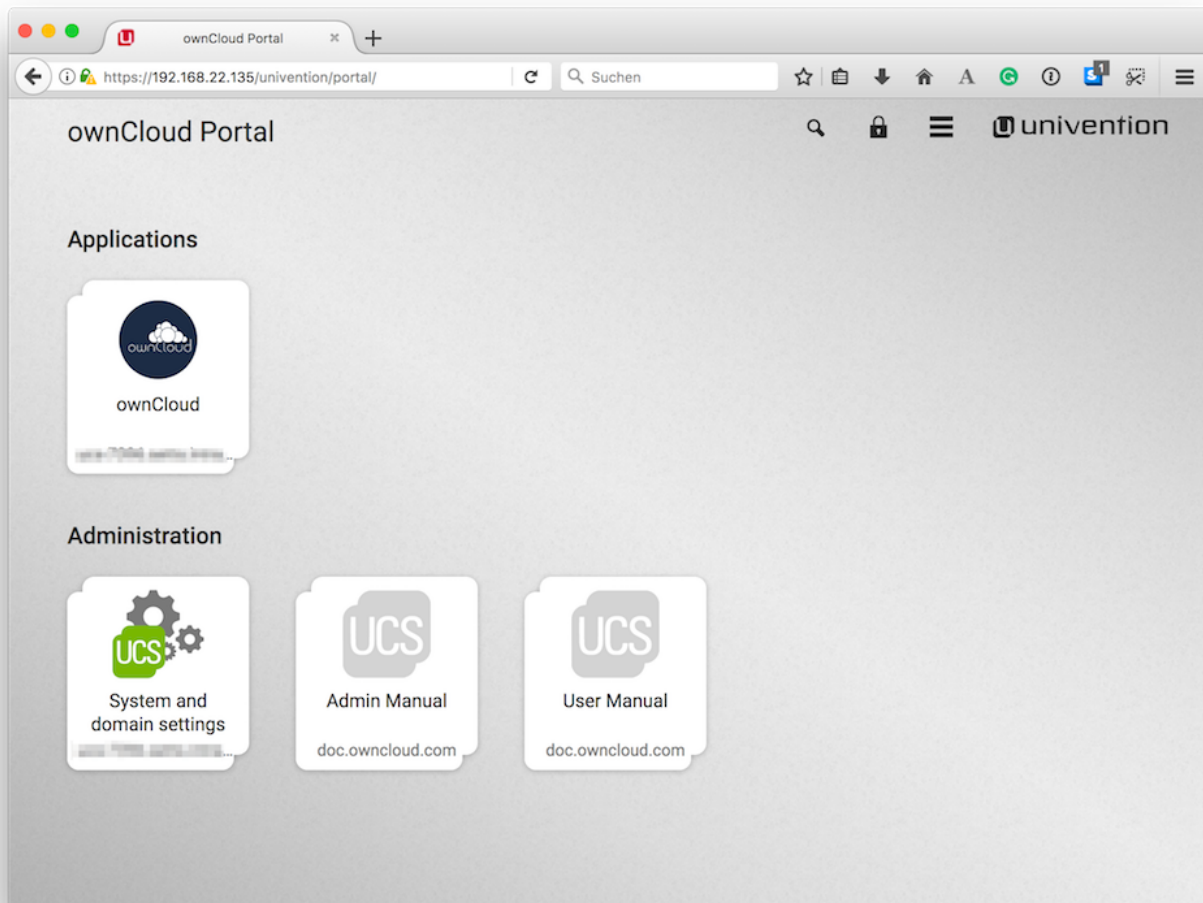
Introduction

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

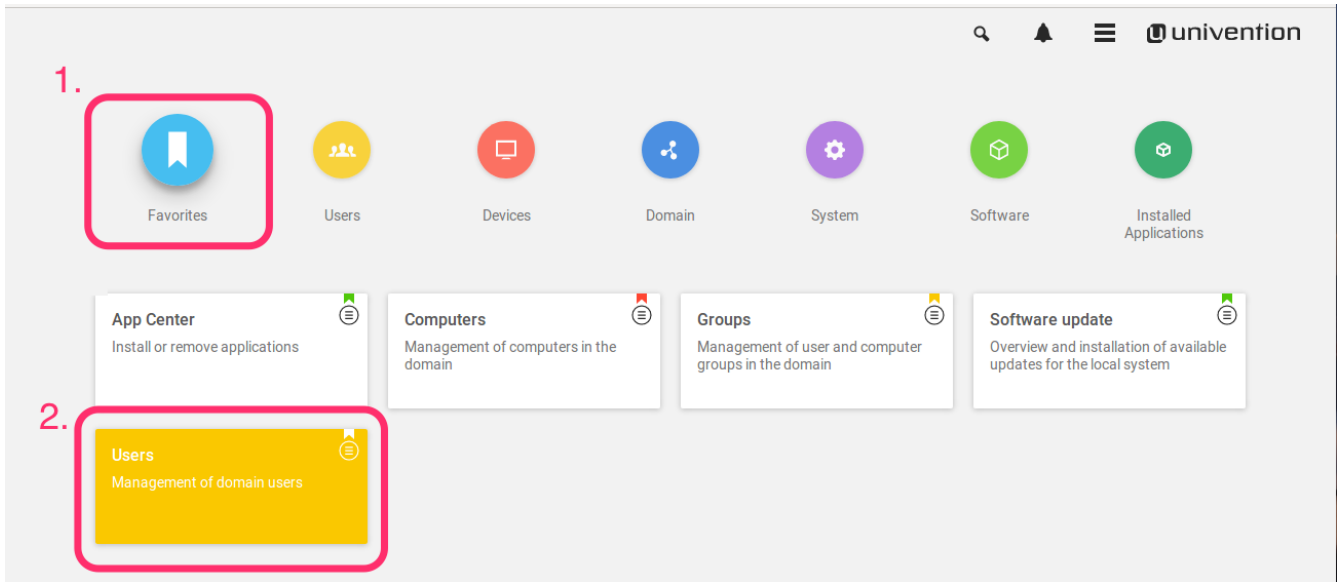
After logging in to the Univention server, under "**Administration**", click the first option, labeled **[System and domain settings]**.



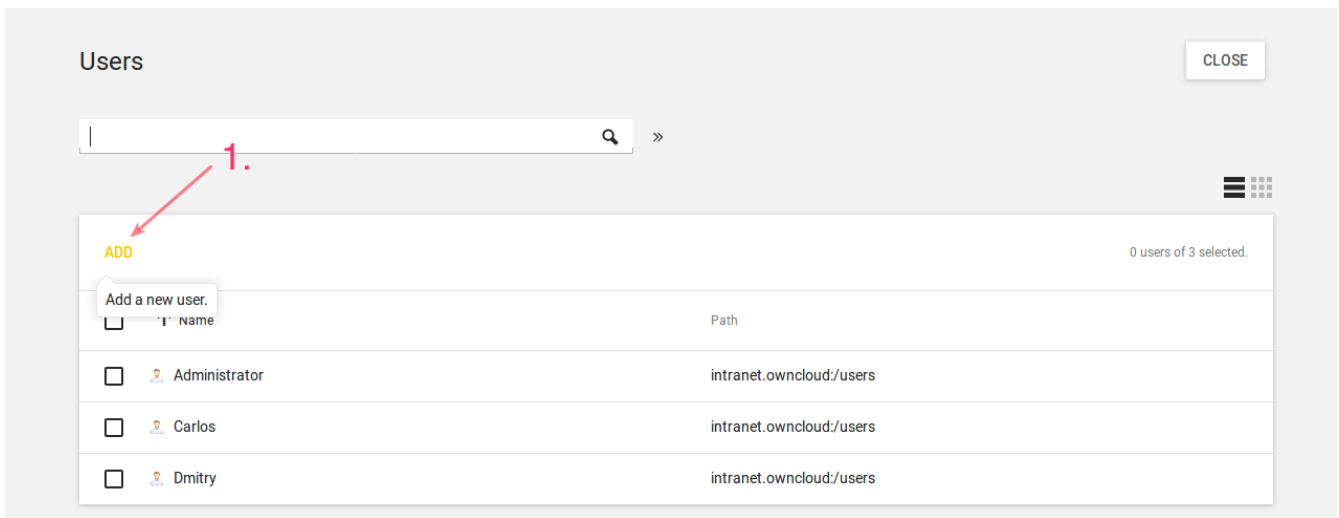
This takes you to the Univention Management Console.

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 *

1.

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. ⓧ

.....

Password * Password (retype) *

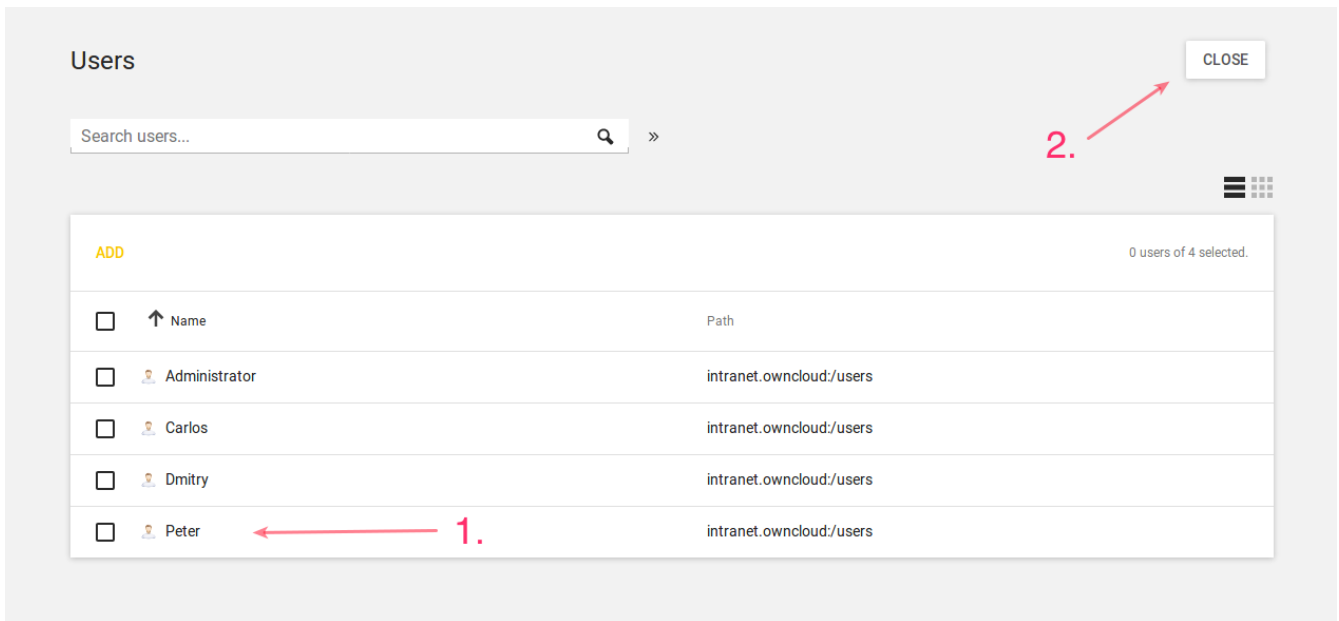
Change password on next login ? 1.

Override password check

Account disabled

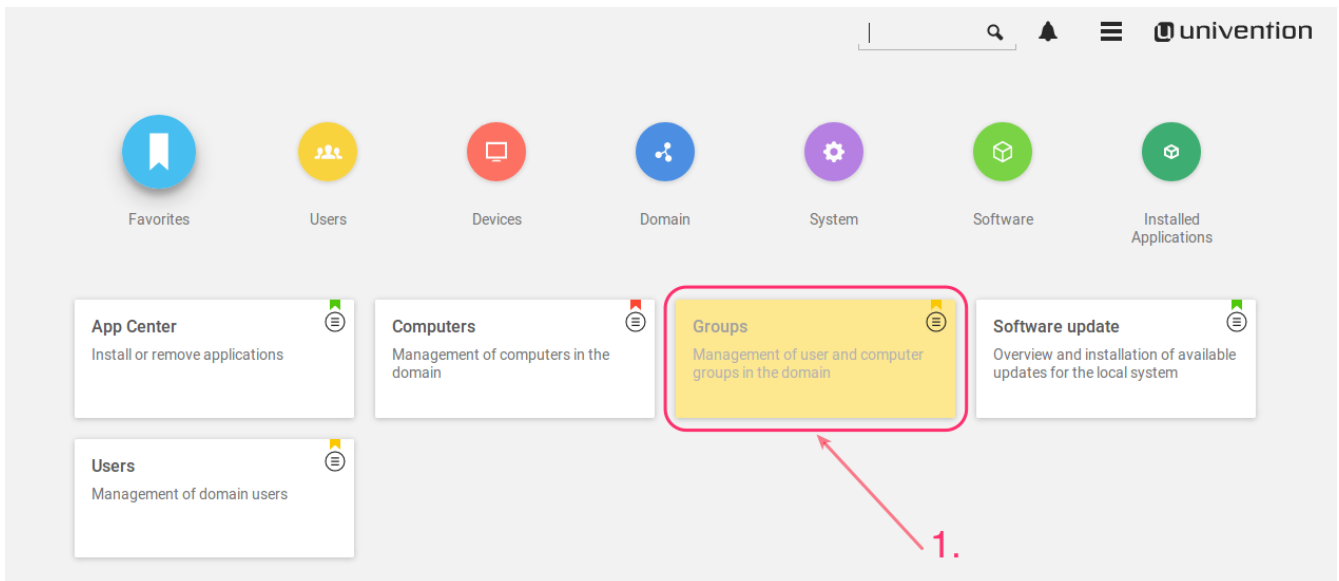
CANCEL ADVANCED BACK 2. **CREATE USER**

The new user will have been created, so click the [**CLOSE**] button, in the top right-hand corner, to go back to "Favorites".

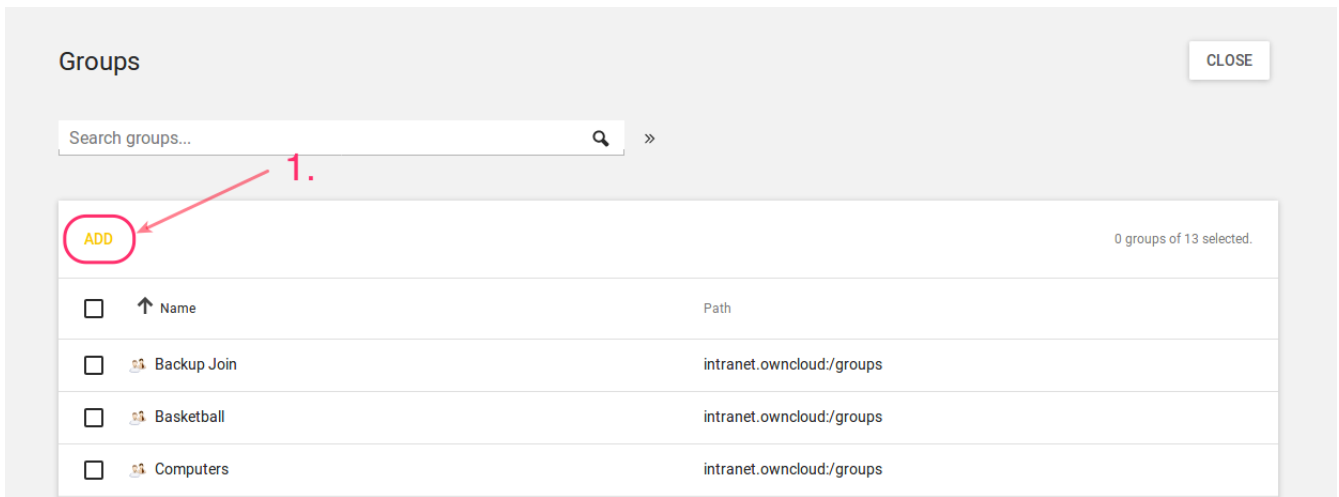


Create the Group

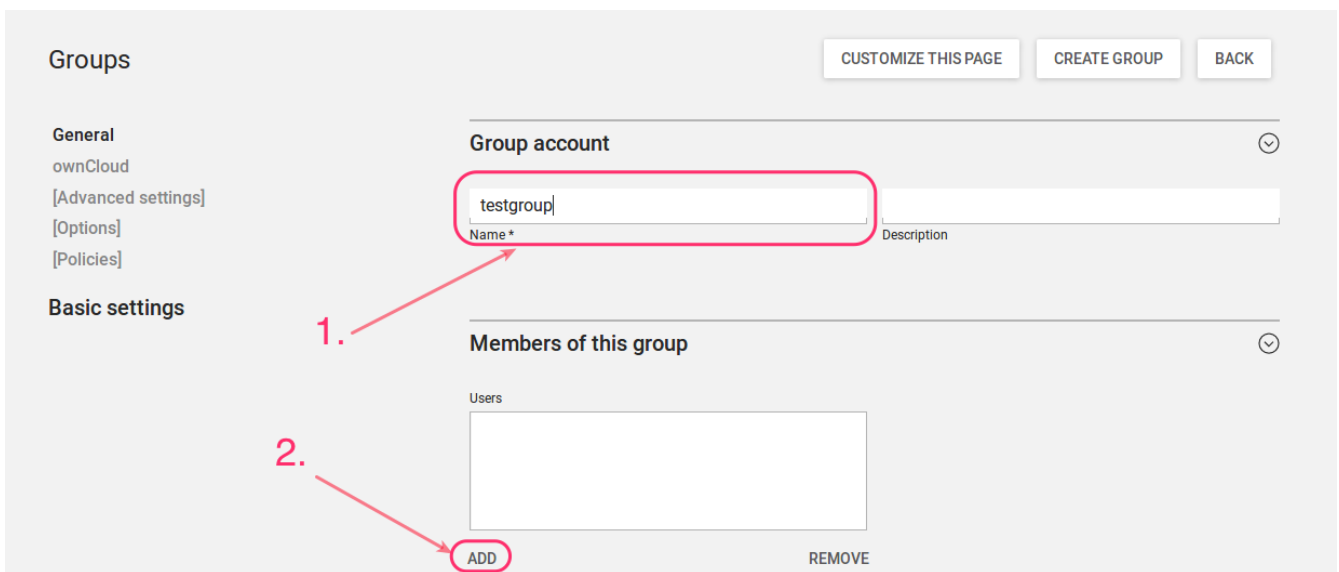
Now it's time to create a new group. Click **[Groups]**, which is located between **"Computers"** and **"Software Update"**.



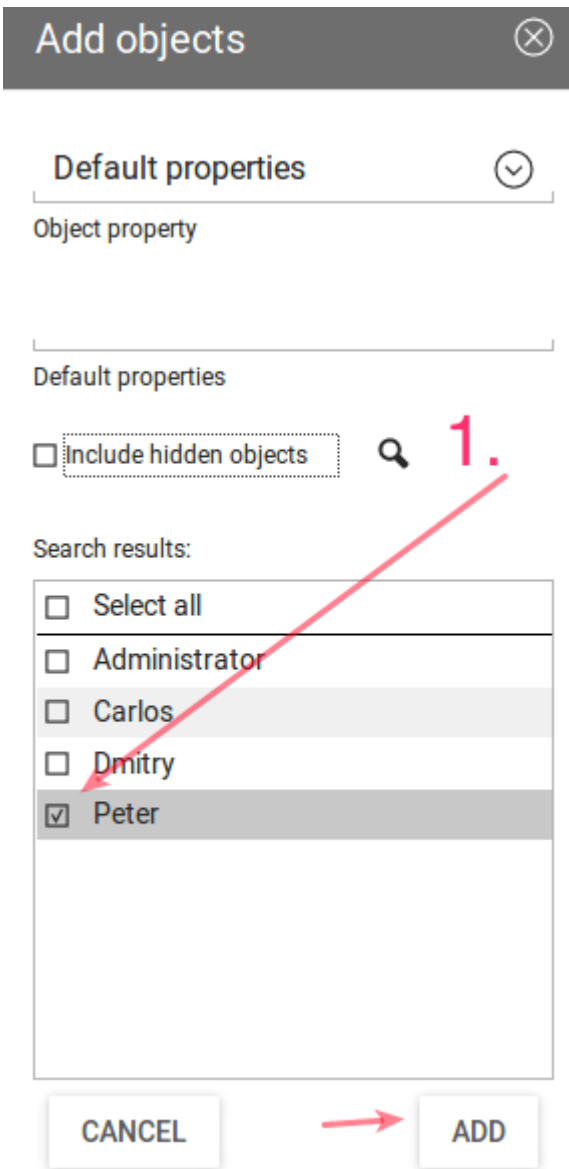
From there, click **[ADD]**, located on the left-hand side of the groups table.



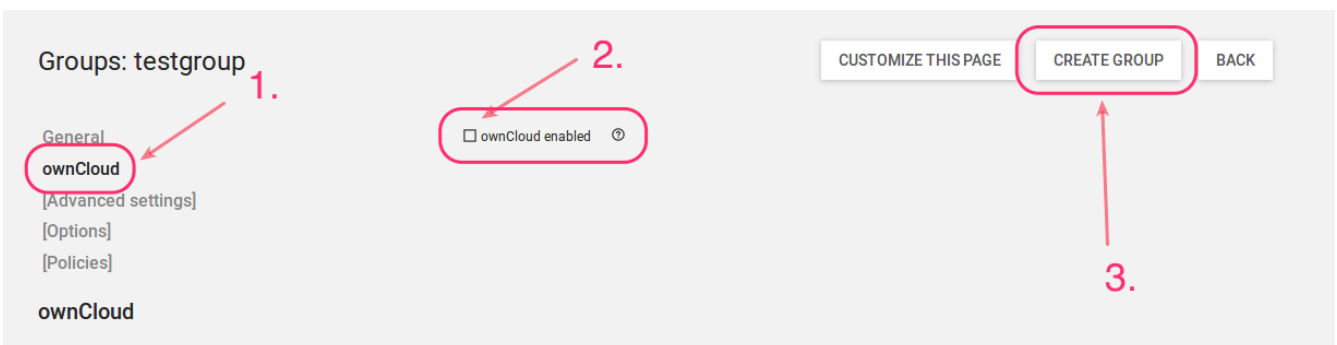
In the next dialog that appears, first enter the name of the group and optionally a description. Then, under "**Members of this group**", click [**ADD**].



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**].



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.

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.

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



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.

Working on Documents in the ownCloud Appliance

Introduction

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.



It is required to open the site with https and the fully qualified domain name. 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.

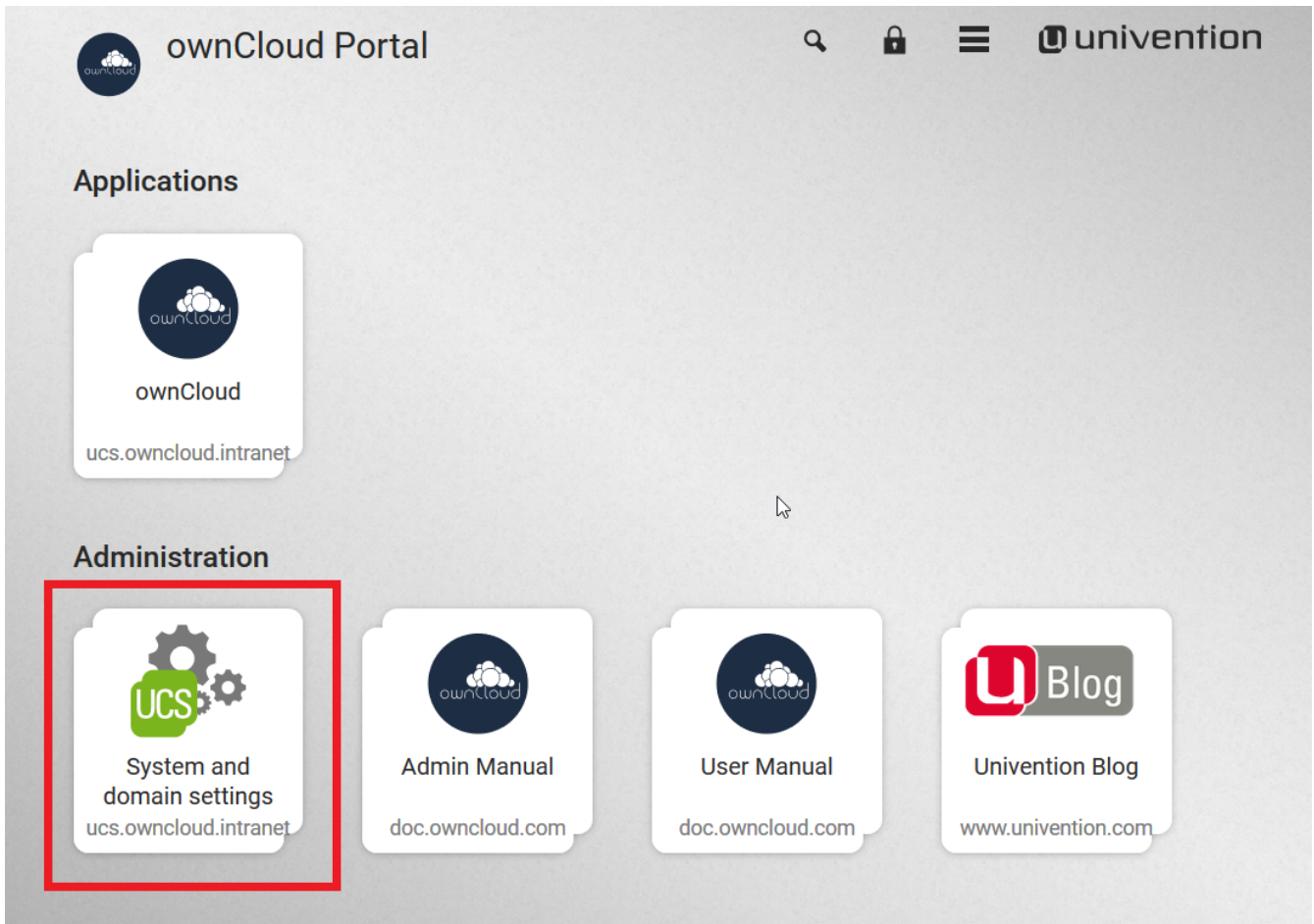
Appcenter

First you have to get to the Appcenter. Here are the steps to do that:

1. Connect to your appliance using the IP address or domain name.

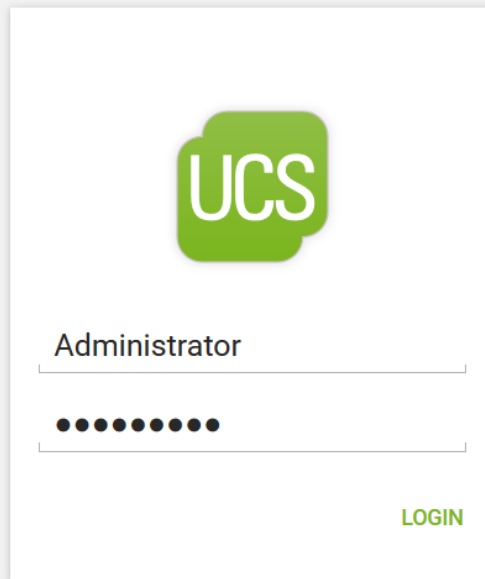
```
https://172.16.40.100  
# or  
https://ucs-2341.CompanyName.com
```

- Login into the management console
 - Click on the [**Domain and System**] settings



- Type in the Administrator as username and the password you set.

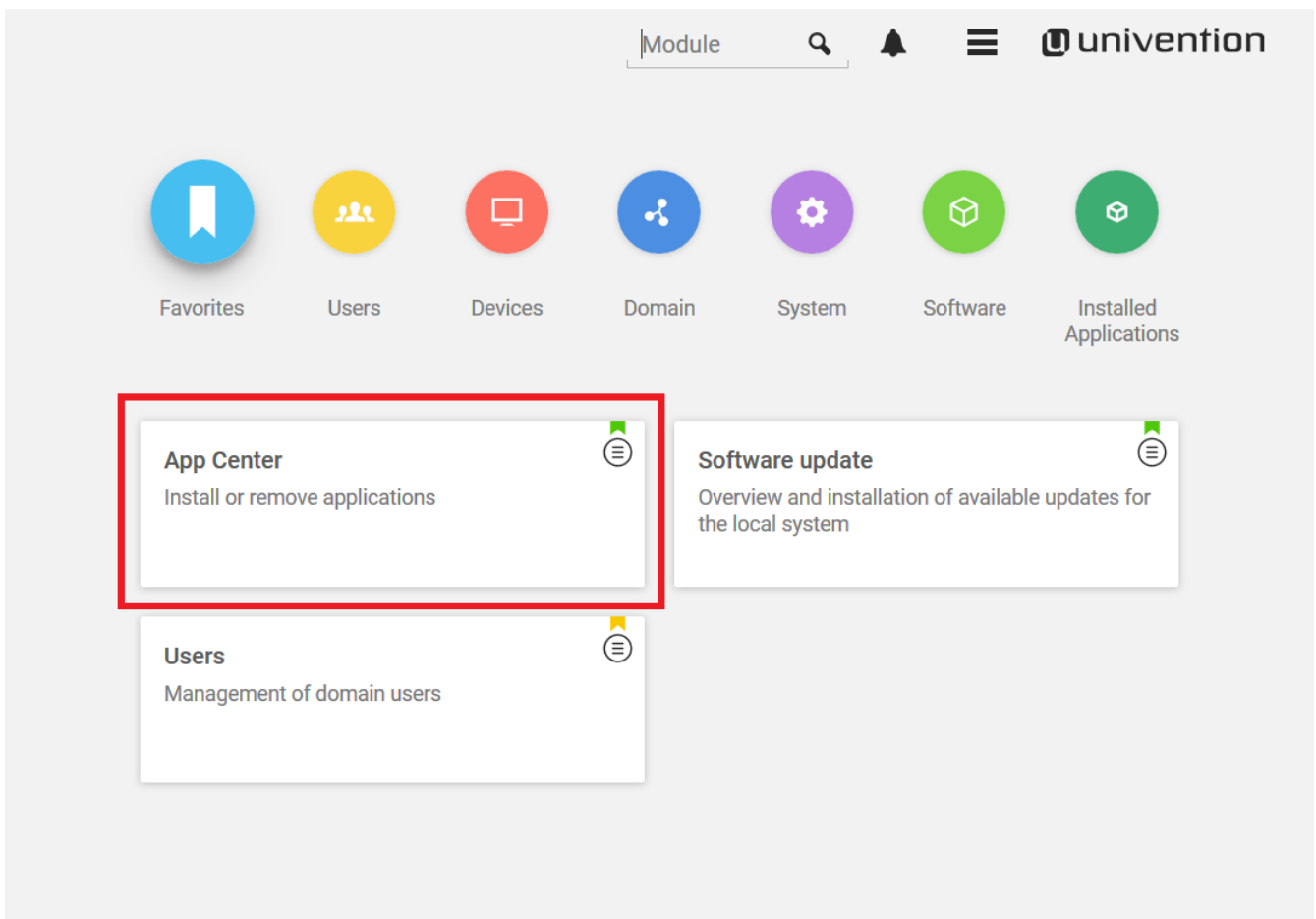
Login at owncloud.intranet



The login form features the UCS logo at the top. Below it, there are two input fields: the first is labeled 'Administrator' and the second contains a series of dots representing a password. A green 'LOGIN' button is positioned at the bottom right of the form.

[How do I login?](#)

- Now you can access the **Appcenter**".



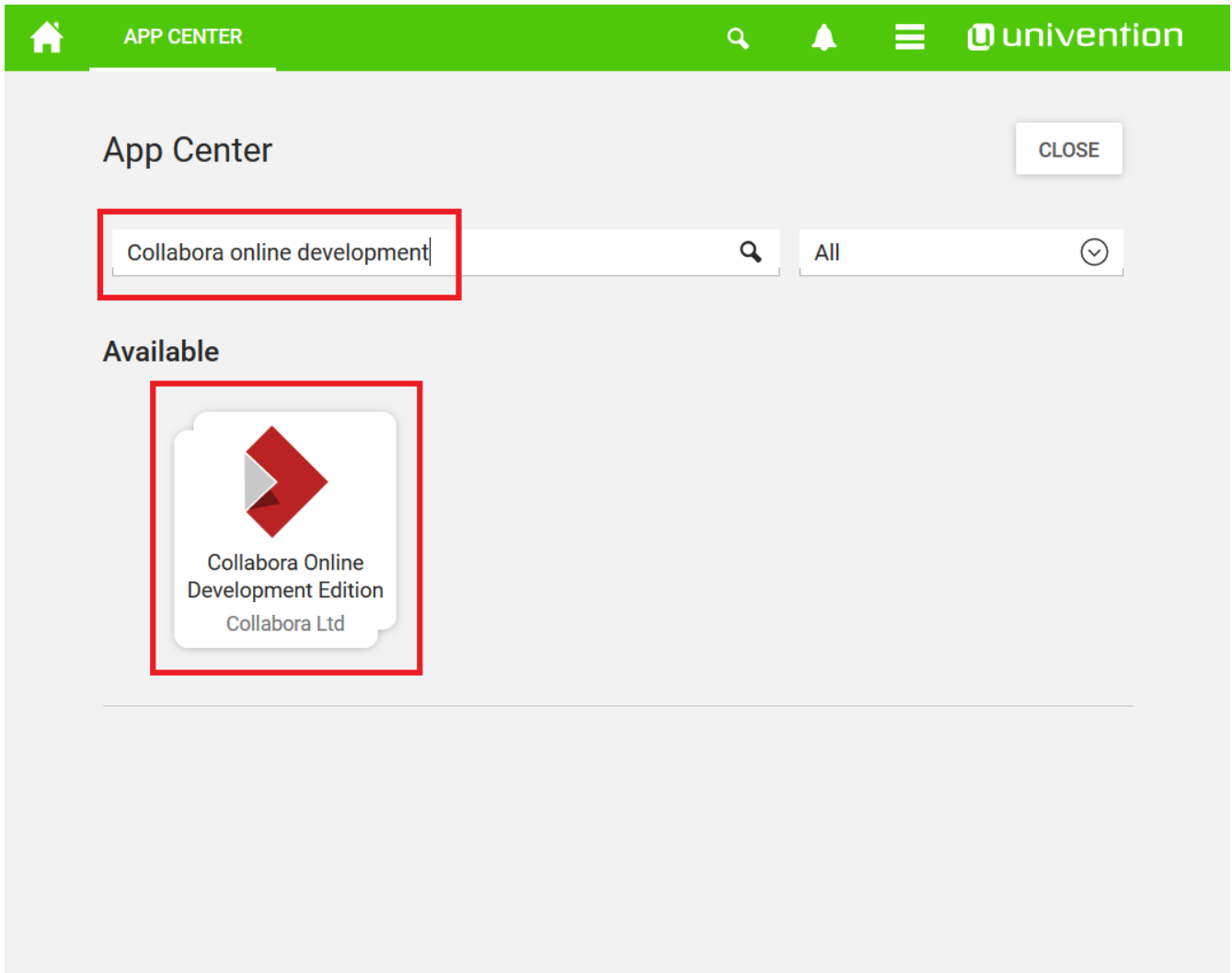
The dashboard includes a top navigation bar with a search bar labeled 'Module', a notification bell, a menu icon, and the 'univention' logo. Below this is a row of seven circular icons representing different modules: Favorites (blue), Users (yellow), Devices (red), Domain (blue), System (purple), Software (green), and Installed Applications (green). The main content area displays three cards: 'App Center' (highlighted with a red border), 'Software update', and 'Users'. Each card has a title, a brief description, and a menu icon in the top right corner.

Module	Description
App Center	Install or remove applications
Software update	Overview and installation of available updates for the local system
Users	Management of domain users

From here on it's your choice to install [Collabora](#) or [OnlyOffice](#).

How to Install Collabora

- Install Collabora in UCS.





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

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) (retry) *

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

- Enable Collabora in ownCloud.



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 WOPISURL 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



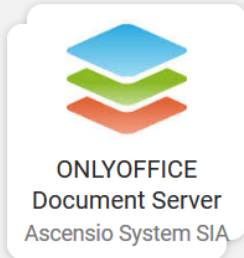
App Center

CLOSE

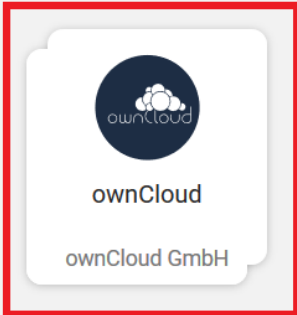
Search applications...

All

Installed



ONLYOFFICE
Document Server
Ascensio System SIA



ownCloud
ownCloud GmbH

Available



ownCloud

PREVIOUS APP NEXT APP BACK TO OVERVIEW



ownCloud GmbH
Installed

OPEN

First steps

Login

The default owncloud-administrator account is:

- Username: owncloud
- Password: owncloud

Install Collabora Online Development Edition app to use Collabora in ownCloud.

Need Help?

In order to learn more about ownCloud on UCS - here is our [documentation](#).

Additional Apps



Username and Password are owncloud

Files ownCloud

- All files
- Favorites
- Shared with you
- Shared with others
- Shared by link
- Tags

Name	Size	M
Documents	35 KB	2
Photos	663 KB	2 hours ago
ownCloud Manual.pdf	4.9 MB	2 hours ago
2 folders and 1 file		5.5 MB

Deleted files

Settings

Settings

Users

Help

Log out

Settings ownCloud

Personal

- General
- Storage
- Security
- Additional

Admin

- Apps
- General
- Storage
- User Authentication
- Encryption
- Sharing
- Help & Tips
- Additional

You are using 5.5 MB of Unlimited

Profile picture

Full name

owncloud

Email

Your email address

For password recovery and notifications

Groups

You are member of the following groups:
admin

Password

Current password New password

Language

English

Federated Cloud

Your Federated Cloud ID: owncloud@ucs-123.owncloud.intranet/owncloud

Share it:

Settings ownCloud

Personal







- General
- Storage
- Security
- Additional

Admin

- Apps
- General
- Storage
- User Authentication
- Encryption
- Sharing
- Help & Tips
- Additional

Apps Management

Show disabled apps

 <p>Admin Config Report 0.1.1 by owncloud.org (AGPL-licensed)</p> <p>Official</p> <p>Show description ...</p> <p>Disable</p>	 <p>Deleted files 0.9.1 by Bjoern Schiessle (AGPL-licensed)</p> <p>Official</p> <p>Show description ...</p> <p>Disable</p>
 <p>Federation 0.1.0 by Bjoern Schiessle (AGPL-licensed)</p> <p>Official</p> <p>Show description ...</p> <p>Disable</p>	 <p>Provisioning API 0.5.0 by Tom Needham (AGPL-licensed)</p> <p>Official</p> <p>Show description ...</p> <p>Disable</p>
 <p>Share Files 0.10.1 by Michael Gapczynski, Bjoern Schiessle (AGPL-licensed)</p>	 <p>Versions 1.3.0 by Frank Karlitschek, Bjoern Schiessle (AGPL-licensed)</p>

Settings ownCloud

Personal







- General
- Storage
- Security
- Additional

Admin

- Apps
- General
- Storage
- User Authentication
- Encryption
- Sharing
- Help & Tips
- Additional

Apps Management

Show enabled apps

 <p>Default encryption module 1.3.1 by Bjoern Schiessle, Clark Tomlinson (AGPL-licensed)</p> <p>Official</p> <p>Show description ...</p> <p>Enable</p>	 <p>Update notification 0.2.1 by Lukas Reschke (AGPL-licensed)</p> <p>Official</p> <p>Show description ...</p> <p>Enable</p>
 <p>Collabora Online 2.0.5 by Collabora Productivity based on work of Frank Karlitschek, Victor Dubiniuk (AGPL-licensed)</p> <p>Approved</p> <p>Show description ...</p> <p>Enable Uninstall App</p>	 <p>Example ownCloud Theme 1.0.0 by Philipp Schaffrath (AGPL-licensed)</p> <p>Approved</p> <p>Show description ...</p> <p>Enable Uninstall App</p>
 <p>External Sites 1.2</p>	 <p>External user support</p>

Files ownCloud

Files Office Market

Shared with you
Shared with others
Shared by link
Tags

Name	Size	Modified
Documents	35 KB	39 minutes ago
Photos	663 KB	39 minutes ago
ownCloud Manual.pdf	4.9 MB	39 minutes ago
2 folders and 1 file		5.5 MB

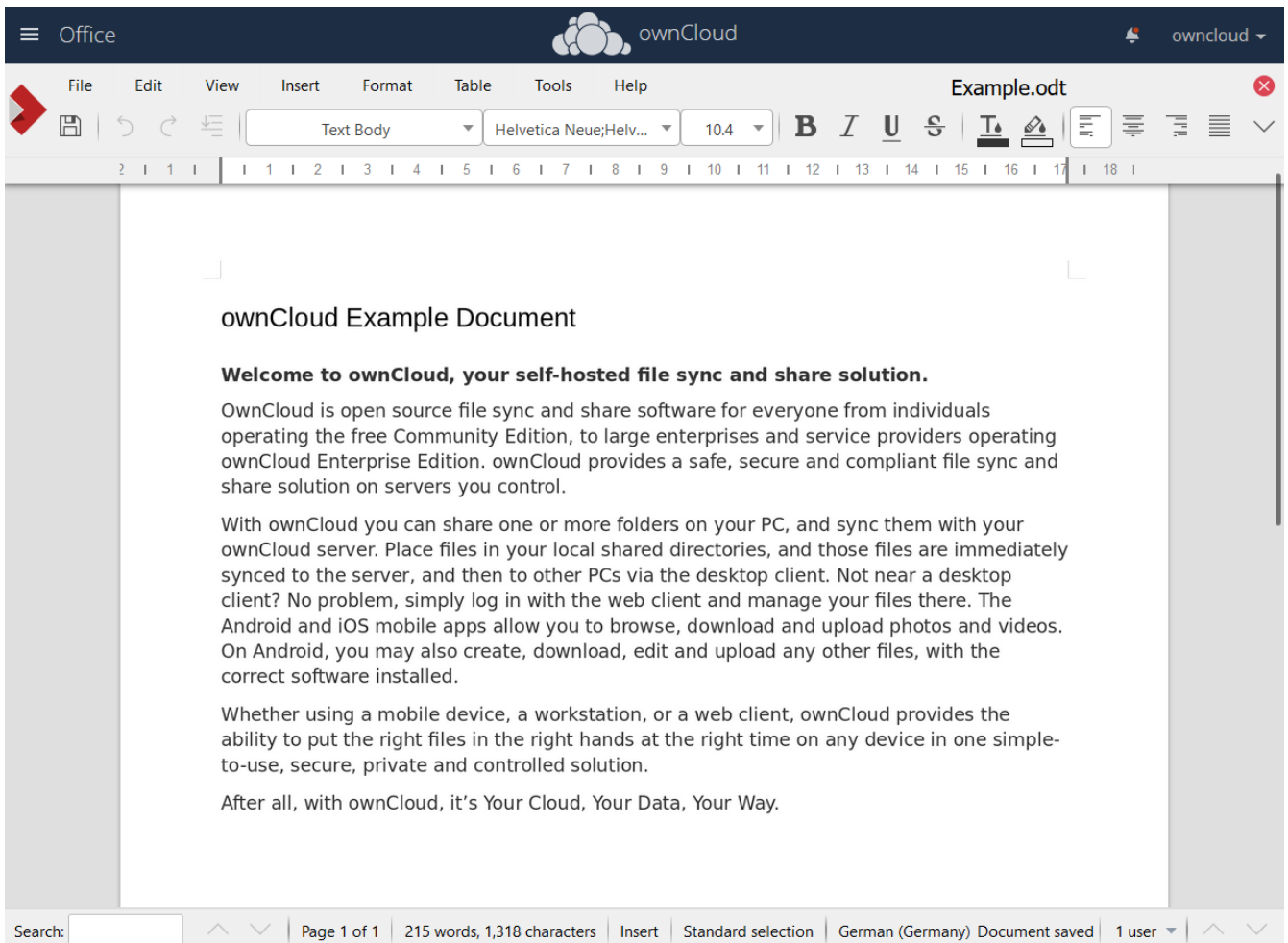
Deleted files
Settings

172.42.16.155/owncloud/index.php/apps/richdocuments/index

Office ownCloud

+ New Document
+ New Spreadsheet
+ New Presentation
Upload

Example.odt



Now you can use Collabora within ownCloud. Start by creating a new Document.

How to Install OnlyOffice

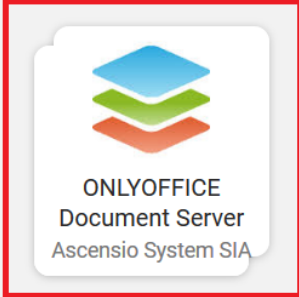
- Search for "OnlyOffice" or select it from the application list in the Appcenter.

APP CENTER univention

App Center CLOSE

onlyoffice All

Available




ONLYOFFICE
Document Server
Ascensio System SIA

- Install 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

ONLYOFFICE Document Server

CANCEL INSTALLATION

Installation of ONLYOFFICE Document Server

Please confirm to install the application ONLYOFFICE Document Server on this host.

CANCEL


INSTALL

After the installation is complete, return to the Appcenter overview

ONLYOFFICE DOCUMENT SERVER

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. Please 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 perspective of the user browser.

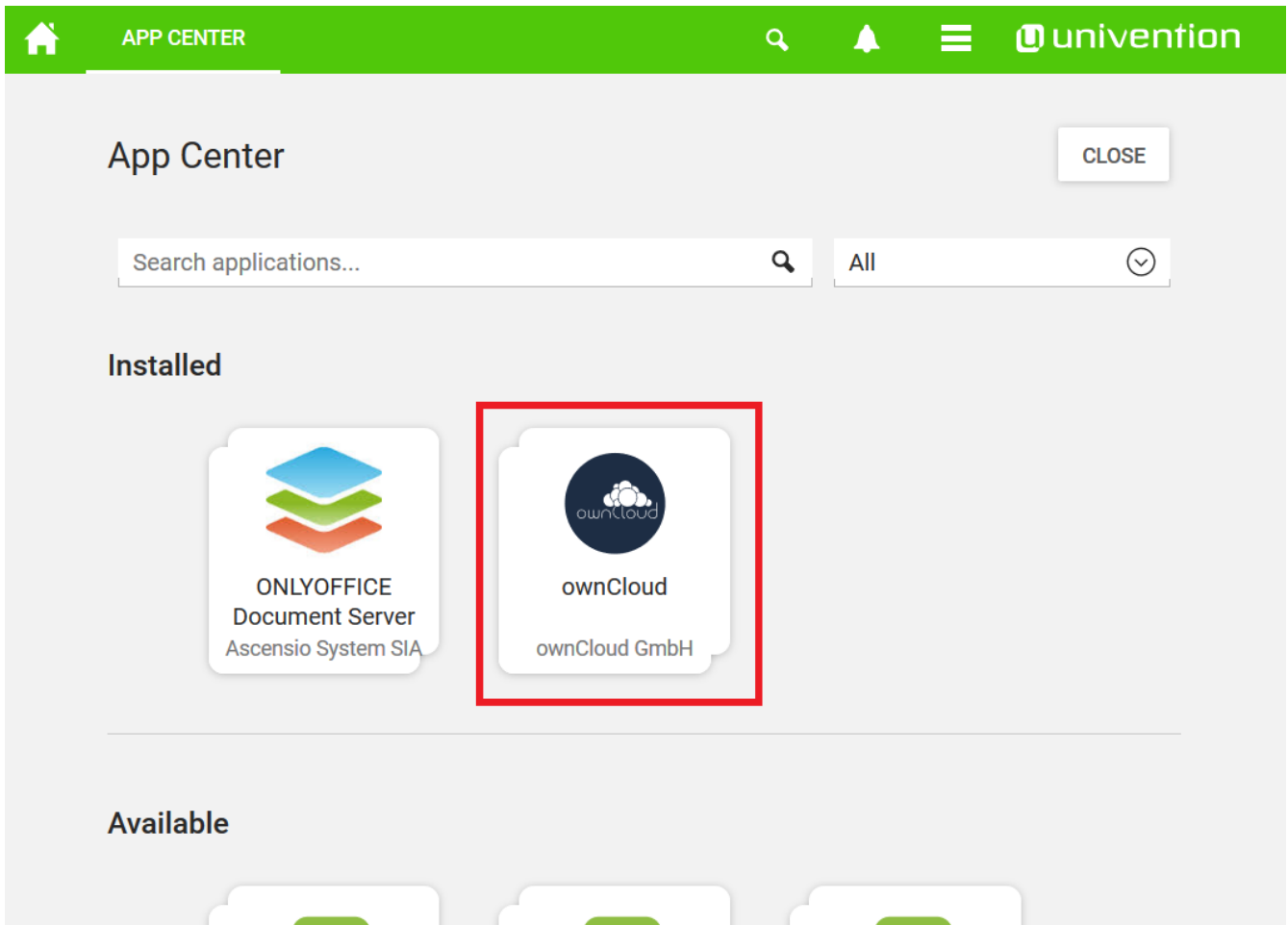
Configuration of ONLYOFFICE plugin in Nextcloud

- 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*

- Install the ownCloud OnlyOffice connector App
 - Go to ownCloud



ownCloud

PREVIOUS APP NEXT APP BACK TO OVERVIEW



ownCloud GmbH
Installed

OPEN

First steps

Login

The default owncloud-administrator account is:

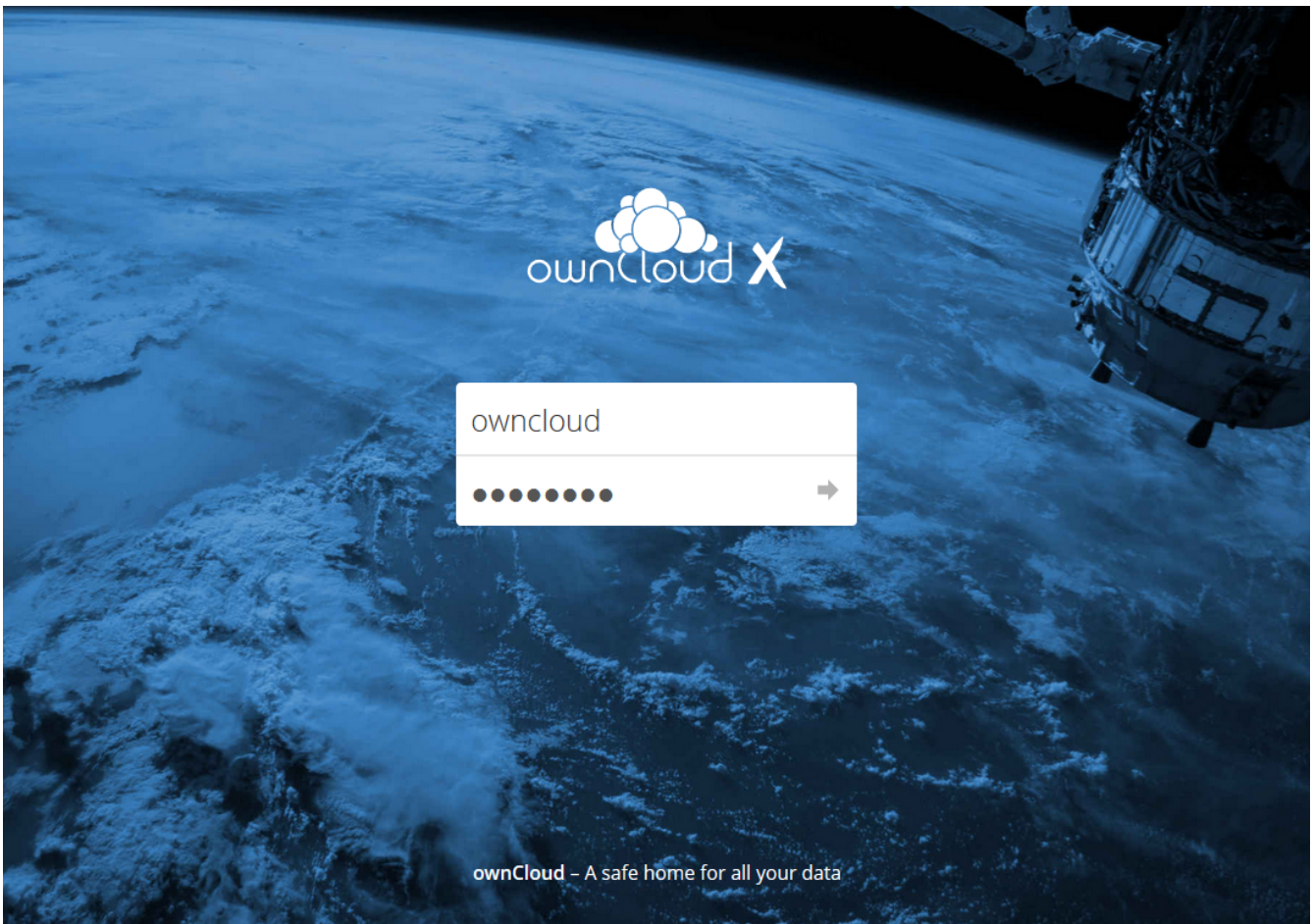
- Username: owncloud
- Password: owncloud

Install Collabora Online Development Edition app to use Collabora in ownCloud.

Need Help?

In order to learn more about ownCloud on UCS - here is our [documentation](#).

Additional Apps



Username and Password are owncloud

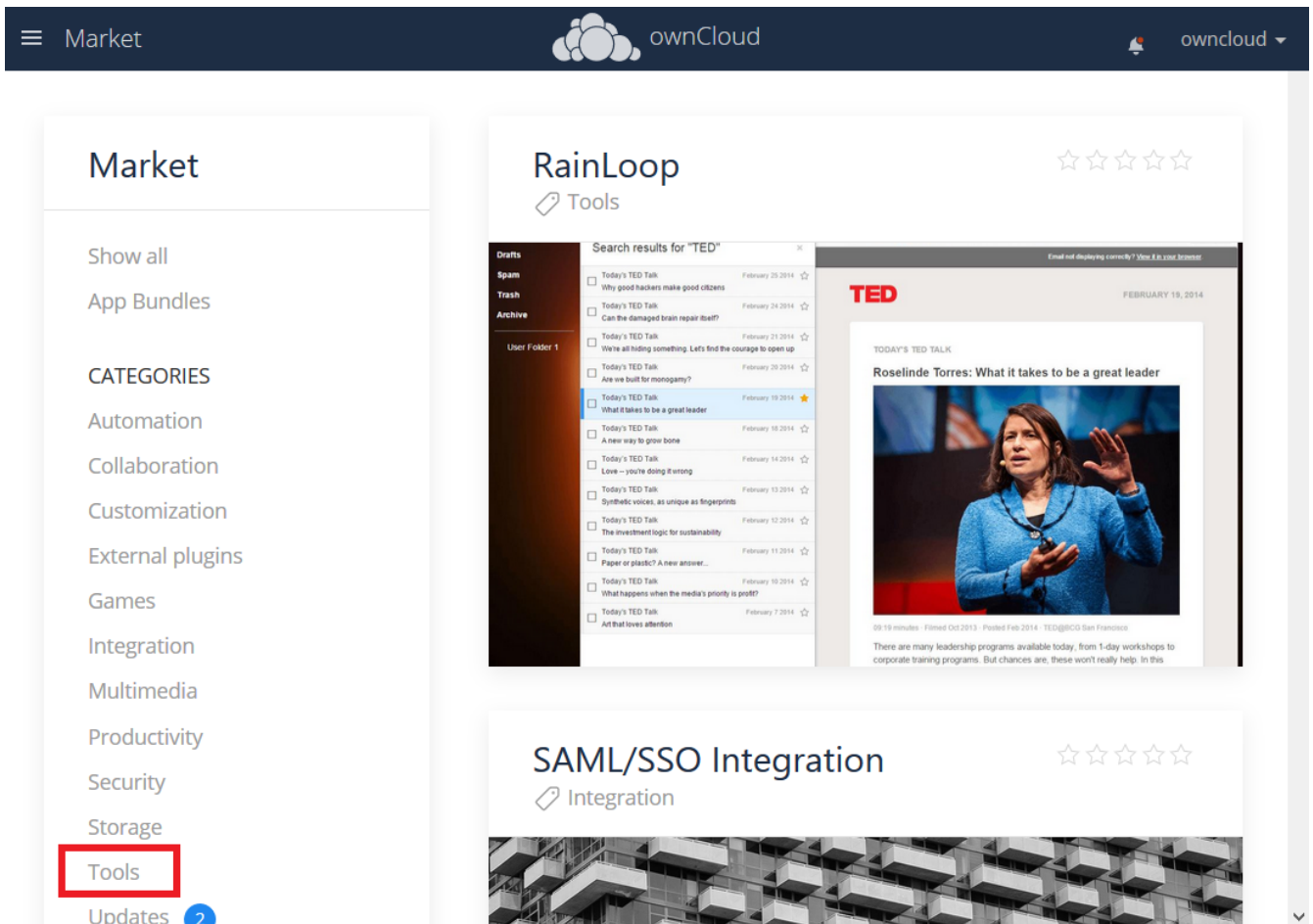
• Market

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

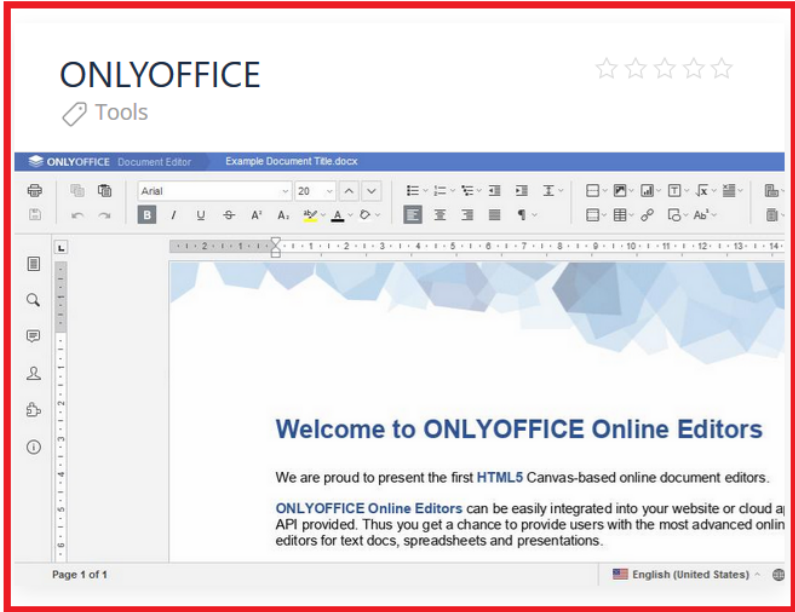
Name	Size	Modified
Documents	35 KB	in 2 hours
Photos	663 KB	in 2 hours
ownCloud Manual.pdf	4.9 MB	in 2 hours
2 folders and 1 file		5.5 MB

<https://ucs.owncloud.intranet/owncloud/index.php/apps/market/>

- Tools



- Install OnlyOffice



ONLYOFFICE Tools

☆☆☆☆

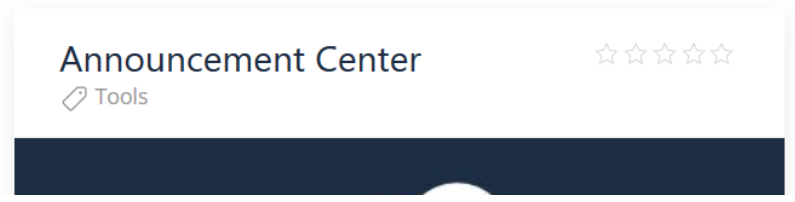
ONLYOFFICE Document Editor Example Document Title.docx

Welcome to ONLYOFFICE Online Editors

We are proud to present the first HTML5 Canvas-based online document editors.

ONLYOFFICE Online Editors can be easily integrated into your website or cloud application via API provided. Thus you get a chance to provide users with the most advanced online editors for text docs, spreadsheets and presentations.

Page 1 of 1 English (United States)

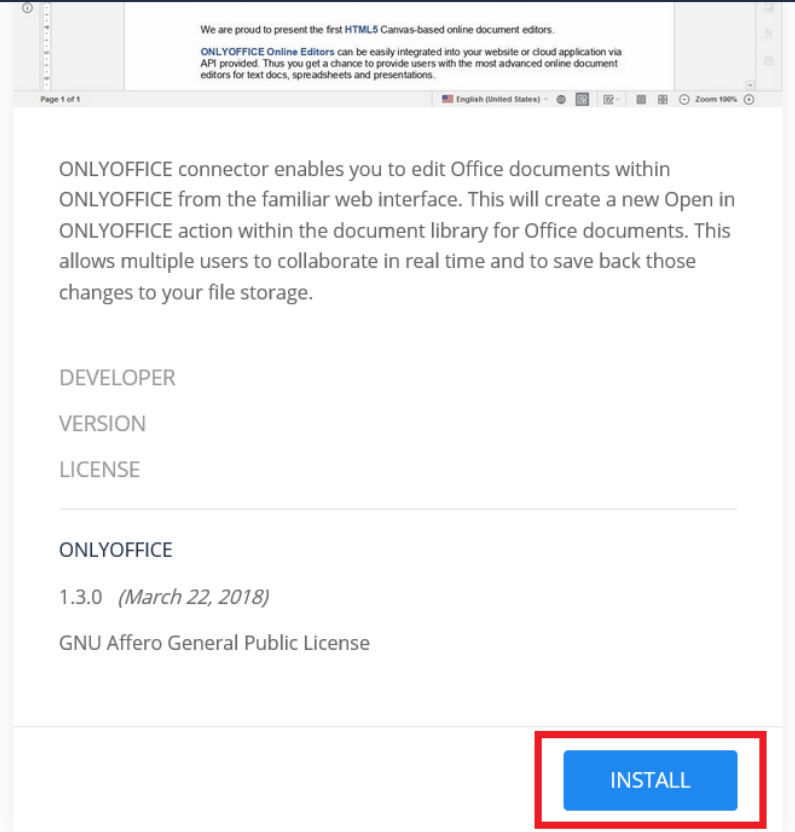


Announcement Center Tools

☆☆☆☆

- Collaboration
- Customization
- External plugins
- Games
- Integration
- Multimedia
- Productivity
- Security
- Storage
- Tools
- Updates **2**
- SETTINGS
- Add API Key

START ENTERPRISE TRIAL



ONLYOFFICE connector enables you to edit Office documents within ONLYOFFICE from the familiar web interface. This will create a new Open in ONLYOFFICE action within the document library for Office documents. This allows multiple users to collaborate in real time and to save back those changes to your file storage.

DEVELOPER

VERSION

LICENSE


ONLYOFFICE

1.3.0 (March 22, 2018)

GNU Affero General Public License

INSTALL

- Go to the OnlyOffice settings inside ownCloud.

Market  owncloud

- Collaboration
- Customization
- External plugins
- Games
- Integration
- Multimedia
- Productivity
- Security
- Storage
- Tools
- Updates 2

SETTINGS
Add API Key

[START ENTERPRISE TRIAL](#)

We are proud to present the first HTML5 Canvas-based online document editors.
ONLYOFFICE Online Editors can be easily integrated into your website or cloud application via API provided. Thus you get a chance to provide users with the most advanced online document editors for text docs, spreadsheets and presentations.

Page 1 of 1 English (United States) Zoom 100%

ONLYOFFICE connector enables you to edit Office documents within ONLYOFFICE from the familiar web interface. This will create a new Open in ONLYOFFICE action within the document library for Office documents. This allows multiple users to collaborate in real time and to save back those changes to your file storage.

DEVELOPER

VERSION

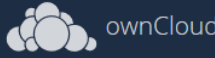
LICENSE

ONLYOFFICE

1.3.0 (March 27, 2018)

agpl

[UNINSTALL](#)

Market  owncloud

- Collaboration
- Customization
- External plugins
- Games
- Integration
- Multimedia
- Productivity
- Security
- Storage
- Tools
- Updates 2

SETTINGS
Add API Key

[START ENTERPRISE TRIAL](#)

We are proud to present the first HTML5 Canvas-based online document editors.
ONLYOFFICE Online Editors can be easily integrated into your website or cloud application via API provided. Thus you get a chance to provide users with the most advanced online document editors for text docs, spreadsheets and presentations.

Page 1 of 1 English (United States) Zoom 100%

ONLYOFFICE connector enables you to edit Office documents within ONLYOFFICE from the familiar web interface. This will create a new Open in ONLYOFFICE action within the document library for Office documents. This allows multiple users to collaborate in real time and to save back those changes to your file storage.

DEVELOPER

VERSION

LICENSE

ONLYOFFICE

1.3.0 (March 27, 2018)

agpl

[UNINSTALL](#)

- Settings**
- Users
- Help
- Log out

<https://ucs.owncloud.intranet/owncloud/index.php/settings/personal>

The screenshot shows the ownCloud Admin 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" followed by a notification bell icon and "owncloud" with a dropdown arrow. Below the header is a left sidebar with two 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 is titled "You are using 5.5 MB of Unlimited". It contains several sections: "Profile picture" with a large teal 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; "Groups" with the text "You are member of the following groups: admin"; "Password" with two text input fields labeled "Current password" and "New password" (with an eye icon) and a "Change password" button; and "Language" with a dropdown menu set to "English" and a "Help translate" link. At the bottom left, the URL "https://ucs.owncloud.intranet/owncloud/index.php/settings/admin?sectionid=general" is visible.

- Enter the OnlyOffice server address in the following format and **save** it:

`https://<your-domain-name>/onlyoffice-documentserver/`

The screenshot shows the ownCloud settings interface. The browser address bar at the top displays `https://ucs.owncloud.intranet/owncloud/index.php`. The left sidebar contains navigation menus for 'Personal' (General, Storage, Security, Additional) and 'Admin' (Apps, General, Storage, User Authentication, Encryption, Sharing, Help & Tips). The main content area is titled 'ONLYOFFICE' and includes a description of the Document Service Location. A red box highlights the 'Document Editing Service address' input field, which contains the text `:loud.intranet/onlyoffice-documentserver`. Below this is the 'Advanced server settings' section with a checkbox for 'Open file in the same tab' and a list of file formats: docx, xlsx, pptx, ppsx, txt, and csv. A red box highlights the 'Save' button. At the bottom, the 'Email server' section is partially visible, showing a 'Send mode' dropdown set to 'php'.

- Now you can create a new document by clicking on the **[Plus]** button.

Files ownCloud

- All files
- Favorites
- Shared with you
- Shared with others
- Shared by link
- Tags

Deleted files

Settings

2 folders and 1 file

35 KB in 2 hours

663 KB in 2 hours

4.9 MB in 2 hours

5.5 MB

annual.pdf

+

- Upload
- Folder
- Document
- Spreadsheet
- Presentation

<https://ucs.owncloud.intranet/owncloud/index.php/apps/files/?dir=/&fileid=9#>

Apps ownCloud

ONLYOFFICE Document Editor mynewtest.docx Go to Documents

Arial 11

B / U / A^2 / A_2 / ab^2 / A^2 / A_2

Welcome to OnlyOffice

Line Spacing: Multiple 1.15

Paragraph Spacing: Before 0 cm, After 0.35 cm

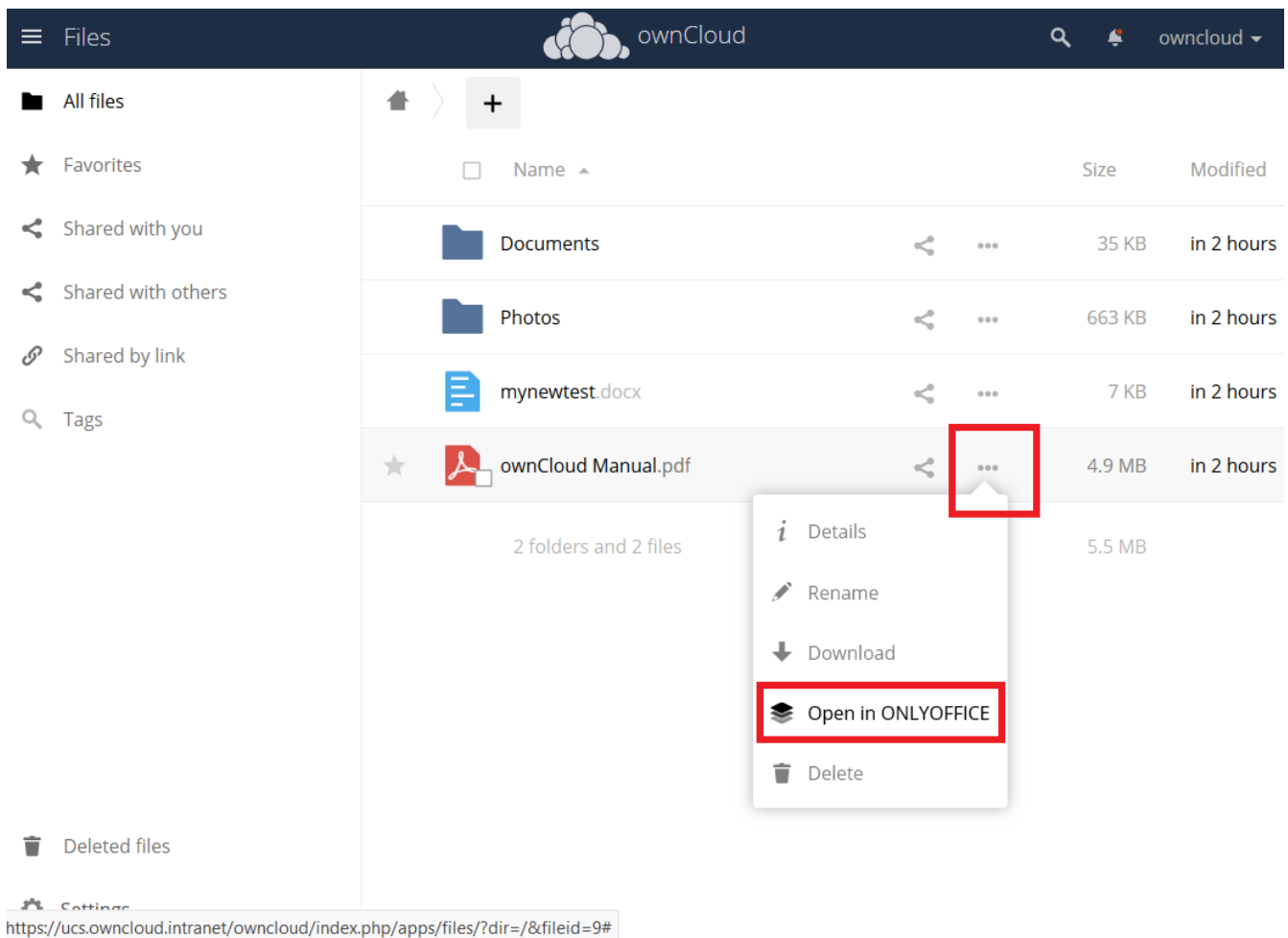
Don't add interval between paragraphs of the same style

Background color

Show advanced settings

Page 1 of 1 All changes saved English (United States) Zoom 100%

PDF documents can also be viewed in OnlyOffice



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

ONLYOFFICE Enterprise Edition

If you purchased the ONLYOFFICE Enterprise Edition and received the `license.lic` file, you need to import it:

```
/var/lib/univention-appcenter/apps/onlyoffice-ie/Data/license.lic
```

Now your ONLYOFFICE instance is registered and you have access to the enterprise features.

Additional information can be found in the [ONLYOFFICE Documentation](#)

Troubleshooting

If you are not able to open documents: Check the defined Collabora Online Server in your ownCloud settings by navigating to (Settings > Admin > Additional > Collabora-Online) and make sure that the server address is configured correctly. It should be configured with the domain name of your appliance. If you find localhost:port being configured, remove it and replace it with the domain name of your appliance without any port.

WND in the Appliance

Introduction

Here are the steps to configure WND in the Appliance.



Windows Network Drive is available only in the Enterprise Edition of ownCloud.



You will need both of the following described steps for each share.



The steps need to be done in / on the docker host (appliance virtual machine) and not inside the docker container

WND Listener

Create a service following the instructions below that checks the share for changes:

- For each WND mount point distinguished by a SERVER - SHARE pair,
 - place one copy of a file with following content under `/etc/systemd/system/owncloud-wnd-listen-SERVER-SHARE.service`
 - replacing the all upper case words `SERVER`, `SHARE`, `USER` and `PASSWORD`
 - in both, the **filename** and in the **contents** below with their respective values.Take care to also adjust the paths in `WorkingDirectory` and `ExecStart` according to your installation.

```
[Unit]
Description=ownCloud WND Listener for SERVER SHARE
After=docker.service
Requires=docker.service
[Service]
User=root
Group=root
WorkingDirectory=/root
ExecStart=/usr/bin/univention-app shell owncloud occ wnd:listen -vvv SERVER
SHARE USER PASSWORD
Type=simple
StandardOutput=journal
StandardError=journal
SyslogIdentifier=%n
```



```
KillMode=process
RestartSec=1
Restart=always
[Install]
WantedBy=multi-user.target
```

- Run once for each created file the following commands:

```
sudo systemctl enable owncloud-wnd-listen-SERVER-SHARE.service
sudo systemctl start owncloud-wnd-listen-SERVER-SHARE.service
```

WND Process Queue

Create or add a `crontab` file in `/etc/cron.d/oc-wnd-process-queue`.

- Make a `crontab` entry to run a script iterating over all `SERVER SHARE` pairs with an appropriate `occ wnd:process-queue` command. The commands must be **strictly sequential**. This can be done by using `flock -n` and tuning the `-c` parameter of `occ wnd:process-queue`

```
0 */15 * * * root /usr/bin/univention-app shell owncloud occ wnd:process-queue
-vvv SERVER SHARE
```

Further Reading

Please see also:

- [The ownCloud forum](#) and the
- [Windows Network Drive Configuration](#) documentation.

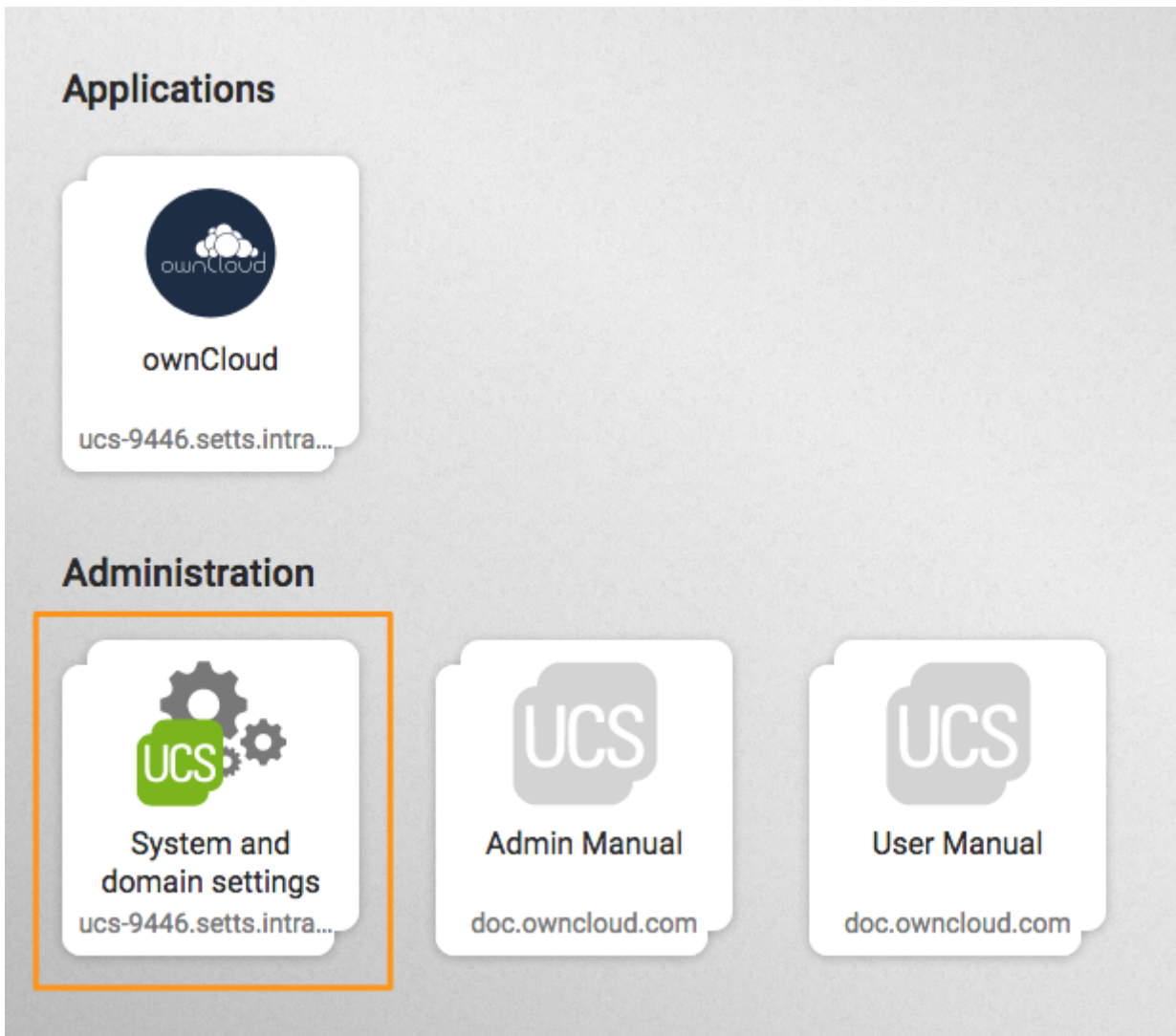
Install Antivirus Software in the ownCloud Appliance

Introduction

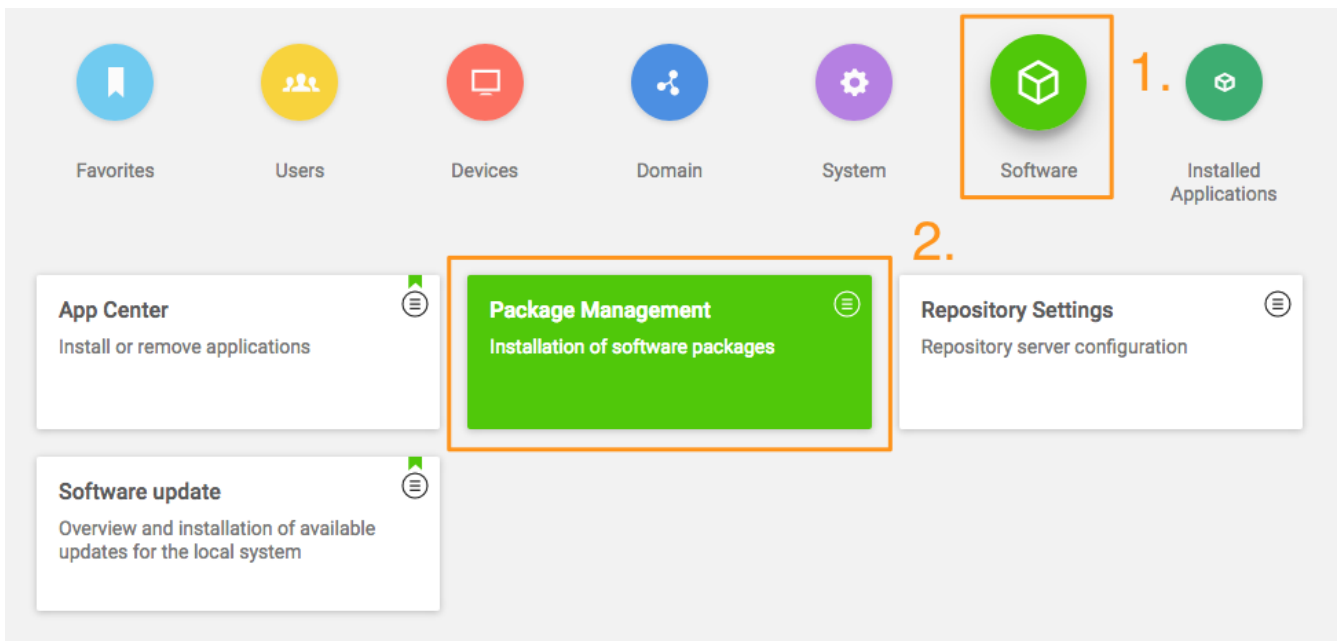
This guide details how to enable a virus scanner in the ownCloud Appliance.

Install ClamAV and Related Components

First, start the appliance and go to "**System and domain settings**".



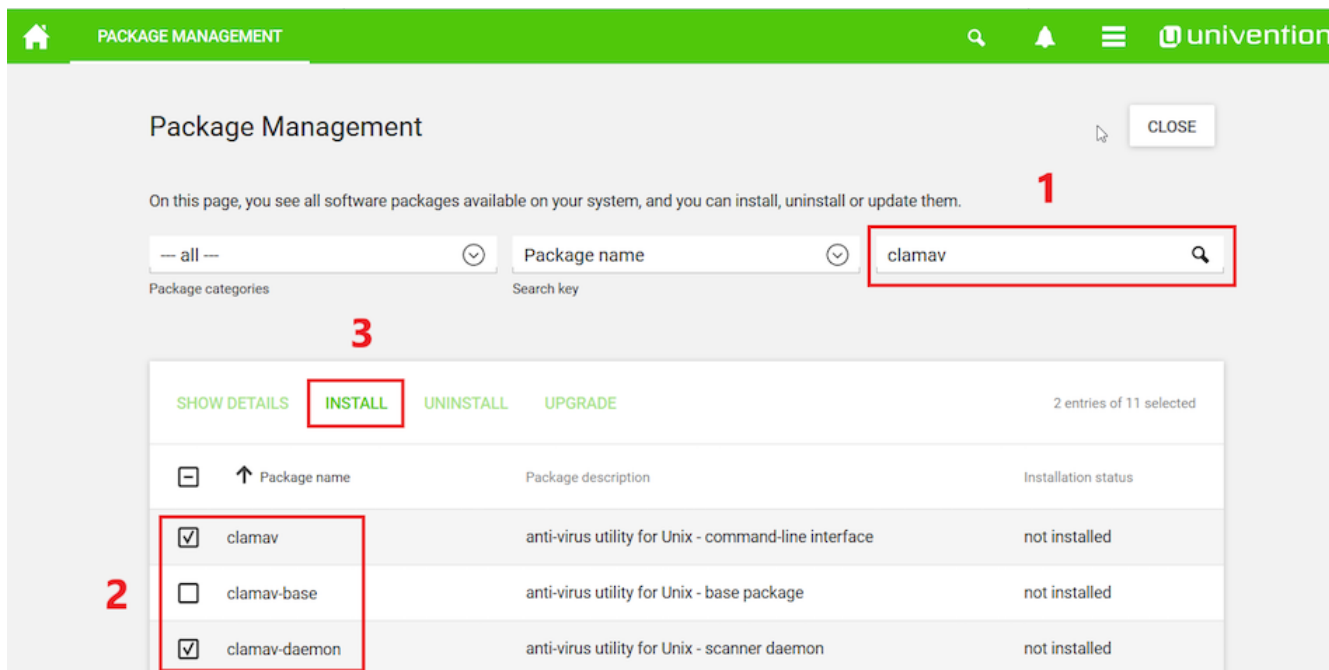
When there, log in with the administrator account. After you have done that, click [**Software**] and open "**Package Management**", as in the screenshot below.



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".



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**].

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

The installation should only take a few minutes.

Configure ownCloud to Use ClamAV

Start the ClamAV service:

```
systemctl enable clamav-daemon.service
systemctl start clamav-daemon.service
```

Next you need to configure ClamAV in your ownCloud instance. Please refer to the [ClamAV documentation](#) for instructions on how to do that.

Troubleshooting

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:

```
# 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 and gently end the `freshclam` process with this command:

```
sudo kill -15 -x freshclam
```

Start the refresh process again with this command:

```
sudo freshclam
```



When the app is enabled — but is not configured or has an incorrect configuration — it will reject **all** uploads for the entire instance. To avoid this situation, make sure the ClamAV service is running and you have the execution mode correctly

configured in ownCloud.

Configure index.php-less URLs

Introduction

If you want URLs without the trailing "index.php", e.g., <https://example.com/apps/files/> instead of <https://example.com/index.php/apps/files/>, you can enable it by following these steps:

Prerequisites:

Log in to the Docker container running ownCloud, and execute the following command on the host system of the appliance:

```
univention-app shell owncloud
```

Your web server needs to have the following modules enabled: `mod_rewrite` and `mod_env`. If you have not yet enabled these modules, or are not sure if you have, execute these commands:

```
a2enmod env rewrite
```

You need an `owncloud.conf` in your `/etc/apache2/sites-available/` directory.

Open `/etc/apache2/sites-available/owncloud.conf` in nano, Vim, or your editor of choice, and paste the following:

```
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`, as follows:

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

Enable index.php-less URLs

Adjust your config.php to look like the following:

```
'overwrite.cli.url' => 'https://example.com/owncloud',  
'htaccess.RewriteBase' => '/owncloud',
```

Execute the command:

```
sudo -u www-data ./occ maintenance:update:htaccess
```

Restart or reload your Apache server, by running the following command:

```
service apache2 reload
```

Now you should have index.php-less URLs.

Unresolved directive in modules/admin_manual/pages/appliance/maintenance/index.adoc -
include::partial\$section_page.adoc[]

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
```

How to Update ownCloud

Introduction

This page shows how to update an ownCloud installation hosted on an ownCloud X Appliance:



Do not use ownCloud's built-in Web Updater!

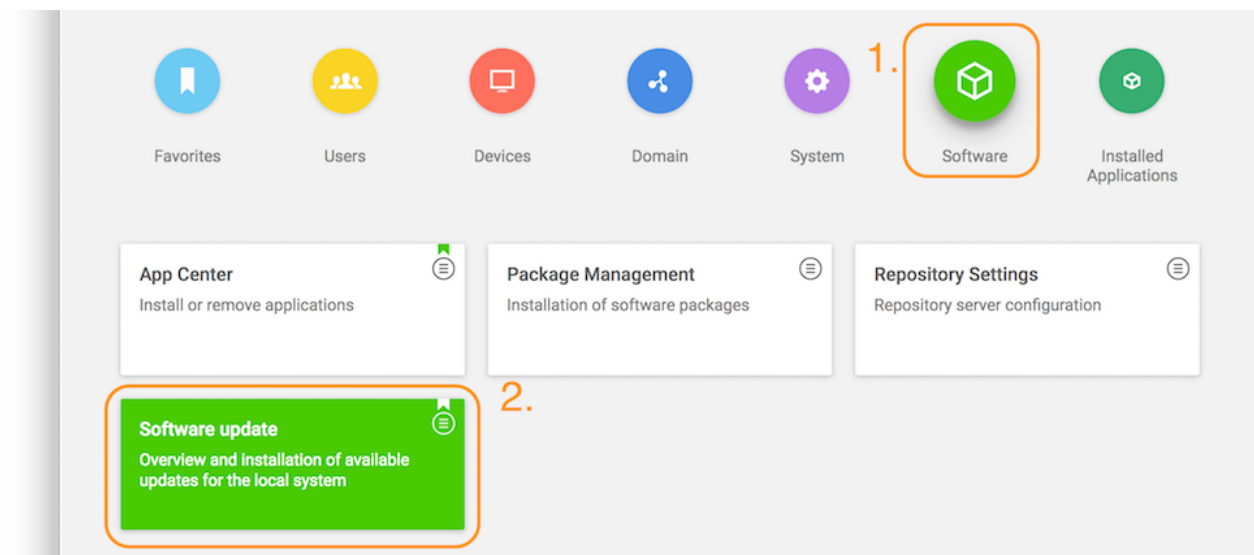
Use the Univention Management Console

Using the Univention Management Console, there are two paths to upgrade an existing ownCloud installation:

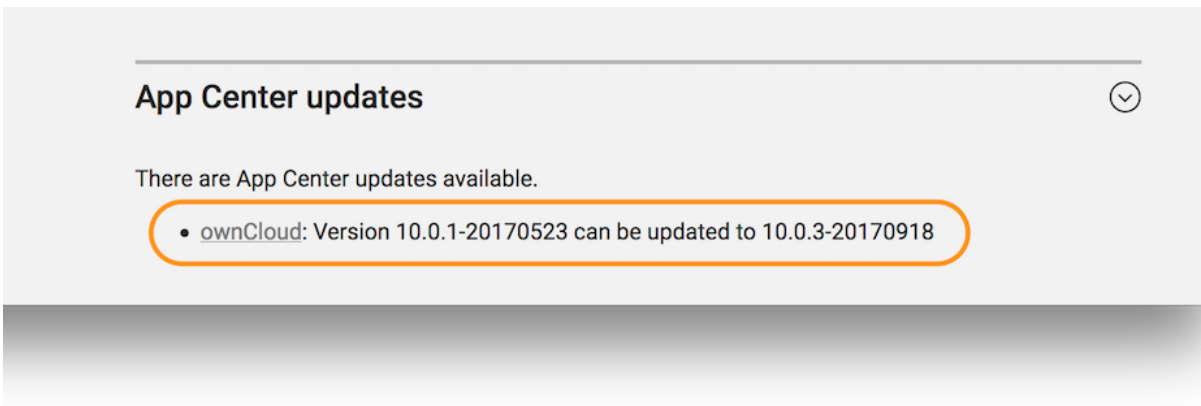
- [In-place Upgrade \(for 10.0 users\)](#)
- [Uninstall the Existing Version and Install the New Version \(for 9.1 users\)](#)

In-place Upgrade (for 10.0 users)

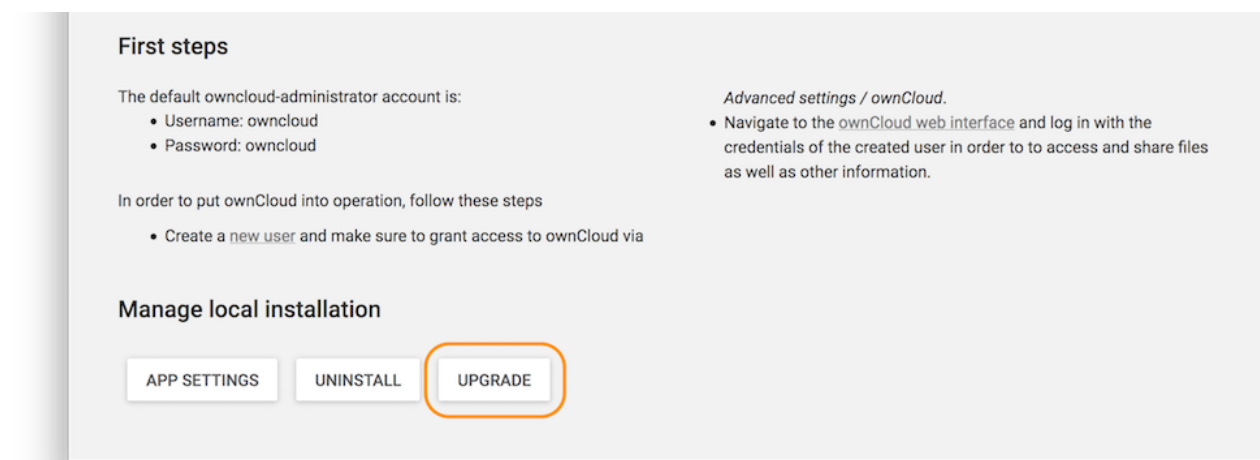
To perform an in-place upgrade, after logging in to the Univention server, under "**Administration**", click the first option labeled **[System and domain settings]**. This takes you to the Univention Management Console. From there, click the **[Software]** shortcut (1), and then click **[Software update]** (2).



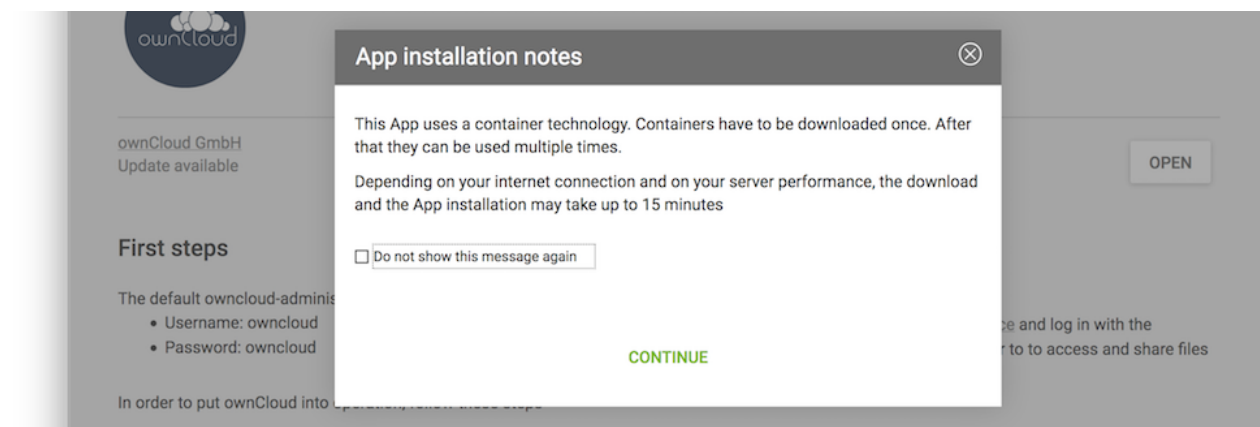
This will load the Software update management panel, after a short time scanning for available updates. If an update is available, under "**App Center updates**" you will see "**There are App Center updates available**". If one is, as in the image below, click **[ownCloud]** which takes you to the ownCloud application.



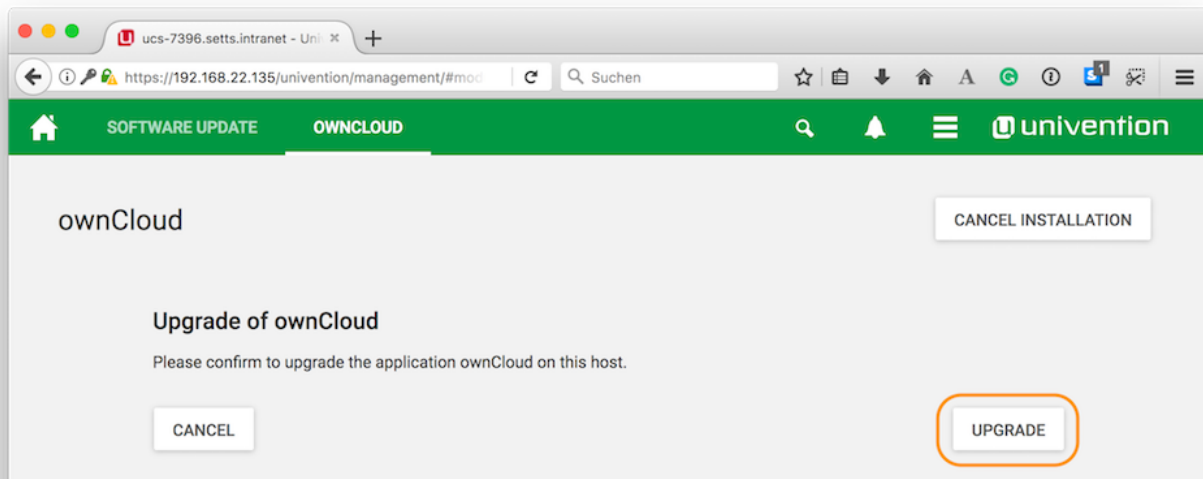
When there, part-way down the page you'll see the **"Manage local installation"** section. Under there, click **[UPGRADE]**.



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]**.



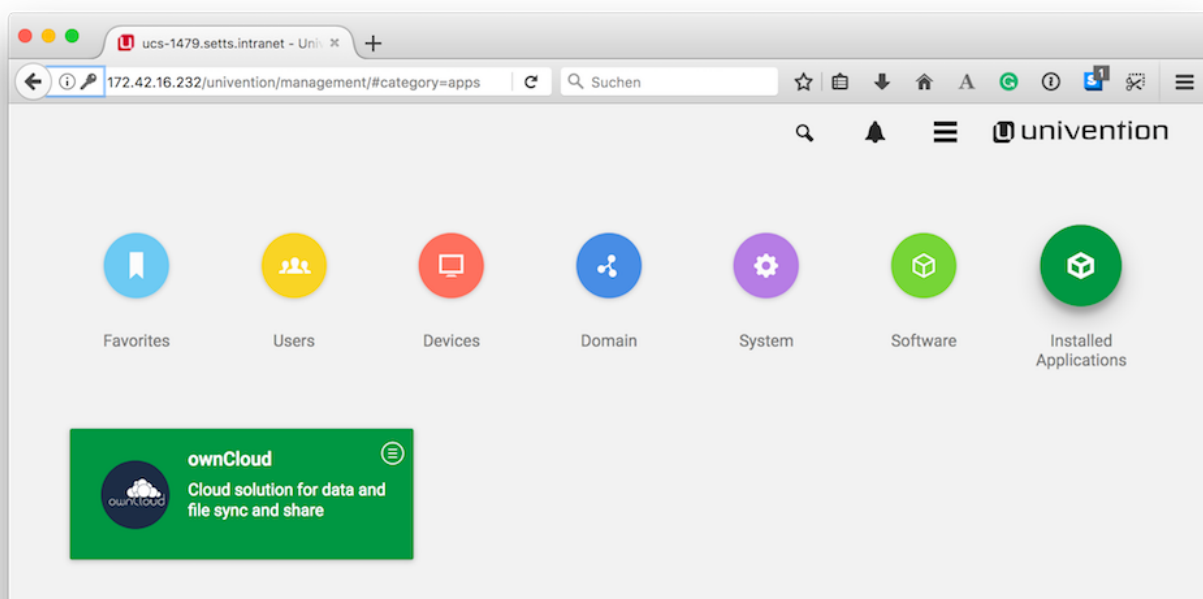
Next an upgrade confirmation page appears. To accept the confirmation, click **[UPGRADE]** on the far right-hand side of the confirmation page.



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)

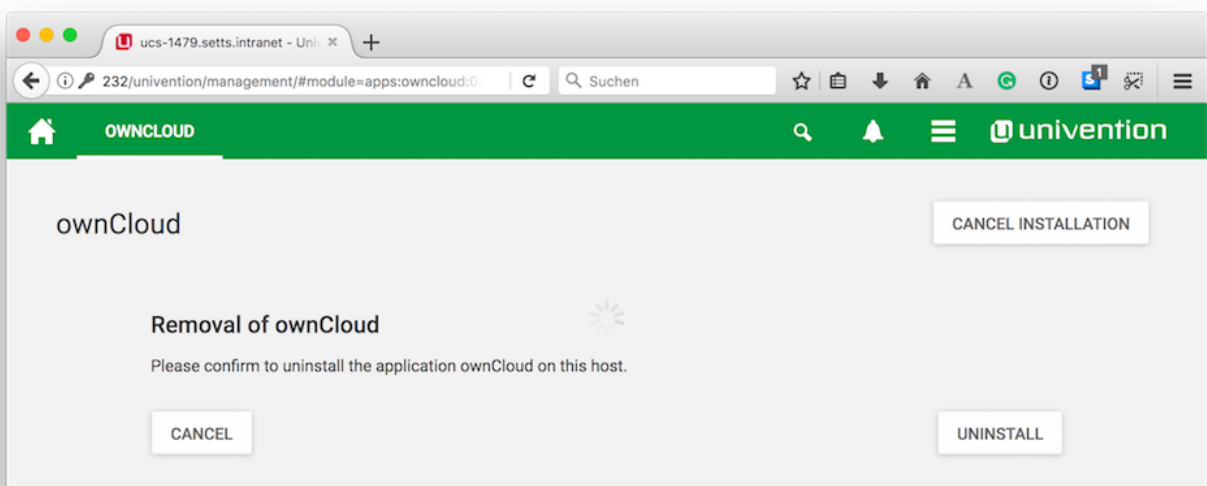
Open your ownCloud X Appliance and go to the "**System and Domain Settings**" dashboard. Then, after logging in, click [**Installed Applications**], and then click [**ownCloud**].



This takes you to the ownCloud app settings page. From there, begin uninstalling ownCloud by clicking [**UNINSTALL**] under "**Manage local installations**"

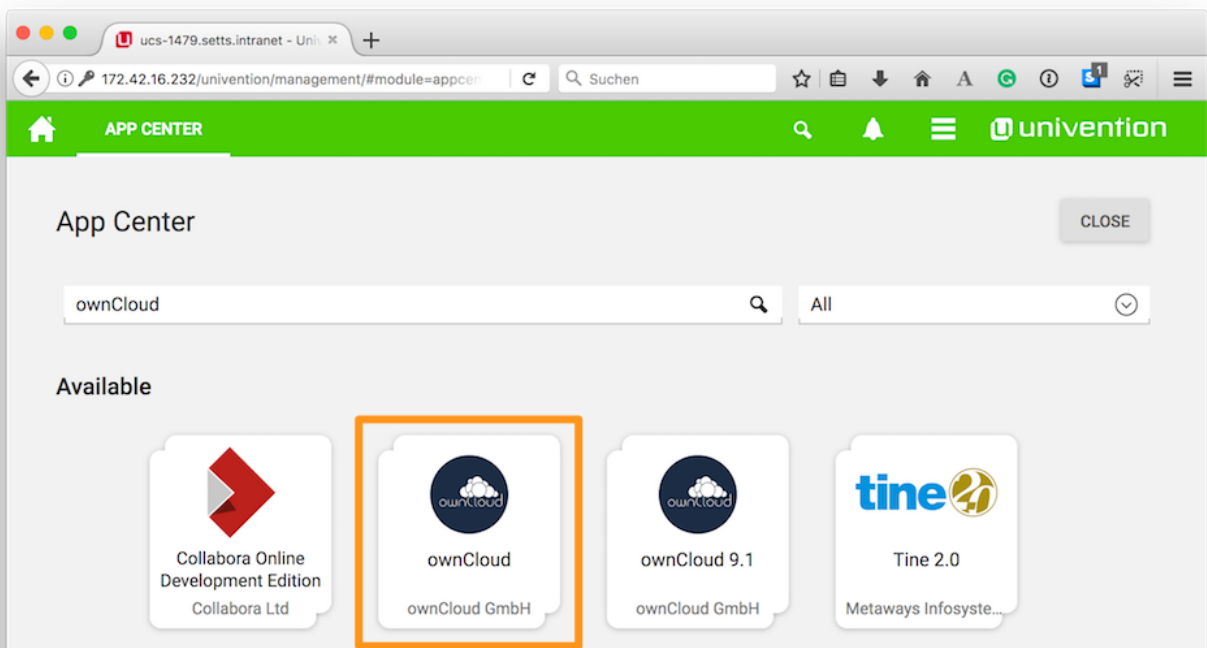


This takes you to an uninstall confirmation page. On that page, click [**UNINSTALL**] on the lower left-hand side of the page.



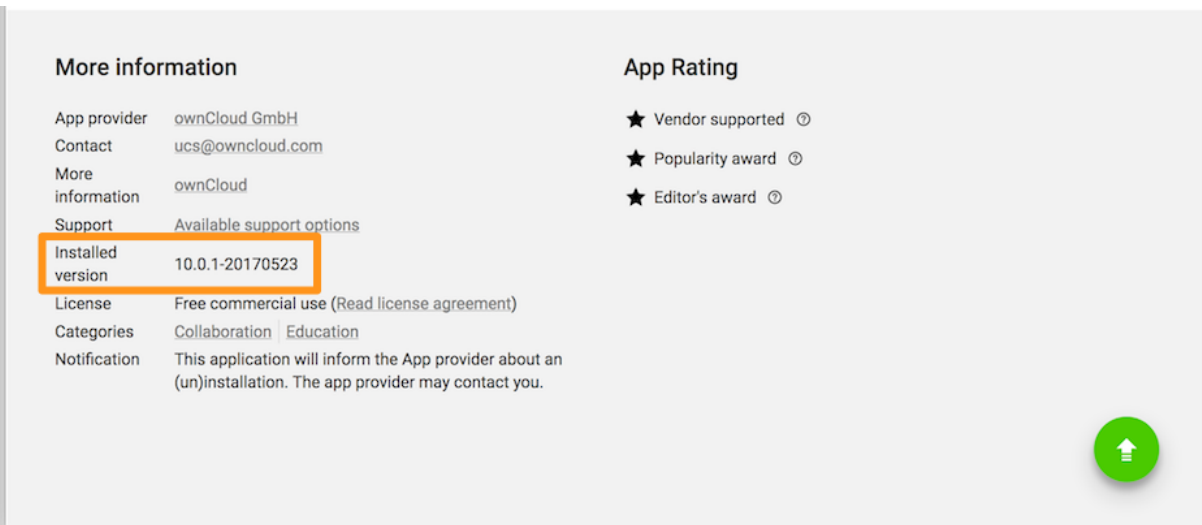
Follow the process until it's finished. Then, click on [**Close**] in the upper right corner.

Your data and users will remain.

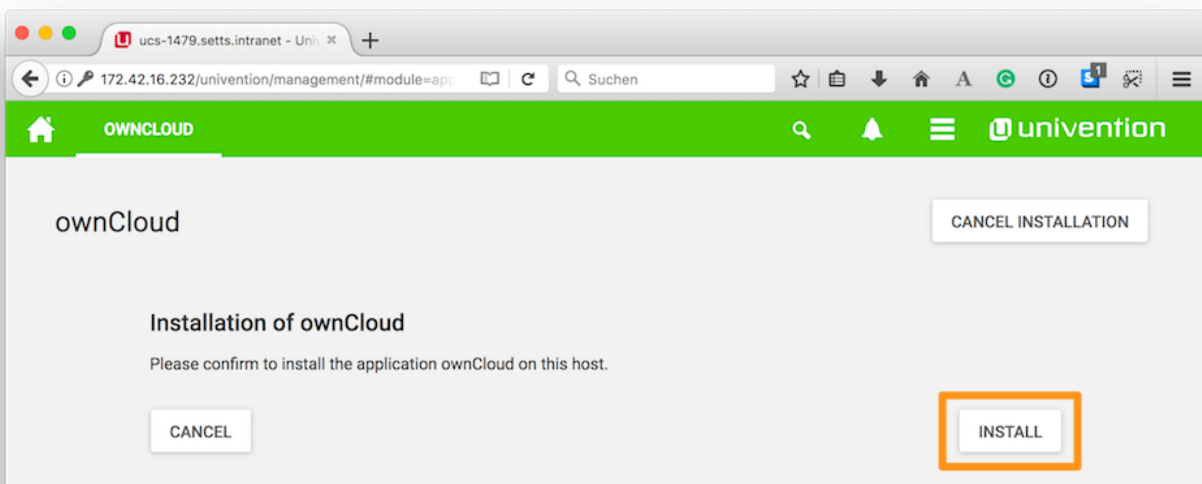


Following that, go to "**Software - Appcenter**", and search for **ownCloud**. At the moment, two matching results will be returned. Pick the one that does not contain a version number.

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.

Your data and users will persist.

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.

```
root@ucs-9446:~# 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:

The following 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`

Troubleshooting

If you have encountered an issue, here is what support needs in order to get a quick resolution of your issue:

1. Log file located at `/var/lib/univention-appcenter/apps/owncloud/data/files/owncloud.log`
2. Config Report generated with `occ configreport:generate > config_report.json` (you have to login to the container with `univention-app shell owncloud`)
3. The status of your docker containers `docker ps > docker.txt`
4. The status of your appliance `univention-app info > univention.txt`
5. Docker Logs: find out your docker ID of the ownCloud container and then execute `docker logs <containerID or container name>`. Here is an example: `docker logs owncloud_owncloud_1`

Restore a snapshot to get your appliance to a functional state again.

ownCloud on QNAP

Introduction

If you have a QNAP NAS, you will soon be able to install the ownCloud app from the App Center and enjoy a ready-to-use ownCloud. The free-of-charge community edition can be used with up to five users and an unlimited number of guest users.

If you want to use Enterprise features, you'll need to purchase a license from the QNAP store, where you can also obtain licenses for additional users, after you've bought a license for the initial five.

The QNAP ready-to-use ownCloud installation should only be changed within very tight limits. If you change the database or web server configuration, the installation will likely break.

All configuration should happen in the Web interface. However, command-line configuration via `occ` commands is available.

Minimum Requirements

Hardware

For ownCloud to properly run on a QNAP NAS device, at least 2 GB of RAM are necessary. However, we recommend at least 4 GB for a smooth operation.

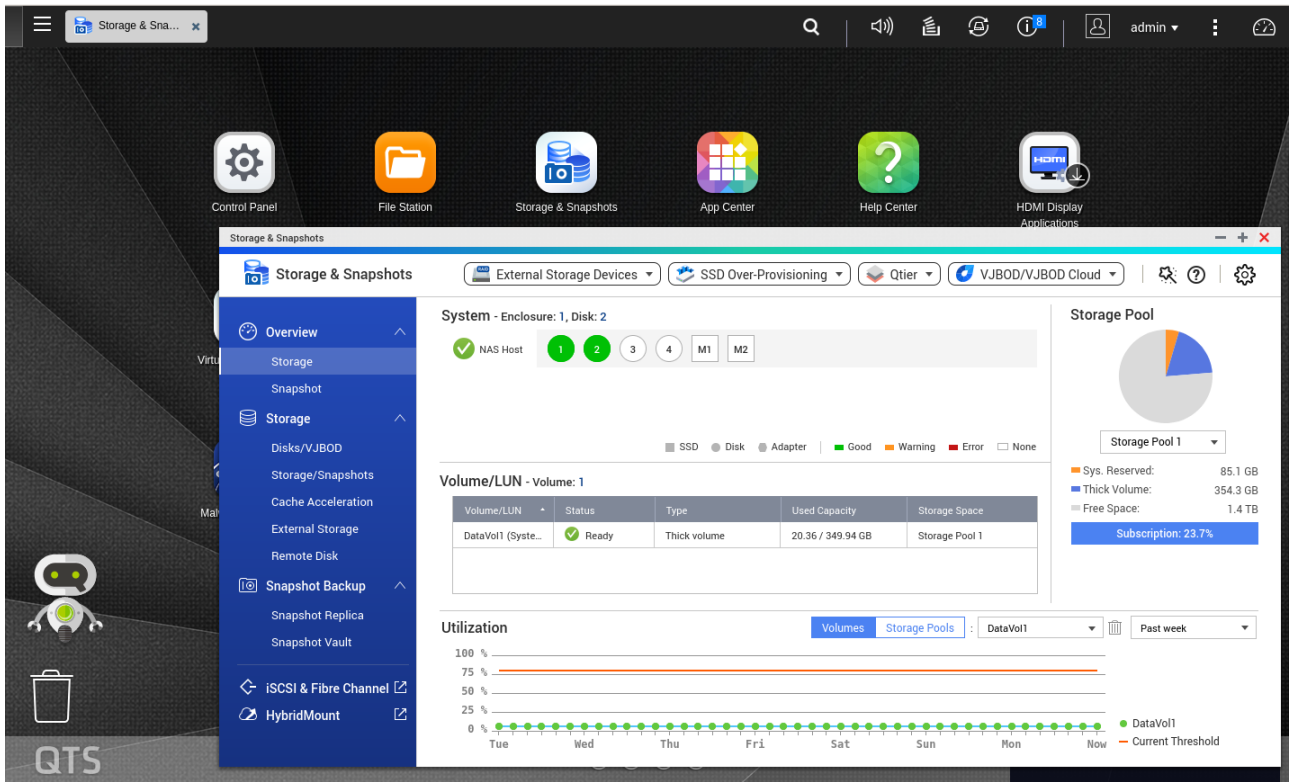
Operating System

The ownCloud app works on QNAP NAS devices running QTS version 4.5.4 and higher.

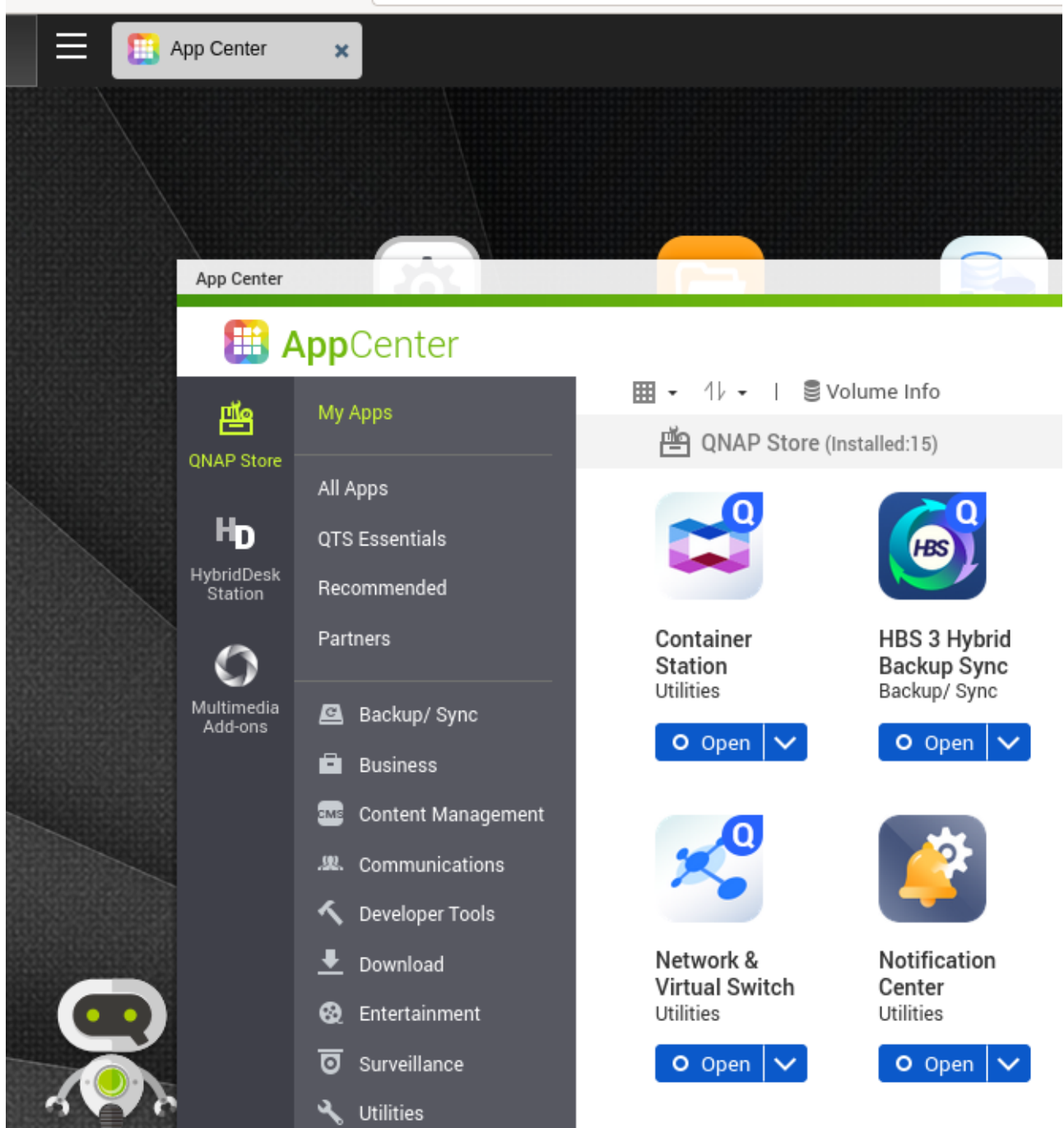
Preparation

If you haven't done so already, perform the following steps on your QNAP system:

1. Create a storage pool in addition to the system volume. You can combine hard disks and solid state disks in RAID groups for flexible storage. This pool can be resized later if necessary. Go to **Main Menu > Storage & Snapshots** or click on the icon.



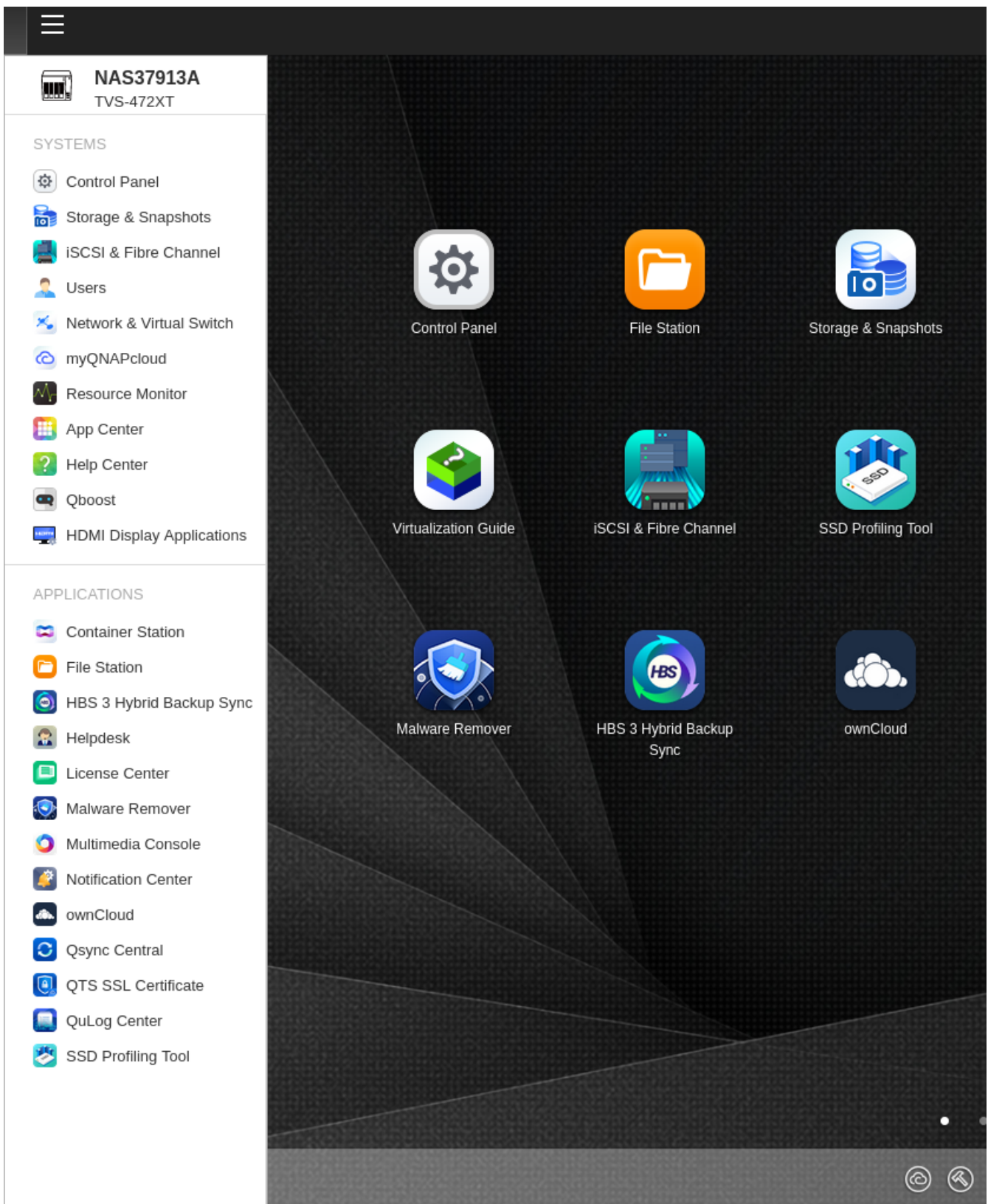
2. Via the App Center install Container Station version 2.0 or higher.



Installation of ownCloud

In the App Center search for ownCloud and click **[Install]**. Confirm that you want to install this app. During installation, you'll see a progress bar.

After a successful installation, ownCloud will show up on your desktop and in the App Center under **QNAP Store > My Apps**. Click **[Open]** under the ownCloud icon and proceed with the configuration.



Configuration

First Steps

Log in as user **admin**. The default password is **admin** until you change it. In the upper right-hand corner, click on **Admin > Settings**. In the left-hand navigation bar, you find personal configuration options and administration-specific options. Under **Personal > General** you can change the

password of your admin user.

For more information on the web interface, refer to the [Web UI](#) documentation.

Configure your Email.

Email is an essential tool in ownCloud for notifying users, user registration, password resets, etc. Logged-in as admin, you can configure email in the **Admin › General** settings.

For more information, refer to section [Email Configuration](#).

Cron

ownCloud performs regular tasks in the background. In order to schedule them, a mechanism called "cron" is used. It's already set up for you, so you don't need to do anything. Make sure not to change cron-related settings unless you have a very good reason to do so.



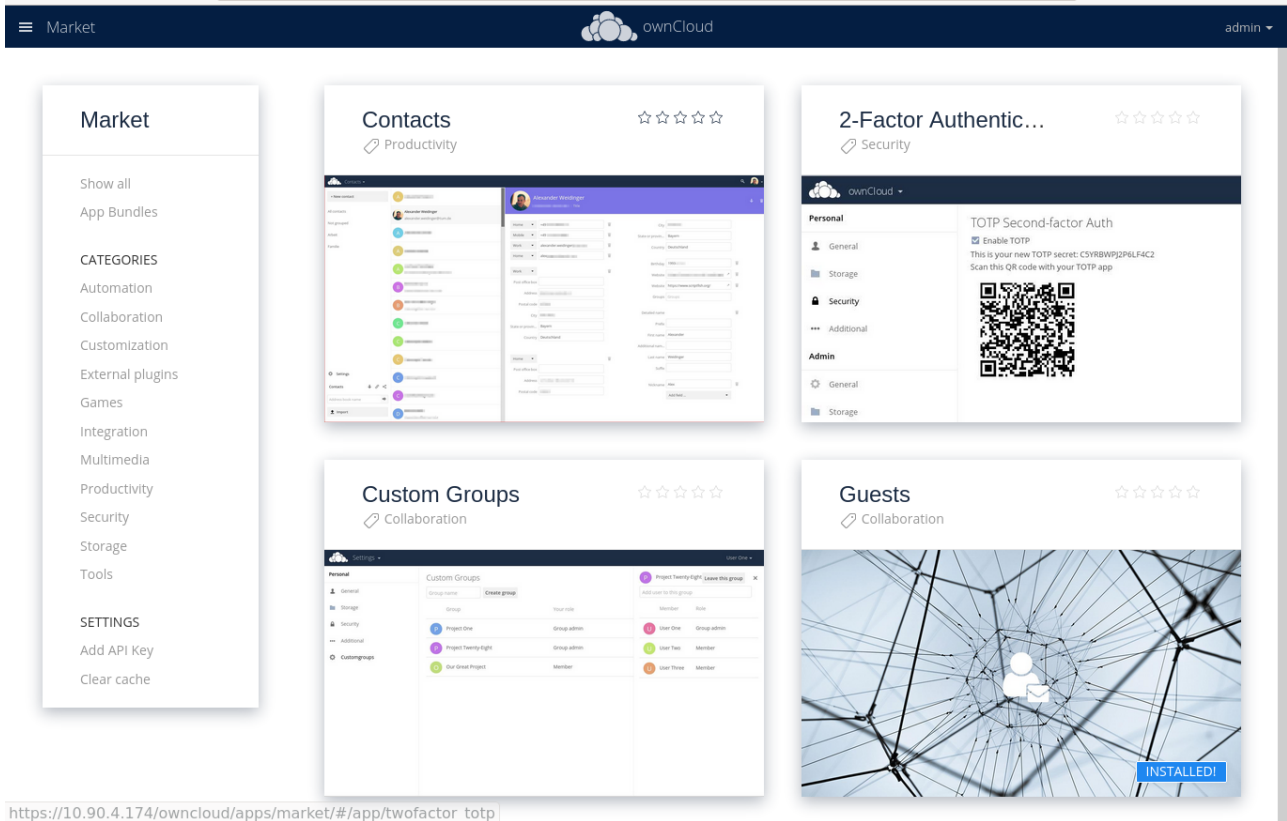
In general, we recommend keeping the default settings in the admin section.

Users

A key feature of ownCloud is to allow users to share files. In the free community edition you can create up to five users, including an admin user, and optionally grant access to an unlimited number of guest users.

Prerequisites:

1. An email server must be configured and working.
2. To share files with external users, the Guests app must be installed and enabled in **Settings › Admin › Apps**. For detailed information on the Guests app, see the [Guests App section](#).



Managing Users

In the **Admin** > **Users** section you can create, disable, enable or delete users, add them to groups, grant administrator privileges and more.

Username	E-Mail	Groups	Password	Groups	Group Admin for	Enabled	Quota	Last Login
admin	admin	admin	*****	admin	no group	<input type="checkbox"/>	Default	11 minutes ago
user1	user1	no group	*****	no group	no group	<input checked="" type="checkbox"/>	Default	never
user2	user2	no group	*****	no group	no group	<input checked="" type="checkbox"/>	Default	never
user3	user3	no group	*****	no group	no group	<input checked="" type="checkbox"/>	Default	never

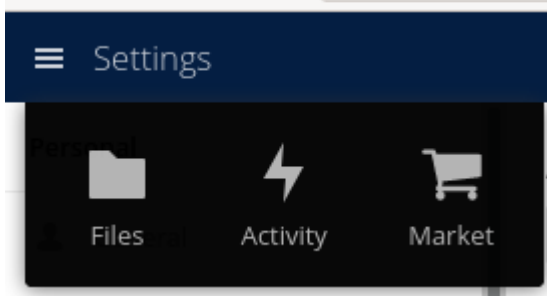
For detailed information see [User Management](#).

After you have created users, they can upload files and share these with other ownCloud users and guest users. Folders can be created and shared as well.

Once a regular user shares a file or folder specifying an external email address, the recipient of the email becomes a guest user. Guest users must be able to access ownCloud either from within the same local network or via the internet.

Enabling ownCloud Apps

With the free community edition, you can use all apps that are published under the GPL or similar public licenses, e.g. the GNU Affero General Public License. These apps you can simply enable and enjoy. In the upper left corner, click on the main menu with the three bars, select **Market** and install what you like.



A bundle of Enterprise Apps is published under the ownCloud Commercial License and only available with the Enterprise Edition. To see what's not included in the free community edition, select **App Bundles** in the left-hand navigation bar.

Enterprise Edition and Licensing

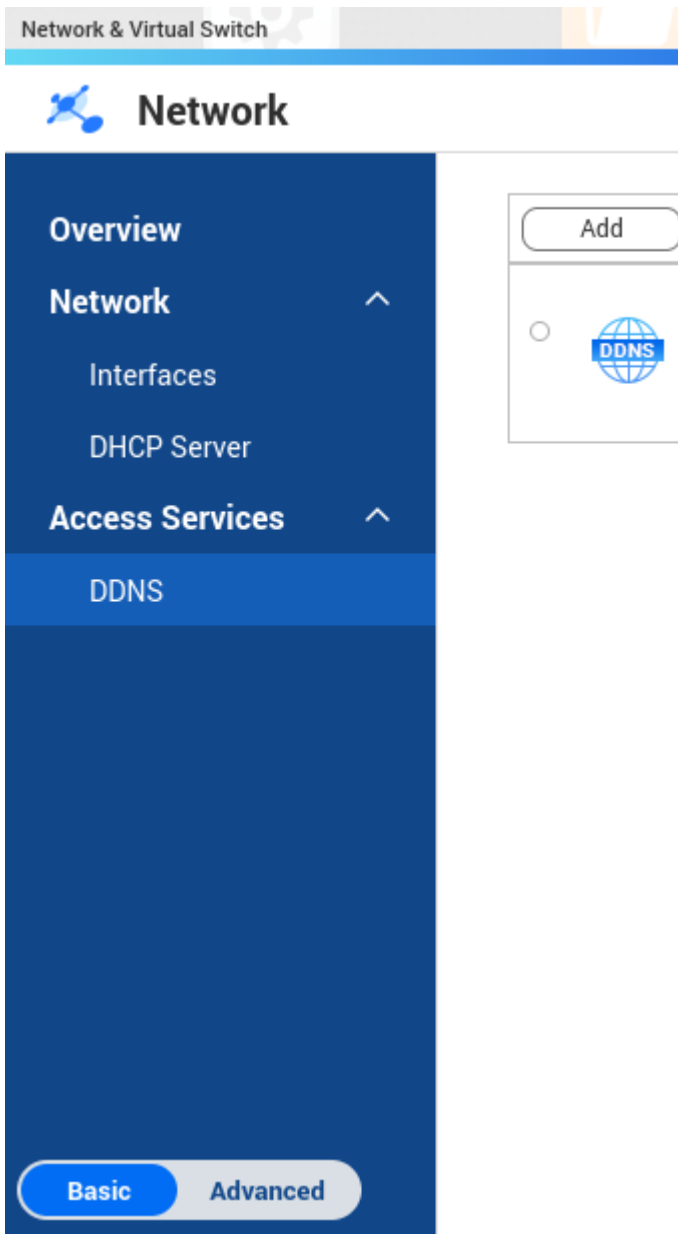
If you want to use enterprise features, obtain a license from the QNAP Store and activate it in the QNAP LicenseCenter. If you want to have more regular users, you can buy additional licenses.

Licenses are valid for a year. If you don't renew them, only the first five users created will remain enabled and only non-enterprise apps. Should you decide to buy licenses again at a later point in time, you can enable the users you want to become active again in the web interface.

Users can also be enabled or disabled via **occ** commands. For more information on the ownCloud command line interface, see below. This would be particularly useful if the admin user accidentally gets disabled.

Accessing your QNAP ownCloud from the Internet

If you want to connect to your ownCloud on QNAP from the Internet, you need to configure the network accordingly. In the **[Main]** menu of your QNAP NAS, select **SYSTEMS › Network & Virtual Switch**. Under "Access Services" click on **DDNS (Dynamic Domain Name Service)** then **[Add]**. Here you can configure the DDNS settings.



If you want to assign a static IP address, you need to access your QNAP device via `ssh` on the command line and edit the file `custom/user.config.php` in your top-level ownCloud app directory, e.g. `/share/CACHEDEV1_DATA/.qpkg/ownCloud`. Create an entry like in the following example with the correct IP address:

```
<?php
CONFIG = array(
    'overwriteprotocol' => 'https',
    'overwritehost' => '203.0.113.0',
    'overwrite.cli.url' => 'https://203.0.113.0/owncloud/',
);
```

ownCloud on QNAP is set up as a subdirectory by default.

You may also want to check out the QNAP FAQ: <https://www.qnap.com/en-us/how-to/faq/article/how-do-i-access-the-files-stored-on-my-nas-at-home-when-im-outside>

If you want to use SSL certificates for increased security, check out the respective QNAP article: <https://www.qnap.com/en/how-to/tutorial/article/how-to-use-ssl-certificates-to-increase-the-connection-security-to-your-qnap-nas>

For more information on command-line access, see below.

Accessing ownCloud via Clients

Besides logging in to ownCloud via the web interface, you can access it from iOS and Android devices by installing the respective apps, and there are desktop clients available for Windows, Mac OS X and various Linux distributions.

For more information, check out the [ownCloud Client Releases](#)

Using External Storage

With your ownCloud you can also use external storage services and devices. For more information, see section [External Storage Configuration](#).

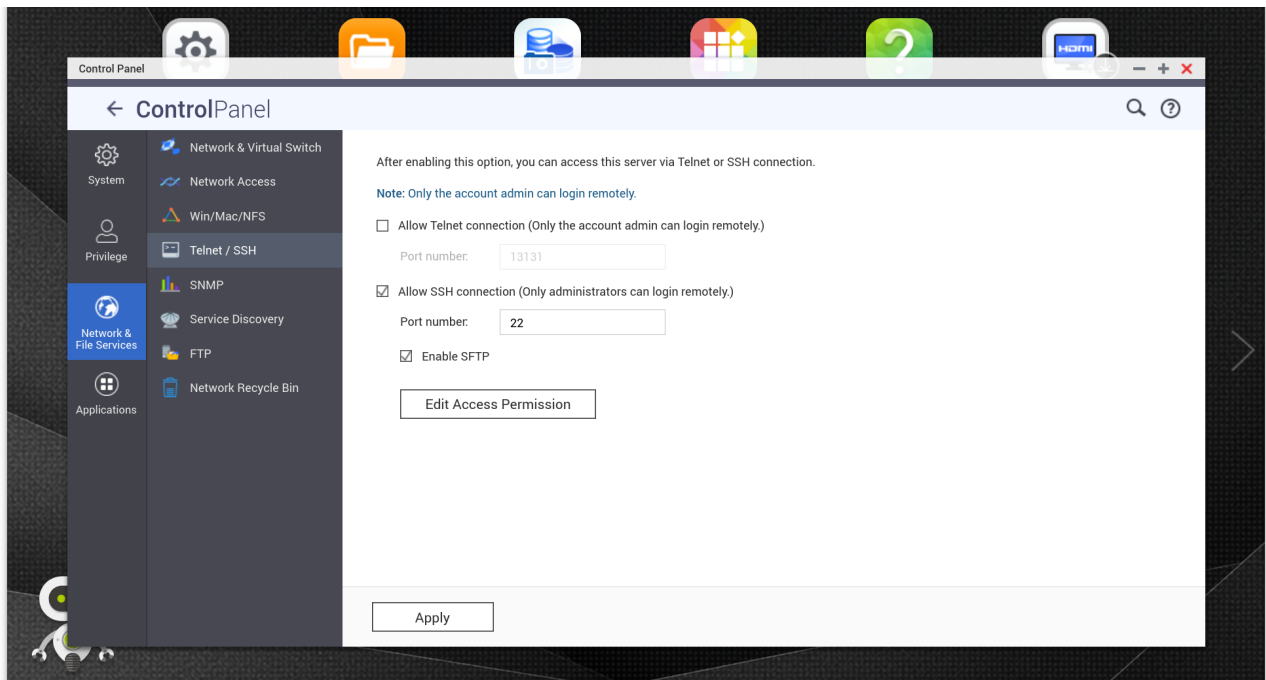
Secure Shell (SSH)

You may need to log in to your ownCloud on QNAP from the command line, e.g. to run `occ` commands.

Prerequisites

Secure shell (ssh) access needs to be enabled in the Control Panel:

1. In the Control Panel click on **Telnet / SSH** in the section **Network & File Services**.
2. Click on the checkbox **Allow SSH connection** and specify the port number (default 22).
3. Next, check **Enable SFTP**. Once you click **[Apply]**, your admin user can log in to your NAS remotely.



Access From a Windows machine

On Windows you need to install PuTTY from a source you trust, then start PuTTY and enter the host name or IP address in the **Session dialog**. Port should be **22** and connection type **SSH**. Click **[Open]**. A command line prompt appears. Press **y** for yes. You'll be asked for a user name. Enter **admin** and in the next step the admin user's password.

You are logged in to the QNAP NAS Console Management - Main menu.

Access From Linux or OSX machines

Open a terminal and enter the command:

```
ssh admin@<your-nas-IP>
```

Enter the admin user's password and you'll be in the QNAP Console Management - Main menu:

Console Management

In the Console Management you have several options that might be useful at some point:

```
+-----+
| Console Management - Main menu |
| |
| 1: Show network settings      |
| 2: System event logs         |
| 3: Reset to factory default (password required) |
| 4: Activate/ deactivate a license |
| 5: App management            |
| 6: Reboot in Rescue mode (w/o configured disk) |
| |
```

```
| 7: Reboot in Maintenance Mode |
| Q: Quit (return to normal shell environment) |
| | |
+-----+
>>
```

Press `q` to quit and confirm with `y` for yes and you'll be logged in with your regular shell.

occ commands

Besides the web interface, ownCloud also offers a command-line interface (occ) for administrator tasks. Access via `ssh` needs to be enabled.

Running occ Commands

To issue `occ` commands, you need to use `ssh` to log in to your QNAP device. Then navigate to the top-level directory of your ownCloud app, e.g. `/share/CACHEDEV1_DATA/.qpkg/ownCloud`.

ownCloud on QNAP lives in a Docker container, therefore `occ` commands look a little different than on regular installations. The prefix `system-docker-compose exec --user www-data owncloud` is needed:

```
system-docker-compose exec --user www-data owncloud occ <your-command>
```

For more information on which `occ` commands are available and how to use them, check out section [Using the occ Command](#).



Unless you know exactly what you are doing, you shouldn't run commands that change the database connection (could be done with `occ:config:*` and `occ:db:*`), the redis connection (could be done with `occ:config:*`) or remove a license key (could be done with `occ:config:*`).

Backing up and Restoring the Database

To prevent data loss, the ownCloud database should be backed up regularly. To do so, you need to log in to your QNAP device via `ssh` and navigate to the ownCloud app root directory, e.g. `/share/CACHEDEV1_DATA/.qpkg/ownCloud`. Here you can create a database snapshot with a time stamp by entering the following command:

```
system-docker-compose exec db pg_dumpall -c -U owncloud > \
owncloud_database_$(date +%Y-%m-%d_%H_%M_%S).sql
```

For more information, see section [Backing up ownCloud](#). ownCloud on QNAP uses PostgreSQL.

Should something happen and you need to restore the data, perform the following commands:

Delete / drop the current database

```
system-docker-compose exec db dropdb owncloud -U owncloud
```

Create a new database

```
system-docker-compose exec db createdb owncloud -U owncloud
```

Restore data to database

```
cat ownCloud_database_xxxxx.sql | system-docker-compose exec \
  -T db psql -U owncloud -d owncloud
```

Troubleshooting

General

Via the QuLog Center app on your QNAP NAS, you can check the log entries.

Some features are unavailable because no destination volume has been configured. Go to [here](#) to configure a destination volume for storing logs.

System Event Log

Specify keywords

Total log entries:40

<input type="checkbox"/>	S...	Date	Time	User	Source IP	Applica...	Category	Content	+
<input type="checkbox"/>	i	2021/06/22	15:28:57	System	127.0.0.1	Storage...	Volume	[Storage & Snapshots] Finished initializing volume/LUN "DataVol1"...	
<input type="checkbox"/>	x	2021/06/22	15:28:41	System	127.0.0.1	App Ce...	App Ins...	[App Center] Failed to install ownCloud 10.8.0. You must first...	
<input type="checkbox"/>	i	2021/06/22	15:28:36	System	127.0.0.1	App Ce...	App Ins...	[App Center] Hybrid Backup Sync enabled [App Center] Failed to install ownCloud 10.8.0. You must first install and start...	
<input type="checkbox"/>	i	2021/06/22	15:28:31	System	127.0.0.1	Hybrid ...	System	[Hybrid Backup Sync] container-station >= 2.0. system migration.	
<input type="checkbox"/>	i	2021/06/22	15:28:15	System	127.0.0.1	App Ce...	App Ins...	[App Center] Installed Hybrid Backup Sync	

Page 1 / 1 | Display item: 1 - 40 , Total: 40 | Show 50 Item(s)



The event notifications in the top toolbar will also tell you if something has gone wrong. Look for the i in a circle.

Specific Problems

- What to do if you forgot to install the Container Station?

An error message will pop up during the installation of ownCloud. Click on the link [**System Event**

Log in the pop-up window to find out what actually went wrong or hit **[OK]** and install the Container Station. Then start the installation of ownCloud again.

Enterprise Edition

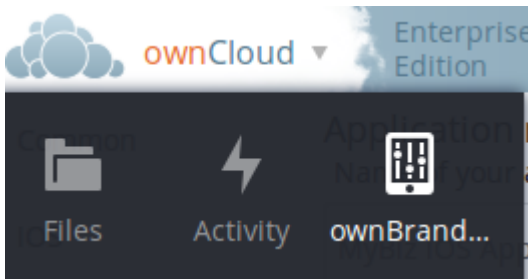
In this section, you will find all the information you need for managing ownCloud Enterprise Edition.

Unresolved directive in modules/admin_manual/pages/enterprise/clients/index.adoc - include::partial\$section_page.adoc[]

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://customer.owncloud.com) 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 a Branded Android App

Building and distributing your branded Android ownCloud app is fairly simple, and the process is detailed in [Building Branded ownCloud Clients](#).

Custom Client Download Repositories

See [Custom Client Download Repositories](#) to learn how to test and configure custom download

repository URLs for your branded clients.

Unresolved directive in modules/admin_manual/pages/enterprise/collaboration/index.adoc - include::partial\$section_page.adoc[]

Collabora Online / Secure View

Introduction

Collabora Online allows you to work with all kinds of Collabora office documents directly in your browser. This application can connect to a Collabora Online (or other) server (WOPI-like client) where ownCloud is the WOPI host.

When Collabora Online is properly set up and integrated into ownCloud Server, secure view functionality is available. Secure view is a mode where users can place limitations on files and folders that are shared.

These limitations can include:

- No copying
- No downloading
- No editing
- Watermarking
- Optional printing and exporting to PDF with watermarks included, which can be adjusted

Documents never leave the server when shared with secure view.



Collabora Online Server opens them and streams the files to the user's browser with watermark applied (much like a video stream). Consequently, there's no way to extract the original document from the browser.

Secure view is enforced on a received share if at least 1 share has secure view enabled.



If a file or folder has been shared multiple times to different groups with different permissions, secure view will be enforced if at least 1 received share has secure view enabled as a result of membership in the group. This restriction propagates to any reshares.

Prerequisites

- ownCloud **10.3** or above
- *Enterprise Edition*
- [ownCloud Collabora Online](#) app version **2.2.0** or above
- Collabora Online Server **4.0.10** or above, set up and integrated



This functionality does not work with public links.

Configure ownCloud for Collabora Online / Secure View

To configure ownCloud for use with Collabora, you need to set up a WOPI server and configure ownCloud to connect with this server. You can also configure the secure view option, the watermark pattern and the secure view default open action via the command line. To do so see the [Collabora related occ command set](#).

How to Enable Secure View

To enable *secure view*, navigate to **Settings › Admin › Additional (Admin) › Collabora Online**. At the bottom of the Collabora Online section, check **[Enable Secure View]**.

Once enabled, default share permissions for all users can be enabled. Currently, these default share permissions are:

- **Secure View (with watermarks)**. When enabled, files are shared in secure view mode. In this mode, all the [Limitations and Security Hardening](#) take effect. When this mode and "can edit" are disabled, the share is a regular "read-only" share.
- **Can print / export PDF**.



This option is only visible if **[Secure View (with watermarks)]** is enabled.

When enabled, this mode allows documents to be printed or exported to PDF format — with a watermark — through Collabora Online.



Admins can specify that all shares are "secure view" by default and that the user has to intentionally change this setting.

Secure View Restrictions

When "Secure View (with watermarks)" is enabled, any attempts to download the file will be blocked as shown in the screenshot below. In addition, copy & paste is disabled.



Limitations and Security Hardening

To make sure that the secure view feature is deployed securely and cannot be circumvented, it is important to disable the following extensions:

- [ONLYOFFICE](#)
- [Microsoft Office Online](#)
- [Text editor](#)

Additionally, you might want to *disable public link sharing* via **Settings** › **Admin** › **Sharing** › **Allow users to share via link** so that users cannot accidentally share files publicly without secure view protection.

Supported File Formats

Secure view only supports a limited number of file formats:

- Microsoft Word (.docx)
- Microsoft Excel (.xlsx)
- Microsoft PowerPoint (.pptx)
- OpenDocument Text Document (.odt)
- OpenDocument Presentation Document (.odp)
- OpenDocument Spreadsheet Document (.ods)
- PDF

If a folder shared with Secure View contains unsupported file types (e.g., JPG), they will not be accessible.

Microsoft Office Online / WOPI Integration

Introduction

The WOPI (Web Application Open Platform Interface) app, which is bundled with ownCloud Enterprise Edition, is the connector between ownCloud server and [Microsoft Office Online Server](#) or [Office 365 \(cloud\)](#).

It allows Microsoft Office users to collaboratively work with Office documents in ownCloud in the browser, by connecting ownCloud with your Microsoft Office Online Server or Office 365 (cloud) via [the WOPI protocol](#).

- **Microsoft Office Online Server:** To use it, you need to have a running Microsoft Office Online Server in your data center.
- **Office 365 (cloud):** To use it, you need an active Microsoft 365 subscription.



Please bear in mind:

- WOPI is only available for ownCloud enterprise. It *is not available* in the community version.
- Out-of-the box only the on-premise version of Microsoft Office Online Server is supported.

- If you want to integrate the [Office 365 \(cloud\)](#) version of Microsoft Office Online, you need to [get in touch with us](#).
- This app requires at minimum ownCloud Version 10.5 and php 7.1.

Preparing the Environment

You need an

- [Office Online Server](#) installed, or an
- active Microsoft 365 subscription.

All involved servers (Office Online Server and the ownCloud server) need to be accessible by HTTPS with valid certificates.

Configuring the WOPI App in ownCloud

To configure the WOPI app in your ownCloud installation, add the following configuration to `config/config.php`, and adjust it based on the details of your setup:

```
# ownCloud Support URL: https://owncloud.com/support

# WOPI token:
# For Office Online Server: Replace the token with your own random string
# For Office 365 (cloud): Request the string from us
# (this has to match the '0365_PROXY_SHARED_KEY'
# configuration of the 0365 proxy)
'wopi.token.key' => 'REPLACE_WITH_WOPI_TOKEN_KEY'

# Office server URL
# For Office Online Server: Enter your https://your.office.online.server.tld
# For Office 365 (cloud): Upstream url to Microsoft 0365.
# Microsoft will only accept connections from registered ownCloud domains.
# For Office 365 quality assurance upstream URL:
# https://ffc-onenote.officeapps.live.com/hosting/discovery
# For Office 365 production upstream URL:
# https://onenote.officeapps.live.com/hosting/discovery
'wopi.office-online.server' => 'https://THE_OFFICE_SERVER_URL',

# Proxy URL
# Only for Office 365 (cloud), not needed for Office Online Server
# URL of the 0365 proxy instance.
# Note that you will get a working URL from ownCloud Support
# post a written declaration that your company has an eligible
# Microsoft Business contract.
'wopi.proxy.url' => 'https://o365.example.com',

# Enable Business Flow
# Only for Office 365 (cloud), not needed for Office Online Server
# Necessary for the 0365 proxy key above.
```

```
'wopi.business-flow.enabled' => 'yes',

# Samesite Cookie
# Only for Office 365 (cloud), not needed for Office Online Server
# Necessary to allow e.g. opening ownCloud sharing from O365.
# Use `None` if you are using OpenID Connect.
'http.cookie.samesite' => 'Lax',
```

Restrict Usage to Users in a Specific Group

Microsoft Office Online access can be restricted to users in a specific group, by use of the `wopi_group` configuration key (in `config/config.php`), as in the following example.

```
'wopi_group' => 'admin'
```

In the example above, only users in the `admin` group would be able to access Microsoft Office Online.



If the key is not defined, then all users have access to this Microsoft Office Online service connected via WOPI.

Locking the Document

If you open a document with Microsoft Office Online in ownCloud, it makes use of the WebDAV file locking functionality available in ownCloud server. The idea is to lock the file so other users with access can't make changes to the document while you're editing it.

In other words, the feature ensures that you are the "master editor". Your changes will always be the "master state". Other users can make changes, e.g., with the desktop client, but those will create conflict files for them, which can be resolved afterward. When you close the document, Microsoft Office Online unlocks the file so others can edit it.

You can always click on the lock icon next to your file name and unlock it manually using the button in the sidebar.

Lock Timeout

If a user is editing a file and loses their internet connection, the lock will timeout, freeing the lock after 30 minutes. Refer to [the WOPI documentation](#) for further information.

Known Issues

Document Locks Are Not Released When Using Google Chrome

When editing a document with Google Chrome (and Chromium) via ownCloud in Microsoft Office Online, the document lock is *not released* when the document is closed. The document lock is only released after the 30-minute timeout or a manual lock release. To mitigate the issue, try to remember to manually unlock the document before closing it.

More information about this issue is available in the following links:

- The [file is locked for shared use](#)
- The [file is locked when using Office Online within SharePoint Online](#)

Troubleshooting

Checklist if something is not working:

1. **Client** can reach the **ownCloud Server** (browse to web page and log in)
2. **Client** can reach the **Office Online Server** (via hosting/discovery url with https)
3. **ownCloud Server** can reach the **Office Online Server** (via hosting/discovery url with https)
4. **Office Online Server** can reach **ownCloud Server** (browse to web page and log in)

Make sure TLS 1.2 is being used:

- [Enable TLS 1.2 Support in Chrome](#)
- [Enable TLS 1.2 Support in Microsoft Office Online Server](#)

```
Unresolved directive in
modules/admin_manual/pages/enterprise/document_classification/index.adoc -
include::partial$section_page.adoc[]
```

Document Classification and Policy Enforcement

Introduction

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)
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, such as [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.

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 [Collaborative Tags](#). Different categories of tags can be used to achieve different behaviors for users; these are detailed in the table below.

Table 1. Tag Categories Available in ownCloud

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 Collaborative Tags Management . 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.
Static	These tags can be created by administrators using Collaborative Tags Management . This category is recommended as it enables users to recognize the classification level of files and to be able to filter accordingly. Additionally this tag category should be used for manual classification as users in specified groups can only assign and unassign them but only administrators can edit or delete them. This way administrators can provide a tag linked to a classification policy that specified users can then impose on files.
Invisible	These tags can be created by administrators using Collaborative Tags Management . 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 [Collaborative Tags Management](#), 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 Add-Ons

Microsoft Office does *not* provide classification capabilities out-of-the-box. To extend it, we recommend the [Microsoft Azure Information Protection](#) or [NovaPath](#) add-ons. These extensions come with easy-to-use default classification categories, and provide 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 **Settings** > **Workflows & Tags**. 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`



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 **Settings** > **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 **Settings > Workflows & Tags**. 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:BusinessAuthorizationCategory:Name']/vt:lpwstr`
 - **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.

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 **Settings › 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 the [Workflow](#) extension.

- 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 **Settings › Workflows & Tags**.
- In the [Collaborative Tags Management](#) panel, create a tag of type "*Static*" 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, click **[+]**, then choose "*File*

mimetype" and click [+] 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.
- Click [**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 **Settings** › **Workflows & Tags**.
- In the [Collaborative Tags Management](#) panel, create a tag of type "Static" and give it a meaningful name. Then assign the group you created, in the beginning, to give its 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.

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 an error message: **A policy prohibits uploading files classified as '<tag>'**, where **<tag>** is the tag chosen for the classification rule.



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.



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.



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 click **[Save]**.

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](#) 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)

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'"
```

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.

Unresolved directive in modules/admin_manual/pages/enterprise/external_storage/index.adoc - include::partial\$section_page.adoc[]

Enterprise-Only Authentication Options

Introduction

ownCloud provides several authentication options for mounting storages. Depending on the edition, these options can vary.

Authentication Options

The following table shows which authentication option is available for which edition of ownCloud.

Authentication Method	Free Edition	Enterprise Edition
Username and password	x	x
Log-in credentials, save in session	x	x
Log-in credentials, save in database		x
User entered, store in database		x
Credentials hardcoded in config file *		x
Global credentials		x
RSA public key **	x	x

(*) Note that **Credentials hardcoded in config file** will appear only if the Windows Network Drive (WND) app is installed and enabled. As long you have WND enabled, you can also use this authentication method for other mount types. If you use this authentication method with other mount types but disable WND, you will lose the connection to all the mounts where this authentication method was used.

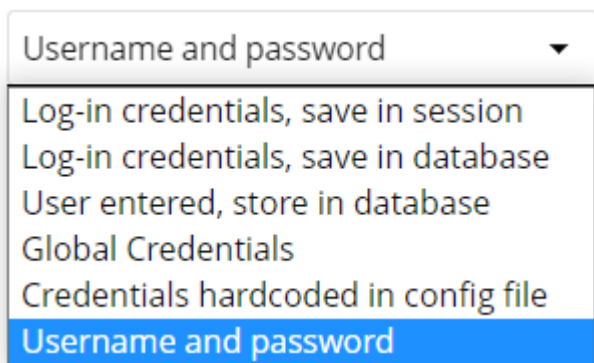
(**) Note that **RSA public key** is only available for SFTP.

Storage Implementations

The following table shows which storage implementation can use the above authentication options. Note that this table does not cover other storage implementations like Google Drive or One Drive etc., as those use other authentication backends.

Storage implementation	Free Edition	Enterprise Edition
FTP	X	X
SFTP	X	X
ownCloud	X	X
SMB/CIFS	X	X
WebDAV	X	X
Windows Network Drive		X

Use the dropdown selector to choose the authentication backend when you create a new external mount.



Authentication Option Details

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.

Credentials hardcoded in config file

Used when all the users will share the same password and the password is not known to the users like for a shared space. The user id is always taken from the session. This authentication option can also be chosen when using OAuth or OpenIDConnect etc. For more details see [Notes for Credentials Hardcoded in Config File](#). 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

<input type="text" value="Username"/>	<input type="text" value="Password"/>	<input type="button" value="Save"/>
---------------------------------------	---------------------------------------	-------------------------------------

RSA public key

This authentication method is limited to SFTP only. Manually enter the public key or press **[Generate]** in the mount form to generate one. Files can be shared.

Authentication Options Allowing Sharing

The following table shows which authentication option allows sharing:

Authentication Option	Sharing Allowed
Username and password	x
Log-in credentials, save in session	
Log-in credentials, save in database	x
User entered, store in database	x
Credentials hardcoded in config file	x
Global credentials	x
RSA public key	x

Notes for Credentials Hardcoded in Config File

- The username taken will be the same as the **user id** of the ownCloud session. For example, ownCloud user "Alice" with password "mysecret" (or even without password) will use "Alice" as username and the password from the config.php file to access the storage. Note that for LDAP, the **user id** is usually like *1223-cbdf-cacc-1234...*, unless the configuration in the user_ldap app is changed.
- The password will be fetched from a key inside the config.php file. For details see the section below. Even if the account doesn't have a password like OAuth or OpenIDConnect etc., the connection with the storage will use the password from config.php. **Note that the password**

will be the same for any user accessing the particular mount!

Defining key/value pairs in config.php

Key/value pairs in config.php must have the following structure:

Listing 19. Example having a single array

```
'customApp.config' => 'the_password',
```

Listing 20. Example having nested arrays

```
'customApp.config' => [  
  'server1' => 'the_first_password',  
  'server2' => 'the_second_password',  
  ....  
]
```

customApp.config

The naming of this key must be a string that is valid as an array key in a PHP array like the above `customApp.config` or as another example `my.config.key`, but not any reserved ownCloud key.

Arrays

You can use an array as described in the example above. When using an array, you can use as many sub-keys according your needs where the naming of the sub-key must be a string that is valid as an array key in a PHP array.

The array syntax is beneficial when having more than one server (host) with a password, but keeping them together in one master key. To access a particular sub-key in the mount definition, use the following scheme:

```
<key>#<sub-key-level-1>#<sub-key-level-2>...
```

From the example above,
`customApp.config` corresponds to `key` and
`server1` corresponds to `sub-key-level-1`.

Value to be entered in the mount point config key field

Single array

Taking the single array example above to use the password for the mount, the value to be entered would be like:

```
customApp.config
```

Nested arrays

Taking the nested array example above to use the password for the mount for the host with sub-key `server1`, the value to be entered would be like:

```
customApp.config#server1
```

LDAP Home Connector

Introduction

The [LDAP Home Connector](#) app enables you to configure your ownCloud server to display your users' Windows home directories on the ownCloud Files pages view, just like any other folder.

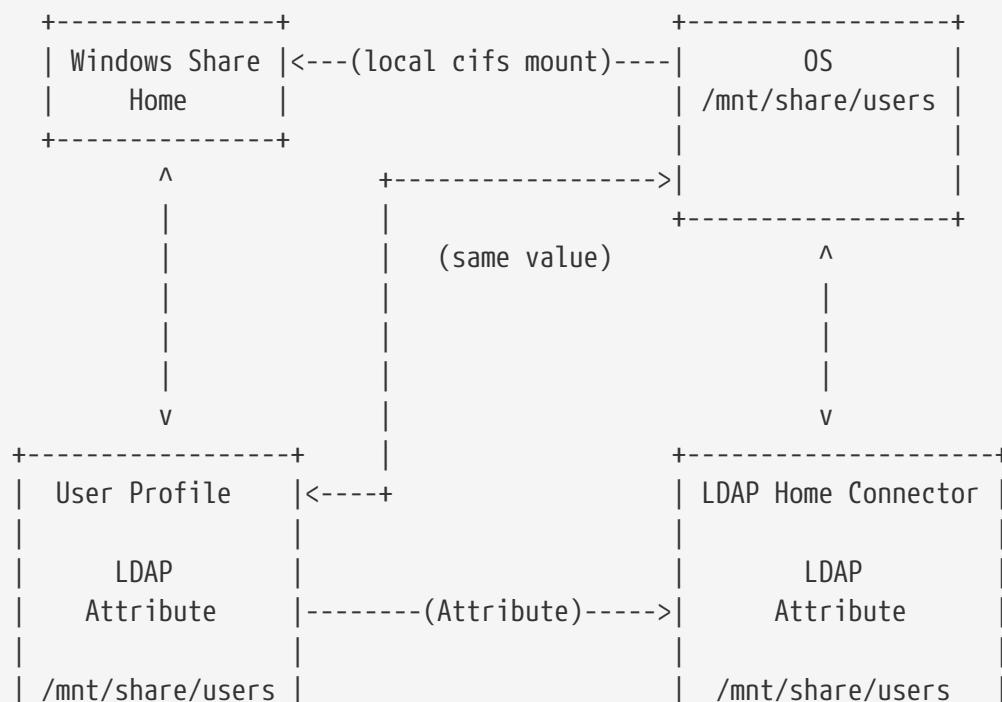
Typically, Windows home directories are stored on a network server in a root folder, such as Home, which then contains individual folders for each user.

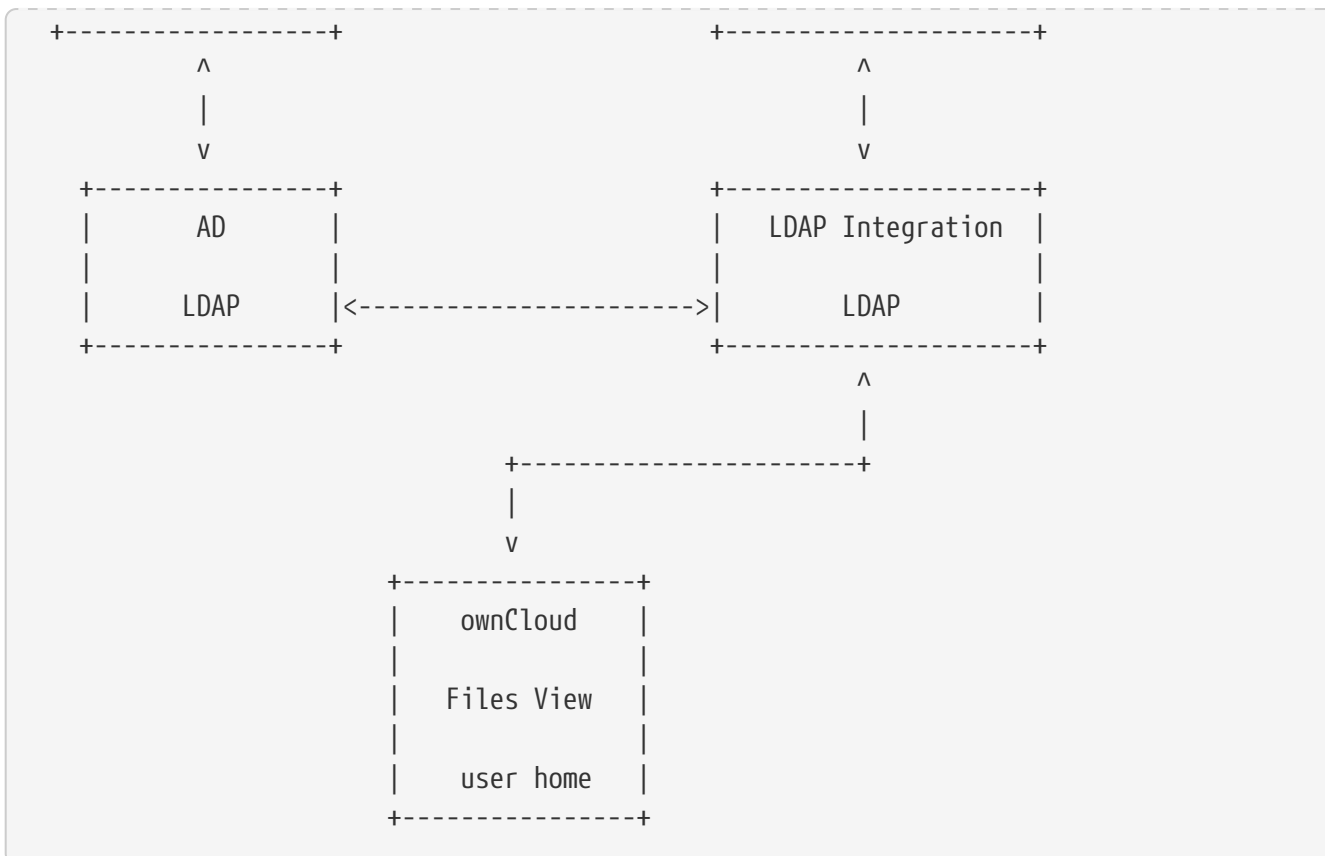
Listing 21. Directory Structure User Home Share

```
Home
  user_1
  user_2
  ...
```

The Windows home directory can be published as a share and due to the permissions set, any user can only see his personal home folder.

To integrate a user's home folder from Windows into ownCloud, the Home share is locally mounted. An LDAP attribute is added to the user's profile containing the path of the local mount and then used by the LDAP Home Connector to show the user's home in ownCloud.





Prerequisites

The following prerequisites are required:

- Mounting cifs is available on the server where ownCloud is installed
- The [LDAP Integration](#) app is enabled and has a working LDAP/Active Directory configuration in ownCloud.
- The [LDAP Home Connector](#) app is installed.

Configuration

The configuration is done in several steps:

1. Mount the root Windows home directory to the ownCloud server
2. Configure Active Directory/LDAP by adding a LDAP attribute to the user profile
3. Use the LDAP Home Connector app to connect it to ownCloud

Mount the Home Directory

For enhanced security, create a file where the credentials are stored accessing the cifs share like:

```
/etc/credentials
```

with the username and password on separate lines, replacing the values according your setup:

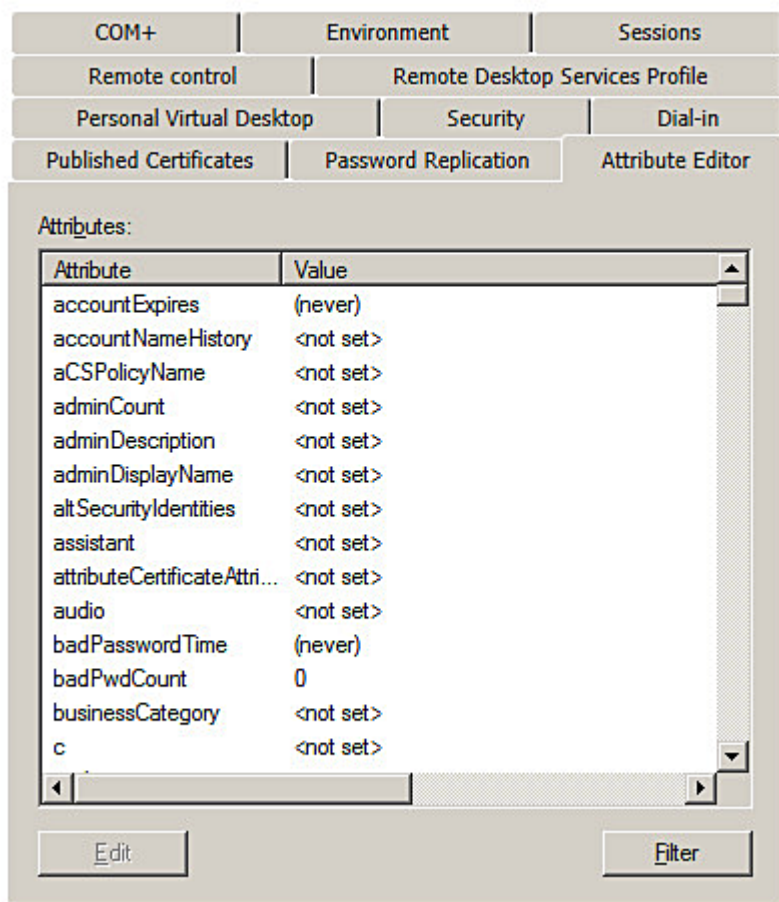
```
username=winhomeuser
password=winhomepassword
```

Create an entry in `/etc/fstab` for the remote Windows root home directory mount and use the credentials file created above, substitute and adapt your parameters and filenames:

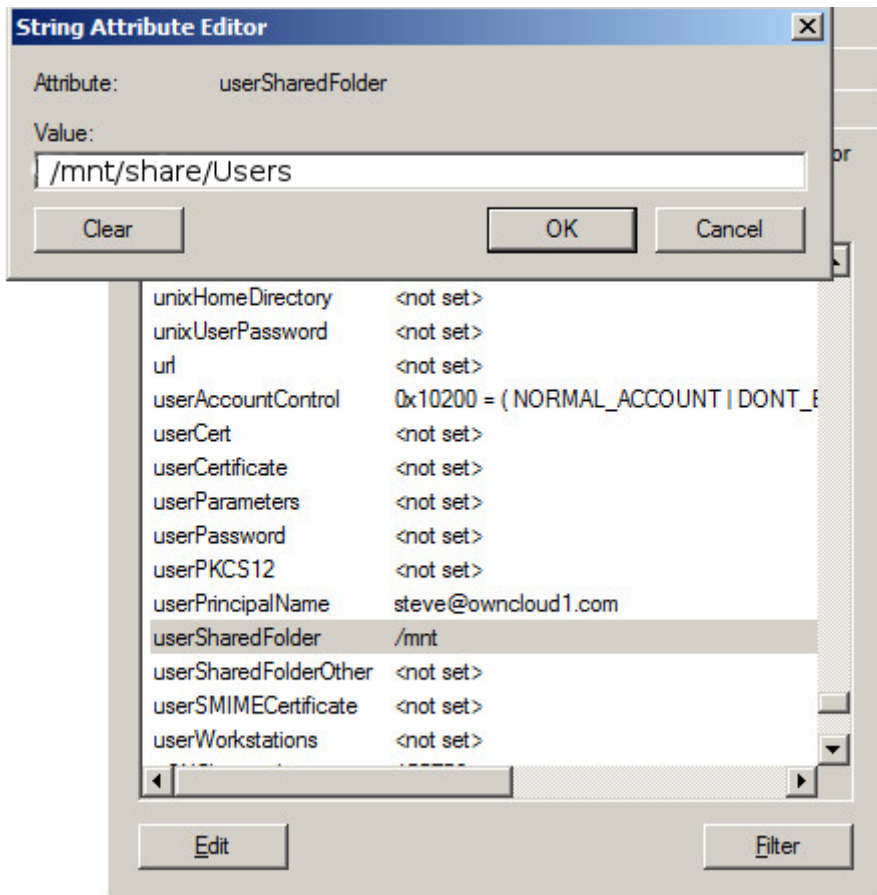
```
//192.168.1.58/home /mnt/share/users cifs credentials=/etc/credentials,uid=33,gid=33
```

Configure the LDAP Server

In Active Directory, open the user profile. Scroll to the **Extensions** section and open the **Attribute Editor** tab.



Use any LDAP attribute that is not already in use (UserSharedFolder in this instance) and click **Edit**. Enter the user's home directory.



Save your changes.

Configure the LDAP Home Connector

- Enable the LDAP Home Connector app.
- 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.
- In the **Attribute name:** field enter the LDAP attribute name from above that contains the home directory and press [**Save**].

LDAP User Home

Display folder as:

Attribute name:

The Windows user's home directory is now available to the user when they log on in ownCloud.

How to Create and Configure Microsoft OneDrive

Introduction

To use the ownCloud OneDrive app, you mandatory need consulting first. Contact sales@owncloud.com to get access to. When granted, follow this guide to use Microsoft OneDrive as an external storage option 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

Microsoft Application Registration Portal Tools Docs Feedback Matthew

Register your application

Application Name
ownCloud OneDrive Storage

Guided Setup
 Let us help you get started

By proceeding, you agree to the [Microsoft Platform Policies](#)

[Create](#)

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.

Copy the password to your preferred password manager, as it is only displayed **once**.

Redirect URLs

Under menu:[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.

Platforms

Add Platform

Web Delete

Allow Implicit Flow

Redirect URLs ⓘ Add URL

http://.../settings/personal

http://.../settings/admin

Logout URL ⓘ

e.g. https://myapp.com/end-session

Application Permissions

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](#)

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`
- `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	886d98b5-1631-4948	Grant access
OneDrive	One Drive	OneDrive OAuth2	58b34aa-7958-4356	Grant access
OneDrive_u2_app4	One Drive	OneDrive OAuth2	954-429b-b9ac-4d3f	Grant access
OneDrive1_u1_app3	One Drive	OneDrive OAuth2	44b4725-8d42-403e	Grant access
OneDrive1_u1_app6	One Drive	OneDrive OAuth2	886d98b5-1631-4948	Grant access
OneDrive_u2_app6	One Drive	OneDrive OAuth2	886d98b5-1631-4948	Grant access

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',
```

The HTTPS prefix, port, and `/index.php` suffix are mandatory.

Configuring SharePoint Integration

Introduction

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 the php modules `php-xml`, `phpseclib` and `php-soap` installed and the SOAP module enabled with `phpenmod soap`. A webserver restart may be required after adding/changing php modules.

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.

Global credentials. These fields can be used for each of the SharePoint mounts

Global credentials is optional. If you fill in these fields, these credentials will be used on all SharePoint mounts where you select: **Use global credentials** as the authentication credentials.

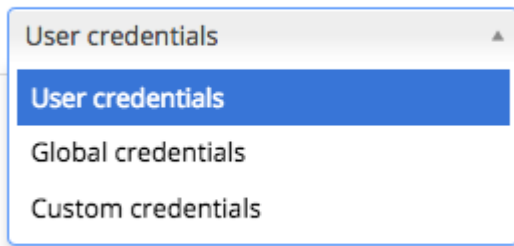
Local Folder Name	Available for	SharePoint Site Url	Document Library
sharepoint 1	All users	https://example.com	folder1
sharepoint 2	All users	https://example2.com	folder2

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 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.

Windows Network Drive (WND)

Introduction

The [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.

Compared to standard SMB access, WND has advanced features like:

1. User lockout prevention and password reset
2. More authentication mechanisms against the backend
3. Listen to change information triggered by the backend
4. Enhanced ACL support
5. Collaborative WND (CWND)

Brief Description of Advanced Features:

User lockout prevention and password reset

Depending on the Windows or Samba policy, users could get locked out of their account if they enter a wrong password a number of times. The lockout prevention tries to avoid this from happening by resetting the password if it is wrong. This is also true for Collaborative WND when using `login credentials saved in database` and a repeatedly running files-scan job which may use outdated credentials. In the case of ownCloud's standard SMB connector, the password won't be reset. It could happen that users get locked out of the file server.

More authentication mechanisms against the backend

Please see the details about the [Enterprise-Only Authentication Options](#)

Listen to change information triggered by the backend

Native Windows File Servers provide the ability to send change notifications regarding modified files and folders somewhere in a share. Samba can send file notifications as well, as long as all the file actions are performed through the SMB protocol. However, it won't work if the action is performed directly inside the filesystem used by Samba. This mechanism then updates the

ownCloud database and provides the changes made to accessing users. Users do not need to manually check for changes in all possible locations of their mount. Changes processed are also propagated to sync clients automatically.

Enhanced ACL support

With enhanced ACL support, both SMB and WND evaluate the file attributes (whether the file is hidden or read-only) to decide what ownCloud permissions the file or folder should have in ownCloud. On top of this, WND can also evaluate the ACLs by using the `ocLdapPermissionManager` in the mount point configuration. This will bring more accurate permissions to ownCloud, especially when each user can have different permissions for the files in Windows. Consider when using CWND, only the default `nullPermissionManager` can be used.

Collaborative WND (CWND)

Compared to a standard WND mountpoint, a collaborative WND mount offers enhanced features. In a CWND, each user shares the same ownCloud internal information for files and folders based on its internal identification (`file_id`). This means that *comments* and *tags* can be shared with all users accessing files and folders of this mount without the need that users must be members of the mount from an ownCloud point of view. A CWND can only be set by an admin in **Settings > Admin > Storage** but not in the users section. With CWND, all accessing users have their own access to the mount with their own credentials but share additional information with other users accessing the same data. See the table below to compare the differences.

Collaborative WND Differences Based on the Mount Type

	Windows Network Drive	Windows Network Drive (collaborative)
Login Credentials	<ul style="list-style-type: none"> User credentials Credentials of the sharer 	<ul style="list-style-type: none"> Log-in credentials, saved in session Log-in credentials, saved in database User entered, stored in database
File ID	Unique per user or from the sharer	Same for all users accessing this mount
Access Rights	From the accessing user or the sharer	From the accessing user
Activities Comments Tags	<ul style="list-style-type: none"> No shared access <ul style="list-style-type: none"> Visibility limited to the user Shared access <ul style="list-style-type: none"> Comments and tags are shared, access based on the sharer 	Comments and tags are shared, access based on the user

More WND Properties

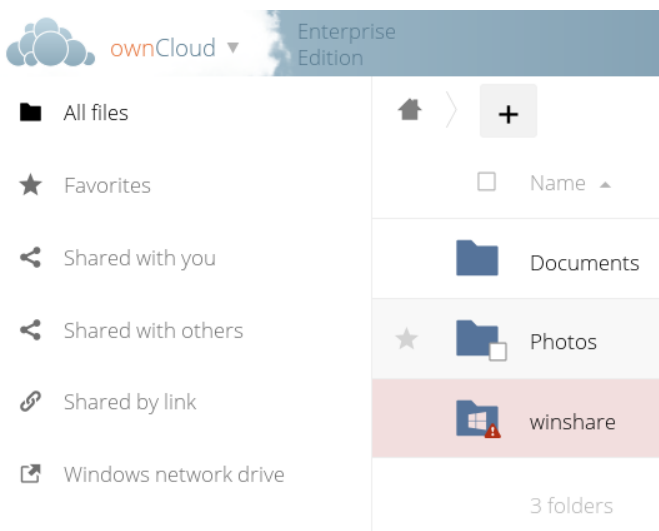
Mounts to a Windows or Samba file server are labeled with a little four-pane Windows-style icon, and the left pane of your Files page includes a Windows Network Drive filter. Figure 1 shows a new Windows Network Drive share marked with a red warning which indicates that ownCloud cannot

connect to the share. The reason is that it may require the user to login, or it is not available, or there is an error in the configuration.

Files are synchronized bidirectionally, 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`. This allows ownCloud to access the shares when the users who own the mounts are not logged in. This access will not work if the mount is session based, where passwords are not stored and are available only for the current active session.

Figure 1. Windows Network Drive share on your Files page



Installation

Install the [External Storage: Windows Network Drives app](#) from the ownCloud Market App or ownCloud Marketplace. To make it work, a few dependencies have to be installed.

- 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.

To install and configure the necessary packages, see the [Prepare Your Server](#) section of the manual installation documentation.



For more information on SMB/CIFS in ownCloud, refer to the [Samba file server configuration documentation](#).



If you encounter errors when using the WND app like `NT_STATUS_REVISION_MISMATCH`, please get in touch with support@owncloud.com.

ownCloud requires at least [Samba 4.7.8](#) or [Samba 4.8.1](#) on the ownCloud server, when:

1. The Windows Network Drive Listener is used; **and**
2. The remote Windows/Samba file server requires at least [version 2.0 of the SMB protocol](#).

The [Windows Network Drive Listener](#) only supports version 1 of the SMB protocol (SMB1) with *earlier* Samba versions.



Background

A [Samba](#) server, often a Microsoft Windows Server, can enforce the minimum and maximum protocol versions used by connecting clients. However, in light of the [WannaCry ransomware attack](#), [Microsoft patched Windows Server](#) to only allow SMB2 as minimum protocol by default, as SMB1 is insecure.

The ownCloud windows network drive listener utilizes the SMB notification feature which works well with SMB1 in conjunction with most Samba versions. However, when the minimum protocol a server accepts is SMB2, ownCloud requires Samba 4.7.8+ (4.8+ etc.) to be able to properly work, as prior versions of Samba had a bug that broke this feature.

Configuration

Enabling External Storage

To enable external storage, as the ownCloud administrator go to **Settings › Storage (in the admin section)**. Tick the checkbox to enable external storage.

Creating a New Share

When you create a new WND share, you need multiple things:

- the login credentials for the share,
- the server address,
- the share name and
- the folder you want to connect to.



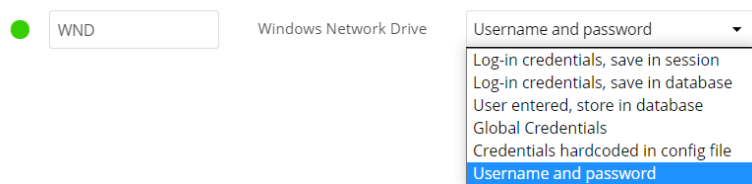
Treat all the parameters as being case-sensitive.

Although some parts of the app might work properly regardless of casing, other parts might have problems if the case is not respected.

Follow this procedure to create a new mount point based on WND

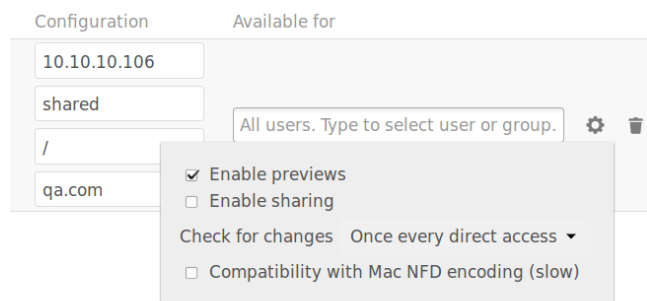
1. Enter the ownCloud mount point for your new WND share. This *must not* be an existing folder.
2. Select your authentication method. See [Enterprise-Only Authentication Options](#) for complete information on the available authentication methods.

Figure 2. WND mountpoint and authorization credentials



3. Enter the address of the server that contains the WND share.
4. The share name provided by Windows or Samba.
5. The root folder of the share. This can be a subfolder name, or the `$user` variable for the user's home directory. 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 3). Sharing is not available for all authorization methods. For details please see the [Enterprise-Only Authentication Options](#). When using large storages with many files, you may want to disable previews, because this can significantly increase performance.

Figure 3. WND server, credentials, and additional mount options



Your changes are saved automatically.



When you create a new mountpoint using login credentials (session based), 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.

Permission Manager

Starting with version 1.0.1 of the Windows Network Drives App [Access Control Lists \(ACLs\)](#) are supported. To obtain the ACL information, two ACL providers can be selected:

- [The Null Permission Manager](#)
- [The ownCloud LDAP Permission Manager](#)

External Storage



Enable external storage

Global credentials for external storage

Username

Password

Save

Folder name	External storage	Authentication	Configuration			Available for
 WindowsNetworkDriv	Windows Network Drive	Username and password	10.0.2.8	opt	Remote subfolder	All users. Type t
 WindowsNetworkDriv	Windows Network Drive	Log-in credentials, save in database	10.0.2.10	Downloads	foo/bar	All users. Type t

Folder name: Add storage:

On standard deployments, you don't need to change anything. Just leave the field empty and the default `nullPermissionManager` permission manager will be used.

Regardless of which provider you choose, an ownCloud administrator should run a `files:scan`, manually, after changing the configuration, to update the permissions correctly. Otherwise, the permissions shown by ownCloud might be incorrect.



Permissions are only auto-updated if there has been a change in the files.

The Null Permission Manager

The `Null Permission Manager` is the default permission manager for ACLs and is used, if no other ACL manager is specified. This is also the case, when no permission is explicitly set. If you want to retain ownCloud's current behaviour, then use this permission manager. When in effect, the Windows Network Drive app uses the file's attributes (e.g., read-only, and hidden), to determine how the user can interact with the file. There are no usage restrictions.

The value to select for this provider is: `nullPermissionManager`.

The ownCloud LDAP Permission Manager

The ownCloud LDAP Permission Manager evaluates ACLs in files along with file attributes to determine the permissions. In order to evaluate the ACLs, it needs access to the user and group membership information of the target Windows or Samba server. Therefore it uses ownCloud's [LDAP Integration app](#) for this.



Both the Windows (or Samba) server and ownCloud's LDAP Integration app must connect to the same Active Directory server so that ownCloud can retrieve the same user and group information.

The use of this provider requires two key things:

- An Active Directory server which contains the standard user and group information that can be used by the [LDAP Integration app](#).
- ownCloud's LDAP Integration app to be [correctly configured](#) to retrieve user and group information from the same Active Directory / LDAP server as the one that the Windows or Samba server uses.



The ownCloud LDAP Integration app must configure the `sAMAccountName` to be the ownCloud server's username.



Some groups, such as `everyone` might not be handled properly. This is because such groups don't exist in the LDAP server, or might not be found if the domain is different, such as `nt authority\system` or `builtin\domain-users`.

The value to select for this provider is: `ocLdapPermissionManager`.

WND Notifications

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 mounted SMB storage. While files changed through the ownCloud Web Interface or sync clients are automatically recognized by ownCloud, recognition is not possible when files are changed directly on remote SMB storage mounts. When using the *listener*, files changed on the SMB backend are recognized and a notification is stored in the database. The *process-queue* job reads these stored notifications and initiates further actions.



The capability of the listener depends on the ability of the used SMB/CIFS storage backend to provide notifications. While Windows file servers have no limitations, some vendors may have restrictions. Please check these with your storage provider. It may be possible, that notifications for Samba only work for the target folder you're listening to, but not for any sub structures. If you're listening on the `/top` folder, you may not receive notifications for `/top/middle/bottom` folder. In this case, you have to setup listeners for every *existing* folder and also for any *new* folders that will be created. With Windows file servers, you will receive notifications for every file or subfolder inside the folder you're listening to.

WND Listener Setup

The WND listener for ownCloud 10 includes two different commands that need to be executed:

- `wnd:listen` Listen to changes and save them in the database
- `wnd:process-queue` Process saved listener changes from the database

`wnd:listen`

This command listens to changes for each host and share configured and stores all notifications gathered in the database. *It is intended to run this command as a service.* The command requires the Windows/Samba account and the host/share the listener will listen to. The command does not produce any output by default, unless an error happens. Each stored notification will be further processed by the `wnd:process-queue` and will be removed from the database after processing.



You can increase the command's verbosity by using `-vvv`. Doing so displays the listeners activities including a timestamp and the notifications received. A *read-only* permission for the used account should be enough, but may need to be increased.

The simplest way, useful for initial testing is, to start the `wnd:listen` process manually, as follows:

```
sudo -u www-data ./occ wnd:listen <host> <share> <username>
```

The password is an optional parameter and you will be asked for it if you didn't provide it as in the example above. If necessary, the workgroup can be set together with the username as well. Use following syntax and set quotes, which is important to keep the backslash '`<workgroup>\<username>`'. The whole example command looks like:

```
sudo -u www-data ./occ wnd:listen <host> <share> '<workgroup>\<username>'
```

In order to start `wnd:listen` without any user interaction like as service, provide the password from a password file.

```
sudo -u www-data ./occ wnd:listen <host> <share> <username> \  
--password-file=/my/secret/password/file \  
--password-trim
```

For additional options to provide the password, check [Password Options](#)

Note that the password must be in plain text inside the file. Neither spaces nor newline characters will be removed from the contents of the file by default, unless the `--password-trim` option is added. The password file must be readable by the apache user (or `www-data`). Also make sure that the password file is outside of any directory handled by apache (web-readable) for security reasons. You may use the same location when using flock in [Execution Serialization](#) below.

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 post booting.

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.

Depending on your requirements, you can wrap that command in a Cron job so it's run every 5 minutes for example.

WND Listener Service Configuration

Create a service for `systemd` following the instructions below that checks for processable notifications:



- Replace the all upper case words `SERVER`, `SHARE`, `USER` and `PASSWORD` in both, the **filename** and in the **contents** below with their respective values.
- Take care to also adjust the paths in `WorkingDirectory` and `ExecStart` according to your installation.

- For each WND mount point distinguished by a `SERVER - SHARE` pair:
 - Replace the all upper case words `SERVER`, `SHARE`, `USER` and `PASSWORD` in both, the **filename** and in the **contents** below with their respective values.
 - Place one copy of a file with the content from below under `/etc/systemd/system/owncloud-wnd-listen-SERVER-SHARE.service`
To do so, enter following command and replace `<name>` with `owncloud-wnd-listen-SERVER-SHARE`:

```
sudo systemctl edit <name>.service
```

Reload the daemon to make it available:

```
sudo systemctl daemon-reload
```

- Take care to also adjust the paths in `WorkingDirectory` and `ExecStart` according to your installation.
 - Password: Create a file readable only by the `www-data` user and outside the directories handled by Apache (let's suppose in `/tmp/mypass`). The file must contain only the password for the share. In this example our file is: `"/tmp/mypass"`. The listener will read the contents of the file and use them as the password for the account. This way, only root and the Apache user should have access to the password.
 - `--password-trim` in directive `ExecStart` removes blank characters from the password file added by 3rdparty software or other services.
- Content template for `owncloud-wnd-listen-SERVER-SHARE`

```
[Unit]
Description=ownCloud WND Listener for SERVER SHARE
After=syslog.target
After=network.target
Requires=apache2.service
[Service]
User=www-data
Group=www-data
WorkingDirectory=/var/www/owncloud
```

```
ExecStart=./occ wnd:listen -vvv SERVER SHARE USER --password-file=/tmp/mypass
--password-trim
Type=simple
StandardOutput=journal
StandardError=journal
SyslogIdentifier=%n
KillMode=process
RestartSec=3
Restart=always
[Install]
WantedBy=multi-user.target
```

- Run the following command, once for each created file:

```
sudo systemctl daemon-reload
sudo systemctl enable owncloud-wnd-listen-SERVER-SHARE.service
sudo systemctl start owncloud-wnd-listen-SERVER-SHARE.service
```

- To list all systemd wnd listeners for ownCloud run the following command, assuming you use the naming convention described above:

```
systemctl list-units | grep owncloud-wnd-listen
```

- Please re-run the following commands if you are changing the contents of a particular listener service:

```
sudo systemctl daemon-reload
sudo systemctl restart owncloud-wnd-listen-SERVER-SHARE.service
```

For more information about configuring services for systemd, read [How To Use Systemctl to Manage Systemd Services and Units](#)

WND Process Queue Configuration

Create or add a `crontab` file in `/etc/cron.d/oc-wnd-process-queue`.



The commands must be **strictly sequential**. This can be done by using `flock -n` and tuning the `-c` (chunk-size) parameter of `occ wnd:process-queue`, see the [wnd occ commands](#) description and the [Execution Serialization](#) below.

- Make a `crontab` entry to run a script iterating over all `SERVER SHARE` pairs with an appropriate `occ wnd:process-queue` command.

```
* * * * * sudo -u www-data /var/www/owncloud/occ wnd:process-queue <HOST> <SHARE>
```


Execution Serialization

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.

It's recommended to force the execution serialization of the `wnd:process-queue` command. 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 /opt/my-lock-file sudo -u www-data ./occ wnd:process-queue <host> <share>
```

In that case, `flock` will try to 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.

The lock file `/opt/my-lock-file` itself will be created as an empty file by the `flock` command if it does not yet exist, but after it has been created the lock file doesn't change. Only an `flock` will be applied and removed. The file won't be removed after the script completes.

You can use `flock` also in cron, see the example below:

```
* * * * * flock -n /opt/my-lock-file -c 'sudo -u www-data /var/www/owncloud/occ  
wnd:process-queue <HOST> <SHARE>'
```

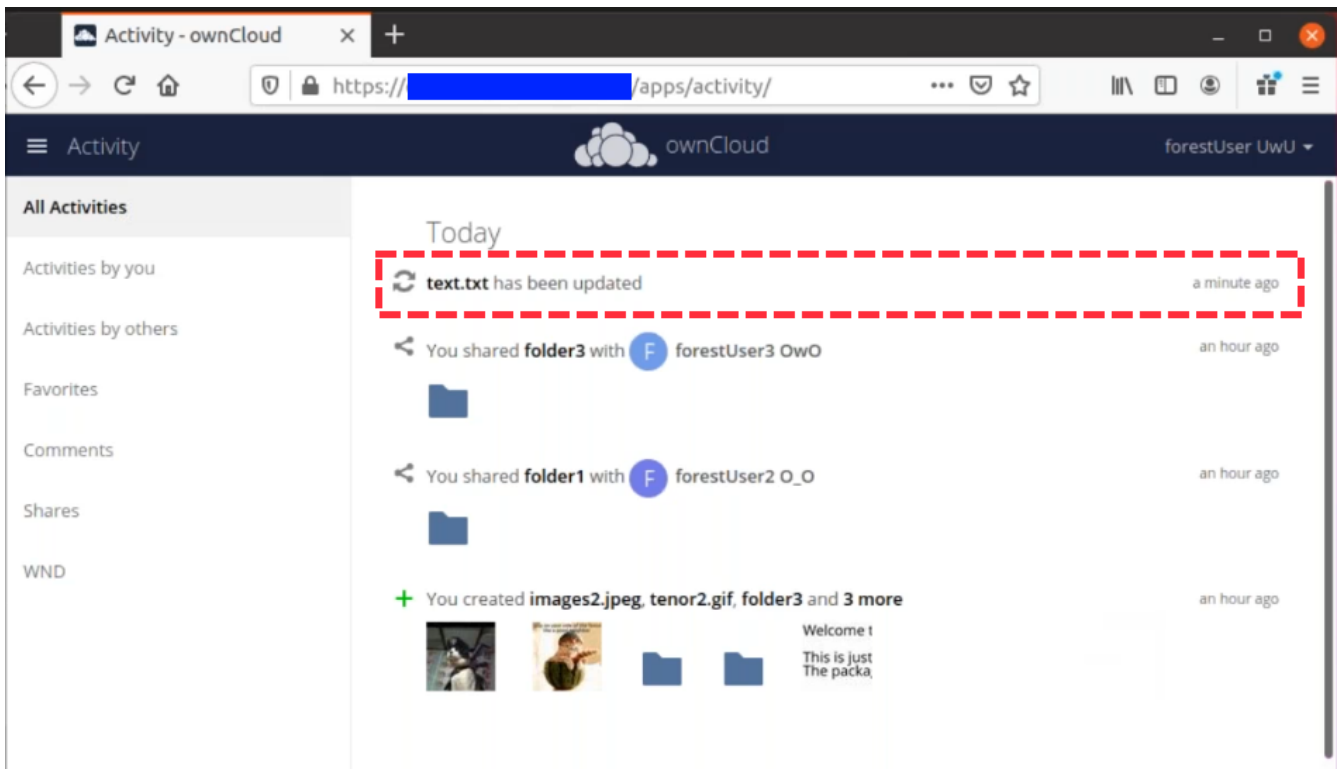
Check [flock's documentation](#) for details and more options.

Activity Extension

From version 2.0.0 the Windows Network Drive app includes an extension of the Activity app. This extension will allow the app to send events to the Activity app so the users know what happened in the Windows Network Drive storage.

Please see Figure 4 how a notification can look like. In this example, one user accessing the same host/share has changed a file. Other users will now get an activity notification about this change.

Figure 4. Activity Notification for a Changed File



This extension requires the following components:

- `wnd:listen` command set up and running in order to get the storage events
- `wnd:process-queue` command running periodically (or manually) over the event queues generated by the `wnd:listen` command
- The Activity app enabled

For setting up the `wnd:listen` and `wnd:process-queue` commands, see their respective sections above.

This extension is disabled by default. This means that no activity will reach the users. In order to enable this extension, you can edit the `config/config.php` file and add the following configuration:

```
'wnd.activity.registerExtension' => true,
```



This configuration will affect all the WND mount points

The events that will be shown to the users are based on what the `wnd:process-queue` detects and changes in the ownCloud's FS. Since the command includes some optimizations, some events might be inaccurate in some scenarios. For example, if multiple files are added in the same folder, there won't be multiple "file added" events but only one "folder modified" in the parent folder.

The events are expected to reach only to the affected users. This filters out the users who cannot access the mount point, and also the users who do not have enough permissions in the Network Drive (Windows, Samba) to access that file.

As part of the Activity app configuration, users can decide which events they want to be notified about and how, in the activity stream or via email.

Users who can access the Windows Network Drive storage via share won't receive activity notifications by default. You can add the following configuration in the `config/config.php` file to enable sending the activity notification to those users.

```
'wnd.activity.sendToSharees' => true,
```



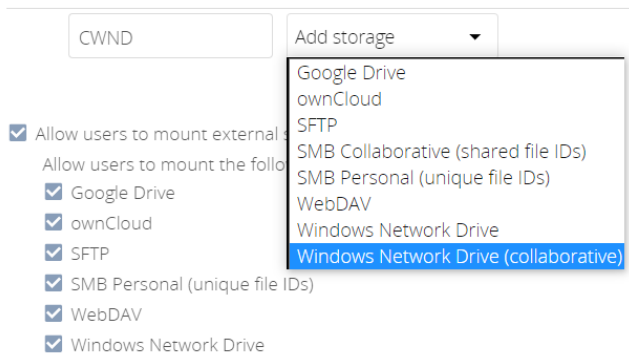
`wnd.activity.sendToSharees` key depends on the `wnd.activity.registerExtension` key to take effect.

Collaborative WND

CWND can only be set by an admin in **Settings > Admin > Storage**. This mount type cannot be selected by users in the user section. To prepare access for your mount point using the CWND mount type, you must provide a *Service Account* (SA) which is an ordinary SMB user granting read access to the share you want to mount. You can use one SA for all CWND mounts or separate ones. The SA is used to gather the contents of a share used by the WND Listener and provides a common `file_id` to all accessing users, while the accessing users can only access those files and folders for which they've been granted rights.

1. As an admin, go to **Settings > Admin > Storage** and create a new CWND based mount point.

Figure 5. Add a Collaborative Windows Network Drive Mount



2. Chose any name for the mount point that fits your needs.
3. Select user login type.

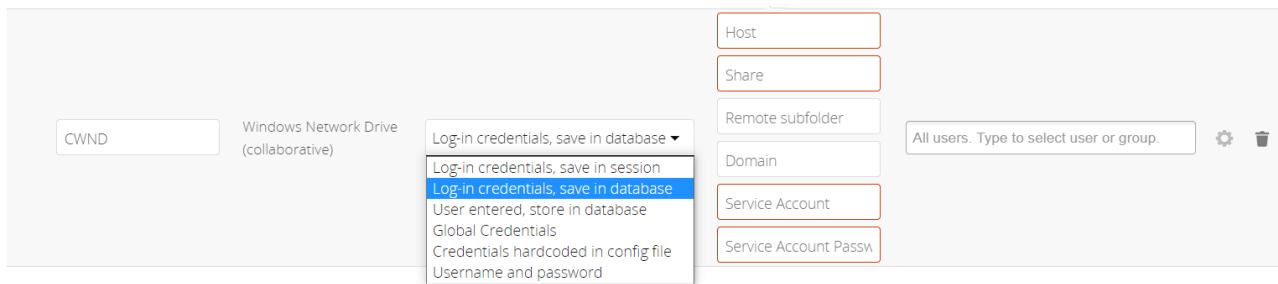


The following three are sensible and working selections for CWND:

- a. Log-in credentials, saved in session
- b. Log-in credentials, saved in database
- c. User entered, stored in database ^[1]

[1] Must be used if user authentication is made with OIDC

Figure 6. Select How User Logs in to the Mount Point



a. Log-in credentials, saved in session

When the user logs in to ownCloud via a browser, the credentials to authenticate CWND are taken from this login. These credentials immediately end when the user logs out because the session has ended.

- This login type can not be set to **Enable Sharing**.
- This login type is by design not compatible with **OIDC authentication**.

b. Log-in credentials, saved in database

Similar to **Log-in credentials, saved in session**, the credentials to authenticate CWND are taken from the login but saved in the ownCloud database. Any re-login also updates the database entry. As the credentials to access CWND are taken from the database, a user logout will not stop CWND access and serving data is continued, e.g. for synchronization.

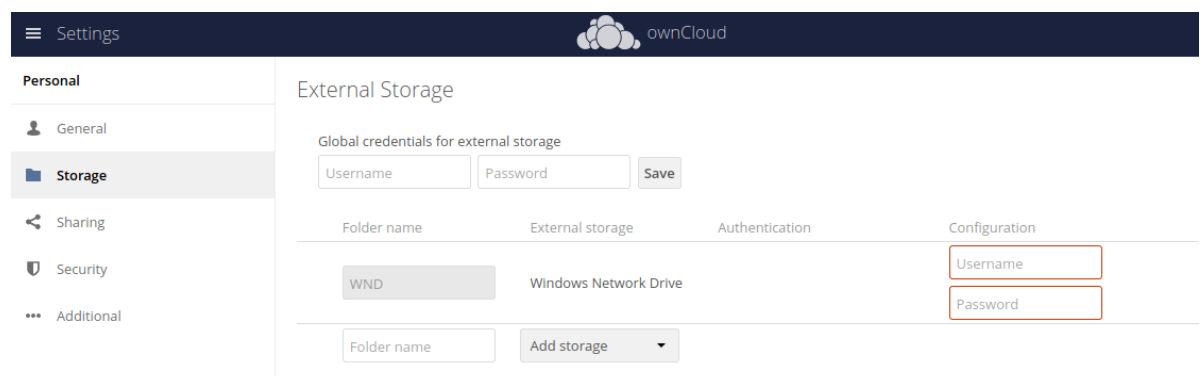
- This login type can be set to **Enable Sharing**.
- This login type is by design not compatible with **OIDC authentication**.

c. User entered, stored in database

User login to ownCloud and providing credentials to access the CWND mount are completely separated. After logging in to ownCloud, the user may see his CWND mounts marked inaccessible. To regain access, the user must enter his share credentials in **Settings** > **Personal** > **Storage** which are then stored into the ownCloud database. As the credentials to access CWND are taken from the database, a user logout will not stop CWND access and serving data is continued, e.g. for synchronization.

- This login type can be set to **Enable Sharing**.
- This login type is by design **the only one compatible with OIDC authentication**.

Figure 7. Re-enter Mount Access Credentials



4. Configure this mount point by adding required data into the corresponding fields

Figure 8. Enter Connection Info and the Service Account



Starting with ownCloud 10.8, you can properly enter the correct password without using the deprecated `occ wnd:set-service-account`, as the security measures have been improved and all fields in the mount settings marked as *password* are now encrypted from the beginning by default. Existing settings are automatically migrated when upgrading.

When everything has been entered correctly, the mount point gets a green button on the left.

Troubleshooting

General or Connectivity Issues

If you encounter issues using Windows network drive, then try the following troubleshooting steps:

First check the connection to the share by using `smbclient` on the command line of the ownCloud server. Here is an example:

```
smbclient -U Username -L //Servername
```

Take the example of attempting to connect to the host `MyHost`, the share named `MyData` using `occ wnd:listen` replacing user and password accordingly. Running the following command would work:

```
sudo -u www-data ./occ wnd:listen MyHost MyData user password
```



The command is case-sensitive, and that it must match the information from the mount point configuration.

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 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.

Basic Setup for One ownCloud Server

1. Go to the admin settings and set up the required WND mounts. Be aware though, that there are some limitations. These are:
 - a. ownCloud needs 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. ownCloud suggests to use *"login credentials, saved in DB"* as the best replacement instead.
 - b. The `$user` placeholder for the share name, such as `//host/$user/path/to/root`, 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 equals one listener per user. 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`.
2. 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.

3. 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
```



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.



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`.

- 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.
- Using the service account password, which is already stored in the database if you setup WND in collaborative mode. In this mode, you set the username and the option for the `occ` command to reuse the password stored in the database. The example command looks like:

```
sudo -u www-data ./occ wnd:listen <host> <share> <username>
--password-from-service-account
```



You need to ensure that the triple of `<host>`, `<share>` and `<username>` (including any kind of workgroup if used) matches the configuration made for the WND collaborative share. The command will fail otherwise.

Reduce WND Notifier Memory Usage

The WND in-memory notifier for password changes provides the ability to notify all *affected* WND storages to reset their passwords. This feature is intended to prevent a password lockout for the user in the backend. However, this functionality *can* consume a significant amount of memory. To disable it, add the following configuration to your `config/config.php`:

```
'wnd.in_memory_notifier.enable' => false,
```



The password will be reset on the next request, regardless of the flag setting.

3rd Party Software Examples

Third party password managers or processes can 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.

plainpass

This provides a bit more security because the `/tmp/plainpass` password as shown below 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.

```
cat /tmp/plainpass | sudo -u www-data ./occ wnd:listen <host> <share> <username>
```



```
--password-file=-
```

base64

Similar to plainpass, the content in this case gets encoded in the [Base64 format](#). There's not much security, but it has additional obfuscation.

```
base64 -d /tmp/encodedpass | \  
sudo -u www-data ./occ wnd:listen <host> <share> <username> --password-file=-
```

pass

Example using "pass"

- You can go through [manage passwords from the command line](#) to set up 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=-
```

HashiCorp Vault

This example uses [Vault](#) as the secrets store. See [HCP Vault](#) on how to setup the secrets store. Then use something like the following:

```
vault kv get -field=password secret/samba | sudo -u www-data ./occ wnd:listen <host>  
<share> <username> --password-file=-
```

Use Vault's ACLs to limit access to the token. Destroy the token after starting the service during boot with systemd.

Password Option Precedence

If both the argument and the option are passed, e.g.,

```
sudo -u www-data ./occ wnd:listen <host> <share> <username> <password> --password-  
file=/opt/pass`
```

then the `--password-file` option will take precedence.

Optimizing wnd:process-queue



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-param`. 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>	<code>file</code> . Other valid values may be added in the future, as more implementations are requested.
<code>--serializer-param</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-param 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.



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 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 from 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.

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 serialize 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-param file=/opt/oc/store

sudo -u www-data ./occ wnd:process-queue host2 share2 -c 500 \
  --serializer-type File \
  --serializer-param 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-param file=/opt/oc/store1

sudo 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, in case the admin has reset some passwords or has been notified about password changes).

Performance on High Number of ACL Targeting Users

The WND app doesn't know about the users or groups associated with ACLs. This means that an ACL containing "admin" might refer to a user called "admin" or a group called "admin". By default,

the group membership component considers the ACLs to target groups, and as such, it will try to get the information for such a group. This works fine if the majority of the ACLs target groups. If the majority of the ACLs contain users, this might be problematic. The cost of getting information on a group is usually higher than getting information on a user. This option makes the group membership component assume the ACL contains a user and checks whether there is a user in ownCloud with such a name first. If the name doesn't refer to a user, it will get the group information. Note that this will have performance implications if the group membership component can't discard users in a large number of cases. It is recommended to enable this option only if there are a high number of ACLs targeting users. In order to enable this setting, you can edit the `config/config.php` file and add the following configuration:

```
'wnd.groupmembership.checkUserFirst' => true,
```

WND Configuration Quick Guide

Introduction

This is a quick guide for installing and configuring the Windows Network Drive (WND) app.

Prerequisites

To successfully use the Windows Network Drive app, you must meet the prerequisites which can be found in the [Server Preparation for Ubuntu 20.04](#). In particular, these are the sections required which address `smbclient` ([Clean Ubuntu 20.04 Installation](#)) and `libsmbclient-php` ([libsmbclient-php Library](#)).

Installation

Install the WND app either via the Web Interface or the command line:

WebUI

- The Windows Network Drive app has to be downloaded from the Market App. Navigate to the Market app, search for Windows Network Drive and install it.
- Post installing enable it via **Settings** > **Admin** > **Apps**.

Command line

```
sudo -u www-data ./occ market:install windows_network_drive
```

```
sudo -u www-data ./occ app:enable windows_network_drive
```

Configuration

WebUI

Enable external shares:

- Navigate to **Settings > Admin > Storage**
- Enable the external storage
- Create a new share and choose Windows network Drives

Configure external share:

- Folder Name: A name for the WND Share
- Authentication: Choose **Log-in credentials, save in database**
- Host: domain name or IP address
- Share: name of the top share
- Remote Subfolder: enter `$user` for every user to get a home drive
- Permission Manager: leave empty to use the default one
- Domain: domain name of your server
- Available for: limit access to groups
- Settings: (gear wheel) enable the options you need



If you plan to use ownCloud **only** in the Web Browser - your setup of the WND is complete.

If you plan to use a desktop client, you need to continue and configure the WND listener and WND process queue.

Commandline

Lastly, you need to setup the wnd listener and process queue to propagate the changes made directly on the storage of your share to the sync client.

This can be done in 2 ways:

- you configure a new systemd service for the listener and setup a process queue cron job
- you setup a cronjob for the wnd:listen command and process queue cron job

WND Listener Configuration

Create a service for systemd following the instructions below that checks the share for changes:

- For each WND mount point distinguished by a SERVER - SHARE pair:
 - Replace the all upper case words **SERVER**, **SHARE**, **USER** and **PASSWORD** in both, the **filename** and in the **contents** below with their respective values.
 - Place one copy of a file with the content from below under `/etc/systemd/system/owncloud-wnd-listen-SERVER-SHARE.service`
To do so, enter the following command and replace `<name>` with `owncloud-wnd-listen-SERVER-SHARE`:

```
sudo systemctl edit <name>.service
```

Reload the daemon to make it available:

```
sudo systemctl daemon-reload
```

- Take care to also adjust the paths in `WorkingDirectory` and `ExecStart` according to your installation.
 - Password: Create a file readable only by the `www-data` user and outside the directories handled by Apache (let's suppose in `/tmp/mypass`). The file must contain only the password for the share. In this example our file is: `"/tmp/mypass"`. The listener will read the contents of the file and use them as the password for the account. This way, only root and the Apache user should have access to the password.
 - `--password-trim` in directive `ExecStart` removes blank characters from the password file added by 3rdparty software or other services.
- Content template for `owncloud-wnd-listen-SERVER-SHARE`

```
[Unit]
Description=ownCloud WND Listener for SERVER SHARE
After=syslog.target
After=network.target
Requires=apache2.service
[Service]
User=www-data
Group=www-data
WorkingDirectory=/var/www/owncloud
ExecStart=/usr/bin/php ./occ wnd:listen -vvv SERVER SHARE USER --password
-file=/opt/mypass --password-trim
Type=simple
StandardOutput=journal
StandardError=journal
SyslogIdentifier=%n
KillMode=process
RestartSec=3
Restart=always
[Install]
WantedBy=multi-user.target
```

- Run the following command, once for each created file:

```
sudo systemctl enable owncloud-wnd-listen-SERVER-SHARE.service
sudo systemctl start owncloud-wnd-listen-SERVER-SHARE.service
```

WND Process Queue Configuration

Create or add a `crontab` file in `/etc/cron.d/oc-wnd-process-queue`.

- Make a `crontab` entry to run a script iterating over all `SERVER SHARE` pairs with an appropriate `occ wnd:process-queue` command. The commands must be **strictly sequential**. This can be done by using `flock -n` and tuning the `-c` parameter of `occ wnd:process-queue`

```
* * * * * sudo -u www-data /usr/bin/php /var/www/owncloud/occ wnd:process-queue  
<HOST> <SHARE>
```

Execution Serialization

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.

It's recommended to force the execution serialization of the `wnd:process-queue` command. 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 /tmp/wnd001 occ wnd:process-queue server1 share1  
* * * * * flock -n /tmp/wnd002 occ wnd:process-queue server1 share2  
* * * * * flock -n /tmp/wnd003 occ wnd:process-queue server2 share3
```

Troubleshooting

- The process queue will not work if there is a backslash in the share path configured in webui.
- The process queue will not work if the share name in the webui is configured starting with a forward slash `/`.

If you encounter issues using Windows network drive, then try the following troubleshooting steps:

Check the connection to the share by using `smbclient` on the command line of the ownCloud server. Here is an example:

```
smbclient -U Username -L //Servername
```

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
```


The command is case-sensitive, and it must match the information from the mount point configuration.

- When the output of the `occ process-queue ..` command shows `0 Storages found`, then this means, that there was no corresponding external storage configuration found, because:
 1. The casing between calling the process queue and the web interface does not exactly match.
 2. The authentication method is not correctly configured, it needs to be **Log-in credentials, save in database**

Unresolved directive in modules/admin_manual/pages/enterprise/file_management/index.adoc - include::partial\$section_page.adoc[]

Advanced File Tagging With the Workflow App

Introduction

The [Workflow App](#) enables admins to specify rules and conditions (file size, file mimetype, group membership and more) to automatically assign tags to uploaded files. Based on those tags automated file operations ('Workflow actions') like File Retention (automated file retention periods) can be conducted. The app has three parts:

- Tag Manager
- Automatic Tagging
- Retention

The Workflow App should be enabled by default (Apps page), and the three configuration modules will be 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



To use tag management, administrators need to install and enable the [Collaborative Tags Management](#) app.

The Tag Manager is used for creating new tags, editing existing tags, and deleting tags. Tags may be marked as **Visible**, **Static**, **Restricted**, or **Invisible**.

Visible

All users may see, rename, and apply these tags to files and folders.

Static

Only users in the specified groups can assign and un-assign the tag to a file. However, only admins can rename and edit the tag.

Restricted

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

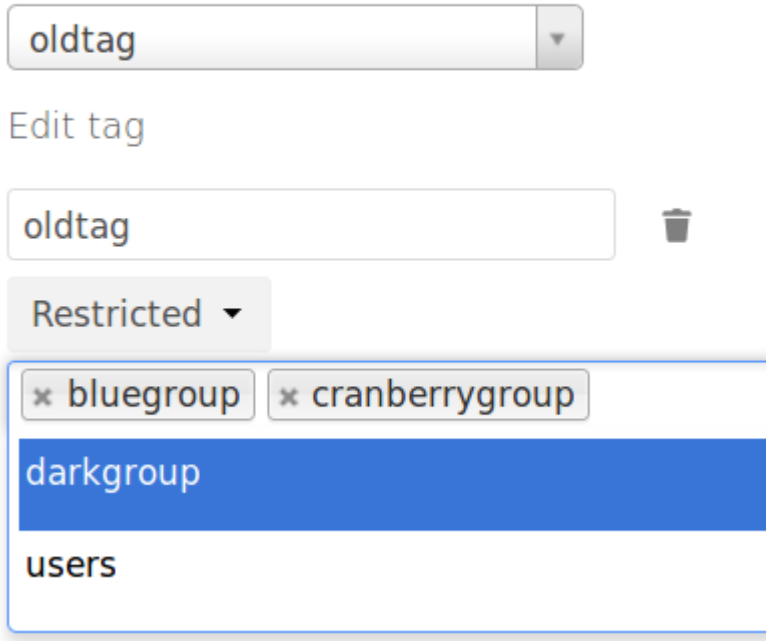
(restricted).

Invisible

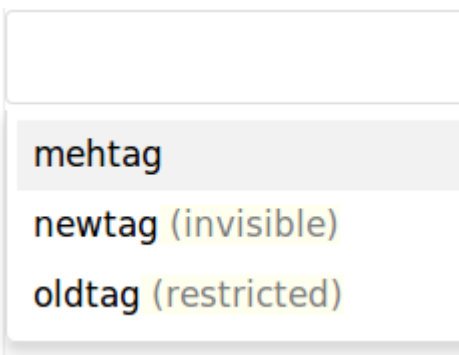
Tags are visible only to ownCloud admins.

To access this functionality, select **Settings** › **Admin** › **Workflow & Tags**.

Collaborative tag management



This is an example of what your tags look like in the **Tags** view on your files page. Non-admin users will not see invisible tags, but visible and restricted tags only.



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:

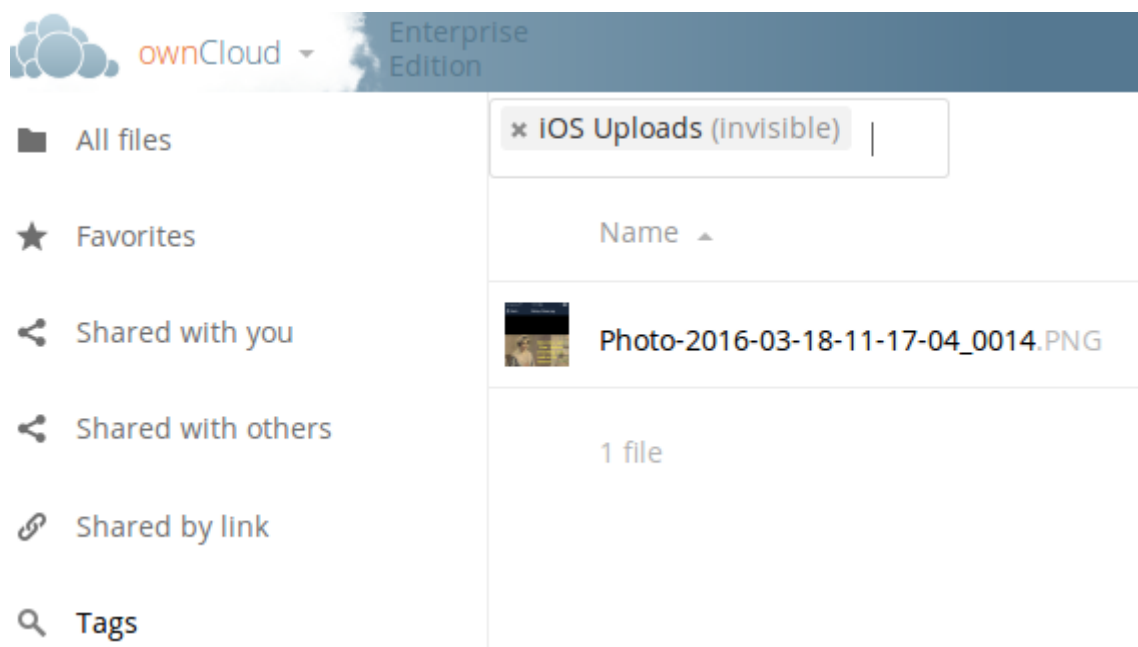
Device type is **iOS Client**

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 is a navigation sidebar with options: All files, Favorites, Shared with you, Shared with others, Shared by link, and Tags. The main area displays a filter for 'x IOS Uploads (Invisible)'. Below the filter, there is a table with a header 'Name' and one row containing a file icon and the name 'Photo-2016-03-18-11-17-04_0014.PNG'. Below the table, it indicates '1 file'.

Automatic Tagging is especially useful with the Retention module.

The settings of a workflow can be fine-tuned post creation, see the example below:

Add tags ▾ + Add new workflow

Edit workflow

Big File WF

Conditions:

File size is greater than ▾ 100 MB 

Select a condition ▾ +

Add tags: the big files ✕

Update workflow Cancel

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).



ownCloud does not preserve directory mtimes (modification time), though it does update file mtimes.

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

This is the default setting and 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.

You can define the way that the retention engine behaves by adding the following `config.php` setting. The value can be either `tagbased` (default) or `userbased`.

```
'workflow.retention_engine' => 'userbased',
```

File Lifecycle Management

Introduction

The File Lifecycle Management extension allows service providers to manage the lifecycle of files within ownCloud to

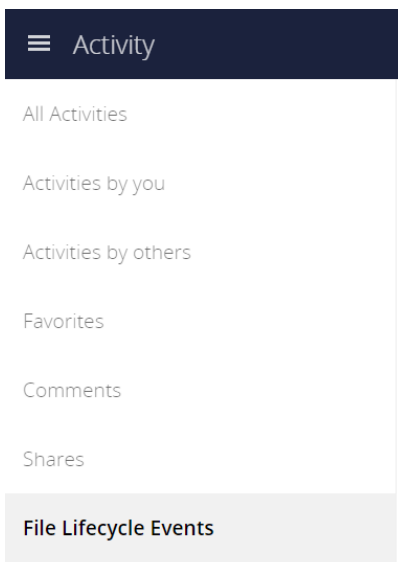
- keep storage usage under control by limiting the time users can work with files before they are cleaned up automatically
- comply with regulations (like GDPR or company policies) by imposing automated retention and deletion policies for files that contain e.g., personal data and may only be stored in the company for a certain period of time.

To impose a workflow of Use ⇒ Archive ⇒ Delete, the extension equips ownCloud with a dedicated archive and allows administrators to define rules for automated archiving (days passed since upload) and subsequent deletion of files (days passed since archiving). Only files are archived as folders do not consume storage space and existing folder structures should be kept available. The archiving and deletion processes are controlled by background jobs.

Depending on the desired level of enforcement, the extension provides two policies to control the restoration of files from the archive if they are still needed:

- **Soft policy:** Users can restore files in self-service
- **Hard policy:** Only administrators or group administrators can restore files on request

Users can view the lifecycle status for a file and see when the file is scheduled for archiving or deletion. All lifecycle events of a file are displayed transparently. They can be tracked for individual files as well as for a whole user account using the [Activity](#) stream.



To stay informed, users can also receive regular Activity summaries by email. For auditing purposes, the extension integrates with the [Auditing](#) app to provide all events of interest in the logs.

Setup & Configuration

See the [lifecycle occ command set](#) for details when using the command line.

Archive Location

By default, archived files are stored within the ownCloud data directory but outside the users' files directories so that they are not accessible using the Web UI and other clients.

Type	Location
User files	<code><datadir>/<userid>/files</code>
Archived files	<code><datadir>/<userid>/archive/files/</code>

Setting Upload Times for Existing Files

File Lifecycle Management uses the *upload time* of files (server time at which they first appeared on the ownCloud server) to determine when to archive them. As ownCloud Server generally does not store this metadata, the File Lifecycle Management extension takes care of this when it is enabled.

When File Lifecycle Management is set up on an existing ownCloud installation, you therefore have to set an *upload time* for all files that existed before the extension has been enabled. The same applies if it was temporarily disabled. Only then can the archiving policies work. To set an upload time for all files that do not yet have one, you can use the `occ` command `lifecycle:set-upload-time`.



Files without an *upload time* will not be considered for archiving.



You only have to conduct this process once when setting up File Lifecycle Management on an installation with existing files or if it was temporarily disabled. Files added after enabling File Lifecycle Management will be tracked automatically.

Example to set missing upload time values to November, 1st 2019:

```
sudo -u www-data ./occ lifecycle:set-upload-time 2019-11-01
```



The extension only considers files. Folder structures are kept available.

Policy Configuration

Overview

File Lifecycle Management uses policies to determine which files to archive and when, as well as when to expire the files from archive. In addition, a soft and a hard policy are available to control whether users can restore archived files in self-service or not.

Three options are available for controlling the archiving and expiration policies, all set via the `config:app:set occ` command under the `files_lifecycle` app:

- `archive_period` - The number of days passed after upload (or restore) that files will be archived
- `expire_period` - The number of days passed after archiving that files will be permanently deleted
- `excluded_groups` - Allows defining groups of users that are exempt from the Lifecycle policies (comma-separated group ids)

Example to set the time passed since upload (or restore) for archiving files to 90 days:

```
sudo -u www-data ./occ config:app:set files_lifecycle archive_period --value='90'
```

To query existing values, use this example command:

```
sudo -u www-data ./occ config:app:get files_lifecycle archive_period
```

Restoration Policies for Users

Soft Policy

The *soft policy* aims at use cases where users should be allowed to restore files from the archive in self-service if they are still needed. It imposes a soft archiving enforcement but on the other hand relieves IT departments when archived files need to be restored. The *soft policy* is used by default. To switch from the hard policy to the soft policy, use this `occ` command:

```
sudo -u www-data ./occ config:app:set files_lifecycle policy --value='soft'
```

Hard Policy

The *hard policy* is designed to enforce strict controls on user data, forcing archiving after the defined time and requiring escalated permissions in order to restore. If the archived data is still

needed, users need to get in contact with a privileged manager and request the restoration.



When the *hard policy* is in place only administrators (or also group administrators, depending on the configuration) are able to restore files from the archive by impersonating the respective users. The [Impersonate app](#) has to be installed and enabled as a prerequisite. Apart from that, system administrators can also use *occ* commands to restore data from the archive (see section [Restoring Files](#)).

To put the *hard policy* in place, use this *occ* command:

```
sudo -u www-data ./occ config:app:set files_lifecycle policy --value='hard'
```

Archive and Expiration Background Jobs

To put File Lifecycle Management into actual operation, there are two *occ* commands for archiving files and for permanently deleting them from the archive. Scanning the database for files that are due for archiving or expiration, given the chosen policies, can take some time. For this reason, these jobs are delegated to specific *occ* commands which should be executed using CRON on a daily schedule.

Archiving Background Job

To move files scheduled for archiving (days since upload/restore > *archive_time*) into the archive, execute the following *occ* command:

```
sudo -u www-data ./occ lifecycle:archive
```



There is a dry-run mode (append *-d*) that simulates the execution of this command to allow checking the configuration before putting the actual process in place.

Archive Expiration Background Job

To permanently delete files from the archive that have met the policy rules (days since archiving > *expire_period*), execute the following *occ* command:

```
sudo -u www-data ./occ lifecycle:expire
```



There is a dry-run mode (append *-d*) that simulates the execution of this command to allow checking the configuration before putting the actual process in place.

Restoring Files

If archived files are still needed, users can restore them in self-service (*soft policy*) or have to request the restoration via privileged managers (*hard policy*).



When files have been restored, they can again be used for the same amount of time as they were initially available.

Apart from that, system administrators can restore files from the archive using the `occ` command `lifecycle:restore`:

Restoration by Path

When a user `alice` requests to restore all files, e.g., in the folder `/work/projects/project1`, a system administrator can execute the following command:

```
sudo -u www-data ./occ lifecycle:restore /alice/archive/files/work/projects/project1
```

Restoring All Files from All Archives

File Lifecycle Management provides a way to restore all files from all archives back to their owners' file directories. To do this, system administrators can use the `restore-all` `occ` command:

```
sudo -u www-data ./occ lifecycle:restore-all
```

The command will restore all files from all users and report on the progress.



There is a dry-run mode (append `-d`) that simulates the execution of this command to allow checking the configuration before putting the actual process in place.

Enabling/Disabling the User Interface Components

In some scenarios it can be desired to disable the whole user interface for this app. This can be done by setting the following configuration value:

```
sudo -u www-data ./occ config:app:set files_lifecycle disable_ui --value='yes'
```

To enable the user interface components again, this config value needs to be removed:

```
sudo -u www-data ./occ config:app:delete files_lifecycle disable_ui
```

Audit Events

During archiving, restoring and expiration, Audit events are emitted. Logging those to the `audit.log` requires the minimum version 2.0.0 of the [Auditing](#) app.

Further Notes about Archived Files

- File shares will disappear after archiving. When restoring archived files, shares will also be restored.

- Users' archives currently can't be transferred with the occ command `transfer-ownership`
- Files within a user's trash bin are not archived. The regular trash bin deletion policies have to be used to take care of those.
- Archived files count towards the user's quota

Unresolved directive in modules/admin_manual/pages/enterprise/firewall/index.adoc - include::partial\$section_page.adoc[]

File Firewall

Introduction

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.



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 [**Add Group**]. After setting up your rules you must click [**Save Rules**].

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.

Logging

Save Rules

Blocked Requests Only ▾

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.

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 displays two rule configurations in a web interface. The first rule is titled "No support outside o". It has two conditions: "User Group" is "support" and "Request Time" is "between" "05:00 pm +0545" and "09:00 am +0545". The second rule is titled "No QA outside of the". It has two conditions: "User Group" is "qa-team" and "IP Range (IPv4)" is "is not" "192.168.1.0/24". Each rule has a "Delete" button. At the bottom of each rule configuration are buttons for "+ Add rule", "+ Add group", and "Delete".

Logging

Save Rules

Blocked Requests Only ▾

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.

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 contain) with a given string.

Request Type

The request (is a public link share | 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 | greater or equal) to the given size.

File Mimetype Upload

Block a request based on the mimetype of a file being uploaded. The match can be the complete mimetype, part of the mimetype from the start or end of the mimetype. Negative matches are also supported; i.e., all mimetypes that don't match the supplied mimetype, or all mimetypes that don't start or end with the partial mimetype supplied.

The full list of conditions is (File mimetype upload):

- is
- is not
- begins with
- doesn't begin with
- ends with
- doesn't end with



The complete list of available mimetypes which ownCloud supports is available [in the ownCloud core source](#).

Common Mimetypes

suffix	mimetype
avi	video/x-msvideo
exe	application/x-ms-dos-executable
flv	video/x-flv
mp4	video/mp4

suffix	mimetype
mkv	video/x-matroska
msi	application/x-msi
php	application/x-php

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
- 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
```



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**.



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`

Installing & Upgrading ownCloud Enterprise Edition

Introduction

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 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 if 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` like in this example:

```
'license-key' => 'test-20150101-XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX-YYYYYY',
```

It is also possible to activate your Enterprise Edition on the webUI. Open owncloud and navigate to: **Settings** › **Admin** › **General**. Copy your license key into the field **Enter a new license:** and click **Save** to confirm.

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.



if you want to remove the current license, open ownCloud and navigate to **Settings** › **Admin** › **General** and click [**Remove current license key**].

User Counting

Your ownCloud Enterprise License Key is valid for the purchased amount of users, as per the ownCloud EULA - ownCloud Commercial License. When you generate a `config.report`, you will get:

- a counting of the enabled users,
- the ownCloud guest users — if the guest app is enabled and
- the number of user directories created.

The latter is the user number you will need licenses for. Guest users are currently counted with a fair use policy — which means, that you can't have more guest users than you have licensed users. If you exceed the number of licensed users, please contact your account manager or ownCloud Partner and true-up as per your contract or EULA with us. The user directories are created on first login. When a user is deleted, the user directories are deleted as well. Users which are disabled count. The last login is not relevant.

Supported ownCloud Enterprise Edition Apps

See [Supported Apps in ownCloud](#) for a list of supported apps.



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.

Oracle Database Setup & Configuration

Introduction

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, create synonym, alter session TO owncloud;
```

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 to install the [Oracle Instant Client](#) (OCI8) extension from the Ubuntu Community Wiki.



This *should* work for other Debian-based distributions too, 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, where you have to specify the correct OCI8 version. For PHP7.x use `oci8-2.2.0`



Provide: `instantclient,/usr/lib/oracle/12.2/client64/lib` when requested, or let it auto-detect the location, if possible.

```
sudo pecl install oci8-2.2.0
```

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

Debian & Ubuntu

PHP Version	Filename
7.3.0	<code>/etc/php/7.3/apache2/conf.d/20-oci.ini</code>

RedHat, Centos, & Fedora

PHP Version	Filename
7.3.0	<code>/etc/opt/rh/rh-php73/php.d/20-oci8.ini</code>

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:

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$database; (requires DBA privileges)
```

Show ownCloud Tables in Database:

```
Oracle : SELECT table_name FROM user_tables;
```

Quit Database:

```
Oracle : quit
```

Unresolved directive in modules/admin_manual/pages/enterprise/logging/index.adoc - include::partial\$section_page.adoc[]

Auditing

Introduction

The [Auditing](#) app is an Enterprise only app and available on the marketplace. It traces user and admin actions, in particular the following events:

- Login and logout events of users
- File system operations (create / delete / move; including actions on the trash bin and versioning)
- Sharing operations (user / group sharing, sharing via link, changing permissions, calls to sharing API from clients)
- Custom Groups events
- File tagging operations (add / remove tags)
- File commenting operations (create / update / delete)
- User management operations (creation / deletion / activation / deactivation of users, group management)
- User settings changes
- Impersonation events
- Enabling / disabling of ownCloud Apps
- Executions of OCC commands (CLI)



You may also want to check out the [ownCloud App for Splunk](#). For more information, read this [section](#).

Installation and Enabling

Download the [Auditing](#) app from the marketplace and enable it in the ownCloud app settings.

Figure 1 Auditing



Auditing

2.1.2

by ownCloud GmbH (OCL-licensed)

Show description ...

Disable

Configuration

It is advised to redirect messages into a separate file. To do so, add these lines to `config.php` and adjust the target path accordingly. Otherwise make sure to adjust the server log level to 1 (or 0), or else the Auditing app won't log anything. Configuring a separate file circumvents the global log level. Note that the target path must be writable for the web server user:

```
'log.conditions' => [  
  [  
    'apps' => ['admin_audit'],  
    'logfile' => '/var/www/owncloud/data/admin_audit.log'  
  ]  
]
```



All messages regardless of log level will be logged there.

To ignore all CLI triggered events (default is to include them), set the following option:

```
sudo -u www-data ./occ config:app:set admin_audit ignore_cli_events --value='yes'
```

Grouped Logging

With each log message, a number of users are calculated to be the 'audit context'. This is the list of users which are related to the log message. Additionally, each log message includes a list of groups that the users are a member of, to enable filtering / splitting of the log messages at a later date. In cases when users are members of many groups, to reduce the data output, the group list can be filtered by adding the following to your `config.php`. Change the groups needed accordingly:

```
'admin_audit.groups' => [  
  'group1',
```

```
] 'group2'
```

When the filter is configured, only the filtered list of groups will be output in *auditGroups*, else, all groups that the *auditUsers* are a member of are output.

View and Download Logs



If you have configured a different logfile than the default, you must download it manually.

To download your logfile on your admin page. Click **Settings** › **Admin** › **Download logfile**. The default location for manually downloading the standard ownCloud log is `data/owncloud.log`.



See [Logging Configuration](#) and [File Tagging](#) for more information on logging and tagging.

Connect with Splunk Cloud

Install the Universal Forwarder

Connect to the deployment server, change `input-prd-your-server-here` according your setup:

```
splunk set deploy-poll input-prd-your-server-here.cloud.splunk.com:8089
```

Install the Splunk Cloud credentials

```
splunk install app path/to/splunkclouduf.spl -auth admin:changeme
```

Monitor the `admin_audit.log`

To Monitor the ownCloud Splunk audit log, add this to `inputs.conf`, assuming you use the custom logging path/file from above:

```
[monitor://var/www/owncloud/data/admin_audit.log]
disabled = false
sourcetype = _json
index = main
```

Finally, configure the following `props.conf` to ensure the time field is correctly used and the fields are extracted.

```
[_json]
INDEXED_EXTRactions = json
KV_MODE = json
TIMESTAMP_FIELDS = [Time]
category = Structured
```


Extra Fields

The audit app listens for internal ownCloud events and hooks and produces a rich set of audit entries useful for reporting on usage of your ownCloud server.

Log entries are based upon the internal ownCloud logging system, but utilise extra fields to hold relevant data fields related to the specific event. Each event will contain the following data at a minimum:

Key	Type	Description
<code>remoteAddr</code>	string	The remote client IP
<code>user</code>	string	The UID of the user performing the action, or IP <code>x.x.x.x.</code> , <code>cron</code> , <code>CLI</code> , <code>unknown</code>
<code>url</code>	string	The process request URI
<code>method</code>	string	The HTTP request method
<code>userAgent</code>	string	The HTTP request user agent
<code>time</code>	string	The time of the event e.g.: <code>2018-05-08T08:26:00+00:00</code>
<code>app</code>	string	Always <code>admin_audit</code>
<code>message</code>	string	Sentence explaining the action
<code>action</code>	string	Unique action identifier e.g.: <code>file_delete</code> or <code>public_link_created</code>
<code>CLI</code>	boolean	If the action was performed from the CLI
<code>level</code>	integer	The log level of the entry (usually <code>1</code> for audit events)

Output

Files

`file_create`

When a file is created.

Key	Type	Description
<code>path</code>	string	The full path to the create file
<code>owner</code>	string	The UID of the owner of the file
<code>fileId</code>	string	The newly created files identifier

`file_read`

When a file is read.

Key	Type	Description
<code>path</code>	string	The full path to the file

Key	Type	Description
owner	string	The UID of the owner of the file
fileId	string	The files identifier

file_update

Key	Type	Description
path	string	The full path to the updated file
owner	string	The UID of the owner of the file
fileId	string	The updated files identifier

file_delete

Key	Type	Description
path	string	The full path to the updated file
owner	string	The UID of the owner of the file
fileId	string	The updated files identifier

file_copy

Key	Type	Description
oldPath	string	The full path to the source file
path	string	The full path to the new file
sourceOwner	string	The UID of the owner of the source file
owner	string	The UID of the owner of the file
sourceFileId	string	The source files identifier
fileId	string	The new files identifier

file_rename

Key	Type	Description
oldPath	string	The original path file
path	string	The new path file
fileId	string	The files identifier

file_trash_delete

Key	Type	Description
owner	string	The UID of the owner of the file
path	string	The full path to the deleted file

file_trash_restore

Key	Type	Description
owner	string	The UID of the owner of the file
fileId	string	The restored files identifier
oldPath	string	The original path to the file
newPath	string	The new path to the file
owner	string	The UID of the owner of the file

file_version_delete

Key	Type	Description
path	string	The full path to the version file deleted
trigger	string	The delete trigger reasoning

file_version_restore

Key	Type	Description
path	string	The full path to the file being restored to the new version
revision	string	The revision of the file restored

Users

user_created

Key	Type	Description
targetUser	string	The UID of the created user

user_password_reset

Key	Type	Description
targetUser	string	The UID of the user

group_member_added

Key	Type	Description
targetUser	string	The UID of the user
group	string	The GID of the group

user_deleted

Key	Type	Description
targetUser	string	The UID of the user

group_member_removed

Key	Type	Description
targetUser	string	The UID of the user
group	string	The GID of the group

user_state_changed

Key	Type	Description
targetUser	string	The UID of the user
enabled	boolean	If the user is enabled or not

group_created

Key	Type	Description
group	string	The GID of the group

group_deleted

Key	Type	Description
group	string	The GID of the group

user_feature_changed

Key	Type	Description
targetUser	string	The UID of the user
group	string	The GID of the group (or empty string)
feature	string	The feature that was changed
value	string	The new value

Sharing

Sharing events come with a default set of fields

Key	Type	Description
fileId	string	The file identifier for the item shared
owner	string	The UID of the owner of the shared item
path	string	The path to the shared item

Key	Type	Description
shareId	string	The sharing identifier (not available for public_link_accessed or when recipient unshares)

file_shared

Key	Type	Description
itemType	string	file or folder
expirationDate	string	The text expiration date in format yyyy-mm-dd
sharePass	boolean	If the share is password protected
permissions	string	The permissions string e.g.: "READ"
shareType	string	group user or link
shareWith	string	The UID or GID of the share recipient (not available for public link)
shareOwner	string	The UID of the share owner
shareToken	string	For link shares the unique token, else null

file_unshared

Key	Type	Description
itemType	string	file or folder
shareType	string	group user or link
shareWith	string	The UID or GID of the share recipient

share_permission_update

Key	Type	Description
itemType	string	file or folder
shareType	string	group user or link
shareOwner	string	The UID of the share owner
permissions	string	The new permissions string e.g.: "READ"
shareWith	string	The UID or GID of the share recipient (not available for public link)
oldPermissions	string	The old permissions string e.g.: "READ"

share_name_updated

Key	Type	Description
oldShareName	string	The previous share name

Key	Type	Description
shareName	string	The updated share name

share_password_updated

Key	Type	Description
itemType	string	file or folder
shareOwner	string	The UID of the share owner
permissions	string	The full permissions string e.g.: "READ"
shareToken	string	The share token
sharePass	boolean	If the share is password protected

share_expiration_date_updated

Key	Type	Description
itemType	string	file or folder
shareType	string	group, user or link
shareOwner	string	The UID of the owner of the share
permissions	string	The permissions string e.g.: "READ"
expirationDate	string	The new text expiration date in format yyyy-mm-dd
oldExpirationDate	string	The old text expiration date in format yyyy-mm-dd

share_accepted

Key	Type	Description
itemType	string	file or folder
path	string	The path of the shared item
owner	string	The UID of the owner of the shared item
fileId	string	The file identifier for the item shared
shareId	string	The sharing identifier (not available for public_link_accessed)
shareType	string	group or user

share_declined

Key	Type	Description
itemType	string	file or folder
path	string	The path of the shared item
owner	string	The UID of the owner of the shared item

Key	Type	Description
fileId	string	The file identifier for the item shared
shareId	string	The sharing identifier (not available for public_link_accessed)
shareType	string	group or user

federated_share_received

Key	Type	Description
name	string	The path of shared item
targetuser	string	The target user who sent the item
shareType	string	remote

federated_share_accepted

Key	Type	Description
itemType	string	The path of shared item
targetUser	string	The target user who sent the item
shareType	string	remote

federated_share_declined

Key	Type	Description
itemType	string	The path of shared item
targetuser	string	The target user who sent the item
shareType	string	remote

public_link_accessed

Key	Type	Description
shareToken	string	The share token
success	boolean	If the request was successful true or false

public_link_removed

Key	Type	Description
shareType	string	Link

public_link_accessed_webdav

Key	Type	Description
token	string	The token used to access the url

federated_share_unshared

Key	Type	Description
<code>targetUser</code>	string	The user who initiated the unshare action
<code>targetmount</code>	string	The file/folder unshared
<code>shareType</code>	string	<code>remote</code>

Custom Groups

custom_group_member_removed

Key	Type	Description
<code>removedUser</code>	string	The UID of the user that was removed from the group
<code>group</code>	string	The custom group name

custom_group_user_left

Key	Type	Description
<code>removedUser</code>	string	The UID of the user that left the group
<code>group</code>	string	The custom group name
<code>groupId</code>	integer	The custom group id

custom_group_user_role_changed

Key	Type	Description
<code>targetUser</code>	string	The UID of the user that changed role
<code>group</code>	string	The custom group name
<code>groupId</code>	integer	The custom group id
<code>roleNumber</code>	integer	The new role number: 0 = member, 1= admin

custom_group_renamed

Key	Type	Description
<code>oldGroup</code>	string	The old custom group name
<code>group</code>	string	The new custom group name
<code>groupId</code>	integer	The custom group id

custom_group_created

Key	Type	Description
<code>group</code>	string	The custom group name created

Key	Type	Description
groupId	string	The custom group id
addedUser	string	The UID of the user added
admin	boolean	true or false

Comments

All comment events have the same data:

Key	Type	Description
commentId	string	The comment identifier
path	string	The path to the file that the comment is attached to
fileId	string	The file identifier

Config

config_set

Key	Type	Description
settingName	string	The key
settingValue	string	The new value
oldValue	string	The old value
created	boolean	If the setting is created for the first time

config_delete

Key	Type	Description
settingName	string	The key

Console

command_executed

Key	Type	Description
command	string	The exact command that was executed

Tags

tag_created

Key	Type	Description
tagName	string	The tag name

tag_deleted

Key	Type	Description
tagName	string	The tag name

tag_updated

Key	Type	Description
oldTag	string	The old tag name
tagName	string	The new tag name

tag_assigned

Key	Type	Description
tagName	string	The tag name
fileId	string	The file identifier to which the tag was assigned
path	string	The path to the file

tag_unassigned

Key	Type	Description
tagName	string	The tag name
fileId	string	The file identifier from which the tag was unassigned
path	string	The path to the file

Apps

app_enabled

Key	Type	Description
targetApp	string	The app ID of the enabled app
groups	string []	Array of group IDs if the app was enabled for certain groups

app_disabled

Key	Type	Description
targetApp	string	The app ID of the disabled app

Auth

user_login

Key	Type	Description
success	boolean	If the login was successful
login	string	The attempted login value

user_logout

File Lifecycle

(requires at least v1.0.0)

lifecycle_archived

Key	Type	Description
path	string	The path to the file that was archived
owner	string	The UID of the owner of the file that was deleted
fileId	integer	The file ID for the file that was archived

lifecycle_restored

Key	Type	Description
path	string	The path to the file that was restored
fileId	integer	The file ID for the file that was restored

lifecycle_expired

Key	Type	Description
fileId	integer	The file id of the file that was expired

update_user_preference_value

Key	Type	Description
key	string	The key
value	string	The value associated with the key
appname	string	The name of the app
user	string	The UID of the user who has the preference key-value for the app

user_preference_set

Key	Type	Description
key	string	The key
value	string	The value associated with the key
appname	string	The name of the app

Key	Type	Description
user	string	The UID of the user who has the preference key-value for the app

remove_user_preference_key

Key	Type	Description
key	string	The key
appname	string	The name of the app
user	string	The UID of the user whose preference key is deleted for the app

remove_preferences_of_user

Key	Type	Description
user	string	The UID of the user whose user preferences are deleted

delete_all_user_preference_of_app

Key	Type	Description
appname	string	The name of the app whose user preferences are deleted

Impersonate

impersonated

Key	Type	Description
user	string	The current user who did an impersonate action
targetUser	string	The user who is being impersonated

impersonate_logout

Key	Type	Description
user	string	The user who performed impersonate action

SMB ACL

before_set_acl

Key	Type	Description
user	string	The user who is trying to set the ACL
ocPath	string	The owncloud instance path
smbPath	string	The SMB path
descriptor	array	The descriptor array. It contains to following keys:

descriptor[] keys

Key	Type	Description
revision	integer	Always 1
owner	string	The SMB owner
group	string	The SMB group
acl	array	A list of ACEs. The list could be empty. Each ACE contains following keys:

acl[] keys

Key	Type	Description
trustee	string	The SMB user affected by this ACE
mode	string	allowed or denied
flags	string	Inheritance flags
mask	string	Permission mask
flagsAsInt	integer	The inheritance flags as integer value
maskAsInt	integer	The permission mask as integer value

after_set_acl

Key	Type	Description
user	string	The user who is trying to set the ACL
ocPath	string	The owncloud instance path
smbPath	string	The SMB path
descriptor	array	The descriptor array. It contains to following keys:

descriptor[] keys

Key	Type	Description
revision	integer	Always 1
owner	string	The SMB owner
group	string	The SMB group
acl	array	A list of ACEs. The list could be empty. Each ACE contains following keys:

acl[] keys

Key	Type	Description
trustee	string	The SMB user affected by this ACE
mode	string	allowed or denied
flags	string	Inheritance flags

Key	Type	Description
mask	string	Permission mask
flagsAsInt	integer	The inheritance flags as integer value
maskAsInt	integer	The permission mask as integer value

Key	Type	Description
oldDescriptor	array false	The previous descriptor array or false if the previous descriptor couldn't be fetched. The previous descriptor will have the same keys

Unresolved directive in modules/admin_manual/pages/enterprise/reporting/index.adoc - include::partial\$section_page.adoc[]

Metrics

Introduction

The [Metrics App](#) provides a building block for reporting of ownCloud Server. For simple use cases, it ships with an integrated dashboard that summarizes information about users, storage as well as shares and allows exporting it to a CSV file. Additionally, it adds a Metrics HTTP API endpoint to ownCloud Server, which can be used to obtain the Metrics data in regular intervals. Thus, more sophisticated analysis and visualizations can be conducted.

The Metrics data are provided as snapshot values in the JSON format and are optimized to be consumed by professional data analyzers (like Splunk, ELK or Prometheus/Grafana) to collect statistics, derive visualizations and to set alerts for certain events of interest. They can be perfectly combined with the ownCloud Audit Logs (provided by the [Auditing App](#)) to gather time series data and to create a reporting engine for ownCloud.



Internet Explorer 11 is not compatible with Metrics, because new web technologies have been used that are not supported by IE 11.

If you want to use Splunk in addition, check out [ownCloud App for Splunk](#).

Specifically, the Metrics extension adds:

- an API endpoint which allows querying snapshot values of the system data as well as per-user metrics
- API endpoints for downloading metrics as CSV files
- a dashboard that displays the snapshot data in the ownCloud Web UI and offers a CSV download in the system view and the user view.



If you're operating very large instances with regard to users, files or shares, better use a special setup so you won't put the production database under huge load when gathering the values. For this, replicate your installation (application server and read-only database) and install and use the Metrics app on the replica.

The following screenshots give you an impression of the Metrics app.

Figure 1. Metrics System Overview

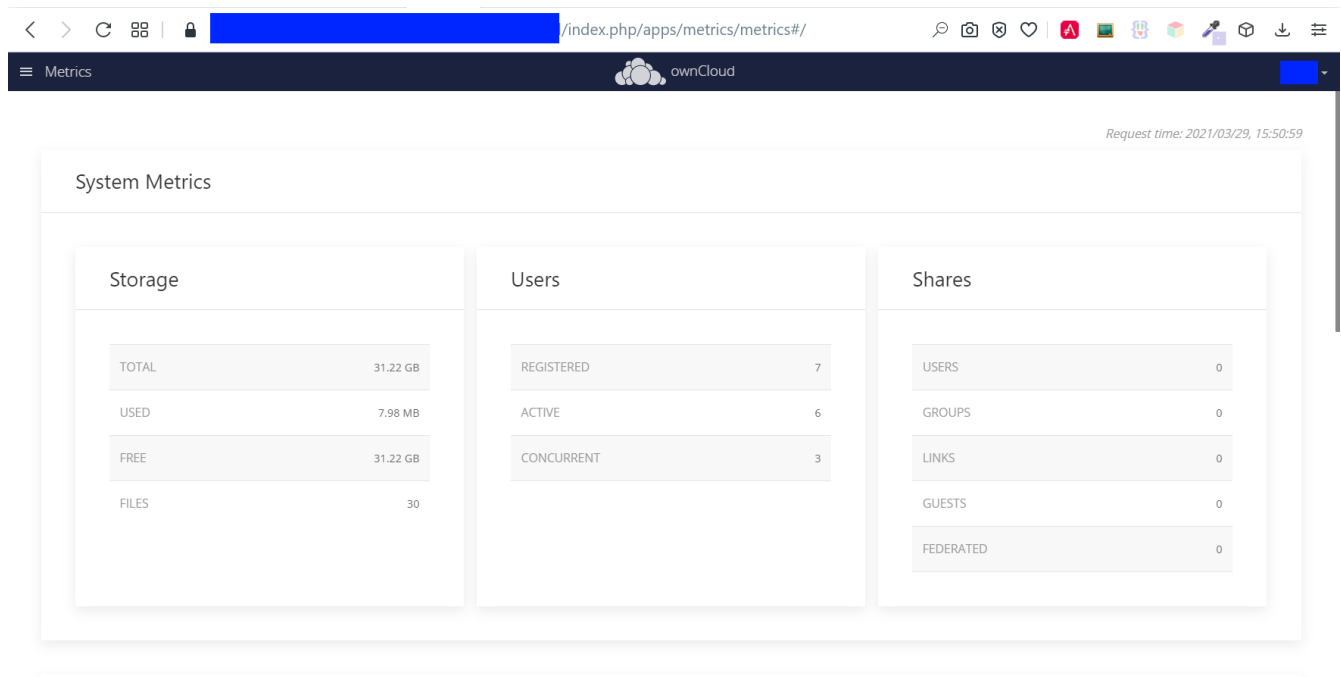
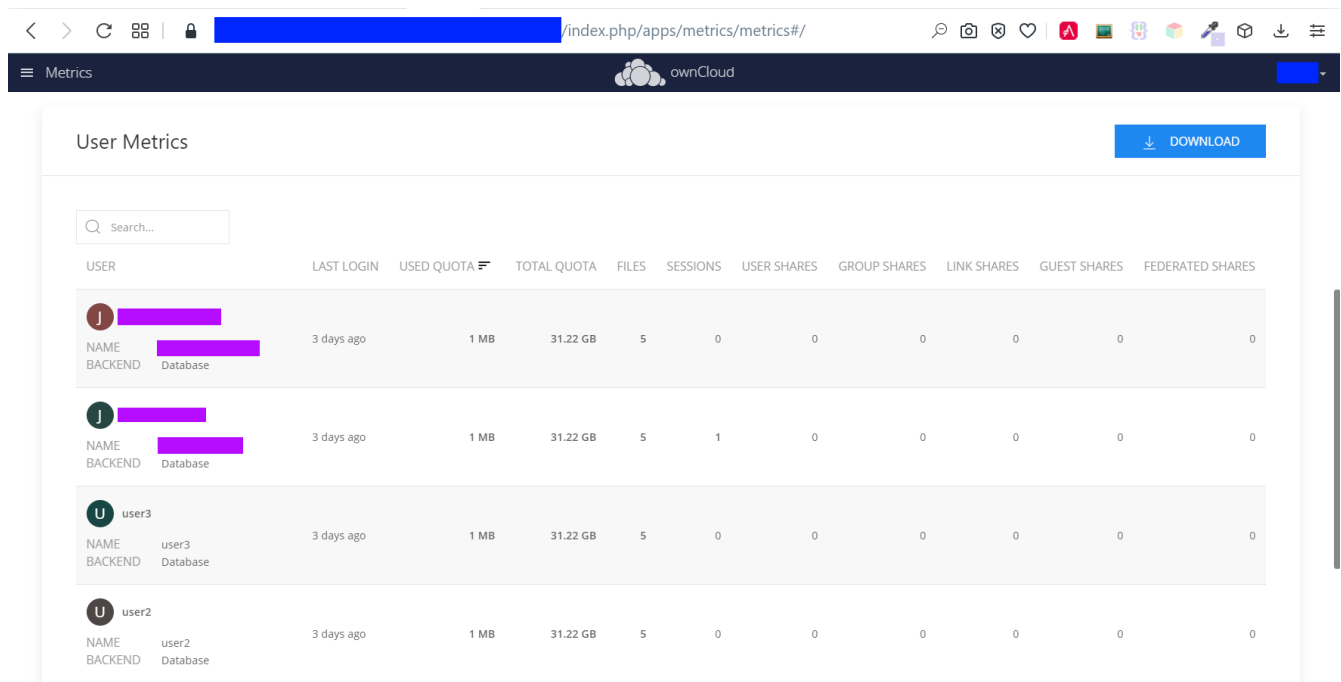


Figure 2. Metrics User Overview



Available Data

The following data is available for analysis:

System data

- Date/Time stamp - Server time of the request
- Storage
 - Used storage (this also includes storage for avatars and thumbnails)

- Free storage
- Total storage (used + free)
- Number of files
- Number of users
 - registered (total number of known users)
 - active (number of users with `lastLogin` less than two weeks ago)
 - concurrent (number of users with at least one active session)
- Shares
 - Number of user shares
 - Number of group shares
 - Number of guest shares
 - Number of link shares
 - Number of federated shares

Per-user data

- User ID
- Display name
- User backend
- Last login
- Active sessions
- Quota
 - Quota limit
 - Quota usage
- Number of files
- Shares
 - Number of user shares
 - Number of group shares
 - Number of guest shares
 - Number of link shares
 - Number of federated shares

Usage

Authorization

To get started, you have to set a secret for authenticating requests at the endpoint.

See the following `occ` command on how to set it. Make up a passphrase, referred to as `<your-metrics-secret>` in the example below. The Metrics secret is necessary to use the dashboard.


```
sudo -u www-data ./occ config:system:set "metrics_shared_secret" --value "<your-metrics-secret>"
```



This token gets stored in config.php as `metrics_shared_secret`, which could also be done manually instead of using the occ command.

Dashboard User Interface

The dashboard is enabled by default. You can disable it with the following command:

```
sudo -u www-data ./occ config:app:set metrics disable_dashboard --value=yes
```

Endpoints and Parameters

Metrics Endpoint

To query for the Metrics data, use the following endpoint:

```
https://<your owncloud>/ocs/v1.php/apps/metrics/api/v1/metrics
```

- URL Parameters
 - `users=true`
 - `shares=true`
 - `quota=true`
 - `userData=true`
 - `format=json`
- Header `"OC-MetricsApiKey: <your-metrics-secret>"`

Except for the header, all other parameters are optional. You can split the query into parts by setting the respective parameters to `false`.

See the `curl` example to request the complete output:

```
curl -H "OC-MetricsApiKey: <your-metrics-secret>" \  
  "https://<your  
owncloud>/ocs/v1.php/apps/metrics/api/v1/metrics?users=true&files=true&shares=true&quo  
ta=true&userData=true&format=json"
```



Replace `<your-metrics-secret>` with your respective system config value and `<your owncloud>` with the URL of your ownCloud instance.

CSV Download Endpoints

Downloading the current user and system metrics as CSV files is possible via the Web UI. If you want to set up cron jobs for downloading the metrics regularly without admin permissions, there are also public endpoints that require the configured token instead of admin privileges.



In the following `curl` examples, replace `<your-metrics-secret>` with your respective system config value and `<your owncloud>` with the URL of your ownCloud instance.

To receive user metrics, use:

```
curl -H "Content-Type: application/csv" \  
-H "OC-MetricsApiKey: <your-metrics-secret>" \  
-X GET https://<your owncloud>/index.php/apps/metrics/download-api/users > \  
/path/to/download/storage/user-metrics.csv
```

For system metrics, use:

```
curl -H "Content-Type: application/csv" \  
-H "OC-MetricsApiKey: <your-metrics-secret>" \  
-X GET https://<your owncloud>/index.php/apps/metrics/download-api/system > \  
/path/to/download/storage/system-metrics.csv
```

Limitations

The Metrics app was designed for ownCloud deployments up to 250 users. On deployments with more than 250 users, it can take considerably longer to gather the requested data. To reduce the time needed, exclude `userData` and `quota`.

Generate a Config Report

Introduction

Generating a config report when using an Enterprise version does not differ from the Community Edition. For more details see the documentation how to [Generate a Config Report](#).

Unresolved directive in modules/admin_manual/pages/enterprise/security/index.adoc - include::partial\$section_page.adoc[]

Ransomware Protection

Introduction

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.



It is essential to be aware that user data needs to be synchronized with your ownCloud Server using the ownCloud Desktop synchronization client. Data that is not synchronized and stored in ownCloud cannot be protected.

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](#).

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 more than 3,000 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 an [occ command](#)



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.



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.



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.



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 **Settings** › **Personal** › **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.



Locking is enabled by default. If this is not desired, an administrator can disable it in the **Settings** › **Admin** › **Security** panel.

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.

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. <code>.crypt</code>) 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 when 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.

`<timestamp>` must be in the Linux timestamp format.

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.

Limitations

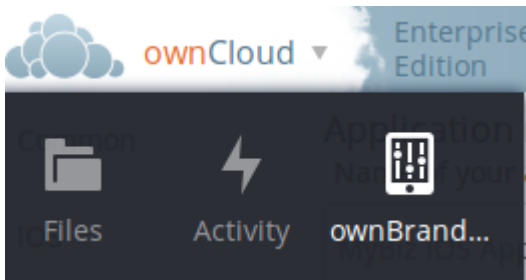
- Ransomware Protection works with master-key based storage encryption. With credential-based storage encryption, only Ransomware Prevention (Blocking) works.
- Rollback is not based on snapshots:
 - The [trash bin retention policy](#) may delete files, making them unrecoverable. To avoid this, set `trashbin_retention_obligation` 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.
- Recovery capabilities in received shared folders are currently limited. Changed file contents and deletions can be restored but MOVE operations can't. The case when a ransomware attack renames files in a received shared folder is therefore not yet covered.
- 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.

Unresolved directive in modules/admin_manual/pages/enterprise/server_branding/index.adoc - include::partial\$section_page.adoc[]

Enterprise Server Branding

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, 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.

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

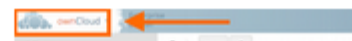
This is the image shown on the login page just above the Username and Password fields. This image is used when the browser does not support svg, we recommend this to be the same as the previous one (Login page logo) (png format) (width: 252px height: 122px) **i**

Delete image

Upload



Logo icon



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](https://inkscape.org/) 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](https://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.

Always edit only your custom theme files. Never edit the default theme files.

Unresolved directive in modules/admin_manual/pages/enterprise/user_management/index.adoc - include::partial\$section_page.adoc[]

- [Shibboleth Integration](#)
- [SAML 2.0 Based SSO](#)

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/`. Further Shibboleth specific configuration as defined in `/etc/apache2/conf.d/shib.conf`.

```
Unresolved directive in
modules/admin_manual/pages/enterprise/user_management/user_auth_shibboleth.adoc -
include::example$enterprise/user_management/shibboleth/apache-2.4-configuration.conf[]
```

To allow users to login via the IdP, add a login alternative with the `login.alternatives` option in `config/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.

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) C
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

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:

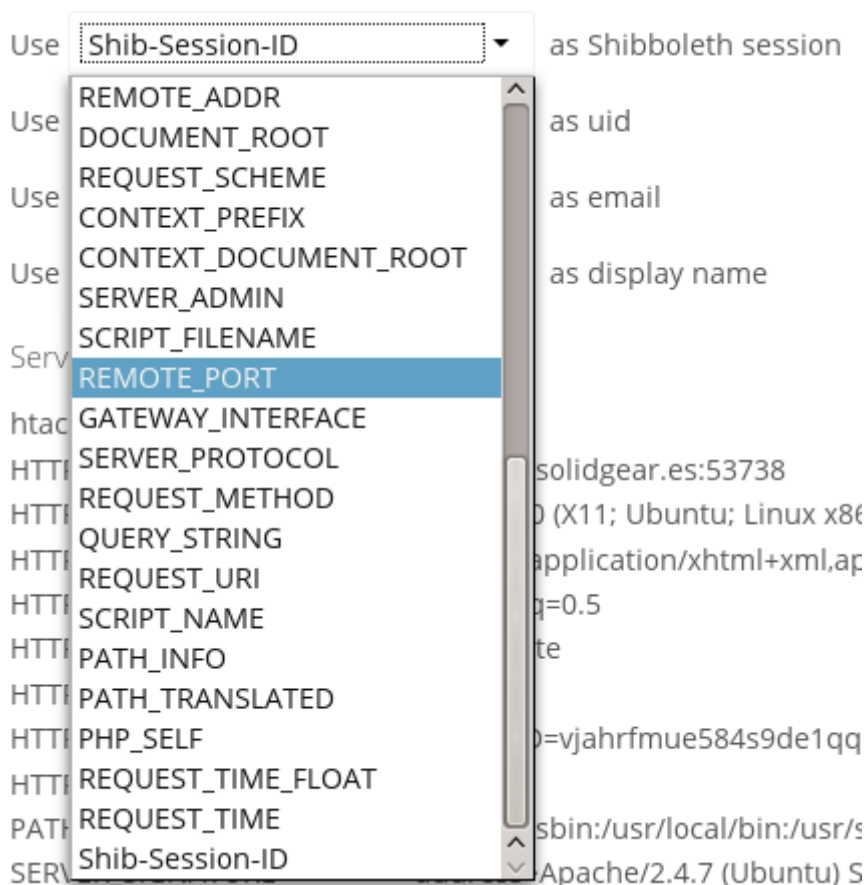
```
sudo -u www-data ./occ shibboleth:mode notactive
sudo -u www-data ./occ shibboleth:mapping --uid login
```

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**.

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.

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 ./occ config:app:set user_shibboleth \
uid_mapper --value="OCA\User_Shibboleth\Mapper\ADFSMapper"
```

You may view the currently configured mapper using:

```
sudo -u www-data ./occ shibboleth:mapping
```

The following mappers are provided with the app:

Class	Description
<code>OCA\User_Shibboleth\Mapper\NoOpMapper</code>	The default, does not alter the UID
<code>OCA\User_Shibboleth\Mapper\ADFSMapper</code>	Splits the UID around a <code>;</code> character and takes the first piece
<code>OCA\User_Shibboleth\Mapper\GUIDInMemoryMapper</code>	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/config.php`.

Known Limitations

Encryption

File encryption can only be used together with Shibboleth when [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.

PHP-FPM is incompatible

The provided shibd, apache and ownCloud configuration only works with `mod_php`. Make sure that you have disabled PHP-FPM and enabled `mod_php` on your server. CentOS 8 now installs PHP-FPM by default, so make sure to swap.

Other Login Mechanisms

You can allow other login mechanisms (e.g., LDAP or ownCloud native) by creating a second Apache virtual host configuration; such as in the below example.

```
Unresolved directive in
modules/admin_manual/pages/enterprise/user_management/user_auth_shibboleth.adoc -
include::example$enterprise/user_management/shibboleth/other-login-mechanisms-
vhost.conf[]
```



The second location in the above configuration is **not** protected by Shibboleth, and you can use your other ownCloud login mechanisms.



The above configuration can be used with multi-factor authentication as well.

If you use the above configuration, after it's enabled, configure the alternative logins option with a button to point to `/login-shib`. This will trigger the Shibboleth session and redirect the user back to `/login`. At this point, the existing session will be picked up, continuing with the authentication process.

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`.

SAML 2.0 Based SSO with Active Directory Federation Services (ADFS) and mod-shib

Preparation

Before you can setup SAML 2.0 based Single Sign-On 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-`

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 `ads2fed.php`, as in the following command:

```
php apps/user_shibboleth/tools/ads2fed.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`:

Define the ownCloud Instance

Use the URL of the ownCloud instance as the `entityID` in the `ApplicationDefaults`

```
<ApplicationDefaults entityID="https://<owncloud server FQDN>/login/saml"
REMOTE_USER="eppn upn">
```



`https://<owncloud server FQDN>/login/saml` is just an example.
Adjust `<owncloud server FQDN>` to the full qualified domain name of your server.

Configure SSO

Configure the SSO to use the `entityID` from the `filtered-metadata.xml`

```
<SSO entityID="https://<ADFS server FQDN>/<URI>/">
  SAML2
</SSO>
```



Grab `<ADFS server FQDN>/<URI>/` from the `filtered-metadata.xml`.

Configure XML

Configure an XML `MetadataProvider` with the local `filtered-metadata.xml` file

```
<MetadataProvider type="XML" path="/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.

Active Directory Federation Services (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 step 2 in [AD FS 2.0 Step-by-Step Guide](#).

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:

```
sudo -u www-data ./occ shibboleth:mode ssoonly
sudo -u www-data ./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 ADFSrv
```

- 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](#)
- [ads2fed Python Script](#)
- [AD FS 2.0 Step-by-Step Guide: Federation with Shibboleth 2 and the InCommon Federation](#)
- [Shibboleth Basic Configuration \(Version 2.4 and Above\)](#)
- [Shibboleth XML MetadataProvider](#)
- [Shibboleth NativeSPServiceSSO](#)

Unresolved directive in modules/admin_manual/pages/troubleshooting/index.adoc - include::partial\$section_page.adoc[]

General Troubleshooting

Introduction

This page gives an overview of general troubleshooting topics and can help to sort out paths addressing your topics.

If you have trouble installing, configuring or maintaining ownCloud, please refer to our community support channel:

- The [ownCloud Forum](#)



The ownCloud forum have a [FAQ category](#) where each topic corresponds to typical errors or frequently occurring issues.

Please understand that this channel essentially consist of users like you helping each other. Consider helping others when you can in return 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 GmbH offers the [Enterprise Edition](#) with commercial support options.

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.

General Troubleshooting

Check the ownCloud [System Requirements](#), especially supported browser versions. When you see warnings about `code integrity`, refer to [Code Signing](#).

Disable Third-Party Apps

Third-party apps may cause problems during upgrades. To avoid this happening, we strongly encourage administrators to always disable [third-party apps](#) before upgrades, and for troubleshooting purposes.

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. Usually you can access them by pressing F12.

For more information on developer tools for Mozilla Firefox, refer to: <https://developer.mozilla.org/en-US/docs/Tools>

To learn more about Chrome or Chromium developer tools, go to: <https://developer.chrome.com/docs/devtools/>



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 configuration details. There are two ways to retrieve this information: using PHP's `phpinfo()` function and using a set of options to PHP on the command-line.

Using PHP's `phpinfo()` Function

Create a plain-text file named "`phpinfo.php`" and place it in your webserver's root directory, for example `/var/www/html/phpinfo.php`.

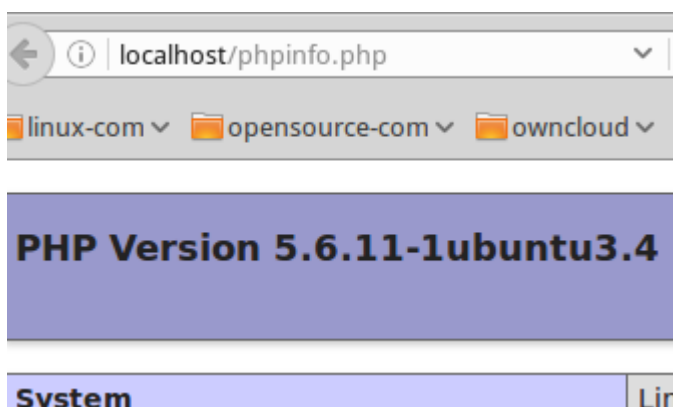


Your webserver's root directory may be in a different location; your Linux distribution's documentation will tell you where it is located.

This file contains the following 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.

Using the Command-Line

To retrieve your PHP version, run the following command:

```
php -v
```

To retrieve a list of PHP's active modules, run the following command.

```
php -m
```

You will see output similar to the following displayed in the terminal.

```
[PHP Modules]
ast
calendar
Core
ctype
curl
date
dom
exif
fileinfo
```

To obtain information about PHP's configuration, you can either retrieve it all at once, by running `php -i` or retrieve information about individual modules, by running `php --ri` followed by the module's name, such as `php --ri curl`.

Debugging Sync Issues



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 [multi-processing module](#) other than `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](#).

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
```

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.

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.



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/php/7.4/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



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:

Apache

- libapache2-mod-php7.4 (or a lower supported version if necessary)
- 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-php7.4 (see above) / mod_php (use fcgi or php-fpm instead)
- mod_xsendfile / X-Sendfile (causing broken downloads if not configured correctly)

PHP

- eAccelerator

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.



Please keep in mind that the `.htaccess` file in the ownCloud directory will be overwritten on update. Post upgrading ownCloud, you need to manually restore these changes. See the section [Backup Manual Changes in .htaccess](#) for details.

```
# 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]
```

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 you 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

Check if your Pound installation supports the HTTP/1.1 verb. If it does not, update to the latest

version.

Misconfigured Web server

Your Web server is misconfigured and blocks the needed DAV methods. Please refer to [Troubleshooting WebDAV](#) above for troubleshooting steps.

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.

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.

Path and Filename Length Limitations

Introduction

Depending on the underlying filesystem of a mount point, the maximum length of a path component and the file name can differ. This is important if you start copying or moving single files or even complete paths from one mount to another where the target mount has a more restrictive length rule than the source. This can also be an issue when using a synchronization client running on an Operating System (OS) with a different filesystem than the source mount filesystem. The following table gives you a brief overview as a guideline.

Limitations

See the [comparison of file systems](#) for in depth details on various filesystem path and file name limitations.



While a filesystem can handle the limits as described in the table below, applications like Explorer, Finder, the Shell or other apps may have issues handling these limits. See the special notes below the table.



The ownCloud database has a size limit storing a path/file string with 4000 bytes. This must not be exceeded.

File Name and Path Length Limitations

Filesystem	max. Path Length	max. Filename Length
(*) Btrfs	No limit defined	255 bytes
(*) ext2	No limit defined	255 bytes
(*) ext3	No limit defined	255 bytes
(*) ext4	No limit defined	255 bytes
(*) XFS	No limit defined	255 bytes
(*) ZFS	No limit defined	255 bytes
APFS	Unknown (**)	255 UTF-8 characters
FAT32	32,760 Unicode characters with each path component no more than 255 characters	8.3 (255 UCS-2 code units with VFAT LFNs)
exFAT	32,760 Unicode characters with each path component no more than 255 characters	255 UTF-16 characters
NTFS	32,767 Unicode characters with each path component (directory or filename) up to 255 characters long (MAX_PATH). <div style="border: 1px solid #ccc; padding: 10px; margin: 10px 0;"> <p>Starting in Windows 10, version 1607, MAX_PATH limitations have been removed from common Win32 file and directory functions. However, you must opt-in to the new behavior. For more details see Enable Long Paths in Windows 10, Version 1607, and Later</p> </div>	255 characters

(*)

In Unix environments, PATH_MAX with 4096 bytes and NAME_MAX with 255 bytes are very common limitations for applications including the Shell. You can get the current limitations by typing the following example commands, see the [getconf manpage](#) for details:

```
getconf NAME_MAX /
255
```

```
getconf PATH_MAX /
4096
```

(**)

Although not officially documented, when searching on the internet there is a limit with path

names exceeding 1024 bytes. Users report warnings in Finder, the Shell or apps about this behavior. This can be verified with:

```
getconf NAME_MAX /  
255
```

```
getconf PATH_MAX /  
1024
```

Note that these limits are true for macOS as well as for iOS because both are using APFS.

Retrieve Log Files and Configuration Settings

Introduction

Generating configreports and preparing log files are essential to support identifying the cause of a problem. Here are instructions for how to collect them.

When you report a problem to [ownCloud Support](#) or our [Forum \(ownCloud Central\)](#) you will be asked to provide certain log files or configurations for our engineers or other supporting staff. This information is necessary in better understanding your issue, your specific configuration, and for further support.

Generate a Config Report

You can use the webUI or the command line to generate a config report. The webUI includes the web server environment, while the command line generated one doesn't as it can't access it. Therefore, if possible, always generate it through the webUI. The configreport app is always part of bundled apps, but it may need to be enabled before it can be used.

Check if it is disabled:

```
sudo -u www-data ./occ app:list --disabled configreport
```

Enable it if it was formerly disabled:

```
sudo -u www-data ./occ app:enable configreport
```

Generate via webUI

To generate a config report using the webUI, navigate to:

Settings › **Admin** › **General** › **"Generate Config report"** › **"Download ownCloud config report"**.

Generate via Command Line

To generate a config report from the command line, run the following command from the root directory of your ownCloud installation:

```
sudo -u www-data ./occ configreport:generate > config_report.txt
```

ownCloud Server Log File

Generate via webUI

You can use the webUI to download your ownCloud Server log file. To do so, navigate to: **Settings > Admin > General > Log > "Download logfile"**.

Generate via Command Line

If the log file is too big, you will need to transfer it from the command line. The location of the log file can be found in your config.php. By default it is in your data directory. Note that you may need to compress the logfile before uploading:

```
'datadirectory' => '/var/www/owncloud/data',
```

When not using the default location for the logfile, it can be specified via:

```
'logfile' => '<your-path>/owncloud.log',
```

LDAP Config

If LDAP is used, viewing the LDAP configuration is important when checking for errors between your ownCloud instance and your LDAP server. To get the output file, execute this command:

```
sudo -u www-data ./occ ldap:show-config > ldap_config.txt
```

Remove Non-Existent Background Jobs

Introduction

During the lifecycle of ownCloud, some background jobs may get removed as they are either superseded by another job or completely obsolete. It can also happen, that an app providing a background job was removed and the job therefore is no longer present. These jobs can be removed manually.

Identification

If the ownCloud log files contain errors like:

```
"Exception: {"Exception":"OCP\AppFramework\QueryException","Message":"Could not resolve OCA\User_LDAP\Jobs\UpdateGroups! Class OCA\User_LDAP\Jobs\UpdateGroups does not exist","Code":0,"Trace":"
```

```
"Exception: {"Exception":"OCP\AppFramework\QueryException","Message":"Could not resolve OCA\User_LDAP\Jobs\CleanUp! Class OCA\User_LDAP\Jobs\CleanUp does not exist","Code":0,"Trace":"
```

```
"Exception: {"Exception":"OCP\AppFramework\QueryException","Message":"Could not resolve OCA\Federation\SyncJob! Class OCA\Federation\SyncJob does not exist","Code":0,"Trace":"
```

these background jobs can safely be removed as they no longer exist.

Removal Process

There is an [occ command set](#) for managing background jobs *triggered by ownCloud*. The following steps are necessary to remove a background job:

1. Identify the **Job-ID** of the background job to be removed
2. Remove the background job based on the **Job-ID**

It is also possible that a background job is triggered manually by the admin when the job has been added to eg. [crontab](#).

Identify the Job-ID of the Background Job to Be Removed

Use the following command to list all active background jobs triggered by ownCloud:

```
sudo -u www-data ./occ background:queue:status
```

The output may look like the following:

```
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
+-----+
| Id | Job                               | Last run                               |
Job Arguments |
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
+-----+
| 1 | OCA\Files\BackgroundJob\ScanFiles | 2022-01-23T14:00:02+00:00 |
|
| 2 | OCA\Files\BackgroundJob\DeleteOrphanedItems | 2022-01-23T14:00:02+00:00 |
|
| 3 | OCA\Files\BackgroundJob\CleanupFileLocks | 2022-01-23T14:00:02+00:00 |
```

```
|
| 4 | OCA\DAV\CardDAV\SyncJob | 2022-01-23T14:00:02+00:00 |
|
...
+-----+-----+-----+-----+
+-----+-----+-----+-----+
```

Remove the Background Job

When you have identified the **ID** of the background job to be removed, run following command to remove it, replace **ID** with the job number of the list:

```
sudo -u www-data ./occ background:queue:delete ID
```



Deleting a job cannot be undone. Be sure that you want to delete the job before doing so.

Remove Jobs Manually Added via Crontab

If an erroring job as been added manually in **crontab**, remove the job from the crontab queue list. First, list the entries of crontab for the web server user:

```
sudo -uwww-data crontab -l
```

Then edit the crontab job list to remove the job by invoking following command:

```
sudo -uwww-data crontab -e
```

Have You Found a Mistake In The Documentation?

If you have found a mistake in the documentation, no matter how large or small, please let us know by [creating a new issue in the docs repository](#).