hyper➜ Content & Digital Asset Management Server
CMS

Version 10.1
Installation Guide

2023-02-24

Index

1 Introduction

The hyper Content & Digital Asset Management Server will be installed on a web server. For the installation on the server you will need an FTP-Client or SCP-Client if you don't have direct access to the file system of the server. The FTP-Client is used for the transfer of the files to your destination server.
After the file transfer, some directories and files require write permissions. This allows the system to write files on your server.
All additional configuration can be done using the graphical user interface. To perform a successful installation of the system you should have basic knowledge about the operating system and web server you use.

Please notice the basic layers of your system and their dependencies in the order the installation and configuration of those software packages have to be done:
   1. Operating System (e.g. Linux)
   2. Web server (e.g. Apache)
   3. Database (e.g. MariaDB/MySQL)
   4. hyper Content & Digital Asset Management Server

2 Prerequisites

The following technical prerequisites must be fulfilled before installation:

On server-side:
  - Operating System: Linux, UNIX-Derivates, MS Windows (is not recommended when used as fully featured DAM system) in latest version if possible
  - WebServer: Apache 2.4 with support of htaccess files or Microsoft IIS with support of web.config files, PHP Version 7+ and the following PHP modules: bcmath, calendar, Core, ctype, curl, date, dom, exif, fileinfo, filter, ftp, gd, gettext, hash, iconv, json, ldap, libxml, mbstring, mysqli, mysqlnd, openssl, pcntl, pcre, Phar, posix, readline, Reflection, session, shmop, SimpleXML, soap, sockets, SPL, standard, sysvmsg, sysvsem, sysvshm, tokenizer, wddx, xml, xmlreader, xmlwriter, xsl, zip, zlib, Zend OPcache
  - RDBMS (Database): MariaDB or MySQL 5+ (required for the standard installation routine), any database with ODBC support (not supported by the standard installation routine)
  - The following free software packages should be installed for full Digital Asset Management (DAM) support:
    - FFMPEG (converting video and audio files)
    - YAMDI (meta data injection into FLV files)
    - UFRAW (for raw images from digital cameras)
    - ImageMagick (converting images)
    - WebP (for webp image format support)
    - XPDF (indexing of PDF-documents)
    - ANTIWORD (indexing older Word-documents)
    - ZIP/UNZIP (packing and unpacking of files)
    - UNOCONV (converting office files)
    - EXIFTOOL (reading meta data of files)
    - TESSERACT (optical character recognition / OCR)
    - OpenSSL (encryption)
    - WKHTMLTOPDF (convert HTML to PDF)
    - X-Server (used for WKHTMLTOPDF)
    - PDFTK (merge PDF files)

On client-side:

- All state-of-the-art browsers (Chrome, Edge, Firefox, Opera, Safari) can be used, favored in the last version. The system is 100% browser based, so no additional client software is required.

3 Installation of additional software packages

We recommend using Linux for production. Depending on the Linux distribution the installation process of the additional software packages can vary.
The following examples are based on Aptitude and Debian 9.
All packages except FFMPEG are already included in Debian.

You can easily install them using:
```
apt-get install xpdf
apt-get install antiword
apt-get install ufraw-batch (for Debian 8,9, 10)
apt-get install dcraw (Debian 11)
apt-get install imagemagick
apt-get install webp
apt-get install yamdi
apt-get install zip
apt-get install tesseract-ocr
apt-get install tesseract-ocr-all
apt-get install libreoffice
apt-get install unoconv
apt-get install openssl
apt-get install pdftk
```

How to install WKHTMLTOPDF?
The current distribution of wkhtmltopdf in apt-get is not patched with the latest version of Qt, and does not support multiple input files and other options. To solve this, you can manually install the updated wkhtmltopdf from the official website itself:
http://wkhtmltopdf.org/downloads.html

If you want to use the package provided by the distribution, use:
```
apt-get install wkhtmltopdf
apt-get install xvfb
```

How to add and install FFMPEG?
Add the Multimedia Repository to your sources in /etc/apt/sources.list. This will also guarantee you to receive all the software updates for FFMPEG.

```
deb http://www.deb-multimedia.org stretch main non-free
```

Install public key:
```
apt-get update
apt-get install deb-multimedia-keyring
```

Aptitude update:
```
apt-get update
```

Finally install FFMPEG:
```
apt-get install ffmpeg
```

4 Architecture

The hyper Content & Digital Asset Management Server is based on the language PHP and other software packages. The software will be delivered in source code. In order to operate the system, you will need a web server that supports PHP. More details about PHP are available at: *http://www.php.net*.
The source code will be compiled automatically through the PHP hypertext preprocessor on the server-side. A compilation of the source code is therefore not necessary. You will have the possibility to access and adopt the source code without recompiling it. Please keep in mind that changes in the source code could have a deep impact on the functionality of the content management system. Please notice the support agreement.

The system requires a MariaDB, MYSQL or ODBC database. Some information will be saved directly in the file system. Where those files will reside can be partly defined by yourself.
The hyper Content & Digital Asset Management Server uses an internal and an external repository. Where those repositories will be located can be defined by you. What is important to notice is, that a repository must be available on one server only. The software can be deployed on more servers if you use load balancing in clustered server nodes.
The internal repository will be usually named „data". That you will find in your installation package.
The external repository will be usually named „repository" and is also part of the software package.

data	Internal Repository
hypercms	Content & Digital Asset Management Server software
mypublication	First of n-Publications (needs access to the external Repository)
repository	External Repository
readme.txt	Readme file

All settings of the system are stored in the main configuration file " hypercms/config config.inc.php". All parameters can be changed any time, for instance to disable language packages, enable or change load balancing and so on. The explanations of the various settings are provided in the file.

The internal repository (data) is the central data storage and has the following structure:

Folder	Description
checkout	Data of checked-out objects, favorites
config	Configurations
connect	Connectors for authentication (LDAP)
content	Content-Repository
customer	Personalization data
eventsystem	Event System
export	Export directory
import	Import directory
include	Include of definitions
link	Link Management indizes
log	Log files
media	Media information
message	Messages
queue	Queue data
report	Report data
session	Session data
temp	Temporary directory
template	Templates
user	Data of Users and Groups
workflow	Workflows
workflow_master	Master Workflows

You won't find more details here. Manual changes in the repository can destroy the data storage!

The external repository (repository) has the following structure:

Folder	Description
component	Component repository
config	Publication configuration
link	Link indexing
media_cnt	Content media
media_tpl	Template media
search	Search engine

This repository consists of files which have relevance for the Publications, such as components, publication configuration settings, link management and media files.

4.1 Instances

The system can be set up for multiple instances. This is strongly recommended if you
have a shared hosting environment with different customers and you want the data to be
strictly separated from each other. This gives you more flexibility, since each customer
uses its own database as well as internal and external repository.
Keep in mind that instances should not be used if you want the inherit templates and
content from one to another publication.

For security reasons you should separate the data and setup the restrictions in the web
servers hosts accordingly. Automating the creation of instances, all necessary steps to
setup a secure environment should be done by experts.
The support for instances is included in the Enterprise Edition of the system, and
provides a management interface for multiple instances.

In order to use instances, a path to the configuration directory of the instances need to
be provided. If a distributed system is used the path need to direct to a central server,
wehere all system nodes can access the configurations.
To enable instances, the path needs to be set only once in the main configuration file
"hypercms/config/config.inc.php":

```
$mgmt_config['instances'] = "/server/instance_configuration/";
```

4.2 Load balancing

The hyper Content & Digital Asset Management Server supports load balancing for tasks
like for file upload, storing content and rendering files. This is especially useful for batch
processing of image, video and audio files that might lead to high workload.

To enable load balancing the system need to be installed on several physical servers.
Make sure that all servers store the files in the same central repository ("data" and
"repository") and use the same database. Therefore a central file storage (e.g. NAS or
SAN) and a central database server is required. Please provide the information to this
resources during the installation procedure.

You and can change the settings in the main configuration file
"hypercms/config/config.inc.php" at any time, see:

```
// URL and absolute path to the external repository on your webserver
// Used for the storage of external content management information
$mgmt_config['url_path_rep'] = ...
$mgmt_config['abs_path_rep'] = ...

// URL and absolute path to the internal repository on your webserver
// Used for the storage of internal content management information
$mgmt_config['url_path_data'] = ...
$mgmt_config['abs_path_data'] = ...
```

Please install the software on the main server using the installation routine. For all other
server use can copy the files in the directory "hypercms" to ensure the same settings on
all servers. Please change the settings $mgmt_config['url_path_cms'] and
$mgmt_config['abs_path_cms'] in the main configuration file
"hypercms/config/config.inc.php" of the local installation.

Before a server can distribute the load to others, it must be configured for load balancing. This must be set manually after installation and can be done in the main configuration file "hyperCMS/config/config.inc.php".
For example, the activate the load distribution to 2 additional servers, configure the array in the main configuration as follows:

```
$mgmt_config['url_path_service'][1] = "http://server1/hypercms/service/";
$mgmt_config['url_path_service'][2] = "http://server2/hypercms/service/";
```

You can also define on an array of resources for additional servers. Keep in mind that no resource may be used twice, since it will lead to an infinite loop, which would be interpreted as a CSRF attack by the system and the user will be logged out from the system.

4.3 Operation in a server cluster

The hyper Content & Digital Asset Management Server can be operated in a server cluster. This will improve the operational availability and performance because of the distributed system.
Per CPU core you can have a work load of approximately 15 concurrent users, that can be handled by one management server. This results for example to 15 * 8 = 120 concurrent users for one CPU with 8 cores.

A third-party load balancer can be used for the load distribution. The system supports a server-wide session handling that comes as part of the system's own load balancing. In order to use a third-party load balancer you need to enable a transparent session ID in php.ini (see 5.1) and enable session synchronization in the main configuration of the system.

// Enable writing of session data for third party load balancers in order to enable session synchronization
$mgmt_config['writesessiondata'] = true;

The software will be installed on several management servers which will be connected to a central internal and external repository server and a database server. The web publications together with the external repository can be distributed on webservers. The architecture can be as followed:
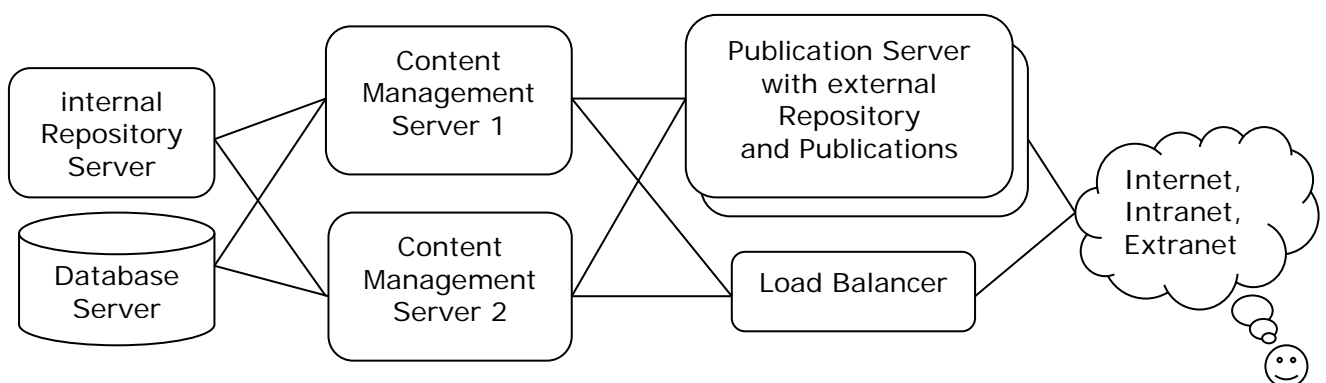
4.4 Cloud Storage Support

The Enterprise Edition of the system supports the storage of multimedia files in a cloud storage (e.g. AWS S3). In order to use a cloud storage, some settings need to be set in the main configuration. The system can save data immediately or delayed (once a day) in order to reduce the data traffic between the cloud storage and the system. This also helps to reduce the costs for data traffic that might be charged by the cloud service provider.
Later you can use the publication management to define if the cloud storage, the storage of the local repository or both should be used.

```
// ----------------------------- Cloud storage settings -----------------------------

// ATTENTION: The following settings only applies for the Enterprise Edition!
// If you are using AWS S3 or Google Cloud as media repository, the system will save all media files
// using the SDK client of the cloud service provider.
// Please note, that you need a cloud service account with your cloud service provider.
// In order to connect with the cloud service, you need provide the credentials for the cloud service.

// For AWS S3 use:
// Enable (true) or disable (false) the AWS S3 Cloud API
$mgmt_config['aws_api'] = false;
// Provide credentials for access
$mgmt_config['aws_access_key_id'] = "";
$mgmt_config['aws_secret_access_key'] = "";
// Provide region code, see also: http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-regions-availability-zones.html#concepts-available-regions
$mgmt_config['aws_region'] = "";
// Provide the name of your AWS S3 bucket (mandatory for cloud storage)
$mgmt_config['aws_bucket'] = "";

// For Google Cloud Platform use:
// Enable (true) or disable (false) the Google Cloud API
$mgmt_config['gs_api'] = false;
// Provide credentials for Google API access (path to Google API JSON key file)
$mgmt_config['gs_access_json'] = "";
// Define default language code to be used for speech-to-text
// See all the supported lanuage codes here: https://cloud.google.com/speech-to-text/docs/languages
$mgmt_config['gs_speech2text_langcode'] = "en-US";
// Provide region code for the storage, see also:
https://cloud.google.com/compute/docs/zones
$mgmt_config['gs_region'] = "";
// Provide the name of your Google Cloud Storage bucket (mandatory for cloud storage)
$mgmt_config['gs_bucket'] = "";
// Optionally provide the path to autoload.php of the Google Cloud API
(https://github.com/GoogleCloudPlatform/google-cloud-php) if you are not using the included API
// $mgmt_config['google_cloud_api'] = "vendor/autoload.php";

// For MS Azure Blob Storage use:
// Enable (true) or disable (false) the MS Azure Cloud API
$mgmt_config['azure_api'] = false;
// Provide credentials for access (connection statement:
DefaultEndpointsProtocol=https;AccountName=myAccount;AccountKey=myKey;)
$mgmt_config['azure_access_key'] = "";
// Provide the name of your Azure container (mandatory for cloud storage)
$mgmt_config['azure_container'] = "";
// Define daily synchronization for delayed saving of media files in cloud storage (true) or save media files immediately (false)
// If the daily synchronization has been enabled the media files will not be saved in the cloud storage immediately!
$mgmt_config['storage_dailycloudsnyc'] = false;
```

5 Configuration of the webserver

For detailed information about the installation of PHP on different web servers please visit *http://www.php.net*.

The support of htaccess (Apache) or web.config (MS IIS) configuration files is mandatory and must therefore be activated on the web server.

Never mind what web server you will use, it must be prepared to handle all files with the extension „.php" and pass them to the PHP hypertext pre-processor for parsing, compiling and execution. This can be set on any web server, for instance in the configuration file of Apache „http.conf" or in MS IIS directly through the properties of a website/host. More details you will find in the description of your web server.

An important security setting is to restrict the access to certain directories for PHP scripts. For this purpose, the setting "php_admin_value open_basedir" need to be set, usually in the virtual host of the web server.
This ensures that PHP scripts can only access files, where access is required.

The system uses .htaccess files under Apache or web.config files under MS IIS. For the directives of the files to to be accepted by the web server, you need to set the directive "AllowOverride All" in the host.

Example of an Apache host:

```
<VirtualHost 188.40.49.142:80>
        DocumentRoot "/var/www/html"
       php_admin_value open_basedir /var/www/html/:/usr/bin/:/tmp/
        ServerAdmin support@example.com
        ServerName www.example.com
        ServerAlias example.com
        ErrorLog /path-to-logs/error_log
       CustomLog /path-to-logs/access_log common
        <Directory /var/www/html>
                Require all granted
                AllowOverride All
                Options -Indexes +FollowSymLinks
                <IfModule mod_dav.c>
                        DAV Off
                </IfModule>
        </Directory>
</VirtualHost>
```

If you use multiple instances, the internal and external repository of an instance should be placed in a defined location inside a separate virtual host. Access to files should be limited to the files in the virtual host and not outside of the scope of the host.

6 PHP configuration

We recommend to run PHP as a server module (not as CGI version). The binary distribution of PHP can be downloaded for free on *http://www.php.net*
An installation guide for PHP is included in the distribution, but is also available on the PHP website.
We recommend to use only official PHP distributions to guarantee the full functionality.

The following additional PHP modules are required:
- mbstring (for multibyte support)
- bcmath (for Google Video Intelligence and TCPDF)
- ldap (for LDAP support, only Enterprise Edition)

6.1 Configurations in php.ini

To operate the system you will need PHP as a server module on UNIX derivates or MS Windows. You can find more details about „php.ini" on *http://www.php.net.*
The configuration file of PHP „php.ini" and its settings are important for the operation. In order to operate the system as Digital Asset Management system, a few parameters need to be set.

The following parameters of php.ini should be defined:
```
short_open_tag = Off
safe_mode = Off
disable_functions =
passthru,shell_exec,show_source,phpinfo,system,proc_open,chgrp,chown,chmod,
show_source,dl,php_uname,posix_kill,posix_mkfifo,posix_mknod,posix_setegid,
posix_seteuid,posix_setgid,posix_setpgid,posix_setsid,posix_setuid,posix_ttyname
expose_php = Off
max_execution_time = 21600
memory_limit = 3072M
error_reporting = E_ALL & ~E_DEPRECATED
display_errors = Off
error_log = /var/log/php/error.log
register_globals = Off
register_long_arrays = Off
post_max_size = 6000M
upload_max_filesize = 6000M
session.use_cookies = 1
session.cookie_secure = 1
session.cookie_httponly = 1
session.gc_maxlifetime = 21600
date.timezone = <Your local timezone>
```

For large file support (> 2 GB) of the Workplace Integration:
```
output_buffering = Off
```

For the load distribution via an upstream third-party load balancer another setting in php.ini must be taken:
Managing the session ID as an extra transparent parameter in the URL. The extra URL parameter contains the session ID value with a default name of "PHPSESSID". This "PHPSESSID" parameter will be automatically inserted into all links in the HTTP response.

```
session.use_trans_sid = 1
```

7 MariaDB and MySQL configuration

7.1 Full-text search index

The MariaDB and MySQL full-text index by default only indexes words which are 4 characters or longer, which means a search for a expression with 3 characters nothing will be returned. If you want to change the minimum word length you need to edit the MySQL configuration file my.cnf which is usually located in /etc/mysql/my.cnf and add the following line under the [mysqld] section to change the default to 3:

```
[mysqld]
ft_min_word_len = 3
```

If the ft_min_word_len value is already in the file then change the number to the minimum length required.
After making this change the MariaDB or MySQL server must be restarted for it to take effect.
Now that the minimum word length has changed, and new or updated records will use the new minimum word length, but existing records will not be affected. To rebuild the full text index run these queries:

```
REPAIR TABLE object QUICK;
REPAIR TABLE textnodes QUICK;
```

7.2 ngram full-text parser for Chinese, Japanese, and Korean

The built-in full-text parser uses the white space between words as a delimiter to determine where words begin and end, which is a limitation when working with ideographic languages that do not use word delimiters. To address this limitation, the database provides an ngram full-text parser that supports Chinese, Japanese, and Korean (CJK). The ngram full-text parser is supported for use with InnoDB and MyISAM.

The ngram parser has a default ngram token size of 2 (bigram). For example, with a token size of 2, the ngram parser parses the string "abc def" into four tokens: "ab", "bc", "de" and "ef".

As a read-only variable, ngram_token_size may only be set as part of a startup string or in a configuration file which is usually located in /etc/mysql/my.cnf:

```
[mysqld]
ngram_token_size=2
```

In order to create a FULLTEXT index that uses the ngram Parser, modifications need to be made in table "object" and "textnodes" in the file hypercms/database/rdbms/createtabels.sql by adding "WITH PARSER ngram" to the FULLTEXT KEY:

```
CREATE TABLE `object` (
  . . .
  FULLTEXT KEY `object_objectpathname` (`objectpathname`) WITH PARSER ngram,
  FULLTEXT KEY `object_textcontent` (`textcontent`) WITH PARSER ngram
) ENGINE=MyISAM DEFAULT CHARSET=utf8mb4 COLLATE=utf8mb4_unicode_ci;

CREATE TABLE `textnodes` (
  . . .
  PRIMARY KEY  (`textnodes_id`),
  KEY `textnodes_id` (`id`),
  KEY `textnodes_text_id` (`text_id`),
  KEY `textnodes_object_id` (`object_id`),
  KEY `textnodes_multiple` (`id`,`type`),
  FULLTEXT KEY `textnodes_textcontent` (`textcontent`) WITH PARSER ngram
) ENGINE=MyISAM DEFAULT CHARSET=utf8mb4 COLLATE=utf8mb4_unicode_ci;
```

8 Installation

The installation package of the hyper Content & Digital Asset Management Server consists of a compressed file that includes the software as well as the manuals. You will need Adobe Acrobat Reader to open the manuals. This software can be downloaded for free, please visit *http://www.adobe.com*.

This compressed file needs to be transferred to the web root of the web server and the content of the file need to be extracted there. You can also extract the compressed file locally and copy all files to the web server, e.g. using FTP.

8.1 Easy installation

The installation of the system is quite simple. After placing all the files directly in the root directory of the web server, please assign write permissions to the following directories:
- hypercms/config
- data
- repository
- mypublication

Now call to the following URL: http(s)://www.youromain.com/hypercms/
This starts the installation process and takes you to a form that asks you for all the data necessary for the installation. The installer guides you through the installation process and forwards you to the logon form of the system after the successful installation.

8.2 Installation and configuration for advanced users

The installation and configuration of the system can be done or changed any time manually as well. Open the file "hypercms/config/config.inc.php" in the config directory of hypercms in a text editor. This file holds all the main settings. The explanations of the various settings are located in the file itself.

Some settings include specifying absolute paths of the installation as well as the URL's. If you do not know the document root directory of the web server, please ask the server's administrator for the exact path.

After all files are placed on your web server, you must assign write permissions to directories and files on UNIX systems. Even under Windows, this step is necessary so that the files can be written to certain directories.
It is important that all files in the internal and external repositories can also be written by the content management server (web server user). This also applies to the temp folder in the hypercms directory.

After the system is installed on your server, a directory for your publication (website) must be created. In this directory all generated pages will be saved. You can create this directory anywhere within your document root on the web server. It is recommended to create a directory that presents the name of your website.

Please note: Do not use the same publication directory for multiple websites. If you do so, the user of another publication can access the pages as well.

On the presentation server the files "livelink.inc.php", "livelink.inc.jsp" or "livelink.inc.asp" need to be placed in case of an activated link management. These files contain the function for the active link management of the hyper Content & Digital Asset Management Server under various applications.
The files themselves are located in your installation directory "hypercms/function". Therefor you need to copy them in the "config" directory of the external repository for PHP.
Are you using JSP, the file "livelink.inc.jsp" must be present in any web application root. With ASP, a virtual directory named "include" in the IIS (Web server) need to be set up , where the file "livelink.inc.asp" is stored centrally for all publications.
Using ASP please take care that the virtual directory "include" is accessible to both the site and the repository.

The specific settings for your website are saved in the files "Publication.conf.php" in the internal repository and also in the file "Publication.ini" of the external repository. In case you use JSP, the settings are saved in the file "Publication.properties" of the external repository. These files can be found in the "config" directory of the internal and external repository.
Set the values of the individual parameters according to established directories or circumstances. Explanations can be found for each parameter in the file itself

8.3 Setting up automated tasks

The system needs to perform automated tasks. Therefor you need to create scheduled Cron Jobs when using Linux/UNIX or automated tasks if using MS Windows.

The files which need to be executed regularly are located in hypercms/job:
daily.php …. needs to be executed daily (e.g. midnight)
minutely.php … needs to be executed every minute

Please take care that the Webserver User is executing these tasks.

Example for the Cron jobs entries to execute the tasks:
```
* * * * * cd /var/www/html/hypercms/job; /usr/bin/php -f minutely.php
0 1 * * * cd /var/www/html/hypercms/job; /usr/bin/php -f daily.php
```

8.4 Setting up automated software updates

To enable automatic software updates, you need a cron job that is owned by a user with write permissions for the files of the software in order to overwrite the existing files with the new ones.
The web server user should not have write permissions of the system files, it is therefore strongly recommended to use a separate user for this task.
You can define the interval for new software updates according to your requirements in the job. However, a daily check for updates is recommended.

Example of a Cron job for executing daily software updates at 2:00 am:
```
0 2 * * * cd /var/www/html/hypercms/job; /usr/bin/php -f update.php
```

In order to enable the automatic software updates using an alternative update service, the following setting can be used in the main configuration file
/hypercms/config/config.inc.php:

```
// Display update information on home screen for all users (true) or hide (false)
// Keep in mind that only updates installed by function update_software will be
tracked by the system and can be used to display and hide the information.
$mgmt_config['update_info'] = true;

// Define an alternative URL for the software update service
$mgmt_config['update_url'] = "";
```

8.5 Setting up the API keys for DropBox, Google Maps, Google Analytics and YouTube

In order for the system to work with the APIs from DropBox, Google and YouTube, some settings must be set in the main configuration file /hypercms/config/config.inc.php.

Integration of Youtube for videos
Please note the information in the chapter "Uploading Videos to YouTube" in the Users Guide for integrating YouTube for uploading videos.

Settings in the main configuration file /hypercms/config/config.inc.php:
```
// YouTube integration (requires Connector module)
// Please provide the Google API credentials in order to upload videos to YouTube
// Visit: https://developers.google.com/youtube/registering_an_application
$mgmt_config['youtube_oauth2_client_id'] = "";
$mgmt_config['youtube_oauth2_client_secret'] = "";
$mgmt_config['youtube_appname'] = "";
```

Integration von DropBox beim Datei-Upload
You can get an API app key and secret (a.k.a. consumer key and secret) by creating a Dropbox API app at: https://www.dropbox.com/developers/apps/create
Once you have an app created, the app key and secret will be available by going to the App Console and selecting the app here: https://www.dropbox.com/developers/apps

Settings in the main configuration file /hypercms/config/config.inc.php:
```
// DropBox integration
// Please provide a valid Dropbox app-name and app-key
// Keep in mind that the domain needs to be added to your Dropbox developer
account in order to use the app-key
// Visit: https://www.dropbox.com/developers/apps/create
$mgmt_config['dropbox_appname'] = "";
$mgmt_config['dropbox_appkey'] = "";
```

Integration von Google Maps
To create an API Key for Google Maps please visit:
https://developers.google.com/maps/documentation/embed/get-api-key

Settings in the main configuration file /hypercms/config/config.inc.php:
```
// Google Maps integration
// Provide a valid key for Google Maps
// Visit: https://developers.google.com/maps/documentation/embed/get-api-key
$mgmt_config['googlemaps_appkey'] = "";
```

Integration von Google Analytics
Google Analytics can be used to track system component access and usage. However, this setting has nothing to do with tracking the use of a website. For this purpose, the Google Analytics code must be integrated in the template.
You can find more information on creating a tracking ID here:
https://support.google.com/analytics/answer/7476135

Settings in the main configuration file /hypercms/config/config.inc.php:
```
// Google Analytics integration
// Provide a valid key in order to track the users behaviour with Google Analytics
// Visit: https://support.google.com/analytics/answer/7476135
$mgmt_config['googleanalytics_key'] = "";
```

8.6 Content encryption on server

The system allows the content on the server to be encrypted. This can be set for each Publication, see Adminstrators Guide.
The key used for encryption can be stored in the main configuration file on the server for each installation or instance. There are 2 keys, one for the encryption of temporary data and one for the encryption of files and data (based on AES 256).
In addition, the key can also be provided via an external resource.

In case of an externally provided key, please note the following:
- The connection to the external key provider should be encrypted
- The provider of the key should have a protective mechanism that allows the delivery of the keys only to the system
- If the key is lost or changed, the existing content can no longer be decrypted

A simple approach would be the transfer of the key from the key server to the server, on which the system is running, via HTTPS. For the simplest access restriction method, the key server uses an IP restriction, that way only the server on which the system is running can query the key.

This would be defined in the file main configuration file of the system "hypercms/config/config.inc.php" as follows:
$mgmt_config['aes256_key'] = file_get_contents ('https://key-server-name/mykey.key');

Furthermore, 3 encryption strengths are available:
// Encryption strength (weak, standard, strong)
$mgmt_config['crypt_level'] = "standard";

This is a general setting for various encryption algorithms for temporary data in the system. For the files or their content however, "strong" encryption will always be used regardless of the setting made.

Encryption Algorithms:
Strong … AES 256 (based on OpenSSL with fallback to Mcrypt in CBC mode)
Standard … AES 128 (based on OpenSSL with fallback to Mcrypt in EBC mode)
Weak … The main purpose is to gain a short encrypted string, not recommended for sensitive data or files!

9 First time Start

Call the address in your browser you defined in the file „hypercms/config/config.inc.php" as the root for the content management system, e.g.:
http(s)://www.yourdomain.com/hypercms/

Now you should see the logon mask in your browser. If the system cannot be started and you receive an error message from the web server, please double check your settings (especially path information).

The further procedure is described in the various guides. Here you will find more information about all features of the system.

10Workplace Integration with WebDAV

To use the Workplace Integration, the corresponding module must be installed on the server. Note that the Free Edition does not include this module.

Web-based Distributed Authoring and Versioning, or WebDAV, is a set of extensions to the Hypertext Transfer Protocol (HTTP) that allows computer-users to edit and manage files collaboratively on remote World Wide Web servers.
The WebDAV protocol allows interactivity, making the Web a readable and writable medium. It allows users to create, change and move documents on a remote server (typically a web server or "web share"). This has obvious uses when authoring the documents that a web server serves, but it can also be used for storing files on the web, so that the files can be accessed from anywhere.

The hyper Content & Digital Management Server supports WebDAV to access all multimedia files with a client that supports the WebDAV protocol, like the Windows file explorer, MS Office suite, Adobe suite, and much more).

In order to allow transfers of big files, the Workplace Integration uses streams.
This allows you to deal with very large files (tried up to 15GB), without requiring a high number for memory limit.

PHP configuration for large file support
For this to work, output buffering must be turned off. It appears to be on for some php installations. Not turning this off will make PHP return memory-related errors.

In the php.ini configuration file:
`output_buffering=off`

Or if you use PHP settings in Apache:
`php_flag output_buffering off`

10.1 Setup as a network drive

The Workplace Integration enables you to manage multimedia files directly from your local file manager.
The WebDAV-standard allows users to edit files, e.g. Adobe files or MS Office documents directly. This means that files can be opened, edited and saved like they are in the local file system. The download of the file for editing and the upload is not necessary, since the file can be saved directly in the application. Copy, cut and paste is also supported.
In addition, virtual download (name-dl.htm) and access link files (name-dl.htm) can also be provided, which can be included as attachments in e-mail messages, e.g. in MS Outlook. This way the file will not be attached in the e-mail, instead a link for downloading or accessing the file will be included. This setting must be enabled in the respective publication, see Administrators Guide.

Attention: Please note, that the file manager may create a new file and remove the original file when copy and paste is used. This means that the history/versions of the pasted file will be lost!

Integration in a file manager:
If the system was configured for the WebDAV access, the system can be integrated in a standard file manager, e.g. MS Windows Explorer, as a network drive to gain access to all files.
Please keep in mind that not all functionalities of the browser interface of the system are available.

WINDOWS 10 Explorer – How does it work?

1. Simultaneously press the [Windows] and [E] keys so that the Explorer opens. Click on "This PC" on the left. Click on the "Computer" tab at the top and select "Connect network drive".
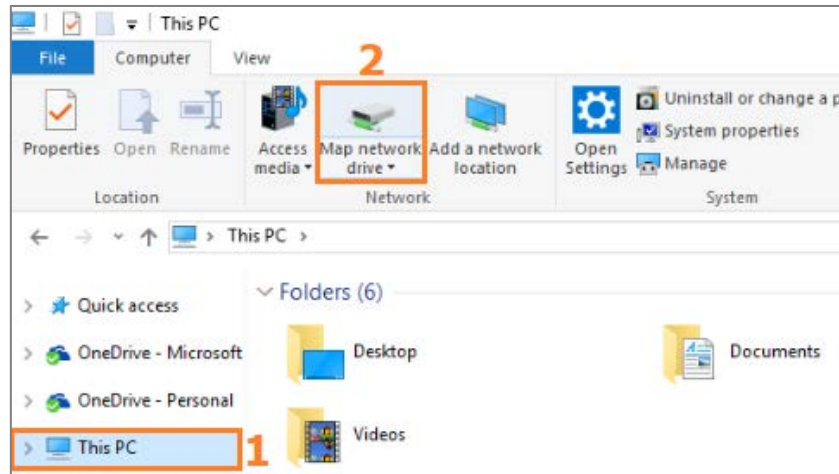
2. Select the desired drive letter and enter the path of the storage:
https://cloud.hypercms.net/cms/webdav/
Make sure that the network drive is automatically reconnected and that you log in with your hyper Content & Digital Asset Management Server user credentials.
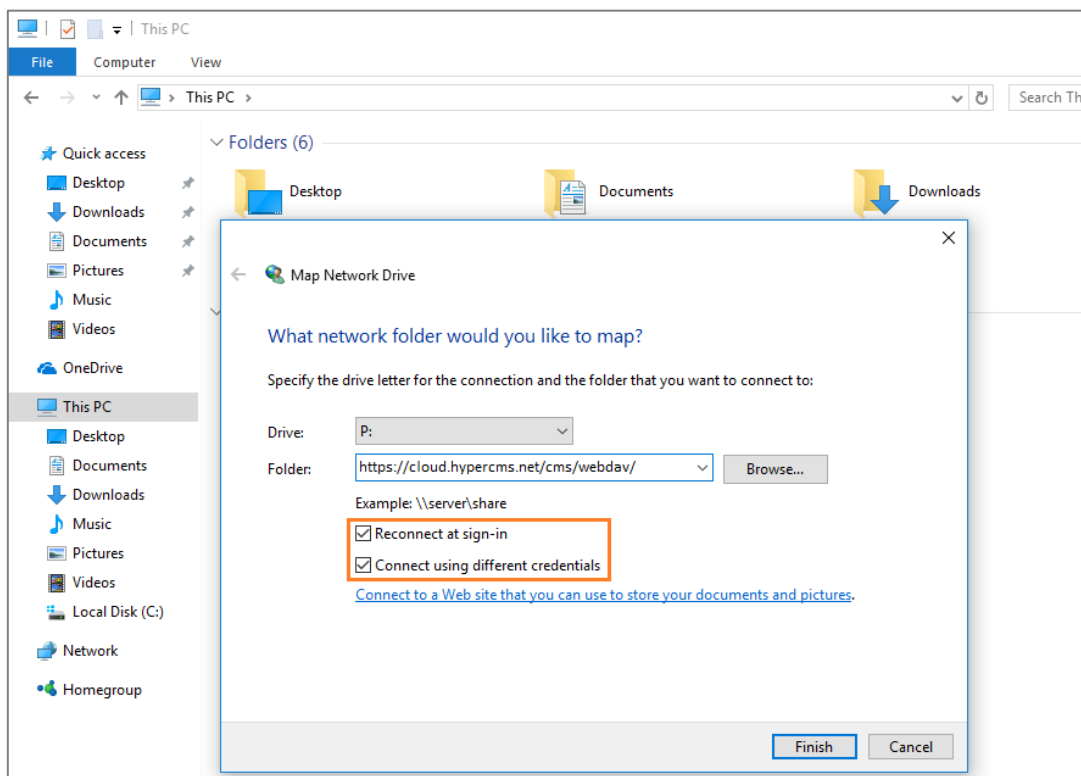
3. Click the "Finish" button to get to the authorization. Enter the user name and password for the hyper Content & Digital Asset Management Server here. If you confirm this step, the network drive is integrated and is visible in the Explorer next to the hard drives.
In the case of an LDAP/AD connection to the system, please note that a password change will only take effect once you have logged into the browser and your new password has been synchronized.

WINDOWS 7 - How it works?

1. Before you can use this feature, you need to set your password once again.
You need access to the option "Map network drive..." in the "Tools" menu of Windows Explorer, which can be opened using the Alt-key in Windows 7.
2. After that you proceed like shown in the screen below and fill in your user name and password in the new window.
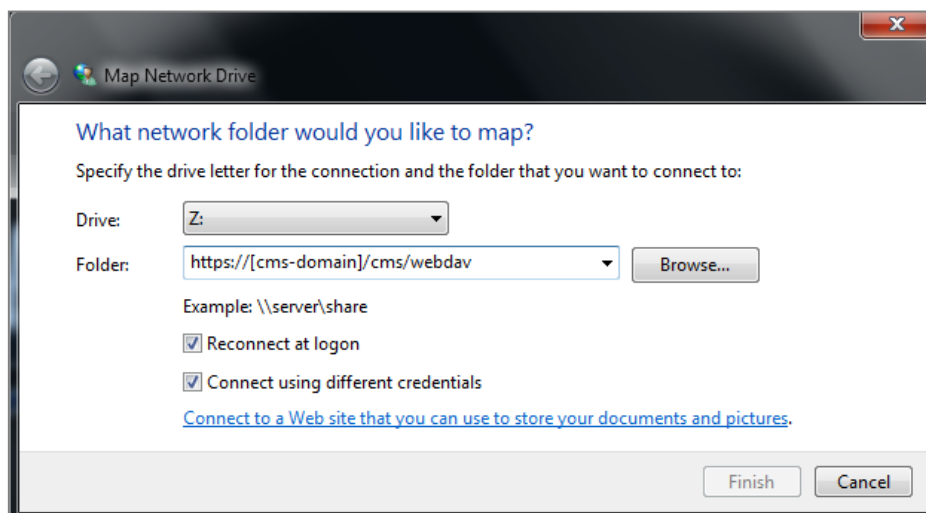
3. Now you should be able to access the network drive.

10.2 Synchronization of files

In addition to the direct access to the files in the system, the files can also be synchronized between the hyper Content & Digital Management Server and the local drive. The advantage is that you can work with the files even without a network connection and synchronize them again when you have a connection to the server again. The same also works on mobile devices with the help of a WedDAV client app. There are several free apps in the app stores that you can use.

There are a variety of WebDAV clients, e.g. the free software CyperDuck (https://cyberduck.io/), which can be downloaded and installed free of charge for all common operating systems. The software can synchronize the files without the integration as a network drive.
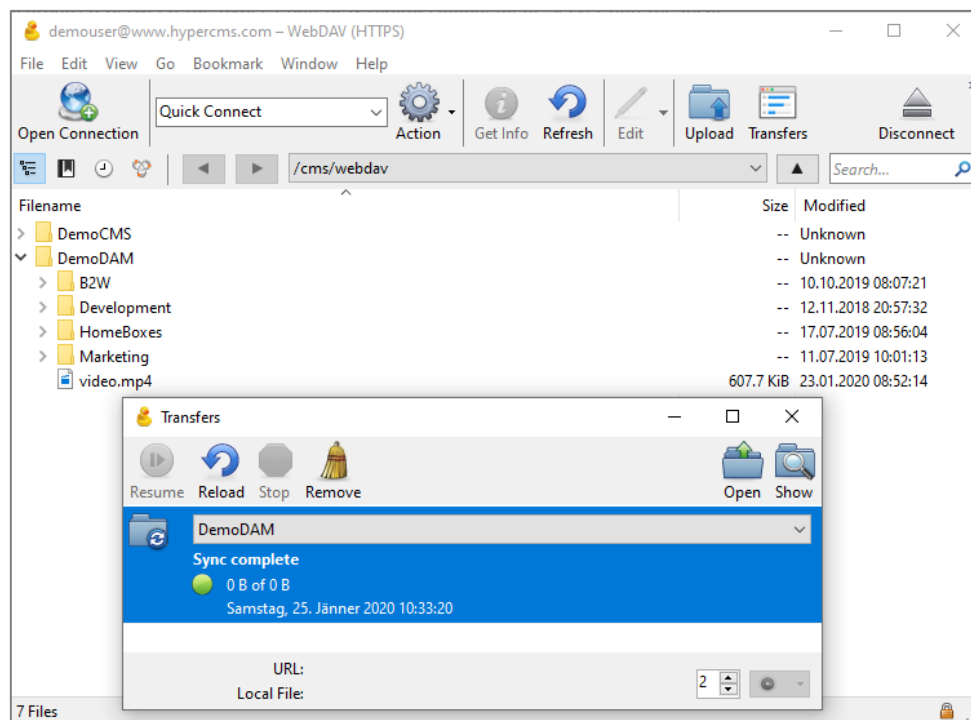
Another free software would be FreeFileSync (https://freefilesync.org/) to enable synchronization of files from two drives. To do this, however, the system must first have been integrated as a network drive. Afterwards, FreeFileSync can be used to set up the synchronization of the files.

10.3 WebDAV with Windows

Mounting a WebFolders fails:
It may happen that mounting a WebFolders on Vista fails with the error message "The folder name is not valid" or something like that. One reason for this may be that the BasicAuthLevel in the Vista configuration is either not configured or with too low a value. This is an entry in the registry under the following path:
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\WebClient\Parameters

Start the Registry Editor with the command "regedit".
In the registry editor go to the above path and set the BasicAuthLevel to the value 2.
If BasicAuthLevel ia not available, right-click the mouse in the right pane, then click on New and DWORD (32-bit). The new entry must be called BasicAuthLevel and should have the value 2. Then restart the PC so that the entry are also active.

The WebDAV connection is very slow:
Instructions for improving the WebDAV Performance:
- In Internet Explorer, open the Tools menu, then click Internet Options
- Select the Connections tab
- Click the LAN Settings button
- Uncheck the "Automatically detect settings" box
- Click OK

Filesize
Windows has introduced a file size limitation of 50000000 bytes in a security update. You may receive one of the following error messages while downloading a file from a WebDAV volume:
"Cannot Copy FileName: Cannot read from the source file or disk" (Windows Vista or XP SP1 with security update 896426 installed)
"Error 0x800700DF: The file size exceeds the limit allowed and cannot be saved." (Windows 7)
"An unexpected error is keeping you from copying the folder. If you continue to receive this error, you can use the error code to search for help with this problem." (Windows 7)
The limitation can only be disabled on client side, by changing registry keys. See this article for detailed instructions: http://support.microsoft.com/kb/900900/en-us
Additional information is also available in this article: https://support.microsoft.com/en-us/kb/2668751

Port
It appears that Windows does not support ports other than the default (80). Make sure your server is not running on a non-default http port.

SNI
It was reported that the Windows 7 and 8 (and likely older clients as well) do not support 'SNI' (server name identification), which is a technology that allows virtual hosting of multiple HTTPS domains on one server.
If you're running into issues with this, make sure you don't host more than one HTTPS-based domain off one IP address, or make sure that it's the default.
In the case of apache, the default https server would be the top-most virtualhost definition.
It was reported that the WinHTTP API (used in the Windows WebDAV client) doesn't support TSLv1.1/TSLv1.2 connections. If you have restricted your server config to only provide TLSv1.1 and above the connection to your server will fail.
See this article with further information: https://msdn.microsoft.com/en-us/library/windows/desktop/aa382925%28v=vs.85%29.aspx

Caching
It was reported that Windows 7 has a 60 second cache, which may be frustrating if you expect an immediate update.
This can be disabled using a registry key. For more information:
http://technet.microsoft.com/en-us/library/ee683963%28v=ws.10%29.aspx

Upload timeouts
An upload of large files taking longer than 30 minutes using Web Client in Windows 7 can cause the following error:
"Error: 0x80070079 The semaphore timeout period has expired"
How to raise the timeout: https://support.microsoft.com/en-us/kb/2668751

10.4 WebDAV with Mac OS Finder

You may encounter a few problems when using the WebDAV feature in Finder.

A WebDAV connected drive may operate extremely slow on some Mac operating systems. Newer Mac operating systems seems to be faster. The reason new Mac operating systems are faster is that they are better at caching small operations. The Mac integrates the WebDAV feature in the file system and many applications such as Finder create an enormous amount of file system operations. If not cached by the WebDAV client in the Mac operating system, these requests will be sent to the server, thus slowing down the WebDAV connection.

- You can speed up the Finder by performing the following operations.
  Open terminal and prevent .DS_Store file creation on network volumes:
  defaults write com.apple.desktopservices DSDontWriteNetworkStores true

- For any network connected drive, in Finder: uncheck "Show icon preview" option for Column view and disable "Show item info" in icon view

Non English characters not working

Finder seems to have a problem with UTF-8 encoded characters mixed with spaces. You should avoid using non English characters in folder names and file names together with space characters. Alternatively, use the free CyberDuck Mac WebDAV client (https://cyberduck.io/) which does not have any problems with UTF-8 encoding. Please note that CyberDuck does not integrate with the file system, thus you will not be able to work with files directly on the server. You must first sync the files to your local file system before you can work on the files.

11 Permalinks

A Permalink (of permanent and hyperlink, also permanent link) in the World Wide Web is a permanent identifier in the form of an URL. A permalink references to a certain content available permanently and primarily via this URL.

When a permalink, or more permalinks in case of multiple languages in one page, is used in a template in order to save the permalink, the navigation/sitemap (function shownavigation) can use the permalinks instead of the paths in the file system for the defintion of the pages URL.
In the install directory is a folder called "rewrite". This folder includes the necessary files for the URL rewriting for the Apache web server.
Copy these files have to the root directory of the website. The index.php needs tob e setup with the values for the publication:

```
// publication name
$site = "hyperCMS";

// text ID array (text-ID as key and URL paramaters as value)
$text_id = array (
"PermaLink_EN"=>"langcode=EN",
"PermaLink_DE"=>"langcode=DE"
);

// alternative URI on error
$alt_uri = "/home/";
```

The array $text_id presents the ID of the field prepared for the permalink and ist reference to the GET parameter for the multilanguage support.
If no multilingualism is used, the value "langcode = XX" can be left blank.

12 Legal reference / flag

12.1 Questions and suggestions

For advanced questions and suggestions, please contact the support.

hyperCMS Support:
support@hypercms.com
http://www.hypercms.com

12.2 Imprint

Responsible for the content:

hyperCMS
Content Management Solutions GmbH
Rembrandtstr. 35/6
A-1020 Vienna – Austria

office@hypercms.com
http://www.hypercms.com

12.3 Legal information

The present product information is based on the version of the program, which was available at the time the document was composed.

The maker reserves the rights of modifications and corrections of the program. Errors and misapprehension accepted.

© 2023 by hyperCMS Content Management Solutions