hyper Content & Digital Asset Management Server

CMS

Version 10.2
Administrators Guide

2026-01-05

Index

1 System management functions

Publication management (centrally)
- **Create new publications**
  A new publication can be added to the system.
  Adjusting publication settings
  Every publication has its own configuration settings as well as its own lines of inheritance.
- **Delete publications**
  Deleting publications from the system.

User management (centrally and decentralised for each publication)
- **Create new users**
  A new user can be added to the system.
- **Management of access permissions, names, email, and user groups for users**
  Users gain access permissions within the page and the asset structure. Users are assigned to user groups and their permissions (e.g. the permission to create new objects).
- **Delete users**
  Deleting users from the system.

Management of user groups (decentralized for each publication)
- **Create new user groups**
  A new user group can be added to the system.
- **Management of all permissions for a user group**
  The user group defines the roles of the users. The permission defines the roles. If there is a change in the permission of a user group, all users in the corresponding user group are affected.
- **Delete user groups**
  Deleting a user group from the system.

System events
View the log file of all system events. The log can be exported as a CSV-file.

Queue of publications
View the list of all objects which are to be published, unpublished or deleted on a specific date and time.

2 Publication management

The hyper Content & Digital Asset Management Server is capable of administrating multiple publications in server mode. Therefore, you have the possibility to create and administer new websites independently of the management of existing websites. You can individually define the configuration of the system for the new publication. The feature enables the management of several websites with just one installation of the hyper Content & Digital Asset Management Server and instantly gives multiple organizations the opportunity to operate independently on the same server.

Select "Administration" from the main menu and then "publication management" to create, edit or delete new publications. This feature is only available for users, who are members of a publication which permits the management of publications in its default settings. In addition, the user must have the necessary permissions in the corresponding user group.

2.1 Create a new publication

In order to create a new publication you need to click the first button of the toolbar. You are then prompted to enter a specific name. You need to define a unique name without special characters for the publication. The name will be used to identify the publication:
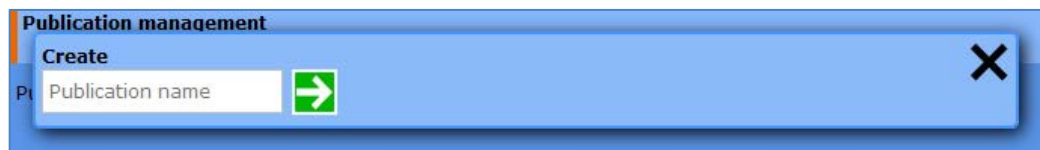
Please pay attention to the differences and dependencies that come with the use of certain technologies or applications on the presentation system. In contrast to PHP Hypertext Preprocessor, Java Server Pages/Java (JSP), and Active Server Pages/VBScript (ASP) need a specific setting for the central functions „livelink.inc.jsp" and „livelink.inc.asp".

In JSP „livelink.inc.jsp" must be stored in each web application root.
If you use ASP, it is necessary to create a virtual folder named "include" under IIS and store the file „livelink.inc.asp" in the folder.
For detailed information on this topic please refer to the installation guide.

Settings for the management system:

Publication management

Publication [DemoCMS ▼] ⊕ Create ⊕ Delete ❓

| Configuration | Inheritance |

Configuration of publication DemoCMS

Management system configuration

Display name (optional)	DemoCMS
Grant publication management	☐ Active
URL of the website	https://www.hypercms.com/demo/DemoCMS/
Directory path of the website	/home/hypercms/public_html/demo/DemoCMS/
Folders to exclude (use ; as delimiter)	
Allow access to Assets only for certain IP addresses (use ; as delimiter)	
Allow access through WebDAV	☑ Active ☐ Download link ☐ Access link
Link management	☑ Active
Default character set	UTF-8
Send e-mail	☑ Active
Mail server name (has effect on sendlink)	hypercms.net
Portal Access link	☐ Active
User for access links	Please select a user ▼
Disable special characters in object names	☐ Active
Only DAM functionality	☐ Active
Enable taxonomy browsing and search	☐ Active
User must provide metadata for file uploads	☐ Active
Enable direct file upload in pages	☐ Active
Watermark options for images -wm /images/watermark.png-#topleft-+10	
Watermark options for vidoes -wm /images/watermark.png-#topleft-+10	
Social Media sharing	☑ Active
YouTube upload	☑ Active
Theme	Select ▼

Enable languages for translation / Taxonomy

Available languages	Selected languages
Afrikaans Akan Albanian Amharic Armenian Azerbaijani	Arabic Bengali Bulgarian Chinese (Simplified Czech Danish

>> <<

Optical Character Recognition (OCR)

Available languages	Selected languages
Afrikaans Akan Albanian Amharic Arabic Armenian	

>> <<

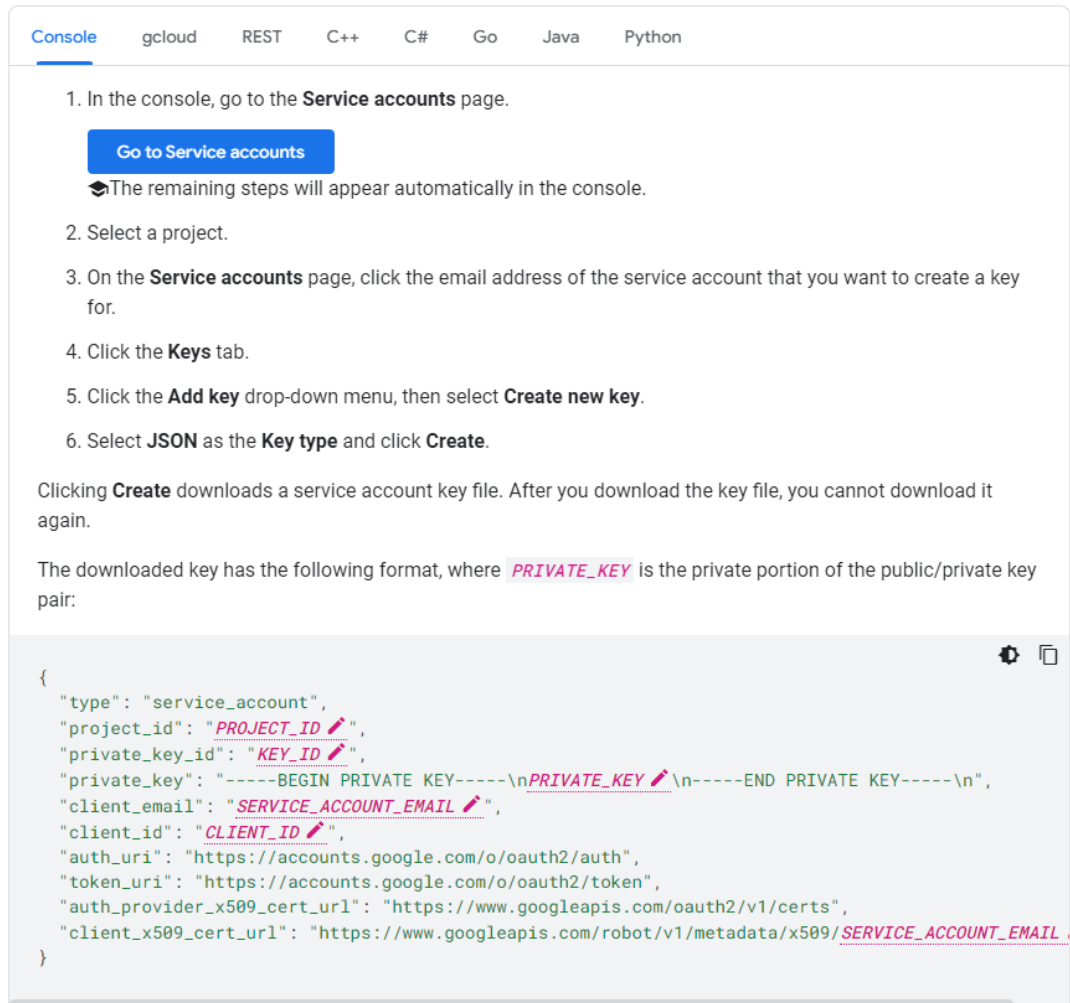|	
Storage limit in MB	5000
Encrypt content	☐ Active
RESTful API	☑ Active
SOAP API	☐ Active
Google Cloud API Key (JSON)	
Google Vision (Image)	☐ Active
Google Video Intelligence (Video)	☐ Active
Google Speech-to-Text (Audio, Video)	☐ Active
Language (languageCode) https://cloud.google.com/speech-to-text/docs/languages	
OpenAI API Key	

- Optional display name for the publication (may include special characters)
- Grant publication management for Administrators to administrate their publications
- Provide the root URL on the webserver for the website
- Provide the root path on the webserver for the website
- Restricted folders: Which folders in the root folder have restricted access?
- Allowed IP addresses for access to assets (multimedia files). Only client with a valid IP can open the files.
- Allow access via WebDAV for workplace integration. This requires the workplace integration module. In addition, virtual download and access links can also be generated as HMTL files, which can be inserted and sent as attachments in e-mail messages, e.g. in MS Outlook.
- Shall the link management be activated? Links will be corrected automatically. This feature should be deactivated for DAM usage, since it cannot really be used.
- Provide the default character set to be used for documents, when no character set is defined
- Send e-mail to users. Enable notifications via e-mail about new tasks and to send/share e-mail links.
- Provide the name of the mail server
- Enable Portal access links used for public access to media libraries. If enabled each user account will provide an access link in the user profile that can be used for public access. However Portal access links excludes all permission except those for Asset or Pages for security reasons.
- Assign user account to be used for general access links: This will assign the permissions of the user to all general access links since the user account will be used for logon to the system.
- Do not allow special characters for object names: Shall users be able to use special characters in object names (assets, pages or folders)?
- DAM (Digital Asset Management) functionality only. Shall the system be used as DAM only? If so, the publication is especially tailored for DAM use.
- Enable the taxonomy for browsing and integration into the search
- Is the user required to enter metadata during the upload of new files
- Watermarking options for images:
  -wm [path to the image file]->[position: topleft, topright, bottomleft, bottomright, center]->[margin in pixels from the borders]
  Example: -wm /home/watermark.png->topleft->10
- Watermarking options for videos:
  -wm [path to the image file]->[position: topleft, topright, bottomleft, bottomright]->[margin in pixels from the borders]
  Example: -wm /home/watermark.png->topleft->10
- Enable Social Media Sharing of Assets (requires Connector module)
- Enable YouTube video integration and upload (requires Connector module)
- Theme/design for the graphical user interface
- Enabled languages for translation service
- Enabled languages for OCR (Optical character recognition), max. 3 additional languages besides the individual language setting of the user
- Storage limit in MB for multimedia files
- Media storage type for all assets of the publication (Connector Module required)
- Encrypts all files and content containers in the repository (Encryption Module required)
- Activate the RESTful API (Connector Module required)
- Activate the SOAP API (Connector Module required)
- Provide Google Cloud API Key as JSON string (Connector Module and Google Cloud Account required)

To create the service account key (JSON string) in the Google Cloud Console follow this instruction:
https://cloud.google.com/iam/docs/creating-managing-service-account-keys#iam-service-account-keys-create-console


```
Console    gcloud    REST    C++    C#    Go    Java    Python

1. In the console, go to the Service accounts page.

   [Go to Service accounts]
   🎓 The remaining steps will appear automatically in the console.

2. Select a project.

3. On the Service accounts page, click the email address of the service account that you want to create a key
   for.

4. Click the Keys tab.

5. Click the Add key drop-down menu, then select Create new key.

6. Select JSON as the Key type and click Create.

Clicking Create downloads a service account key file. After you download the key file, you cannot download it
again.

The downloaded key has the following format, where PRIVATE_KEY is the private portion of the public/private key
pair:
```

```
{
  "type": "service_account",
  "project_id": "PROJECT_ID ✏",
  "private_key_id": "KEY_ID ✏",
  "private_key": "-----BEGIN PRIVATE KEY-----\nPRIVATE_KEY ✏\n-----END PRIVATE KEY-----\n",
  "client_email": "SERVICE_ACCOUNT_EMAIL ✏",
  "client_id": "CLIENT_ID ✏",
  "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_x509_cert_url": "https://www.googleapis.com/robot/v1/metadata/x509/SERVICE_ACCOUNT_EMAIL
}
```

- Enable the Google Vision Cloud Service for automated image tagging (Connector Module required)
- Enable the Google Video Intelligence Cloud Service for automated video tagging (Connector Module required)
- Enable the Google Speech-to-Text Cloud Service for automated subtitles (VTT) for audio files and videos (Connector Module required)
- Provide language code to be used for the used language in the audio or video files (Connector Module required)
- OpenAI API key for the automatic creation of images (text-to-image) using the createAIimage function and DALL-E.

Settings for the publication target system:

- URL of website: What is the name of the root URL on the webserver for the new website?
- File path of website: What is the name of the root folder on the webserver for the new website?
- Repository URL: What is the name of the repository URL on the webserver for the new website?
- Repository file path: What is the name of the repository file path on the webserver for the new website?
- File path of application: What is the name of the root folder of the application on the server (necessary when using JSP or ASP)?
- Operating system on publication server: Which operating system is used on the publication server: UNIX/Linux or Windows?
- Shall components be embedded via HTTP? (or if deactivated components are directly embedded via file system access)
  Please note, that variables during the process of an application are not available for the components when embedding via HTTP because only the result (HTML) is returned.
  This feature should be deactivated when using a server-based application in your templates, pages, or components which require the interaction of objects.
  In **PHP Hypertext Preprocessor (PHP)**, it is possible to dynamically embed components via the file system in addition to the http-method.
  This would also be possible in JSP or ASP. Due to embedding restrictions for e.g. JSP files on the web application, a distributed system with a central repository cannot be realized with conventional methods (file include).
  This setting has no influence on the dynamic functions of the hyper Content & Digital Asset Management Server (link management, and personalization).
  Thus, please note that in **Java Server Pages (JSP)** the embedding of components can only be done via http.
  Please also note that in **Active Server Pages (ASP)**, it is essential that this option is deactivated when using separate hosts (domain names).
  In ASP, the http-method and execution of components via "Server.Execute" is supported.
  The execute-method of the server object is only executable within the same

host (application). Therefore, components cannot be executed when using different hosts for website and repository.

- Remote Client: What is the name of the URL of "remoteclient.php"? Please note that the configuration INI-file must be stored in the same location in the file system.

Each publication is maintained in the management system, but its publication targets do not necessarily have to be located on the same webserver.
With the hyper Content & Digital Asset Management Server it is possible to store published websites on different servers in order to increase performance and reliability. The distribution of the published files on different servers is done by replication (unidirectional). You can use any file transfer tool or the build-in remote client for replication.
For the initial distribution of the whole publication, it is necessary to transfer all files of the root folder of the publication. It might also make sense to transfer the repository as well in order to have local access to all the objects.

Please note: The path of the repository is stored in the main configuration file „config.inc.php". For details please refer to the installation guide.

The configuration settings require detailed information of the webserver. The document root of the website as well as the absolute file paths to the website must be specified here.
Only experienced users should change the settings of the configuration file. For this purpose, we offer specific training.

Settings for Active Directory / LDAP integration and synchronization of the user data:

In order to use the AD or LDAP authentication these main configuration settings in config/config.inc.php in the systems root directory need to be defined in order to include the connector file of the Connector module or your own version in data/connect/ and its function "authconnect":

```
// LDAP/AD Integration
// If you are using LDAP, Active Directory, or any other user directory, you can
specify the file name without extension to be used for the connector.
// The standard connector file "ldap_connect.inc.php" is located in
/hypercms/connector/authconnect/.
// Besides the standard connector, you can make a copy of the file
"ldap_connect.inc.php" and paste it in /data/connect/ in order to modify the code
and define your own connector.
// The system will look in /data/connect/ for the specified connector file and
will fallback to /hypercms/connector/authconnect/.

// Use "ldap_connect" for LDAP/AD
// Specify the file name "ldap_connect" located in /data/connect/ or
/hypercms/connector/authconnect/ in order to connect to an LDAP or AD directory
and verify users.
// Alternatively you can create your own connector file in /data/connect/ and
refer to it. Make sure you use the file extension .inc.php and use the same
function name and parameters.
$mgmt_config['authconnect'] = "";

// Enable (true) or disable (false) the connectivity for all publications
// If enabled the below AD/LDAP settings need to be defined.
// If disabled the AD/LDAP settings need to be defined in the publication
management (per publication).
$mgmt_config['authconnect_all'] = false;

// Define a LDAP/AD user with general read permissions
// This LDAP/AD user is only required if you want to use SSO using the OAuth
remoteclient
$mgmt_config['ldap_admin_username'] = "";
$mgmt_config['ldap_admin_password'] = "";

// Define the connection parameters
// Port 389 is for LDAP over TLS. Port 636 is for LDAP over SSL, which is
deprecated.
// LDAP works from port 389 and when you issue the StartTLS (with
ldap_start_tls()) it encrypts the connection.
// Example: ldapserver.name
$mgmt_config['ldap_servers'] = "ldapserver.name";
// Example: @domain.com
$mgmt_config['ldap_userdomain'] = "";
// Example: OU=Departments,DC=MYDOMAIN,DC=COM
$mgmt_config['ldap_base_dn'] = "";
// Example: 2 or 3
$mgmt_config['ldap_version'] = 3;
// Example: 389 or 636
$mgmt_config['ldap_port'] = "";
$mgmt_config['ldap_follow_referrals'] = false;
$mgmt_config['ldap_use_ssl'] = true;
$mgmt_config['ldap_use_tls'] = false;


// Define the LDAP/AD user filter for the LDAP bind or leave empty if the LDAP
server support the user name for the bind
// This setting will not be applied if MS AD or a user domain is used.
// Use %user% as placeholder for the user name.
// Example: uid=%user%,cn=users
$mgmt_config['ldap_username_dn'] = "";
```

```
// Define the user filter for the search in LDAP/AD
// For Active Directory define "sAMAccountName"
$mgmt_config['ldap_user_filter'] = "sAMAccountName";

// Enable (true) or disable (false) the sync of LDAP users with the system users
// The user information such as name, email, telephone is queried and
synchronized.
// If the user's publication and group membership should also be synchronized
according to certain rules,
// this must be specified in the $mgmt_config['ldap_sync_publications_mapping']
and $mgmt_config['ldap_sync_groups_mapping']
// otherwise the memberships are retained as stored in the system.
$mgmt_config['ldap_sync'] = false;

// Define the user attributes you want so sync with LDAP/AD
// Supported attributes for the sync are 'memberof', 'givenname', 'sn',
'telephonenumber', and 'mail'
// memberof ... user memberships in LDAP/AD
// givenname ... firstname
// sn ... surename/lastname
// telephonenumber ... phone
// mail ... e-mail address
$mgmt_config['ldap_user_attributes'] = array('memberof', 'givenname', 'sn',
'telephonenumber', 'mail');

// Delete the user if it does not exist in the LDAP/AD directory (true) or leave
user (false)
$mgmt_config['ldap_delete_user'] = false;

// Keep existing group memberships of user (true) or not (false)
// Enable this setting if groups are defined manually and by LDAP/AD (mix of
groups)
// Keep in mind that enabling this setting has security implications, since
LDAP/AD groups will not be removed anymore once assigned
$mgmt_config['ldap_keep_groups'] = false;

// Synchronize AD/LDAP groups with publications of the user
// Define mapping based on a search string that defines the users publication
membership, use "," as separator for the assignment to multiple publications
// Mapping: "LDAP search string" => "Publication-name-A,Publication-name-B"
// Example: $mgmt_config['ldap_sync_publications_mapping'] =
array("DC=domain,DC=de"=>"Publication-name-A,Publication-name-B",
"DC=domain,DC=uk"=>"Publication-name-C");
$mgmt_config['ldap_sync_publications_mapping'] = array();

// Synchronize AD/LDAP groups with user groups of the user
// Define mapping based on a search string that defines the users group
membership, use "," as separator for the assignment to multiple groups
// Mapping: "LDAP search string" => "Publication-name-A/Group-name-A,Publication-
name-B/Group-name-B"
// Example for general groups for all publications:
$mgmt_config['ldap_sync_groups_mapping'] = array("OU=MANAGER
GROUP"=>"ChiefEditor", "OU=ALL GROUPS"=>"Editor");
// Example for specific groups per publication:
$mgmt_config['ldap_sync_groups_mapping'] = array("OU=MANAGER
GROUP"=>"Publication/ChiefEditor", "OU=ALL GROUPS"=>"Publication/Editor");
$mgmt_config['ldap_sync_groups_mapping'] = array();
```

```
// Signature template
// If the user data should be used to create a signature for the  e-mails you can
use the following template.
// Leave empty or comment if you don't want to use the signature template.
// Use %firstname%, $lastname%, %email%, and %phone% for the provided user data
from LDAP/AD.
$mgmt_config['ldap_user_signature'] = "Best regards
%firstname% %lastname%
E: %email%
T: %phone%

This message is intended for the individual named above and is confidential and
may also be privileged. If you are not the intended
recipient, please do not read, copy, use or disclose this communication to
others. For electronically send information and pieces of advice,
which are not confirmed by following written execution, in principle no adhesion
is taken over.";
```

The LDAP settings defined in main configuration will be applied for the users of all publications if:

```
$mgmt_config['authconnect_all'] = true;
```

The following publication settings will only be activated if:

```
$mgmt_config['authconnect_all'] = false;
```

LDAP / MS Active Directory	
LDAP/AD Server A value is required	ldap.domain.com
LDAP/AD user domain MS AD: A value is required	domain.com
Base Distinguished Name (DN) A value is required	cn=read-only-admin,dc=example,dc=com
LDAP/AD Version	3
LDAP/AD Port A value is required: 389 (TLS) or 636 (SSL)	389
Follow referrals	☐ Active
SSL	☐ Active
TLS	☑ Active
User Base Distinguished Name for the LDAP bind User name = %user%: uid=%user%,cn=users	uid=%user%,cn=users
LDAP/AD user filter A value is required: sAMAccountName (MS AD)	uid
LDAP/AD Sync (User information, Member of group)	☑ Active
Delete user	☐ Active
LDAP/AD + System Groups (Merge)	☐ Active
LDAP/AD user attributes 'memberof', 'givenname', 'sn', 'telephonenumber', 'mail'	'memberof','givenname','sn','telephonenumber','mail'
Mapping 'LDAP Search' => 'User group' 'OU=MANAGER GROUP'=>'ChiefEditor,Editor' 'OU=ALL GROUPS'=>'Editor'	'OU=MANAGER GROUP'=>'ChiefEditor,Editor' 'OU=ALL GROUPS'=>'Editor'

- LDAP/AD Server: The host / domain controller option is required and provides an array of servers located on your network that serve LDAP or Active Directory. You insert as many servers or as little as you'd like depending on your forest (with the minimum of one of course). For example, if the server name that hosts AD on my network is named ACME-DC01, then I would insert ACME-DC01.corp.acme.org inside the domain controllers. Use , or ; as delimiter for more entries.
- LDAP/AD user domain: The required user domain is the suffix of your user accounts in AD. For example, if your domain DN is

"DC=corp,DC=acme,DC=org", then your account suffix would be `@corp.acme.org`. This is then appended to then end of your user accounts on authentication. For example, if you're binding as a user, and your username is "jdoe", then the system would try to authenticate with your server as "jdoe@corp.acme.org".

- Base Distinguished Name (DN): The required base distinguished name is the base distinguished name you'd like to perform operations on. An example base DN would be "DC=corp,DC=acme,DC=org".
- LDAP/AD Version: The use LDAP protocol version (2 or 3)
- LDAP/AD Port: The optional port is used for authenticating and binding to your AD server. The default ports are already used for non-SSL and SSL connections (389 and 636). Only insert a port if your AD server uses a unique port. If one is not defined, then the system will try to find it automatically by querying your server. It's recommended to include it to limit queries executed per request.
- Follow referrals: The optional follow referrals tell active directory to follow a referral to another server on your network if the server queried knows the information you are asking for exists, but does not yet contain a copy of it locally. This option is defaulted to false. For more information, visit: https://technet.microsoft.com/en-us/library/cc978014.aspx
- SSL / TLS: The SSL & TLS settings are used for protected data transfer. These options are definitely recommended if you have the ability to connect to your server securely.
- User Base Distinguished Name for the LDAP bind: The User Base Distinguished Name is required for some LDAP servers for authentication (bind) the user name (%user%) alone is not supported.
- LDAP/AD user filter: Name for the filter of the user in LDAP/AD. For MS Active Directory this is "sAMAccountName" (requires activated Sync setting).
- LDAP/AD Sync: The user information such as name, email, telephone, and membership is queried and synchronized.
- Delete user: If the user is not found in LDAP/AD, he will also be removed from the publication (requires activated Sync setting)
- LDAP/AD + System Groups (Merge): Keep existing group memberships of user. Enable this setting if groups are defined manually and by LDAP/AD (mix of groups). Keep in mind that enabling this setting has security implications, since LDAP/AD groups will not be removed anymore once assigned. (requires activated Sync setting)
- LDAP/AD user attributes: LDAP/AD attributes that shpuld be used for the update of the user data (requires activated Sync setting). Note that only the following attributes are supported ('memberof', 'givenname', ' sn', 'telephonenumber', 'mail').
- Mapping: If the user's group membership should also be synchronized according to certain rules, this must be specified, otherwise the memberships are retained as stored in the system (requires activated Sync setting).

  Syntax: 'LDAP-Search-String'=>'Group-Name-A,Group-Name-B'
  Example: 'OU=MANAGER GROUP'=>'ChiefEditor,Editor'

To finish the configuration of the publication press "OK" to save the file.

2.2 Edit publication settings

The settings of existing publications can be changed at any time. Just click on the corresponding button "Edit publication" to gain access to the configuration of a publication.
Select the third icon from the list. Now the settings of the publication will appear and can be changed by pressing "OK". Please note that changes instantly have effect on the system.

2.3 Delete publications

Before you can delete a publication, all pages and components need to be removed.

To delete a publication, select the second icon. Then select the item from the drop-down menu you want to delete and press "OK".
When deleting a publication all objects of the management system are removed and all information of users, user groups, media database, link management, and database as well as task lists are lost.

Be careful when removing a publication from the system because all of the data will be lost irretrievably.

3 Inheritance

The inheritance of contents is defined for each publication. The use of inheritance enables the editor to access assets/components from other publications. This is also true for the design templates. Therefore, it is possible to inherit contents and designs between publications separately.
To inherit contents or templates of other publications the corresponding publications have to be selected. Assets which have been inherited can be used but not edited. These can only be edited in the source publication. If you remove a publication from inheritance, already embedded external contents remain in your own publication and can only be removed manually.

When inheriting design templates, the following principle applies when the templates have the same names:
If there are templates with the same name in the allocated publications as well as in your own publication, then always the template of your own publication is used. If the own publication is removed, the template of the assigned publication is used automatically.

You receive access to inheritance settings by selecting the tab within the publication settings. Select the publications in the left window and assign them with the arrow keys to your own publication. Therefore, the contents (assets) of the chosen external publications are available for you own publication.

4 User management

The user management is centralized but it is possible to create users via the main menu item "Administration" or within a publication under the same menu item.

The difference is the following: with the centralized user management, users can be assigned to particular publications whereas within the publication, users can be assigned to user groups. Therefore, it is possible that the administrator of a publication creates a user and gives him/her the rights via the user group membership. This new user is only the member of this publication. The administrator with access to all publications can extend the permissions of the user by giving him/her access to other publications. Nonetheless the user needs to be given the corresponding permissions via the user group management, otherwise the user cannot operate in the publication.

4.1 Search for users

Use the search if you are looking for users. The user ID, name and email address will be searched. The users found appear in the list.
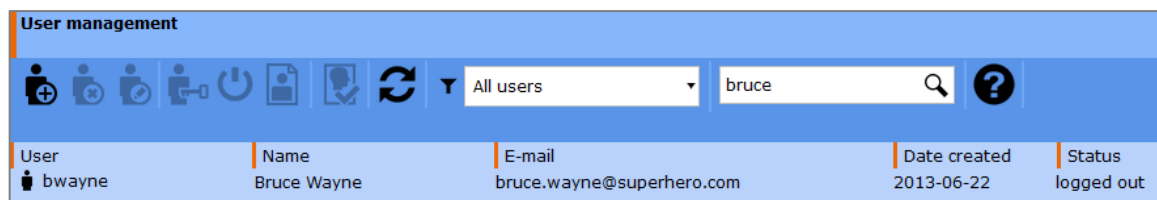
4.2 Create users

The first icon is called „Create user". With that you affiliate the new user with the system for the first time. The user gains access to the system and to a specific website which is registered in the system (in case the system is running in server mode).

Enter the username (a username must be unique in the system) and the password of the new user. Do not forget to confirm the password and afterwards click on "OK". With that the new user is created and can now be configured.

In the case of the centralized user management, the form for user settings and access to publications looks like this:

Settings for user: ckent

Change password

Confirm password

Hash for OpenAPI

478b070d570280405362a97613a1fd95

Name

Clark Kent

E-mail

clark.kent@superhero.com

Phone

Signature

Superman aka Clark Kent

Language

English

Time zone

America/New_York

Theme

Blue

Period of validity

Start   End

Publications		Assigned to publication
Boarderline	>>	DemoDAM
ContentMaster		DemoShowCases
DemoCMS	<<	
Development		
hyperCLOUD		

Home Objects		Selected object
DemoDAM/Brand-Guidelines	>>	Search
DemoDAM/Marketing-Videos		DemoDAM/Marketing-Image
DemoDAM/PR-Documents	<<	All reports
Favorites		Free storage
Free storage per publication		News

Administration
☐ Super administrator

Sign in
☐ User for access links

Save settings ➡

You can define all personal information, the language, time zone and design theme of a user, including a period of validity for the user account. The user can only login and use their account in the given time frame.
If you block the access to the users settings, the user can't select his home screen boxes. In this case, a user administrator needs to assign the home boxes/objects.

By selecting the option „Super Administrator" the user gains administrator permissions and access to all publications.

If it is an automatically created user for access via an access link, it is not possible to login with a user name and password or to reset the password. However, this setting can be changed later, but you should pay attention to the access permissions based on the group membership of the user, as these usually do not correspond to the restricted access through the access link.

Apart from that, the user also needs permissions within the publication which can be granted by the user group membership. For this you need to switch to the publication in which the new user shall operate. In user management select the item "Edit User" from the toolbar. If you select "All users" from the menu than all users of the publication are shown and you can adjust more settings.

The new user can now be assigned to one or multiple user groups. With that the user becomes a member of the user group and also adopts the permissions of this user

group. This is also known as the "role of a user" within the system. You can also set the name and email address of the user. With that the system can notify the member via email (SMTP), if new tasks are available.

The same user can be assigned to multiple groups. He/she has gained permissions of all the groups depending on the position within the page or asset structure.

4.3 Edit user settings

In order to change the user settings, select a user from the list. Edit the user with click on the icon "Edit User" in the toolbar, context menu, or via double click on the list item. The same user form will open, as already described in "Creating users".
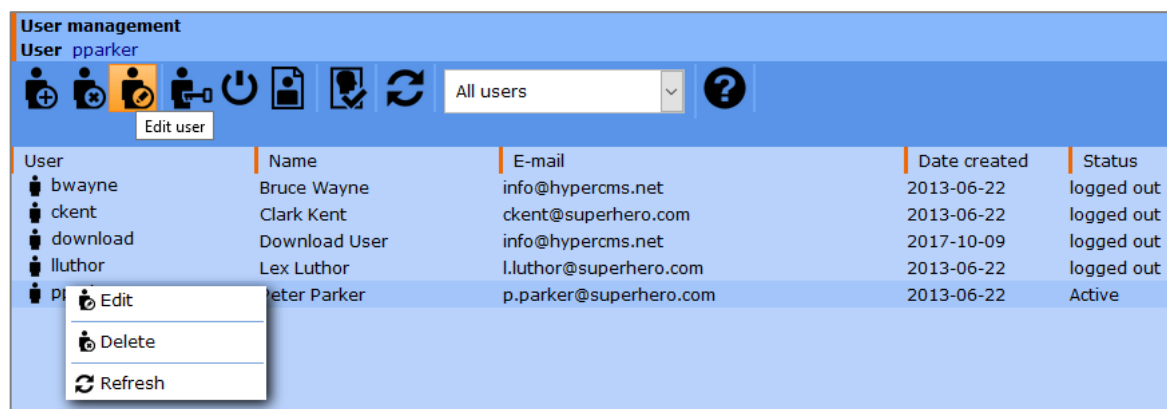
4.4 Delete users

To delete a user, select this user from the list and then click on "Delete user" in the navigator. You are then prompted to either select a user from the whole list or sort by client membership or user group membership:
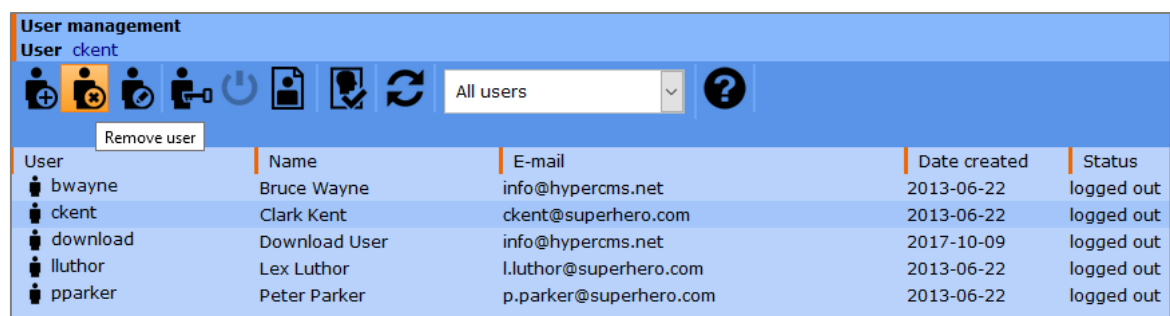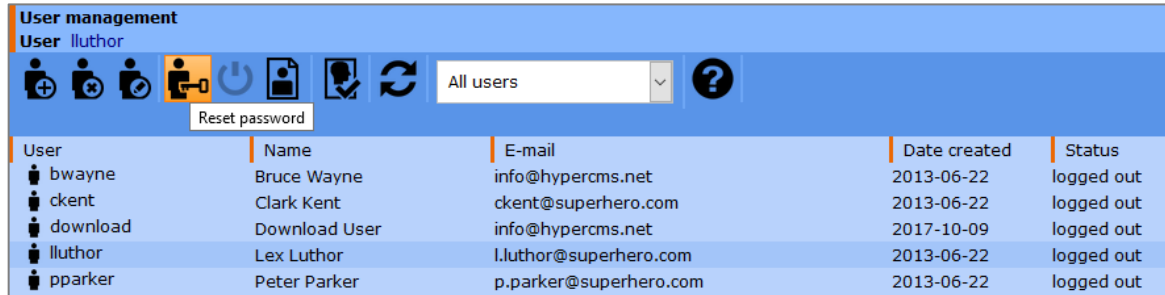
After clicking "OK", you get a confirmation message. If you are really sure to delete this user, you can confirm the deletion. The user account and record of the publication are deleted and the person has no more access to the system or the publication.

Please note: if you delete a person from the main administration, also all the settings of this user are lost irretrievably. This has no effect on the settings of the user group or the publication itself.

4.5 Reset the password of a user

To send the selected user a new password via e-mail, select the "Reset password" item in the toolbar. The user can then log in with the new password and will be required to change it.
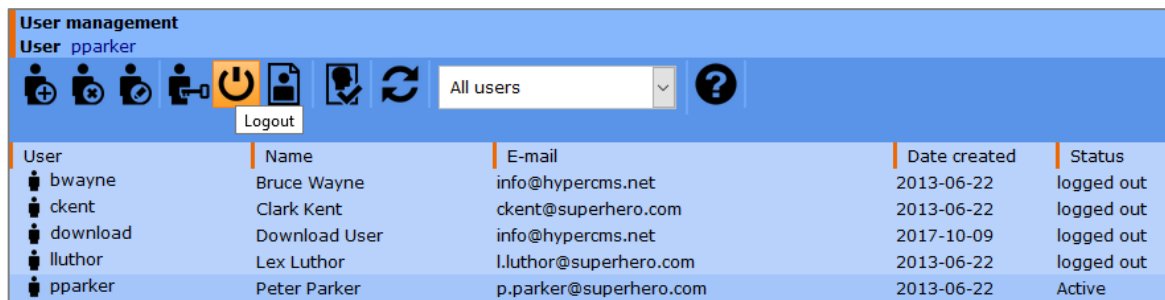
4.6 Log out of a user

In order to logout a user from the system, select the "Logout" item in the toolbar.
All active user session will be removed and the user will not be able to use the system without logging in again.
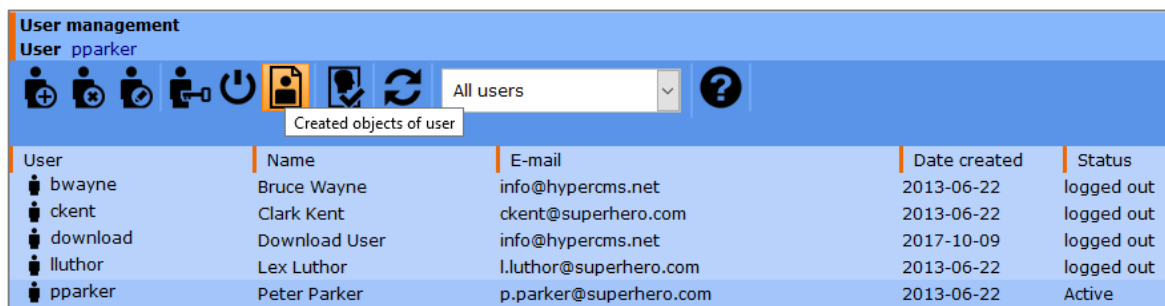
4.7 Show all objects of a user

In order to display all objects owned by a user (owner), select the "Created objects of a user" item in the toolbar.
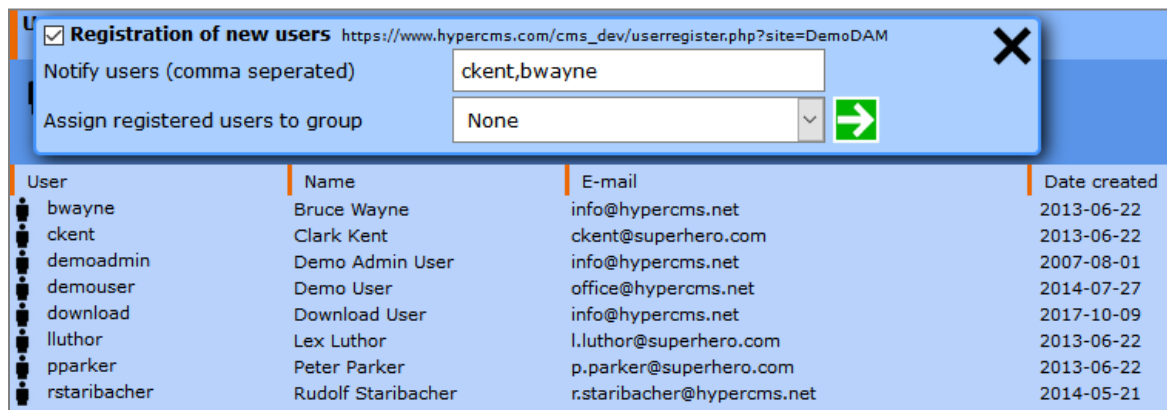
4.8 Registration of new users

The system supports the registration new users through a registration form using the "Registration of new users" element of the toolbar.

The registration for the users of the publication must be to be activated using the checkbox. Optionally, certain users can be notified automatically when new persons have been registered.

The automatic assignment of the registered persons to a user group is also possible. If you want to verify the user before any permissions are assigned to them, then no user group must be assigned. In this case, you can assign the users to any group manually.

The displayed address (URL) serves as a link to the registration form.

In the main configuration file of the system, the registration can generally be activated, so that the link to the registration form also appears in the login mask. In this case, the user himself must select a publication for which he wishes to register.

5 User group management

In the navigator menu tree under "Administration" you will find the user group management. Here you can create, delete, and edit user groups. The scheme is similar to the one from user management.

The user group defines all of the permissions in the system and therefore describes all possible roles of a user. Only when a user is assigned to one or multiple user groups, then the user has certain (local=where do the permissions apply?) permissions in the system.

Please note that one user group exits in each publication. User groups with the same name can be used in several publications but do exist in each client separately. User groups are pre-defined in the system but can also be created individually.
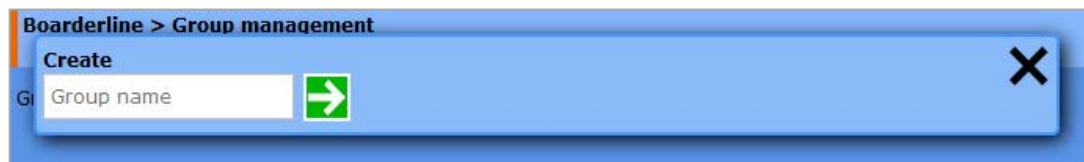
If you create a user group for your web designers, you can restrict their access to the templates. Then this user group can create or upload new templates and template pictures. But the group cannot create new users or user groups nor change the structure of the website and its contents.

Administrators can create new users or user groups and therefore are also responsible for assigning permissions to users and user groups. Editors and chief editors of your website can change structure and contents of your website. Editors can create new contents whereas chief editors can additionally publish and delete contents.

A specific feature comes with the creation of a user group named "default" (not case sensitive). If this group does exist, it is used when a user is sending objects. The recipient of the email can access the object via the link of his/her assigned group. He/she therefore gains the permissions of the group "default". He/she gains the permissions of another group which he/she has been assigned to by the sender, if there is no "default" group in the publication.

5.1 Create user groups

To create a new user group click on "Create user group":
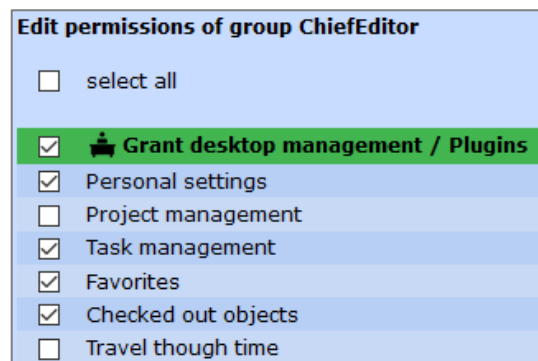
Enter a new name for the user group (a user group name must be unique per page) and click on "OK". You can then assign the permissions for this user group.

With the central checkbox at the beginning ("select all") of the list it is possible to activate and deactivate all the checkboxes at once.
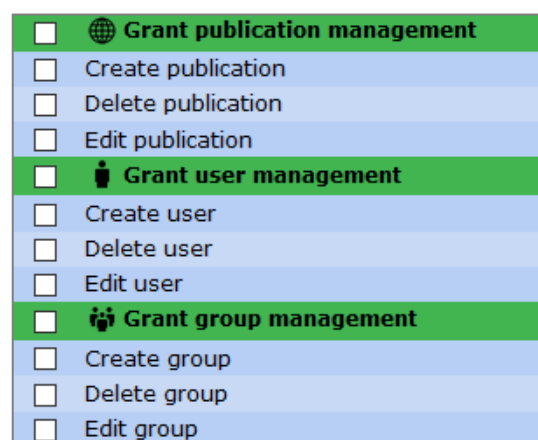
Management of permissions for the desktop:

Access to plugins requires desktop access permission.

Management of permissions for users, user groups, and publications:

The publication management is only available when running a server license
or when the client has been granted management permissions in the basic settings of the publication.

Management of permissions for personalization:

☐	🎙 **Grant personalization management**
☐	Grant customer registration permissions
☐	Create customer registration
☐	Delete customer registration
☐	edit customer registration
☐	Grant customer profile permissions
☐	Create customer profile
☐	Delete customer profile
☐	edit customer profile

Management of permissions for workflows:

☐	⛓ **Grant workflow management**
☐	Grant workflow manager permissions
☐	Create workflow
☐	Delete workflow
☐	Edit workflow
☐	Define workflow field of application
☐	Grant workflow script permissions
☐	Create workflow script
☐	Delete workflow script
☐	Edit workflow script

Management of permissions for templates:

☐	🗔 **Grant template management**
☐	Grant template permissions
☐	Create template
☐	Delete template
☐	Edit template
☐	Grant template media permissions
☐	Create template media category
☐	Delete template media category
☐	Rename template media category
☐	Upload template media
☐	Delete template media

Management of permissions for assets:

Managements of permissions for pages:

Managements of permissions for plugins

By selecting the corresponding checkboxes you can assign permissions to the user group.

When the box is checked the user group has access to the selected functions. Each item of the menu bar can be activated or deactivated for a group (see images above). If you deactivate a main item (see images above, lines in green colour) like e.g. "Publication management", all sub items are also deactivated, even when various sub items are still checked. With that you can leave the individual settings of the sub items alone and just deactivate the main item to e.g. restrict the access to upload files or to create folders.

Afterwards, save your settings by clicking "OK".

In order to give user groups permission to edit contents, you need to give the group also access to the corresponding asset and page structure. To assign the necessary permissions click on the button for "access to folders" and adjust the settings:
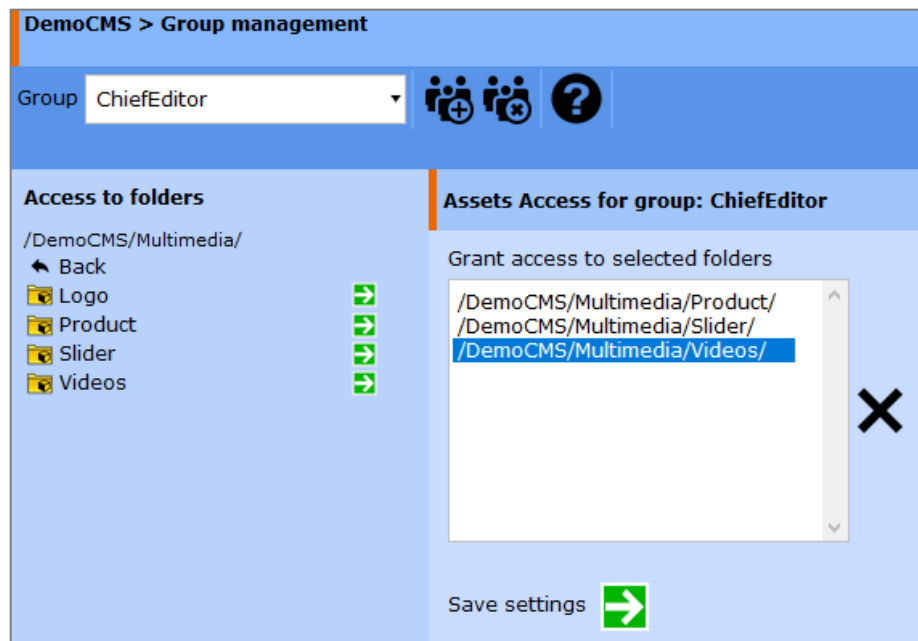
The desktop will show a new navigator window which lists all available folders in the system. Click on the name of the folder to show all sub folders of the folder. With that you can navigate through the structure of your assets and pages just the way you do it when using the navigator. By clicking on the "OK"-icon you can select a specific folder. Folders which have been selected are then shown in the window on the right-hand side. If you want to remove the access to a specific folder, just select it in the form window and click on the remove/delete icon (red cross).

To save your settings and return to user settings, please click on "OK". The described procedure is the same for "access to assets" as well as "access to pages". To save the permissions of the user group click on "OK". Changes will take affect when the user logs in the next time.

If a user is a member of multiple groups, all permissions of all groups are accumulated. He/she therefore has the permissions of all groups depending on the position in the page or asset structure.

5.2 Edit user group settings

To edit the permissions of an existing user group click on "Edit" in the toolbar and select the group you want to change. You get the same windows as already described above under "Creating user groups".

5.3 Delete user groups

To delete a user group select the second icon of the toolbar. Then select the group you want to delete from the drop-down menu and press "OK". All members of this group lose their permissions in the system because they are no more related to the deleted group. The users remain in the system and can be assigned to another group.
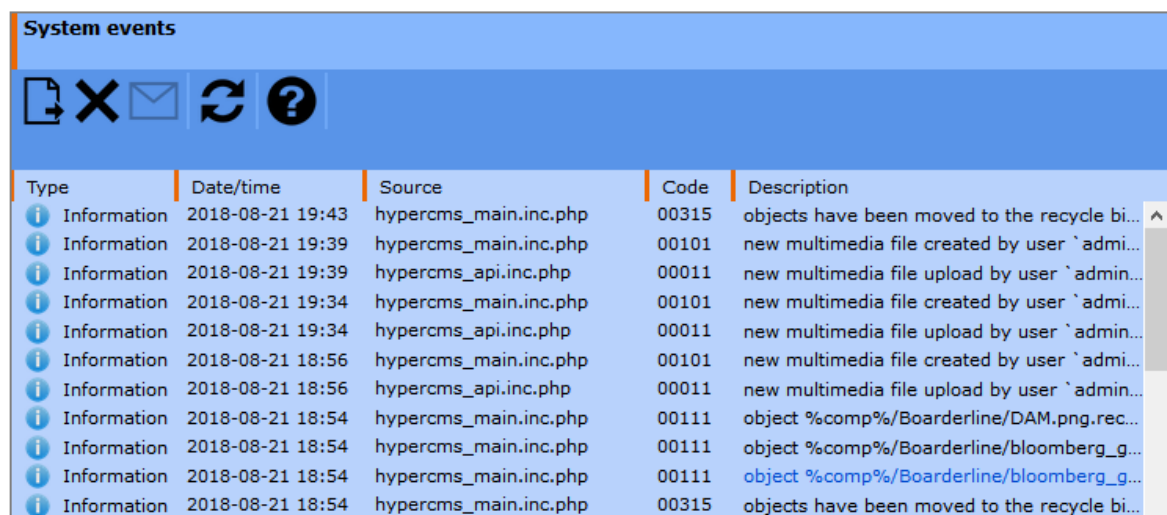
6 System events

By selecting „system events" from the menu in the navigator, you get access to the event log of the system.

The system log presents information, warnings, and errors. Most of the user interaction with the system is logged, e.g. a user deleted an object.
If there are errors displayed in the event log, the time and specific location of the error are logged. With that you can determine which object caused the error and which part of the program code reported the error. Therefore, sources of the error can be easily located and eliminated.
You can clear the log at any time or export it as a CSV-file. The CSV-file can then be archived or opened in other applications (e.g. MS Excel).
You receive the description of the error by clicking on the type or the description (in short) column. You can also sort the entries by clicking on the corresponding column fields.

Publication-specific log files can be activated by the parameter $mgmt_config['publication_log'] = true; in the main configuration file. A new menu item in the administration area of the navigation tree of the publication will be displayed in case the log file exists.
The management of system events also supports the automatic notification of users in case of errors or warnings. For this the user names need to declared.

7 Legal reference / Imprint

7.1 Questions and suggestions

For detailed questions and suggestions please contact the support.

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

7.2 Imprint

Responsible for the content:

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

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

7.3 Legal reference

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 excepted.

© 2026 by hyperCMS Content Management Solutions