

contentACCESS

Manual - version 5.1



AUGUST 17, 2021

TECH-ARROW a.s.
KAZANSKÁ 5, 821 06 BRATISLAVA, SLOVAKIA
All Rights Reserved



Table of Contents

Introduction to contentACCESS.....	12
Services provided by contentACCESS	12
Software requirements.....	13
contentACCESS setup package	13
Installation of contentACCESS.....	16
<i>EULA</i>	18
<i>Installation type</i>	18
<i>Components</i>	20
<i>Prerequisites</i>	25
<i>Base folder</i>	26
<i>Service settings</i>	27
<i>Database connection</i>	28
<i>contentACCESS Central Administration</i>	30
<i>contentACCESS Web Services (Proxy)</i>	32
<i>contentWEB</i>	33
<i>Central login</i>	35
<i>Virtual drive</i>	36
<i>Search service</i>	37
<i>SMTP server</i>	39
<i>Overview</i>	44
<i>Installation</i>	45
<i>Summary</i>	46
contentACCESS components.....	48
contentACCESS Central Administration.....	48
Central administration login.....	49
contentACCESS Automated single sign on	53



Central Administration logout.....54

contentACCESS Central Administration user interface.....55

contentWEB58

Logging in to contentWEB.....59

contentWEB Automated single sign on61

Virtual Drive63

contentACCESS Web Services (Proxy).....63

Central login page.....68

contentACCESS Tools.....72

Installing Outlook forms.....72

Legacy email archive connectors.....80

Legacy archive connector for Metalogix Archive Manager Exchange Edition (MAM EE).....80

Legacy archive connector for Email Lifecycle Manager (ELM)92

Installing TECH-ARROW’s WinShortcutter101

contentACCESS Outlook add-in102

Installation of contentACCESS Outlook add-in102

How to use contentACCESS Outlook add-in.....109

Tenants in contentACCESS114

How to create a new tenant.....114

How to edit and disable a tenant.....118

Tenant limitations.....120

How to provide access to a tenant (adding new tenant administrators)123

Tenant administrator invitation types125

Tenant associations127

Tenant – database association.....127

Tenant – user association.....131

Tenant deletion135



General system configurations.....	136
Connection	136
User interface	137
Users in contentACCESS.....	138
Invitations.....	152
Roles.....	158
Login providers	184
<i>Login providers' context menu options</i>	185
<i>External login provider configuration</i>	186
<i>Associating an enabled provider with a user login:</i>	208
<i>contentACCESS users in third party systems</i>	209
System.....	211
Licensing.....	221
<i>How to activate your license key</i>	222
Notifications	226
System logs — how to find out possible misconfigurations / reasons of potential system/job failures.....	232
Configuration auditing	238
Archive auditing.....	241
Distributed environment in contentACCESS — Clusters.....	245
Statistics	259
Legal hold	262
Task runner.....	263
Indexing.....	266
SMTP Servers.....	270
SMTP Mappings.....	274
How to create/configure databases — All databases	280
Common features.....	287



Databases	288
Schedules	298
Retentions	302
Storages	304
<i>Google drive storage</i>	316
<i>Amazon S3</i>	322
Exchange connections	324
<i>Exchange performance settings – turning off the Exchange throttling policies</i>	331
<i>Mixed Exchange environments in the Email Archive system</i>	332
Importing contentACCESS configurations from files	337
<i>Manual import of Exchange servers/groups/mailboxes to the contentACCESS Address book</i>	344
<i>Importing File Archive root folders to be archived</i>	347
Creating new jobs in contentACCESS	350
Jobs' page, jobs' context menu	353
Filtering in jobs	359
File Archive	368
Introduction to File system archive	368
<i>Editing of already archived files, file versions in File system archive</i>	371
<i>Synchronization of rights to a folder/file</i>	372
File Archive settings	372
<i>File archive Databases</i>	373
<i>File archive System settings</i>	374
<i>File archive Retentions</i>	375
<i>File archive Storages</i>	375
<i>Root folders</i>	376
<i>Aliases</i>	380
<i>File archive Schedules</i>	381



<i>Provisioning settings and managing access to contentWEB</i>	381
<i>Remote agents (file archive)</i>	388
<i>Global rules (remote file archive)</i>	391
<i>Configuring aliases</i>	398
Configuration of jobs available in contentACCESS File Archive.....	400
<i>Configuration of File archive retention changer job</i>	400
<i>Configuration of File system archive job</i>	405
<i>Configuration of a File system restore job</i>	418
<i>Configuration of File system recovery job</i>	424
<i>File system recovery job description</i>	432
<i>Configuration of Delete job in File archive</i>	432
<i>File system delete job description</i>	438
<i>Configuration of File system shortcut synchronization job</i>	438
<i>File system shortcut synchronization job description</i>	442
<i>Configuration of Remote shortcutting job</i>	442
<i>Active/inactive documents in File system archive</i>	452
Email Archive	456
Important settings before creating an Email Archive job	457
<i>Database settings</i>	465
<i>Email archive System settings</i>	466
<i>Email archive Provisioning settings</i>	483
<i>Retention settings</i>	493
<i>Shortcuts in email archiving</i>	493
<i>Storing of archived emails</i>	509
<i>Creating email archive schedulers</i>	511
<i>User experience</i>	512
<i>Exchange 2013+: Mail app in OWA 2013+ or on MS Outlook 2013+ desktop version</i>	513



Exchange 2010: OWA 2010 integration514

Address book objects519

Granting access rights for mailbox users and explicit users to view the mailbox archive541

Creating contentWEB users (option 1):.....542

Manage access to a mailbox archive (option 2)550

Database and store assignment in email archiving553

How to assign database, storage and index zone to an Exchange group?554

How to assign database and storage to a mailbox?.....556

How to move data from source database/storage into a second (target) database/storage?557

Mail app access.....558

Remote agents (email archive).....560

PST import.....563

PST import job description.....576

Creating Email archive jobs: archive, restore, recovery, delete, mailbox move, shortcut synchronization, shortcut repair576

Email archive job.....579

Email archive retention changer job603

Email restore job.....613

Email recovery job.....620

Configuration of Delete job in Email archive630

Journal post processing job636

Mailbox move job639

Shortcut synchronization job644

Shortcut repair job650

Public folder archiving.....657

SMTP archiving670

SharePoint archive plugin674



SharePoint Archive settings675

SharePoint Archive job configuration680

SharePoint archive job description684

SharePoint archive retention changer job configuration684

SharePoint recovery job configuration688

SharePoint recovery job description690

Configuration of Delete job in SharePoint archive691

SharePoint delete job description696

SharePoint archive Provisioning settings.....697

SharePoint provisioning job description.....700

SharePoint publishing job701

SharePoint publishing job description.....704

SharePoint in the contentWEB archive.....704

GDPR plugin.....705

GDPR Settings.....705

GDPR Databases.....705

GDPR Schedules.....705

GDPR Index zones.....706

GDPR Processing.....707

GDPR File system settings707

GDPR Exchange settings.....709

GDPR Applications711

GDPR Jobs.....716

Teams archive.....733

Teams archive databases734

Teams archive System settings.....734

Teams archive Provisioning settings.....739



Teams archive Address book.....746

Removing objects from Teams archive Address book.....761

Teams archive Licensing.....764

Teams archive Jobs765

Teams archive job765

Teams chat archive job769

Custom plugins773

Email management job configuration773

Storage replication plugin783

Sharing plugin785

Datengut plugin786

Email synchronizer plugin788

Categorize to Public folders plugin790

LoboDMS plugin795

ThreatTest799

ThreatTest configuration799

ThreatTest Databases799

ThreatTest System settings799

ThreatTest Schedules802

ThreatTest User experience803

ThreatTest Statistics.....805

ThreatTest Job807

Using ThreatTest app812

officeGATE.....818

Installing officeGATE with Group policy (GPO)818

contentACCESS Mobile820

Virtual drive configurations.....821



Teams application.....827

Application settings829

Terms of use832

FAQ 833

Download sample for the file to be imported does not work.....834

Archiving is not working if MAPI is set to communicate with the Exchange server.....835

Virtual drive is still appearing after the uninstall836

Outlook forms problems836

Unable to open shortcuts of archived files on the server side839

Samples are not shown using “Show sample” option in the import dialog.....840

Do I need to create separate tenants for File archiving and Email archiving?.....841

What is the recommended database size for Email, File and SharePoint archiving841

The TEMP folder is running out of space when archiving big files843

The attachment could not be opened843

After updating Exchange 2013, the EWS connection might not work in contentACCESS844

If Windows authentication is not working in contentACCESS and an alias was created for contentACCESS
.....844

contentACCESS Outlook add-in certificate issue845

PowerShell scripts for setting up Email archive846

Solution for Outlook security patches851

Solution for Outlook security patches through GPO855

Solution for indexing PDF files.....858

O365 SuperUser mailbox configuration.....860

Office365 journaling862

Organizational forms863

Multifactor authentication.....864

Region setting.....866



contentACCESS Mail app installation issue	867
Azure app registration	867



Introduction to contentACCESS

contentACCESS is a modular product primarily designed to solve email archive and file archive scenarios in an organization. It uses built-in or custom plugins, which are able to connect with many kind of input systems and process the information as desired. Based on the plugins, contentACCESS is providing email, SharePoint and file management and also archive in the cloud or on premise. With contentACCESS you can choose from many storage systems to store your data – either with the built-in processing or with a completely custom processing workflow.

contentACCESS provides a simple way of just implementing the actual processing task and writing to a storage or archive system of your choice. You can set demanded plugin instances (jobs) in the background for processing these tasks without any need to change your employees' behavior. It also provides methods for accessing stored content regardless of the target, providing unified access. contentACCESS can be fit to customer needs very easily.

Services provided by contentACCESS

- ✓ **Processing plugins:** Processing plugins are responsible for crawling and processing your data. The way of processing data depends on the framework-functions that the plugin has and on further configurations of the plugin. Besides the basic plugins custom plugins are also available. The crawling method is configurable and is offering different optimizations for different use cases. The crawled data can be filtered by data age, size, file type and further specific properties. The plugin selects the crawling method, the filtering and the target storage and is focusing only on the data processing. A typical use case is to archive emails or files into an archive system, or to export to a file system, etc.
- ✓ **Manual archiving tool:** To manually archive emails directly from your MS Outlook or Outlook Web Access contentACCESS uses **Mail app** application. With this application the end user can archive old emails very easily, and also retrieve them at any time with the help of shortcuts, which replaced the original item.
- ✓ **Clustering:** Helps to optimize your capacities and divide data processing between more servers to make contentACCESS work more smoothly.
- ✓ **Storages:** The contentACCESS framework is offering the following storage providers out of the box: Disk store (simple disk storage), inPoint, iTernity. Third party storages are possible to be implemented as well.
- ✓ **contentWEB:** contentWEB is a web application running in browsers and also on mobiles (mobile browsers), which provide an easy to use interface for accessing processed and stored content. Its functions include folder browsing, item listing, item paging, item filtering, restoring, exporting and searching.



- ✓ **contentACCESS client access and WEB Services:** contentACCESS provides an API for executing plugins on demand, manually processing emails using plugins, unified access of processed elements.
- ✓ **Mobile access:** The processed data for users are accessible through the [contentACCESS Mobile](#) application as well.

Software requirements

The following prerequisites have to be installed on the machine(s) where you want to run the contentACCESS installation wizard:

- MS SQL 2012, MS SQL 2012 R2, MS SQL 2014 SP2, MS SQL 2016, MS SQL 2017, MS SQL 2019
- MS Outlook 2010/2013 (64 bit version) or later – Click-to-Run Outlook is not supported!
- .NET Framework 4.8
- Internet Information Services (IIS) and ASP .NET 4.8

The following prerequisites have to be present if you also want to use the search service:

- Java SE 8.0.1210 or later
- iFilters for indexing (download from [here](#))

These prerequisites are also checked by the installation wizard. If not installed, SQL, Framework, IIS and Java will be installed directly from the wizard during the installation.

- Operating system memory (RAM): 8 GB is recommended
- Free disk space (HDD): 20 GB free space is recommended
- Processor (CPU): 2.4 GHz quad core

Note: For more information about contentACCESS prerequisites you can read the Hardware and software requirements manual [here](#).

contentACCESS setup package

The installation package makes the contentACCESS installation process very transparent and intuitive. This section leads you through the dialogs of the installation wizard and describes the step-by-step installation of the product. To run the contentACCESS setup self-extracting package, the following is required:



- .NET Framework 4.8
- Ability to run the setup as an administrator

What is included in the contentACCESS setup package?

- Under section **Documentation** the contentACCESS manual and the Best practices to the software can be found, and it also contains a link to the contentACCESS website.
- Under **Planning** the links to hardware and software requirements can be found, and the user may download the **contentACCESS Analysis Tool** right from here. The tool is used to measure the performance of file shares to be archived and also the speed of the desired target store. It is also used to analyze the files that will be archived, and can help to set up the correct file archiving strategy.
- Under **Tools** you can find the Legacy MAM retrieve server setup, the Outlook forms used to transparently open the archived email messages directly from Outlook and from here you can also download TECH-ARROW's WinShortcutter. WinShortcutter is a collection of small and useful utilities that are primarily focused at people working in a Windows dominant office environment with a weak MAC support. It is primarily used to open MS Windows shortcuts (.LNK).
- Under **Products** you can read a short description about other software solutions of TECH-ARROW: contentGATE, streamGATE, officeGATE.
- The installation process of the contentACCESS server and it's components can be started on the **Installation** page of the setup. The following components can be installed using the **Installation** page of the wizard:
 - the contentACCESS server
 - [contentACCESS Central Administration](#) – the contentACCESS configuration interface available for system administrators and tenant administrators
 - [contentWEB](#) – the archive user interface also for the end users
 - Central login page – used to log in to the respective application with forms provider or third-party authentication providers
 - [contentACCESS Web services \(Proxy\)](#) – to ensure secure (HTTPS) connection between the user and the contentACCESS server
 - [Virtual drive](#) – a drive that's used to display the contents of the File system archive; the drive is also mandatory to retrieve the archived files from shortcuts
 - [Search service](#) – allows the user to search in selected entities/folders
 - [SMTP server](#) – a server used to process emails

contentACCESS components' prerequisites are the following:



- For Central administration: Internet Information Services (IIS), .NET 4.8
- For contentWEB: IIS, MS Outlook 2010/2013 (64 bit version) or later, .NET 4.8
- For contentACCESS Proxy: IIS, .NET 4.8
- For Central login page: IIS, .NET 4.8
- For the contentACCESS Server: .NET 4.8, SharePoint Server Client components SDK (for SharePoint processing); MS Outlook 2010/2013 (64 bit version) or later (for email processing)

These prerequisites (except of MS Outlook) are installed by the setup package automatically. If any problems occur during the automatic installation, the prerequisites must be installed manually.

SharePoint Client components and the MS SQL server can be installed using the respective application file from the contentACCESS installation package library:

- SharePoint client components:
C:\TECH-ARROW\contentACCESS_Package\Setups\SharePointClient
- SQL Server 2012 Express:
C:\TECH-ARROW\contentACCESS_Package\Setups\SQL

If the Internet Information Services (IIS) haven't been installed automatically, the IIS features must be turned on in the Windows features. Open the Server manager → click the **Roles** node → click **Add roles** → select **Web server (IIS)** in the **Select server roles** window and turn on the features based on the table below:

Management tools	IIS Management Console
Application development features	.NET Extensibility 4.8 ASP .NET 4.8 ISAPI filters ISAPI extensions
HTTP common features	Default document HTTP errors Static content
Performance features	Static content compression
Security	Basic authentication Windows authentication



Do not forget to check the following features in **Add roles and features**:

.Net Framework 4.8 Features	.NET Framework 4.8 ASP .NET 4.8
WCF Services	HTTP Activation TCP Port Sharing

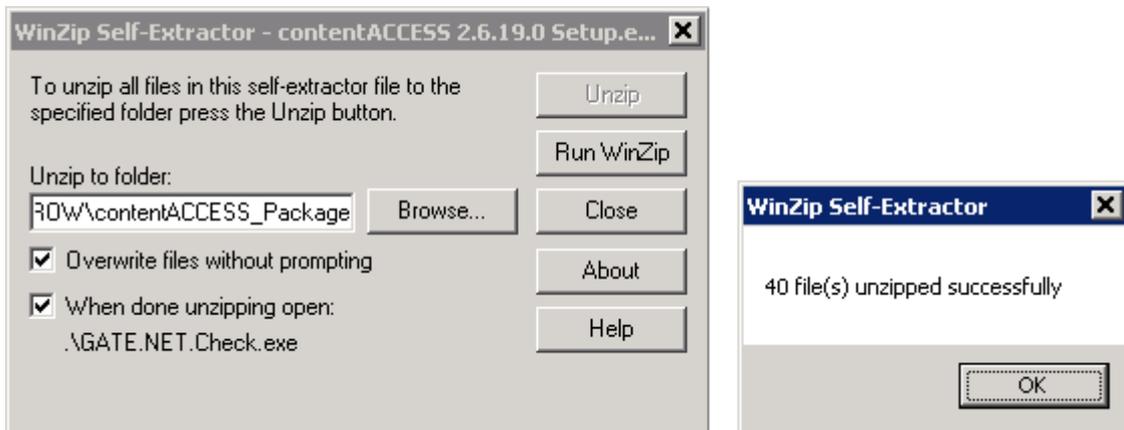
The contentACCESS components can be installed

- on one single machine,
- in a cluster system – when more servers are installed on different machines, and they are all joined with one configuration database
- in a distributed environment – when there is one contentACCESS server installed on one machine and the components are distributed (installed) on different machines

These components are described further in chapter [contentACCESS components](#). contentACCESS installation will be described first.

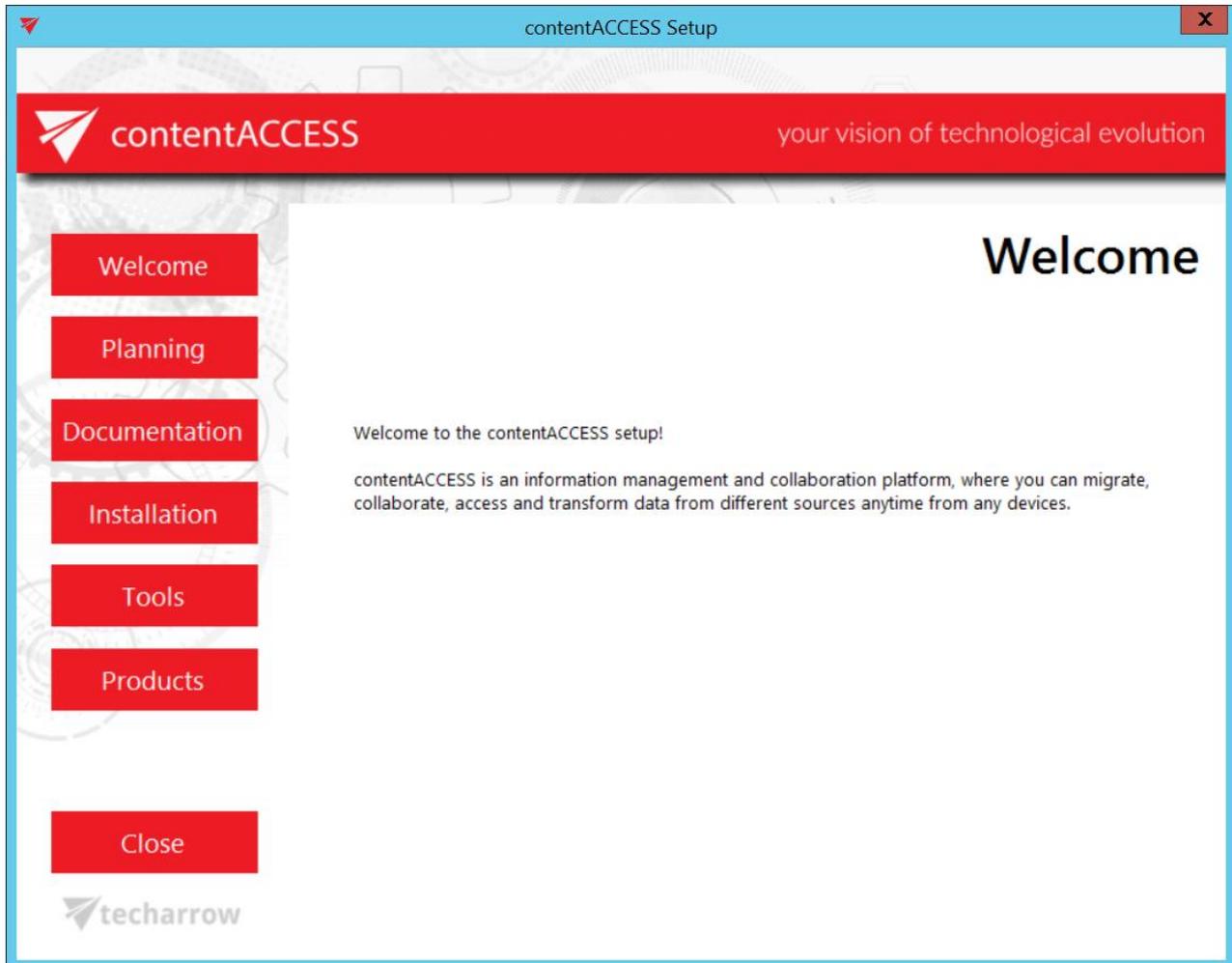
Installation of contentACCESS

To install contentACCESS, first download and run the setup package (contentACCESS X.X Setup.exe). As default it unzips to **C:\TECH-ARROW\contentACCESS_Package** folder, but you can use the **Browse** button if you want to change the directory. Click **Unzip**. After the files have been successfully unzipped, click **OK**.





Welcome! Now the contentACCESS installation wizard will open and it will lead you through all the steps of the deployment process. All components of contentACCESS can be deployed during this deploying process. Click **Installation** on the Welcome page.



Important: Update is supported from contentACCESS version 3.1 and later. Older versions must be updated to contentACCESS 3.1 and then from version 3.1 to the latest version.

If the update is done from an earlier version than 3.3, then some new features must be configured manually after the update.

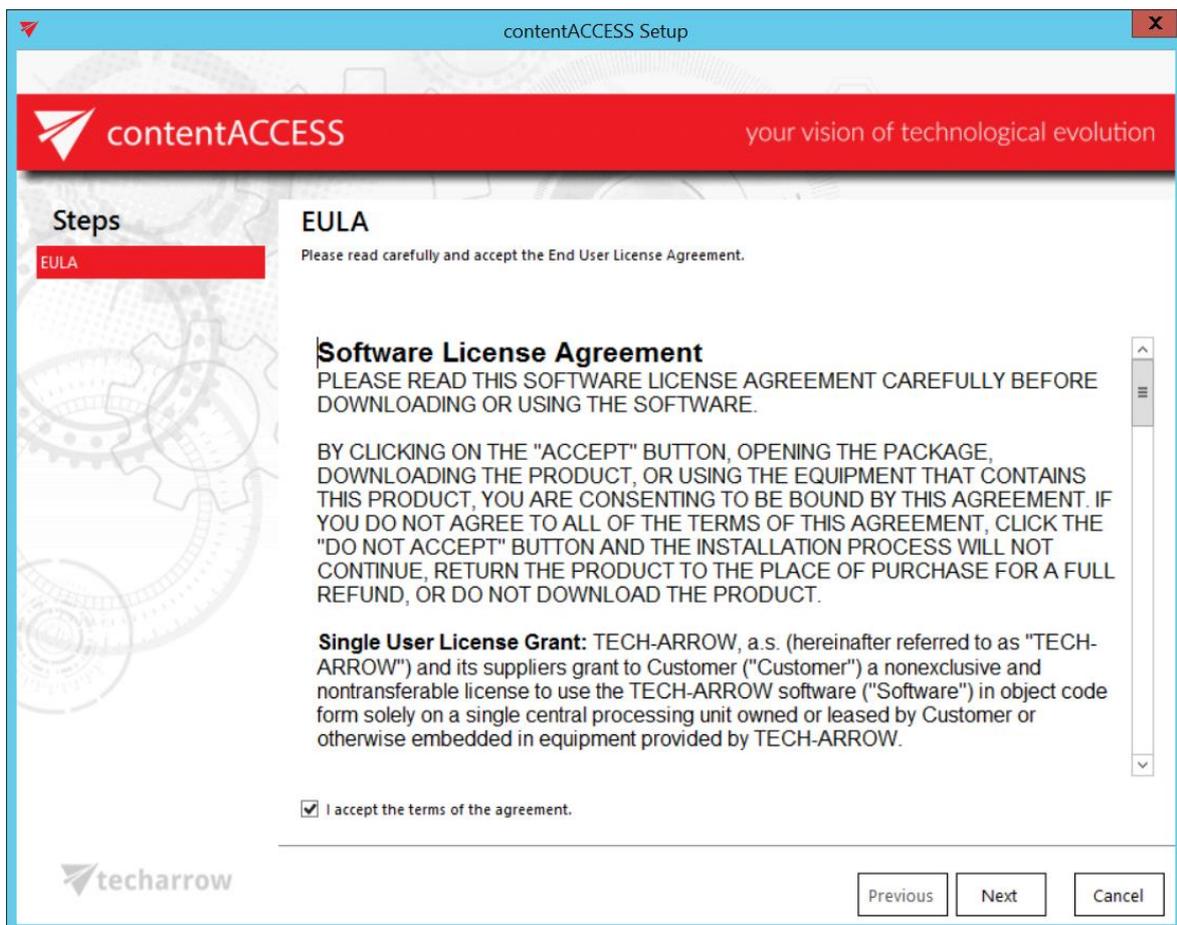
One of these features is the [Task runner](#), which requires a resource storage, where the export files will be stored. This storage must be configured in System -> System -> Resource storage settings. This store must be accessible by all contentACCESS nodes inside a cluster, so it is highly recommended to use a network share.



If the update is done from an earlier version than 3.4, then as a result of some internal changes in the email archive shortcut format, the [Outlook forms](#) must be updated to the latest version to maintain the correct functionality.

EULA

After you have carefully read the End User License Agreement, check checkbox **I accept the term of the agreement** and click **NEXT**.



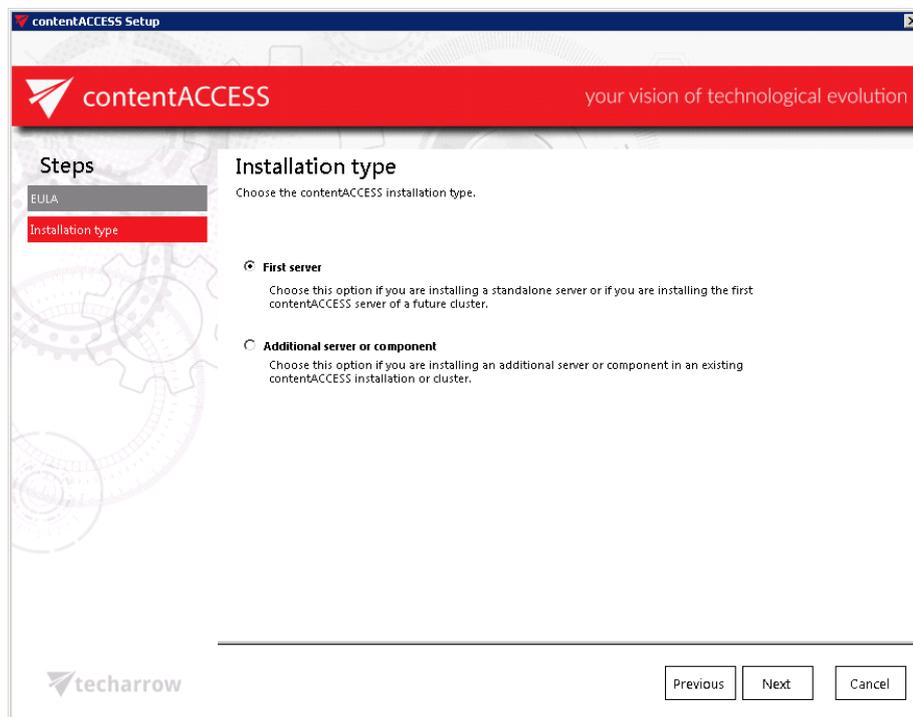
Installation type

This installation step is available at the very first install only. When updating the product, this step is no more available. In this step the user is asked to select between 2 types of installations:

- **First server** – choose this option if a) you are installing a standalone server (so everything will be installed on the same machine as in this use case), or b) you are installing the first contentACCESS server of a future cluster;

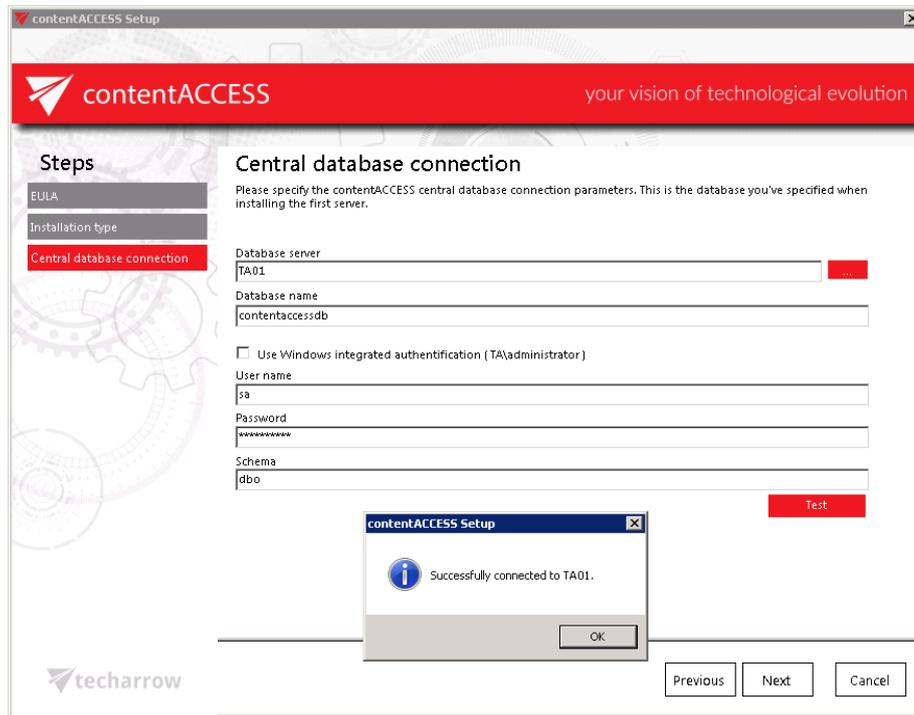


- **Additional server or component** – choose this option if you are installing an additional server or component (Virtual Drive, Central Administration, contentWEB etc.) in an existing contentACCESS environment or in a cluster.



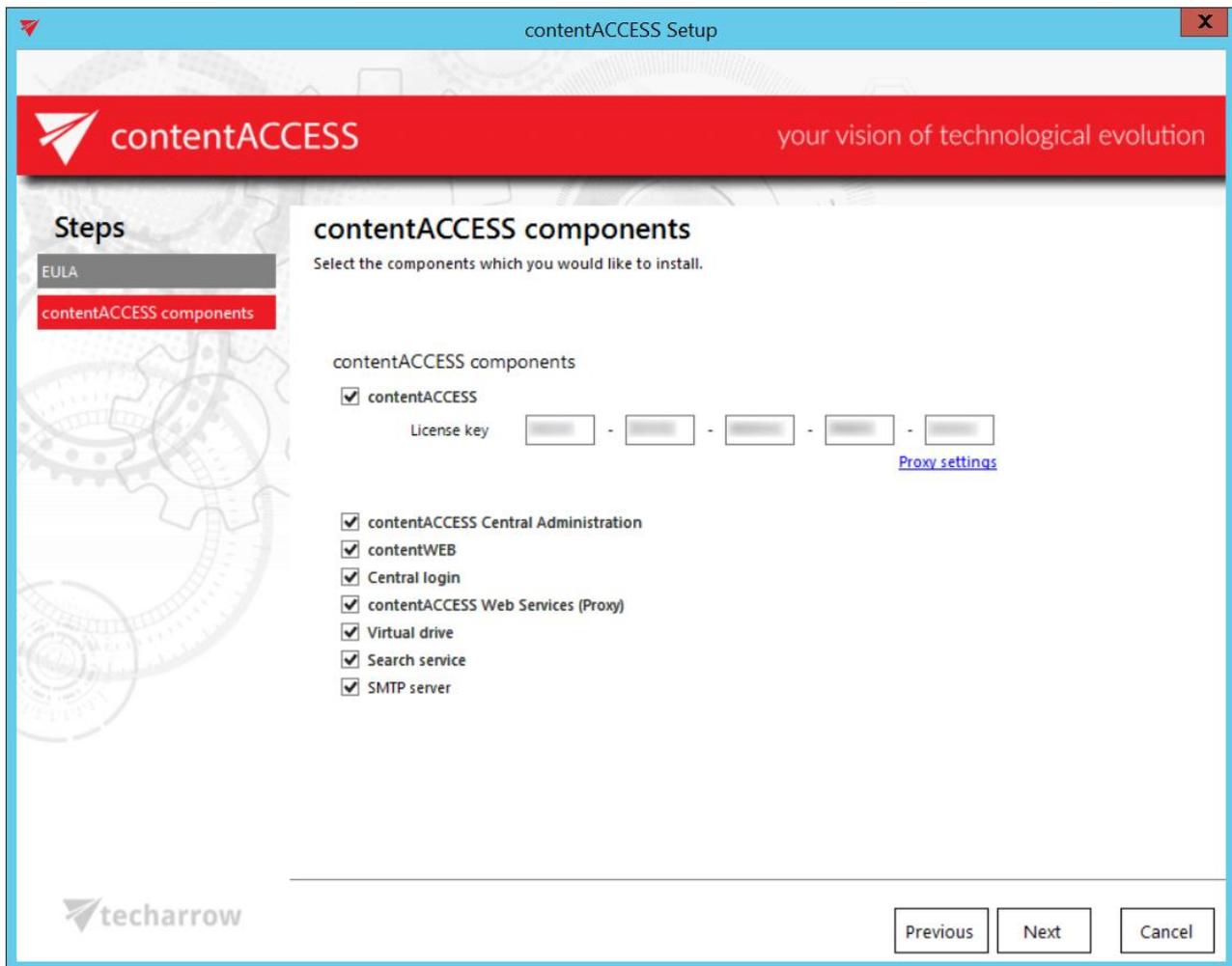
Note: Cluster is a system consisting of multiple servers (nodes) tied to the same configuration database.

In case that you are installing an additional server in a cluster, or a component in an existing contentACCESS environment (i.e. you marked the 2nd radio button), you will be required to set the connection with the already existing central database that you have specified at installing the first contentACCESS server. Test the connection and click **Next**.



Components

In this step you have to choose which contentACCESS components you want to install on a server. The components are fully described in chapter [contentACCESS components](#). It is recommended to read this section before you select the respective components to be installed. Check all the checkboxes in this step if you want to have all components on a single server.



If you have selected the contentACCESS server component, you need to apply the license before proceeding the installation. License activation can be done either **a) online** or **b) offline**.

a) If the machine where the setup is running **has internet connection**, you can activate the license **ONLINE**.

Follow the next steps:

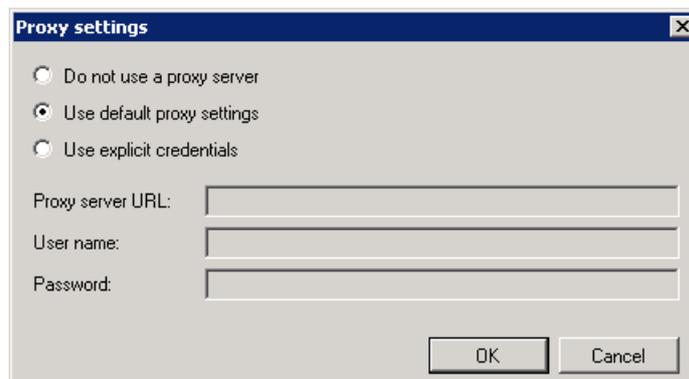
- Choose **Online activation** in the wizard.
- Enter your license key and click **Next**.
- License will be validated and you can continue the installation.

b) If the machine where the setup is running **has NO internet connection**, you can either **1) use the Web Proxy's credentials to activate the license through the configured proxy server** or **2) activate the license offline**.



1st option: Configure the proxy URL and applicable credentials to the proxy. The proxy that you configure here is used by the licensing component to reach the licensing server for the activation. By default the proxy server is disabled. To enable it, open the **Proxy settings** dialog (option **Proxy settings** in the wizard). You can either

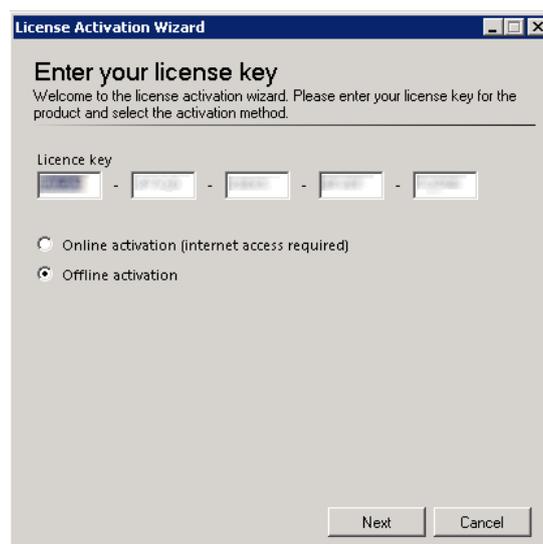
- **Use default proxy settings** that is configured on the contentACCESS server in **Control Panel** → **Internet options** → **Connections tab** → **LAN settings** → **Proxy server**
or you can
- **Use explicit credentials** (explicit proxy server URL and user)



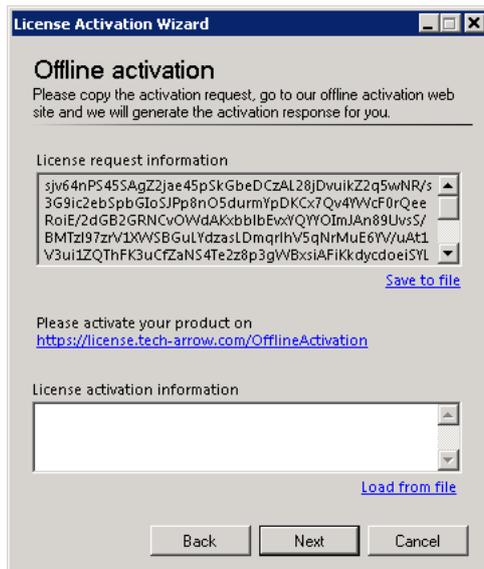
If the proxy is configured, you can continue with online license activation based on point a) above.

2nd option: Activate the license OFFLINE by following the steps below

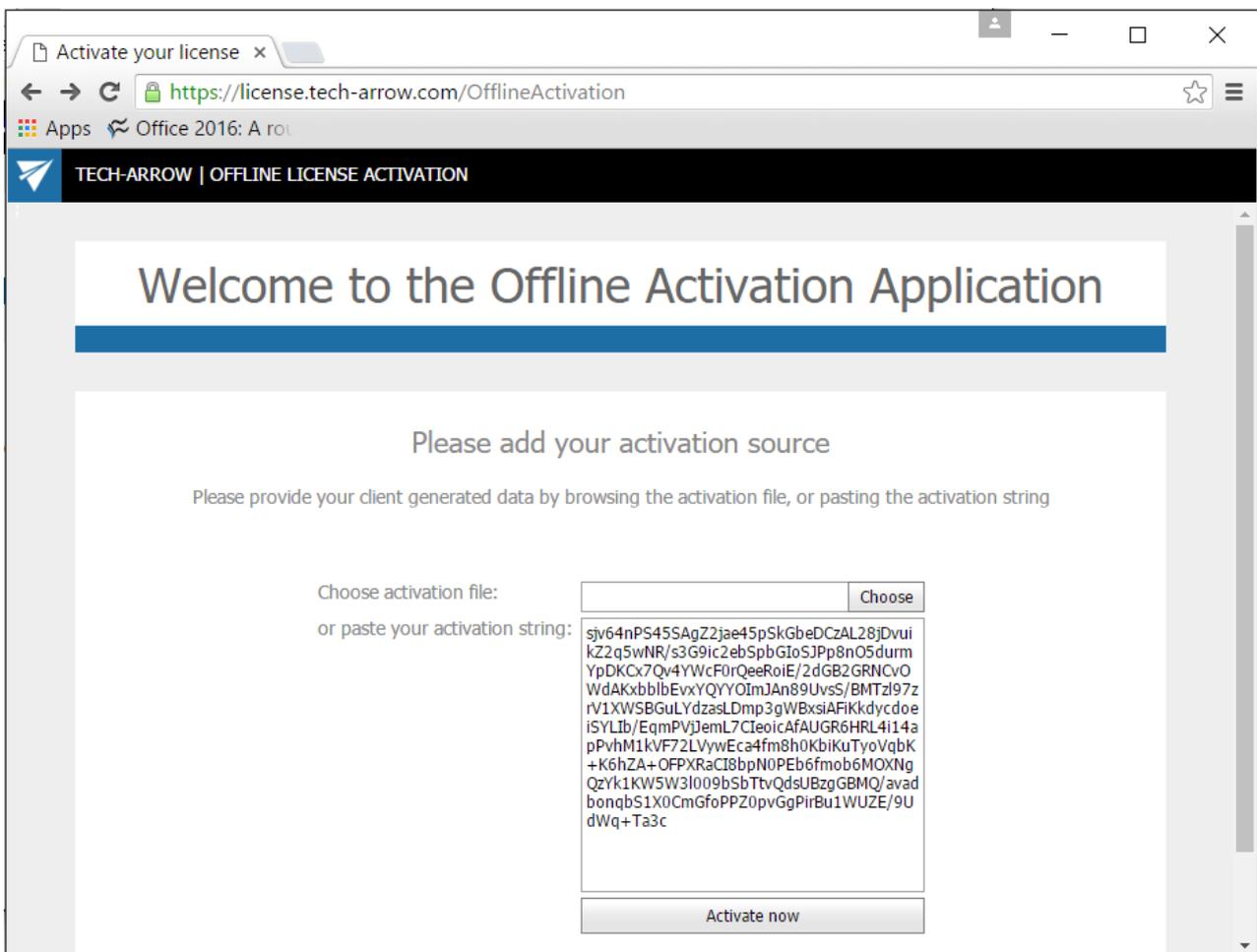
- Insert your license key.
- Select the **Offline activation** button and click **Next**.



- Activate your product on the offline license activation page of TECH-ARROW. The page can be accessed using the link in the activation dialog:

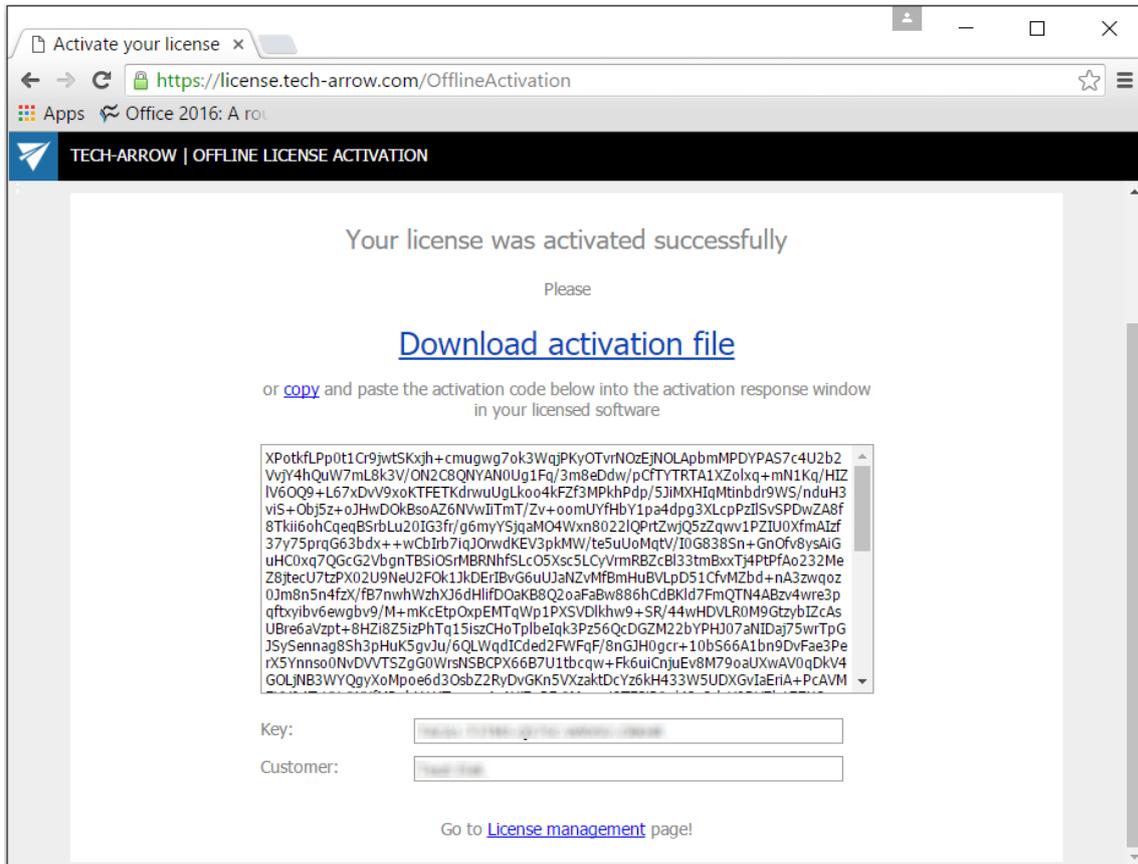


- Copy/paste (or download/upload) the **License request information** from the above wizard and activate it on the offline license activation page. Use the “**Choose**” option to upload the .dat file if you have saved it, or copy the activation string into the text box and click “**Activate now**”.

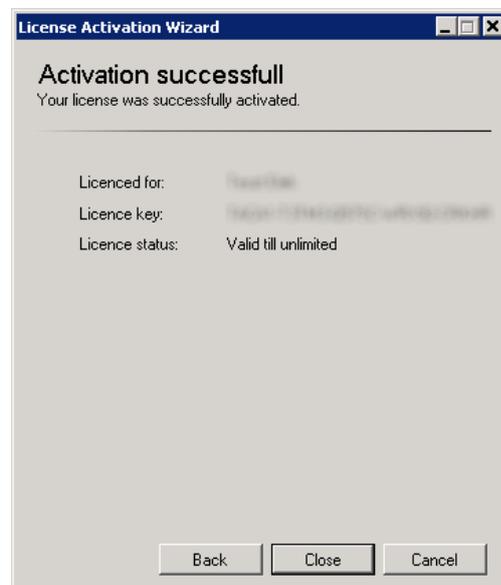
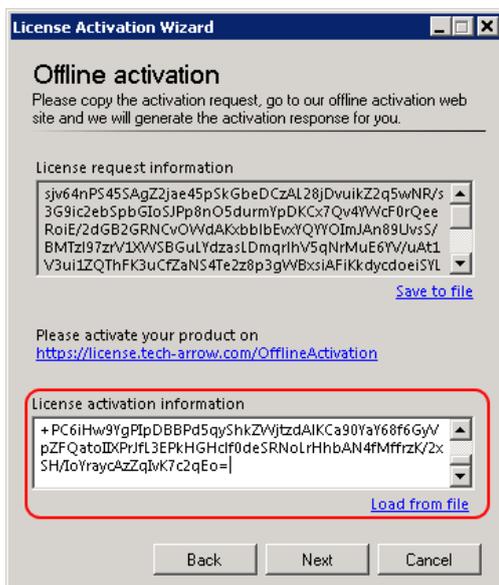




- Copy/paste (or download/upload) the activation code (1st screenshot below) from the web page to the License activation wizard (2nd screenshot below):



- When you have successfully applied the license, click “Next” in the wizard to continue the installation. In the last window click “Close” to complete the activation process.





➤ **Note:** After the expiration date it will be needed to activate the license again. The user can do it in the central administration interface of contentACCESS. For further information refer to section [How to activate your license key](#).

Prerequisites

During this step the wizard will check if your system fulfills the software requirements. Some of the missing prerequisites will be installed directly from the wizard during the installation.

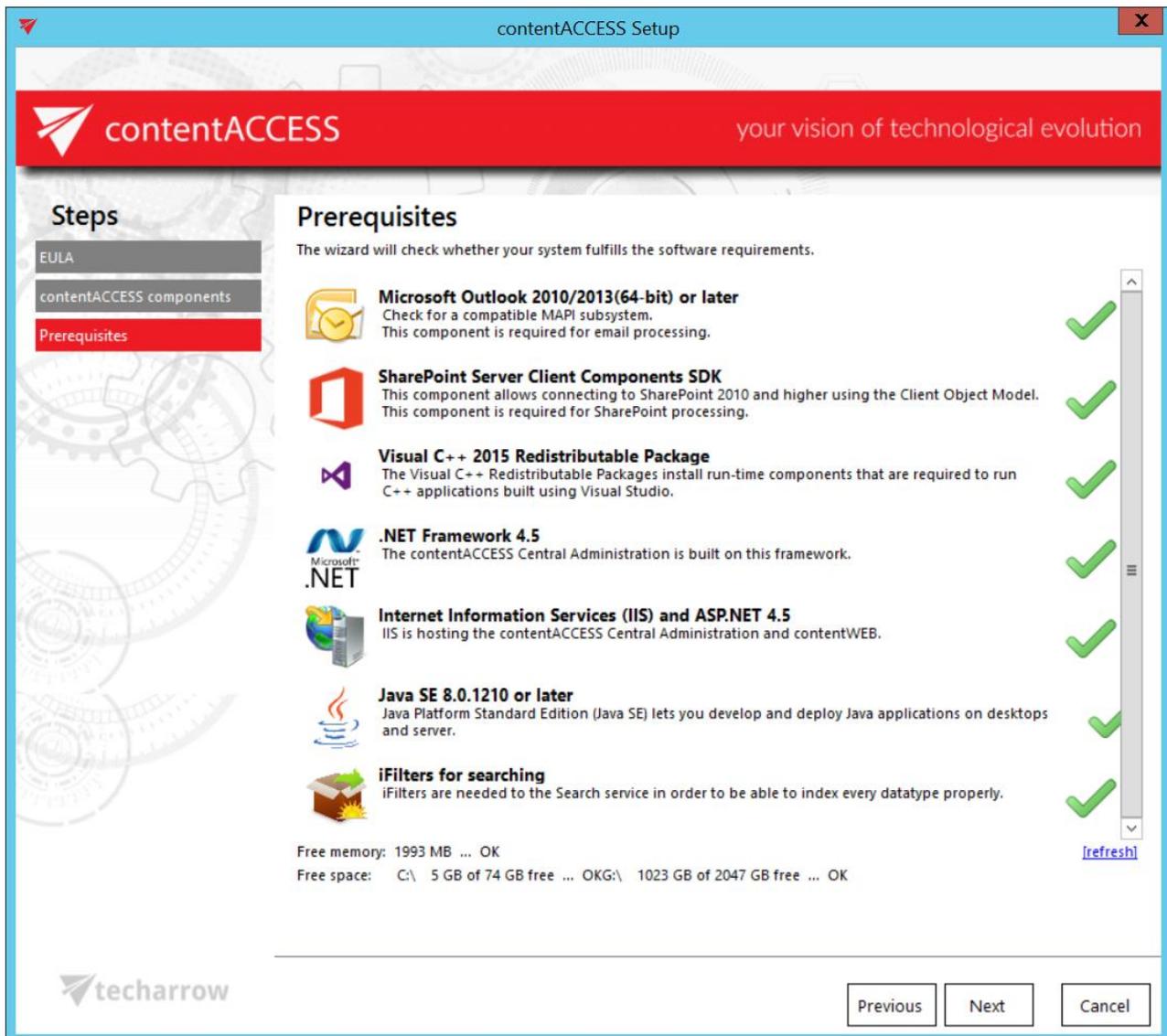
To use [Search service](#), the Java component has to be present on the computer. You don't have to download and install it separately, it will be installed directly from the setup.

Important: The setup will change the value of the **JAVA_HOME** variable to point to the version installed by setup. This may cause other already installed applications (using the older JAVA) to fail, so please check their functionality after the setup is completed. If the computer/server is already running a newer version than the one included in setup, **it will not be touched/downgraded**.

Note: For the [Indexing](#) job to work also for PDF files using the Adobe PDF iFilter, the **Path** environment variable for the PDF iFilter must be set manually. For more details, please see [this](#) FAQ section.

Use the [\[refresh\]](#) button to actualize the prerequisite information after the missing software is installed. If it still doesn't recognize some, restart the PC and start the contentACCESS installation again. Once it is ready, the user can continue with the installation process. After the wizard has run the system requirements check, click **NEXT**.

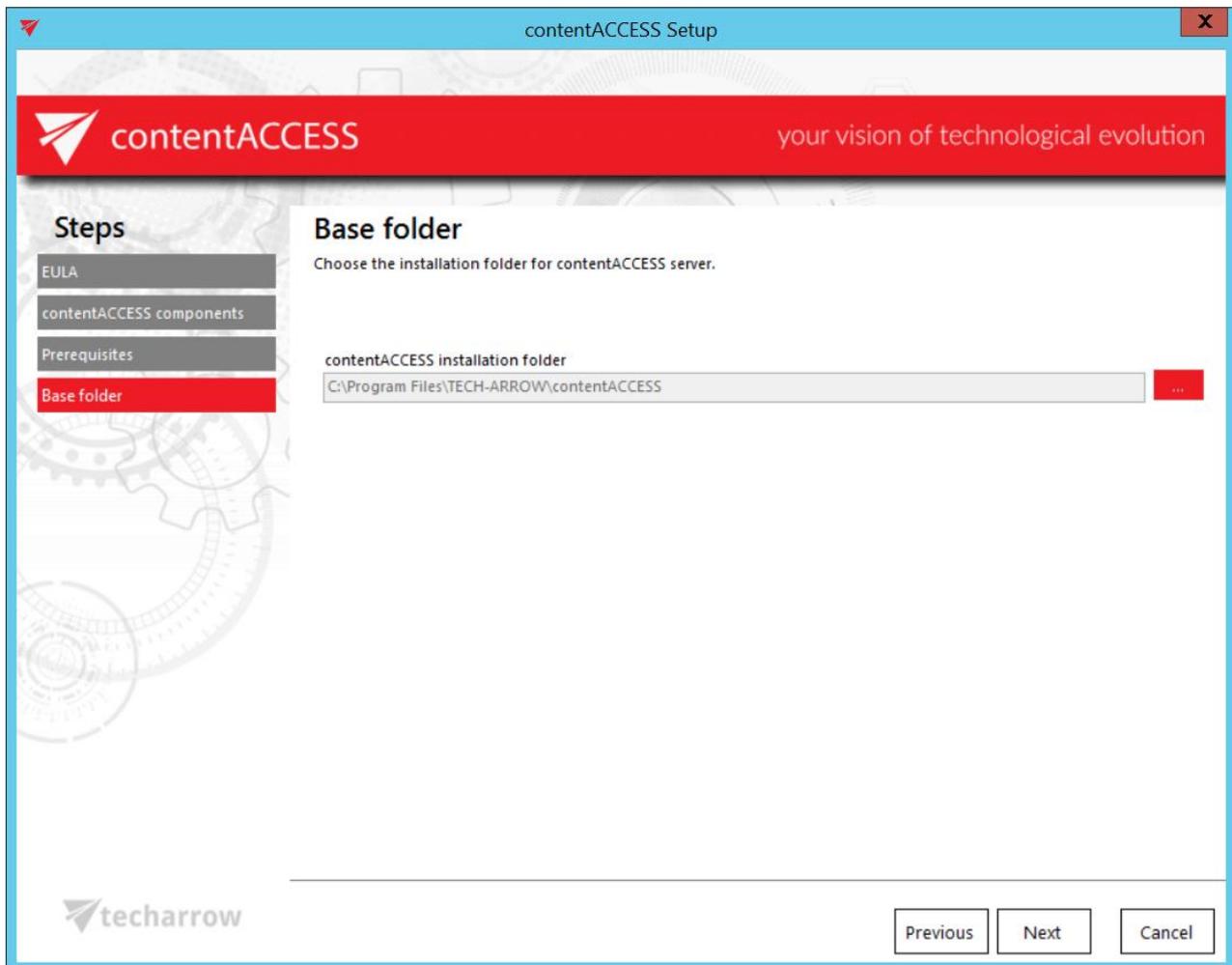
For more information about these requirements, check the section above: [Software requirements](#).



Note: MS Outlook prerequisite will be checked only in case that the license supports email based plugins.

Base folder

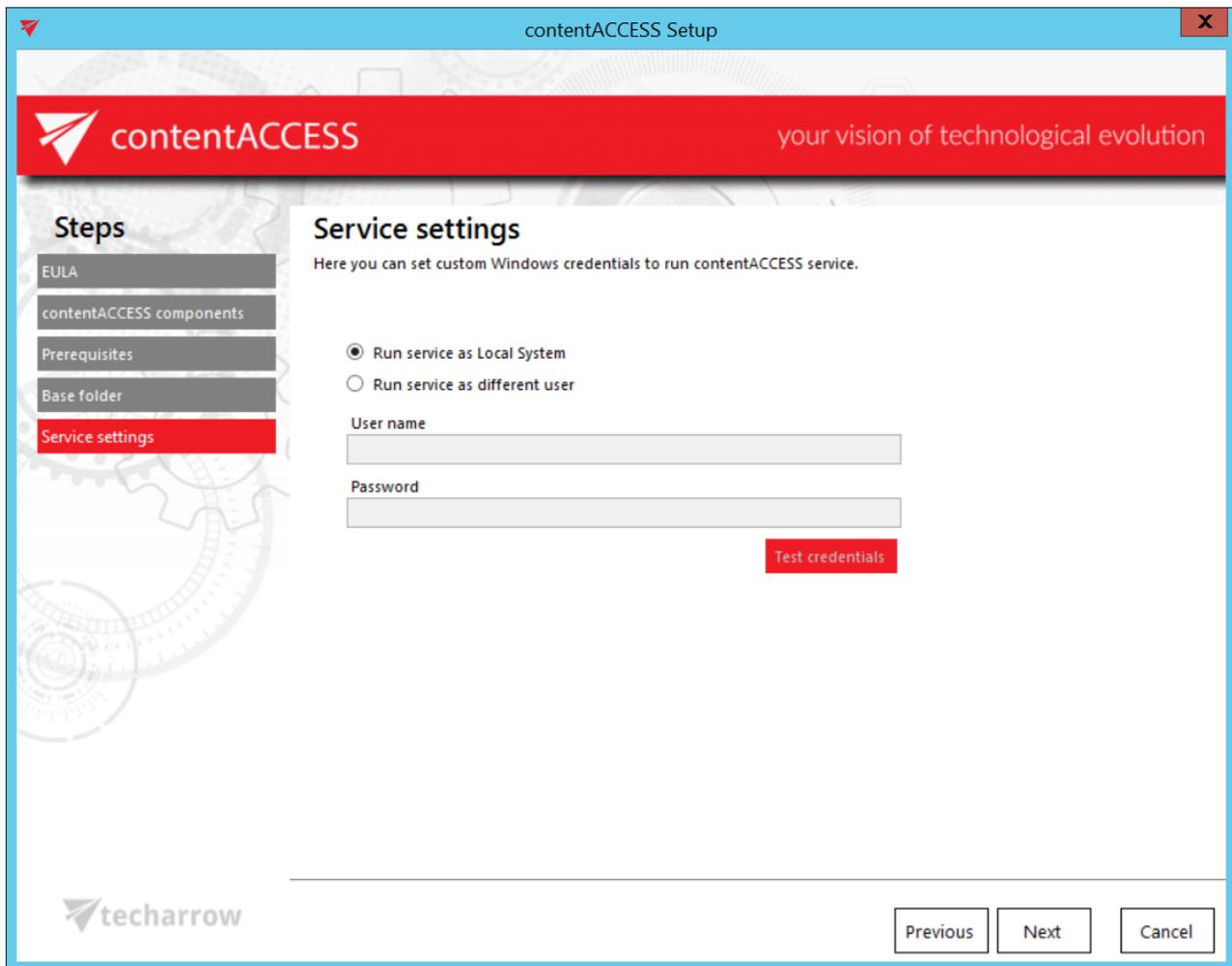
The next step is to select the installation base folder. By default the contentACCESS server, contentWEB and the Central Administration installs in C:\Program Files\TECH-ARROW folder. Other components are automatically installed one level deeper, in the base folder\contentACCESS folder. So if the default base folder is set, then the further components are installed in C:\Program Files\TECH-ARROW\contentACCESS folder. The installation folder can be changed. Click on the  button and browse for the desired destination. Click **NEXT**.



Service settings

The administrator may set here, under which credentials the contentACCESS service should run. There are multiple choices:

- The service can be run as Local System; no credentials are needed;
- The service can be run under custom Windows credentials (local or domain user); the administrator may also run a test to verify if the Windows credentials are OK.



Database connection

The next step is to specify the system database server to be used by contentACCESS. contentACCESS is storing data in MS SQL server. To continue with the installation process, **you will first need to install MS SQL server** (2012 or newer version) or use an existing SQL server installation.

The **Connect to existing SQL server** radio button will be pre-selected. Enter the name of the database server into the **Database server** textbox, or use the  button to locate it. Type the **Database name** into the **Database name** textbox. A system database will be created with the name entered here. Type in a schema (with an optional name) to the **Schema** textbox.

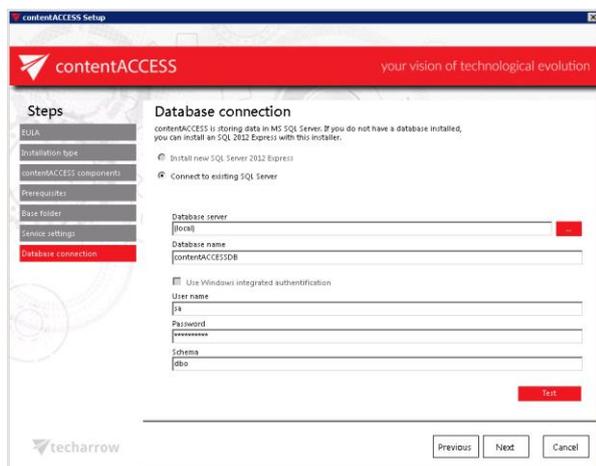
Note: If you are updating to a higher version, then all these above mentioned settings will be preselected and it will not be allowed to change them.



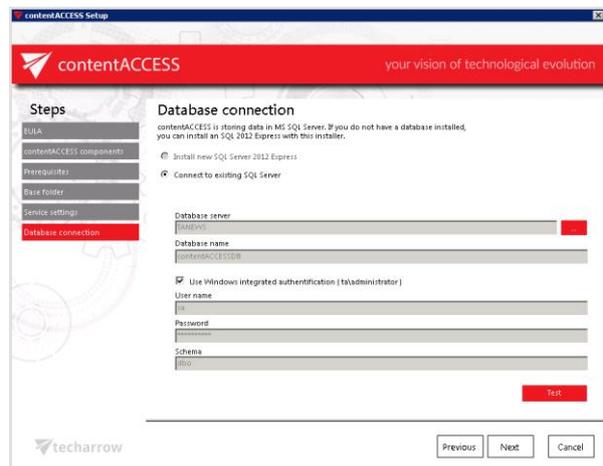
Continue with setting the user credentials to connect contentACCESS with SQL server. Enter the SQL user name and password into the textboxes. You have multiple options here: a) You can use either an SQL user, or b) you can use WIA (Integrated Windows Authentication) with checking the “Use Windows integrated authentication” checkbox. In this second case contentACCESS will connect to SQL with the service credentials specified in step 6 above, in the service settings.

Note: The setup verifies, if the specified database is already existing or not. If it’s not existing (as in this use case), you need to specify an SQL user with the right to create a new database. If the database already exists, then the user must have only access rights on the given database.

If you would like to make sure that all entered data are right run a test connection with a simple click on the **Test** button.

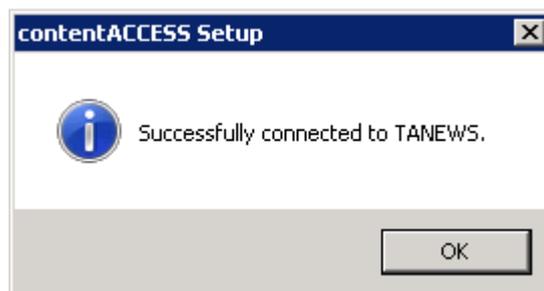


a) Using SQL user



b) Using WIA

If the connection was successfully established the following Setup window will confirm it:



Click **NEXT**.

In the next steps the contentACCESS components’ settings will be specified.



Important: To ensure a trouble free access, it is highly recommended to create an alias for each component, and to specify the connection URL to each of these components in an FQDN format.

contentACCESS Central Administration

On this page you can define the port number that this component will use:

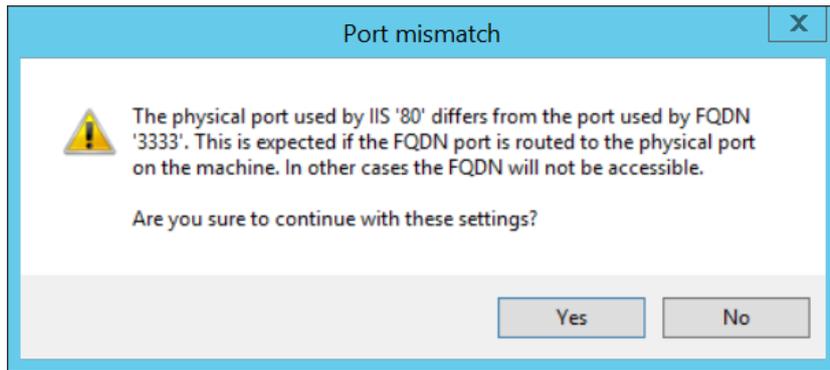
Port: This port is the physical port of Central Administration used by the Internet Information Services (IIS) on the current server.

The physical port cannot be changed later on, for example when updating the product. First the given component (in this case Central Administration) must be uninstalled, and then the port can be changed in the setup wizard. This rule refers to each contentACCESS component.

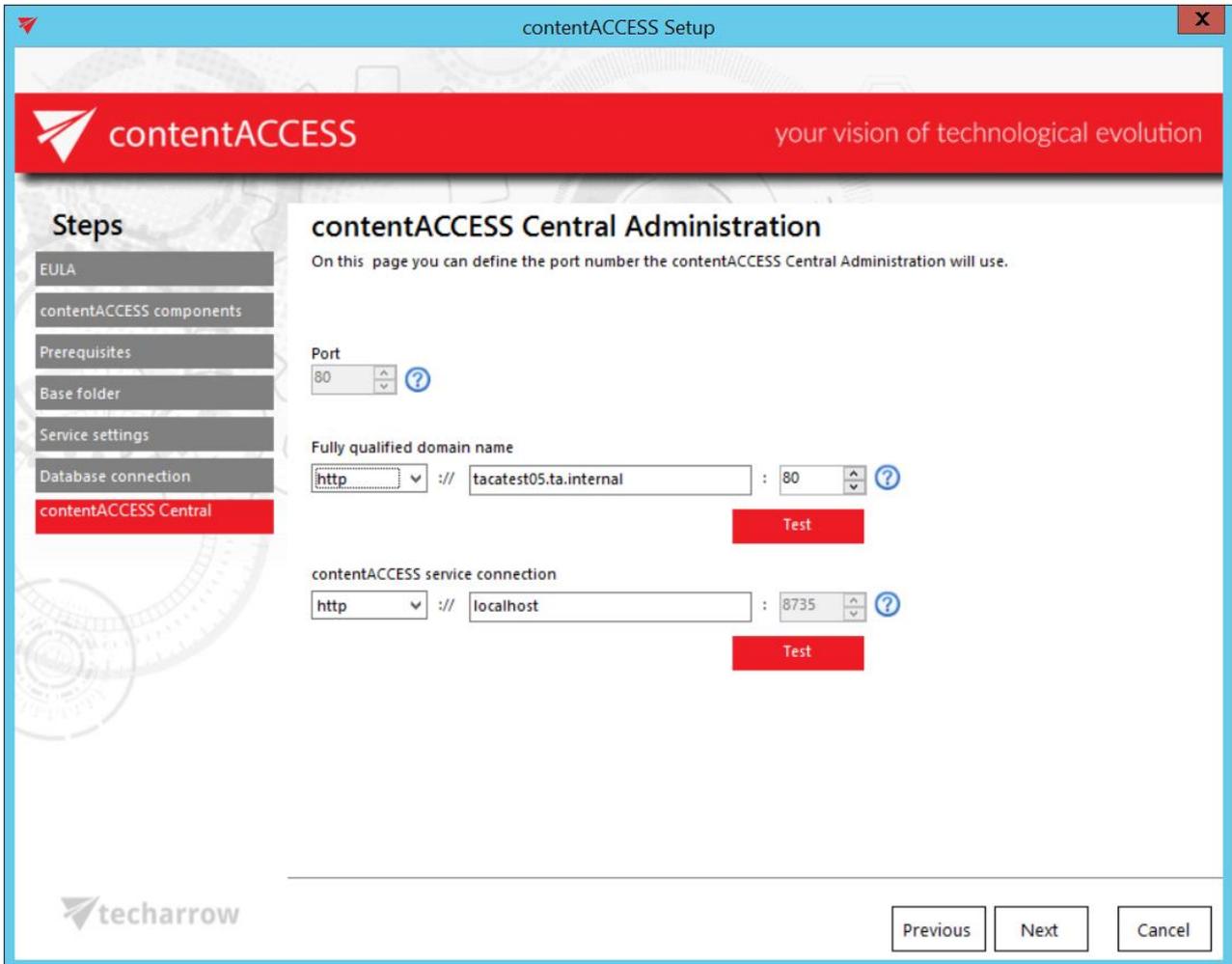
Fully qualified domain name: FQDN enables for the user to access the given component (in this case Central Administration) from everywhere (from home, from the office etc.). From this reason, this URL must be accessible from everywhere where the user is coming from. The FQDN that's defined here is written to the Application settings (**System** tab → Client applications group → **Application settings** page) in the Central Administration, and can be changed from there at any time. By the next update the setup will automatically read the value which is defined in the **Application settings**.

Hint: By double clicking the empty text field the wizard puts there the FQDN of that server. This functionality is the same by FQDN settings of further contentACCESS components, on the next installation pages as well.

Usually the physical port matches the port that FQDN used. However, in special cases, the FQDN port can differ from the physical port on the IIS. In such cases the following warning pops up for the user – this is expected if the FQDN port is routed to the physical port. In such cases the user can continue with these settings. The same rule applies for other contentACCESS components as well.



contentACCESS service connection: This URL is used by the Central Administration to communicate with the contentACCESS server. If contentACCESS server is installed on the same machine, you can use “localhost” as host name.





contentACCESS Web Services (Proxy)

On this page you can define the settings that contentACCESS Web Services (Proxy) will use. The same rule applies for these configurations as for the contentACCESS Central Administration settings above.

Proxy server is a must-have tool for customers who have contentACCESS Email Archive (or any email based plugins) and want to retrieve their archived emails from shortcuts, or they use contentACCESS Mobile.

Port: This port is the physical port of contentACCESS Web Services used by the Internet Information Services (IIS) on the current server.

Note: It is always a good thing to select 80 as port number because this port is enabled on Firewall in most of cases.

Fully qualified domain name: This URL must be accessible from everywhere where the user is coming from. If you want to enable a secure connection for the user, choose https. Keep in mind, that **https must be configured manually on the IIS** (more [here](#)). This value is used for Email archive shortcut retrieve as well. The FQDN that's defined here is written to the **System** settings (**System** tab → **Services** group → **System** page, section **External accessibility settings: Retrieve server FQDN**) in the Central Administration, and can be changed from there at any time. By the next update the setup will automatically read the value which is defined on the **System** page.

If Proxy uses https, the FQDN URLs of further contentACCESS components (contentWEB, Central login page) will be automatically prefilled by the package with https connection, too.

Note: If the user wants to use [MailApp](#), secure connection (https) must be selected here.

contentACCESS service connection: This URL is used by the contentACCESS Web services to communicate with the contentACCESS server. If contentACCESS server is installed on the same machine, you can use "localhost" as host name.

Hint: If the communication port with the contentACCESS server is changed, then the communication between the given component and the contentACCESS service is ensured by the contentACCESS Proxy. If the Proxy is not installed and the port is changed, then the service connection won't be established. The



same rule applies for the connection between the contentACCESS service and another contentACCESS components as well (in the Central administration and Central login page setup windows it is disabled to change the port number).

contentWEB

On this page you can define the settings that contentWEB (contentACCESS archive user interface) will use.

The same rules apply for contentWEB as for the contentACCESS Central Administration settings above with one exception. contentWEB connection with the contentACCESS server supports net.pipe connection as well.

Port: This port is the physical port of contentWEB used by the Internet Information Services (IIS) on the current server.



Fully qualified domain name: This URL must be accessible from everywhere where the user is coming from. By double clicking the empty text field the wizard puts there the FQDN of that server. If you want to enable a secure connection for the user, choose https.

The contentWEB FQDN that's defined here is written to the Application settings (**System** tab → Client applications group → **Application settings** page) in the Central Administration, and can be changed from there at any time. By the next update the setup will automatically read the value which is defined in the **Application settings**.

contentACCESS service connection: This URL is used by contentWEB to communicate with the contentACCESS server. If contentACCESS server is installed on the same machine, you can use "localhost" as host name. There are 3 communication types that can be used between contentWEB and the contentACCESS server:

- http – use this if you want to establish a direct connection with contentACCESS. If direct connection should be used, do not change the port number that's prefilled by the setup package (8736), otherwise contentACCESS proxy connection will be used automatically.
- https – use this to establish a secure connection through the contentACCESS Proxy server
- net.pipe – use this type if contentWEB and contentACCESS are installed on the same machine; this is the fastest and most recommended connection type.

contentACCESS Setup
✕


contentACCESS
your vision of technological evolution

Steps

- EULA
- contentACCESS components
- Prerequisites
- Base folder
- Service settings
- Database connection
- contentACCESS Central
- contentACCESS Web Services
- contentWEB

contentWEB

On this page you can define the settings the contentWEB will use.

Port

Fully qualified domain name

http

://

tacatest05.ta.internal

:

80

?

contentACCESS service connection

net.pipe

://

localhost

:

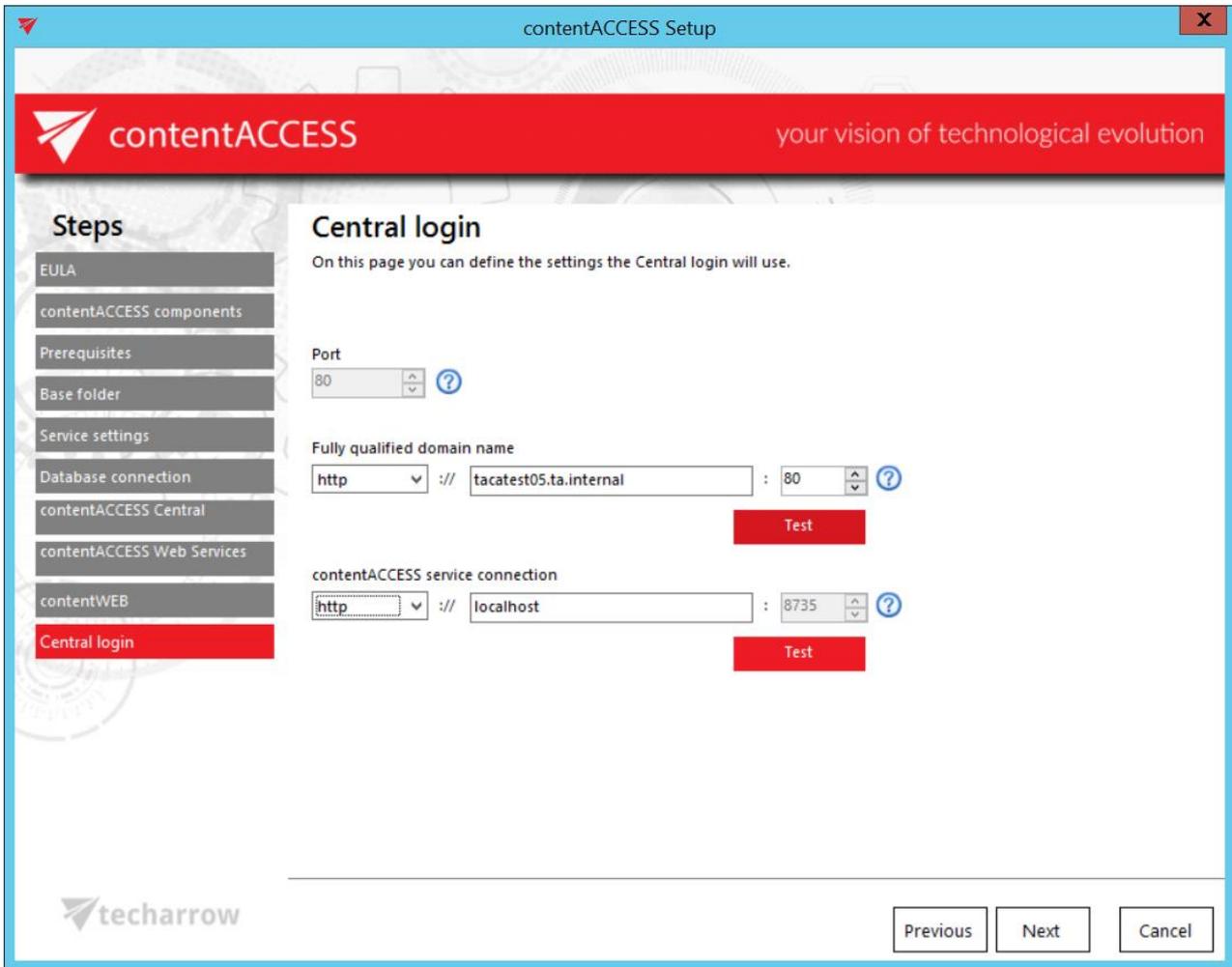
-1

?



Central login

On this page you can specify the settings that the Central login page will use. Same rules apply as for the connection settings of components from above. The FQDN that's first configured is written by the setup to the System settings of the Central Administration (**System** tab → **Services** group → **System** page, section **External accessibility settings: Central login**). It can be changed on the respective page of the Central Administration at any time, and the new configuration will be then read and prefilled by the setup when updating the product.



The screenshot shows the 'contentACCESS Setup' window. The title bar reads 'contentACCESS Setup'. The main header is red with the 'contentACCESS' logo and the tagline 'your vision of technological evolution'. On the left, a 'Steps' sidebar lists various setup stages, with 'Central login' highlighted in red. The main area is titled 'Central login' and contains the following fields and controls:

- Port:** A numeric input field set to '80' with a help icon.
- Fully qualified domain name:** A dropdown menu set to 'http', followed by a text field containing 'tacatest05.ta.internal', a port dropdown set to '80', and a help icon. A red 'Test' button is positioned below this field.
- contentACCESS service connection:** A dropdown menu set to 'http', followed by a text field containing 'localhost', a port dropdown set to '8735', and a help icon. A red 'Test' button is positioned below this field.

At the bottom of the window, there are three buttons: 'Previous', 'Next', and 'Cancel'. The 'techarrow' logo is visible in the bottom left corner.

Virtual drive

Here you define the settings that Virtual drive will use:

Virtual drive fully qualified server name: this value is used to retrieve archived files from shortcuts

Virtual drive letter: drive for publishing the virtual drive content (the archive files)

Cache folder location: When users are editing files through Virtual Drive or file shortcuts, all changes are stored in the folder set here until they are committed to the archive. This folder must have plenty of free space. It is recommended not to set the Temp folder here, as the data may get deleted by the system.

contentACCESS service connection: URL used for the communication with the contentACCESS server. There are 3 communication types that can be used:

- http – use this if you want to establish a direct connection with contentACCESS. If direct connection should be used, do not change the port number that's prefilled by the setup package (8736), otherwise contentACCESS proxy connection will be used automatically.
- https – use this to establish a secure connection through the contentACCESS Proxy server



- net.pipe – use this type if Virtual drive and contentACCESS are installed on the same machine; this is the fastest and most recommended connection type.

The installation package writes/reads these parameters into/from the **Virtual drive configurations** page of Central Administration (**System** tab → **Client applications** group → **Virtual drive configurations** page) during each install/product update.

Further specify the user credentials used to run the Virtual drive service. This can be either Local system user, or an explicit user.

Search service

To use Search service, Java must be installed on the computer where the user is installing the search components (read more in section [Prerequisites](#) above).

Here you define the settings that search service will use:



Search service URL

URL used for the communication with the contentACCESS server. There are 3 communication types that can be used:

- **http** – use this if you want to establish a direct connection with contentACCESS. If direct connection should be used, do not change the port number that's prefilled by the setup package (8736), otherwise contentACCESS Proxy connection will be used automatically.
- **https** – use this to establish a secure connection through the contentACCESS Proxy server
- **net.tcp** – use this type if Virtual drive and contentACCESS are installed on the same machine; this is the fastest and most recommended connection type.

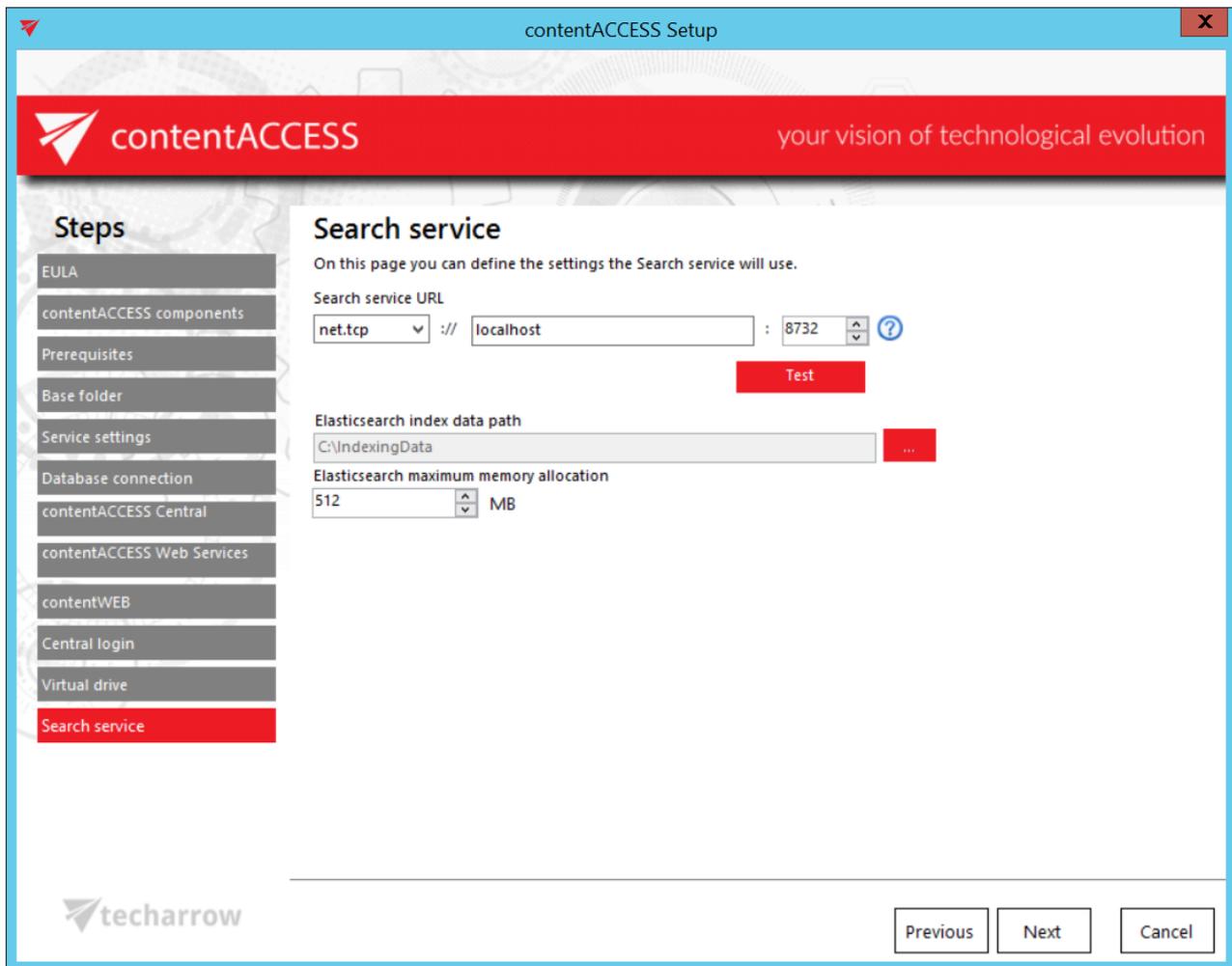
The installation package writes/reads these parameters into/from the Search service settings section of Central Administration (**System** -> **Services** group -> **System** page) during each install/product update.

Elasticsearch index data path

The path where the indexes will be saved. This path must be filled unless you can't continue the installation process.

Elasticsearch maximum memory allocation

The maximum amount of memory in megabytes which can be used by the Elasticsearch service.



SMTP server

The following options can be set on the SMTP server configuration page:

Server name: the name of the server that SMTP server will be listening on

Port: the port the SMTP server will be listening on for incoming emails

Enable encryption on incoming connections (TLS): this option enables the secure connection between the sender and the recipient servers

Certificate: the .pfx certificate file has to be selected here if the user checked the **Enable encryption on incoming connections (TLS)** checkbox

Certificate password: the password for the .pfx certificate. With the Test password button the user can check whether the password he entered for the given .pfx certificate file is correct or not.



Service parameters: The credentials for the service user, under which the SMTP server will run, can be set here

SMTP data path: the location, where the system files regarding SMTP server will be stored

Fully qualified domain name (FQDN): a domain name that can be later used to create new SMTP mappings. This domain will be usable as the domain for an incoming SMTP listener address and goes to the **SMTP domains** list in Central Administration, where it is also possible to add more domains later. The **FQDN** can be the same as the **Server name**.

Database server: SQL database can be configured for SMTP server. SMTP will store its data here.

Note: It is mandatory to set a SQL connection for the SMTP server, otherwise you won't be able to continue the setup process.

- Enter the name of the database server into the **Database server** text box, or use the  button to locate it.
- Type the **Database name** into the next textbox. An SMTP database will be created with the name entered here.
- Type in a schema (with an optional name).

Note: If the use SQL option has been set up properly before and you are updating to a higher version, then all these above mentioned settings will be preselected and you will not be allowed to change them. If the option wasn't set properly before, the fields will be enabled and you will need to fill them.

Continue with setting the user credentials to connect contentACCESS with SQL server. Enter the SQL user name and password into the textboxes. You have multiple options here: a) You can use either an SQL user, or b) you can use WIA (Integrated Windows Authentication) with checking the "Use Windows integrated authentication" checkbox. In this second case, contentACCESS will connect to SQL with the service credentials specified in step 6 above, in the service settings.

contentACCESS Setup
✕


your vision of technological evolution

Steps

- EULA
- contentACCESS components
- Prerequisites
- Base folder
- Service settings
- Database connection
- contentACCESS Central
- contentACCESS Web Services
- contentWEB
- Central login
- Virtual drive
- Search service
- SMTP server

SMTP server

On this page you can define the settings the SMTP server will use.

Server name: Port:

Enable encryption on incoming connections (TLS)

Certificate: No certificate selected... Browse

Certificate password: Test password

Run service as Local System
 Run service as different user

User name:

Password: Test credentials

SMTP data path: Browse

Specify FQDN you want to use as a listener address in the SMTP server.

Fully qualified domain name:

Database server: ...

Database name:

Use Windows integrated authentication

User name:

Password:

Schema: Test



Previous
Next
Cancel

After the installation, the SMTP server is automatically registered into contentACCESS and can be used immediately after setting up some [mappings](#). In case of updating the SMTP server from version 3.3, the server is automatically registered into contentACCESS as soon as the service starts up. The previously specified mappings are injected into contentACCESS and the **Available domains** are filled in based on the domains from the already existing domain mappings. The only case when the registration is not done



automatically and requires some manual settings is when the 3.4 version is installed from the .exe file (C:\TECH-ARROW\contentACCESS_Package\Setups\contentACCESS.SMTPServer_x64.exe).

After the SMTP server has been successfully installed, the user will be able to use the **SMTP server configuration tool** (the default location is C:\Program Files\TECH-ARROW\contentACCESS.SMTPServer\EmailServer.exe). The configuration can be changed **only when the service is stopped** (bottom right corner).

The options about the threads and the delete options are **read-only** and disabled in this tool - those can be set only in Central Administration, section [SMTP Servers](#). In case of manual configuration of the SMTP or a change in the target contentACCESS server's URL, the changes can be set under the **contentACCESS Configuration** section's **Settings** page:



URL: URL of the contentACCESS server

Username: username used to connect to contentACCESS

Password: password for the specified user to connect to contentACCESS

Authentication type: authentication type for the specified user

contentACCESS configuration

Url	<input type="text" value="http://localhost:8736"/>
Username	<input type="text" value="system"/>
Password	<input type="password" value="....."/>
Authentication type	<input type="button" value="Forms"/> <input type="button" value="Reload"/>

The **Send test email** button sends a test email to the first specified [SMTP mapping](#) that is set in Central Administration. Any change that was made in this tool can be saved with the **Save configuration** button.

With the **Statistics** button the user can see some statistics about the emails received and archived by the SMTP server.

Received	
Total emails received	0
Emails received in last 24 hours	0
Email receive failed	0

Archived	
Total emails archived	0
Emails archived in last 24 hours	0

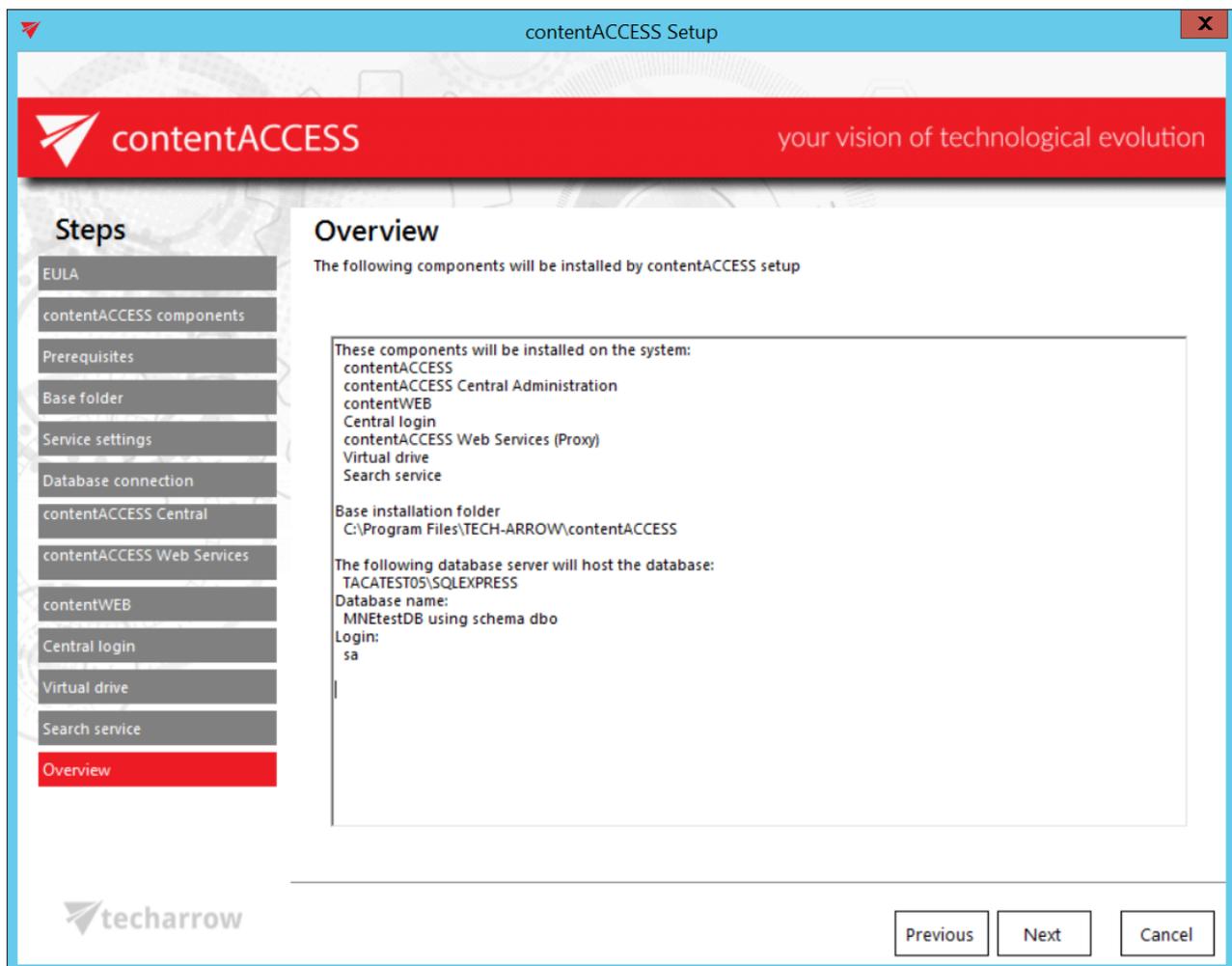
In Progress	
Items waiting for archiving	0



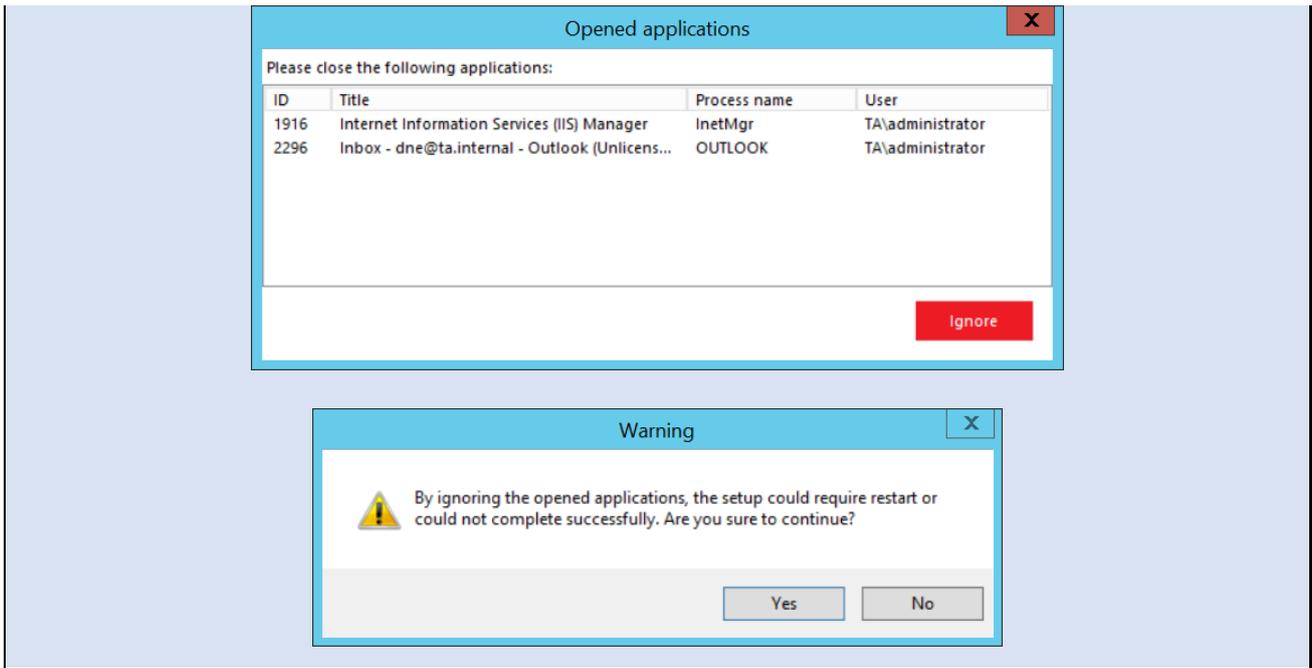
With the **Start** and **Stop** buttons, the underlying service, which is handling the incoming emails and archiving them into contentACCESS, can be started or stopped.

Overview

In this step the contentACCESS setup gives a general overview about the components that you have selected to install on server. Click **NEXT**.

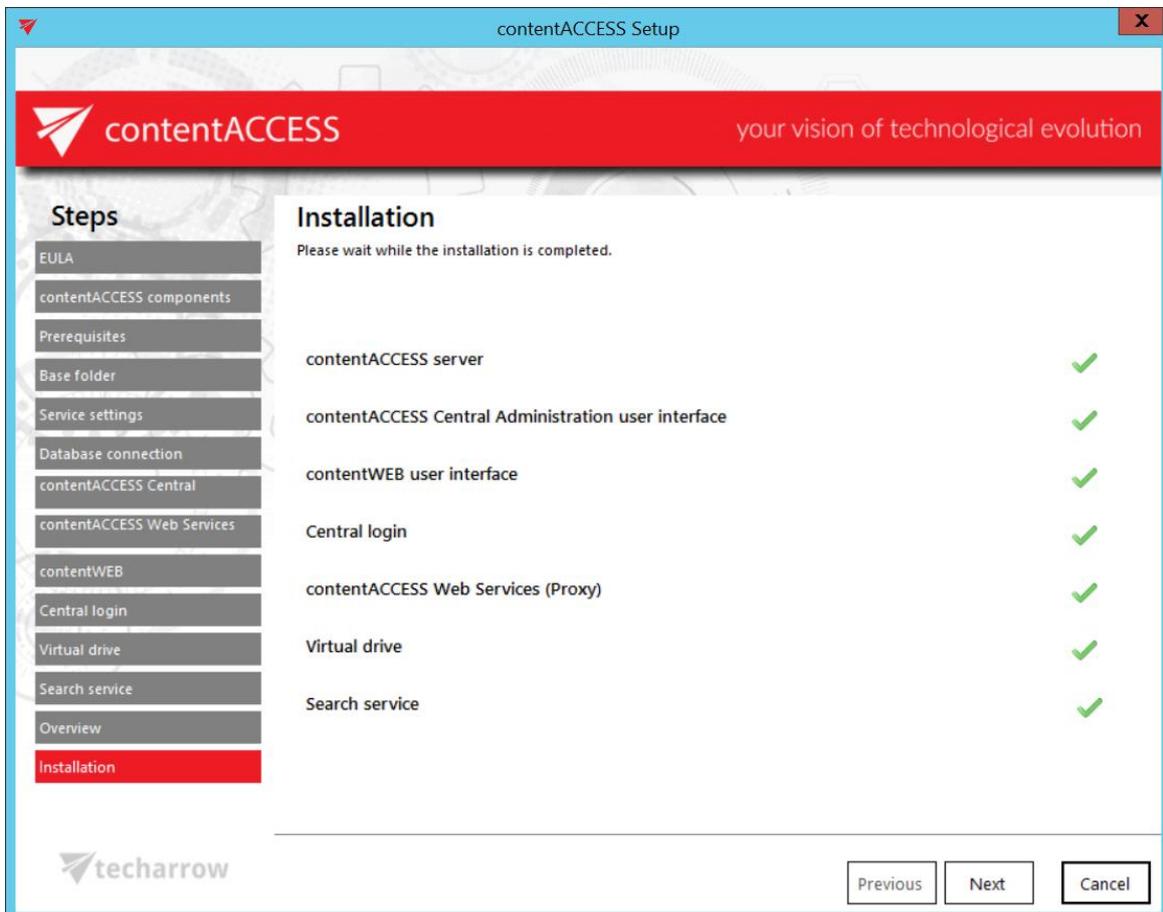


Note: In case that there are unwanted applications running in the background, the setup will warn the user about this. Unwanted applications are: MS Outlook, Services and Internet Information Services. It is possible (but not recommended!!) to kill these applications directly from this window by right clicking on the application in the list and selecting “Kill”. The best approach is to close the running applications manually. You can also skip closing the applications by clicking the “Ignore” button in the pop-up window.



Installation

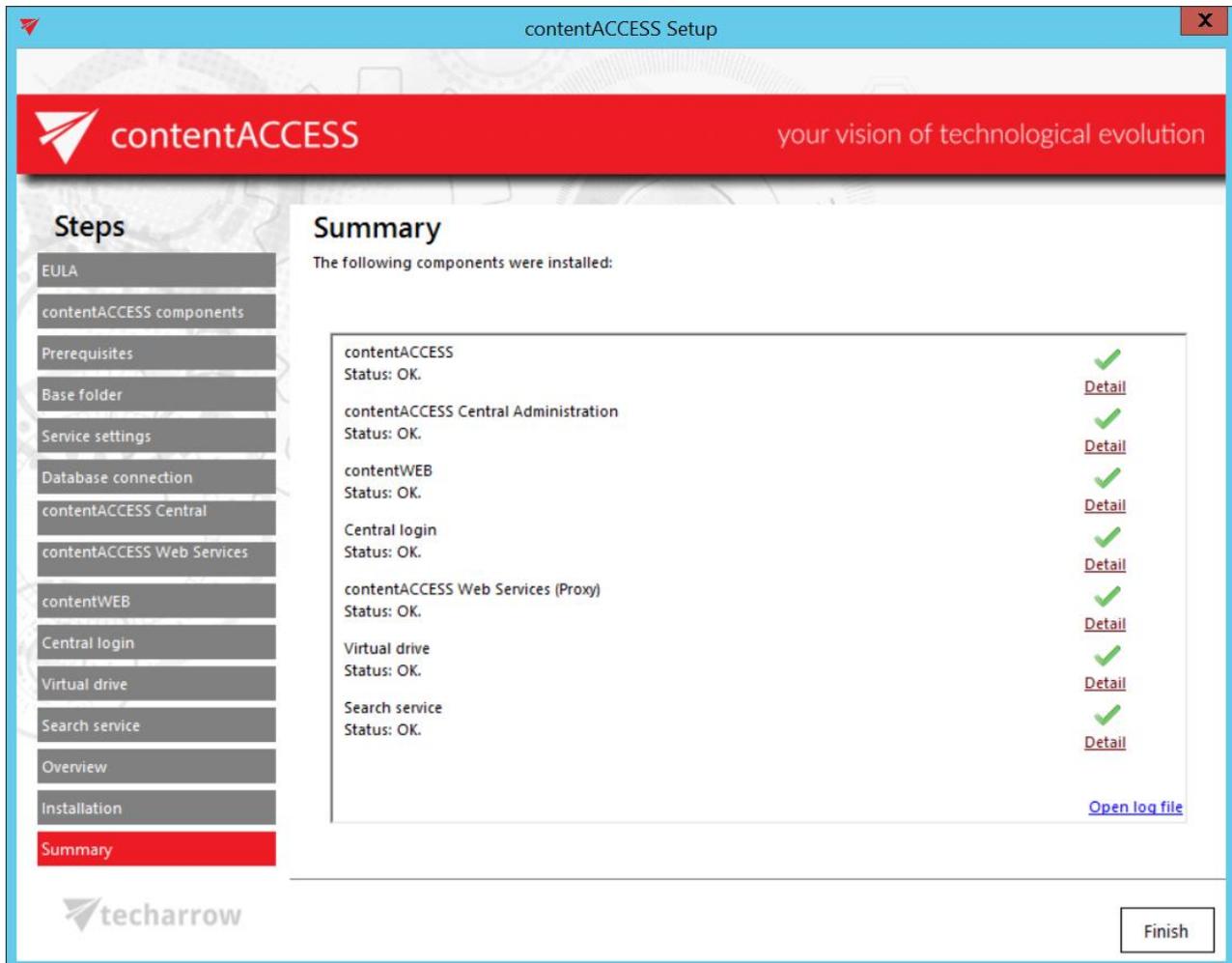
Click **Install** and wait until the installation process is completed. Then click on **NEXT**.





Summary

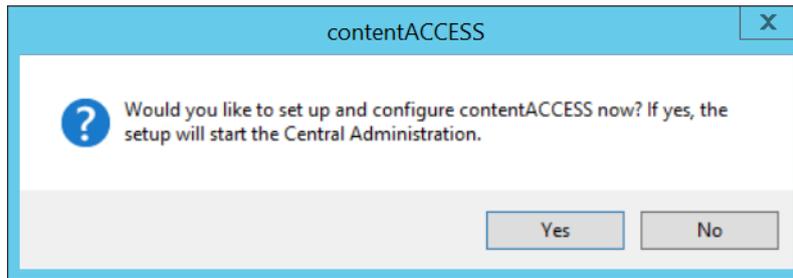
The window will give an overview for you about the already installed products:



Note: If any problem occurred during the installation process, click on [Open log file](#) option in the right down corner of the last setup window (check above). The reason of unsuccessful installation might be included in this log file

Click **Finish** to complete the whole installation process.

After installation is completed and you want to continue with further settings and configurations in the contentACCESS Central Administration, click on **Yes** in the following popup window. This dialog pops up if you have installed the component now or if you have already installed it on another server (distributed environment).





contentACCESS components

contentACCESS has the following components that can be installed by the contentACCESS setup package directly:

- the contentACCESS server
- [contentACCESS Central Administration](#) – the contentACCESS configuration interface available for system administrators and tenant administrators
- [contentWEB](#) – the archive user interface also for the end users
- Central login page – used to log in to the respective application with forms provider or third-part authentication providers
- [contentACCESS Web services \(Proxy\)](#) – to ensure secure connection for the end user and enable email shortcut retrieve
- [Virtual drive](#) – a drive that's used to display the contents of the File system archive; the drive is also mandatory to retrieve the archived files from shortcuts
- [Search service](#) – allows the user to search in selected entities/folders
- [SMTP server](#) – a server used to process emails

contentACCESS Central Administration

contentACCESS is a modular product, with built-in or custom plugins. The built-in plugins are available for on premise Exchange server, Office365, SharePoint and File servers. With these plugins contentACCESS can combine several systems into one archive storage in the cloud or on premise. There are many possibilities to visualize and work with the archived data: use officeGATE (Outlook add-in) to see the data directly in Outlook, use a web browser to see the data using contentWEB, use accessGATE Mobile application to see the data on your smartphones or use accessGATE to interconnect your data with SharePoint.

contentACCESS is software which supports multiple-tenancy. Multi-tenancy is an architecture in which a single instance of a software application serves multiple customers. Each customer is called a tenant. Every tenant of contentACCESS has its own data management processes. This means that every tenant uses its own plugin instances (jobs) and also has its own databases and storages. All these data can be isolated from the data of other tenants. Even if these tenants are isolated from each other, in case of need one or more users with system administrator permission can have the right to manage the processes to more tenants.



Multiple-tenancy might be very useful e.g. for those companies who have more affiliates and would like to build a deeper administration structure for the company as a whole. Each affiliate could become a tenant and could have its own administration. In this case other affiliates would not have a right to manage the processes of another affiliate and everybody could build his own processes in a way he wants. Dividing of tasks and responsibilities could be more transparent and the work would be more effective using this method.

contentACCESS Central Administration is a user interface for administrators, over which they can configure contentACCESS, create new automatically running jobs to process company data, configure these jobs, adjust framework feature settings, set up schedulers, databases, storages, create clusters etc..

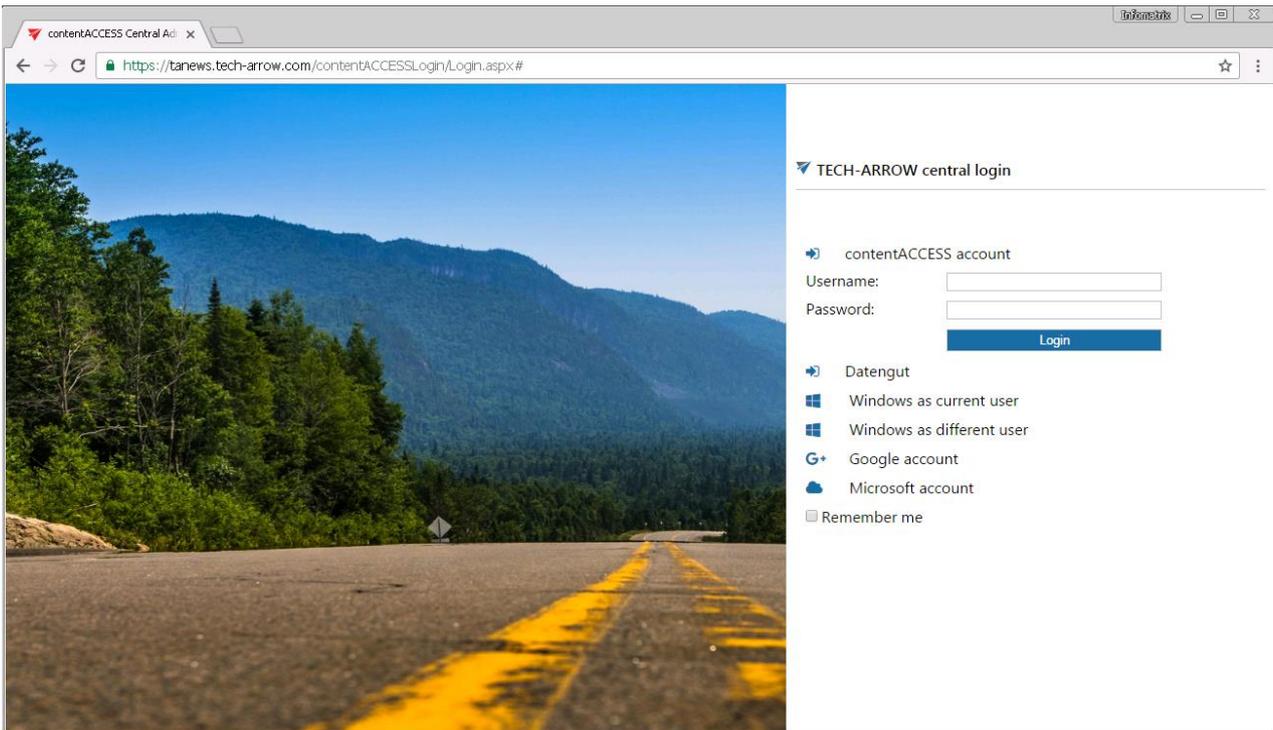
Before you proceed to read the Central Administration, we advise for you to read section [Terms of use](#) to understand the structure of the contentACCESS Central Administration user interface, and to navigate easier on the ribbon.

Central administration login

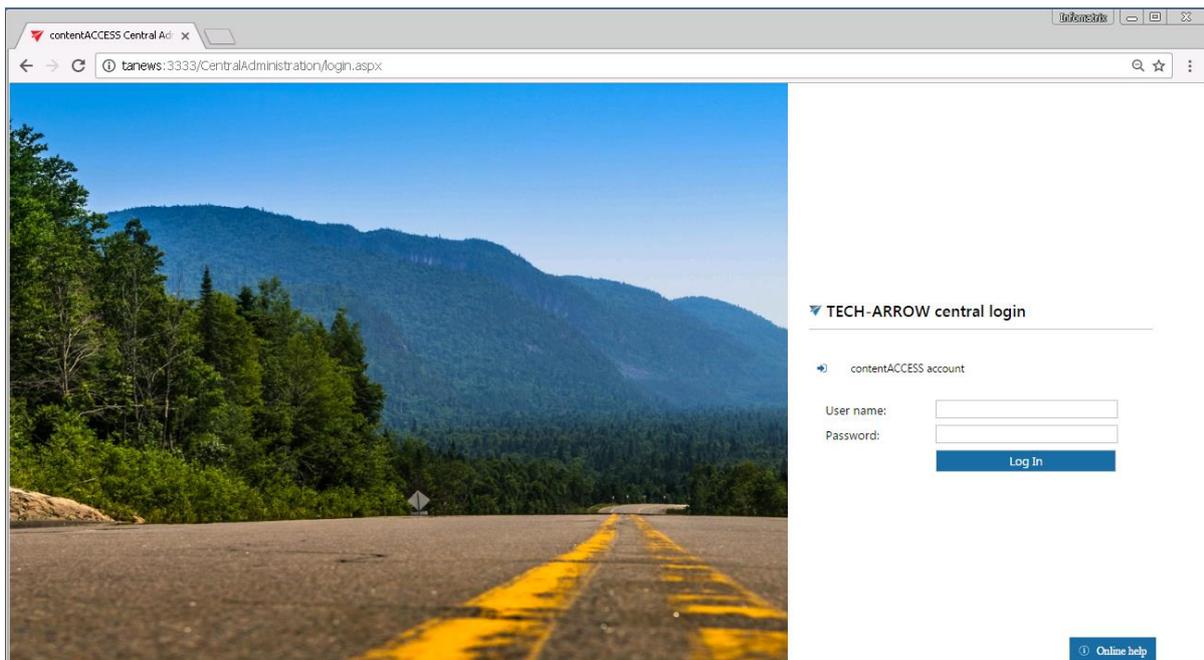
The user can log in to the Central Administration of contentACCESS only in case that he has the **Manage tenant and/or Manage system** permissions. Read the **Roles** section to learn more about roles.

There are 4 possibilities how the contentACCESS Central Administration can be opened:

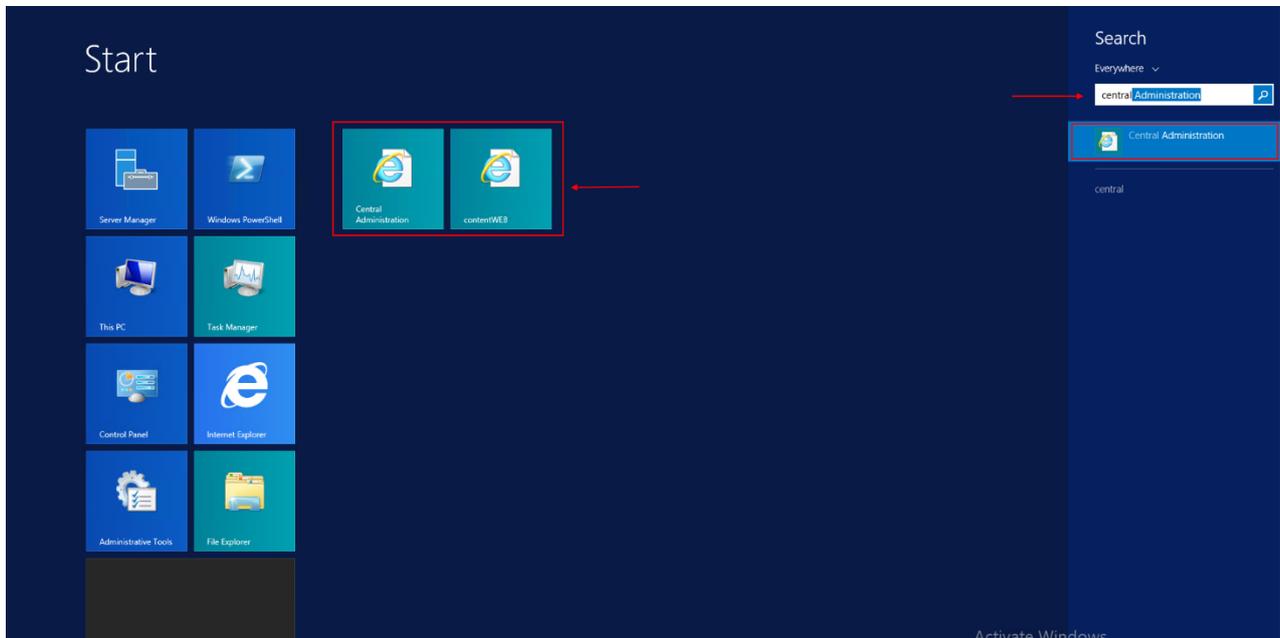
- **Standard login:** using the **standard Central Administration URL**, which is set and can be modified in the **Application settings**:
[http://\[ServerName\]:\[PortNumberOfCentralAdministration\]/CentralAdministration](http://[ServerName]:[PortNumberOfCentralAdministration]/CentralAdministration)
- **From the central login page** –[http://\[Central LoginServerName\]/contentACCESSLogin](http://[Central LoginServerName]/contentACCESSLogin)–which is installed by the contentACCESS setup (read more in section [Installation of contentACCESS](#)). This page URL is set/can be also modified on the System → Services → System page of Central Administration (in the Application settings it's read-only). The same page opens by opening the Central Administration web page from the Start menu of the machine where Central Administration is installed.



- With the “backdoor” Central Administration URL, which should be used in emergency cases only: [http://\[ServerName\]:\[PortNumberOfCentralAdministration\]/CentralAdministration/Login.aspx](http://[ServerName]:[PortNumberOfCentralAdministration]/CentralAdministration/Login.aspx);
On this page you can log in to the Central Administration with **Forms** login provider only, external authentication providers are not allowed. Enter your contentACCESS credentials and sign in.



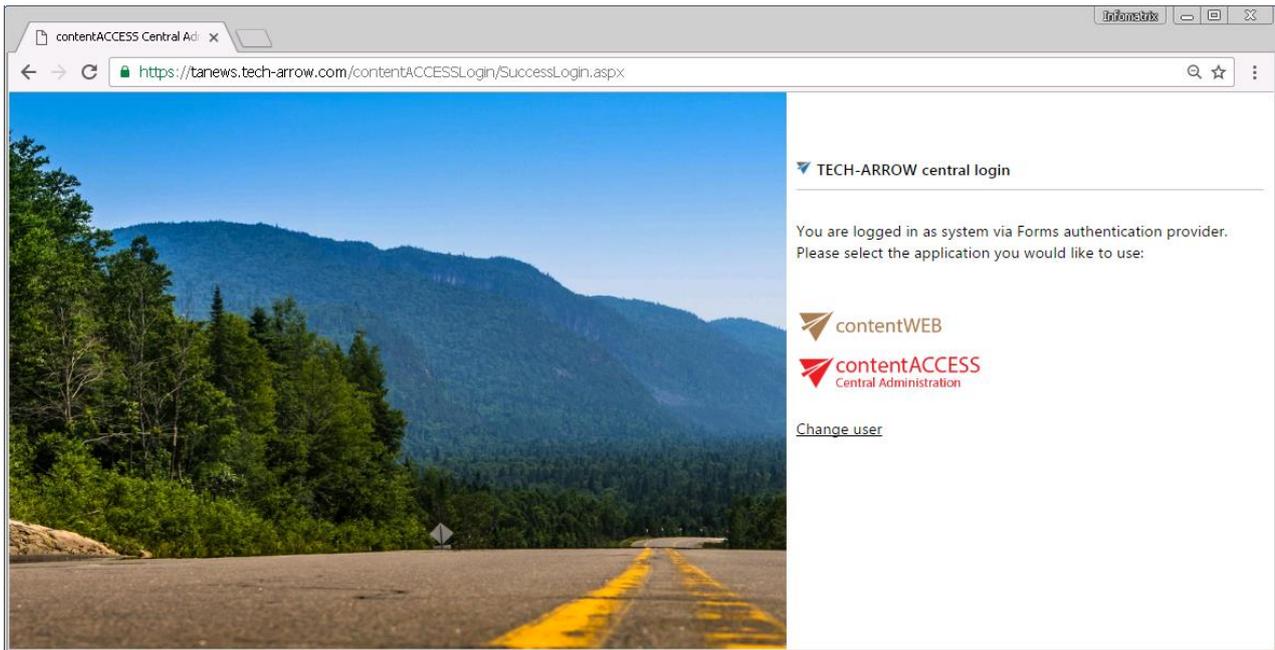
- **Windows start menu:** when working on Windows server 2013 - by typing “Central Administration” in Windows start menu or by clicking on the selected icon



Log in either with:

- a contentACCESS account (Forms login provider) or
- any of your external login providers (Forms, Windows, Microsoft account etc.) if they are configured in the Central Administration (more in section “**Login providers**”).

After a successful login the logged in user gets displayed. The applications allowed for the user are featured on the page under the logged in user. Click “contentACCESS Central Administration” and the central login page will redirect you to the Central Administration. By clicking contentWEB you can log in to the archive, if you have the necessary permissions.



Note: If you use Chrome, it is recommended to turn the password saving off. Learn more [here](#) about how to turn it off.

When you log in to contentACCESS Central Administration for the very first time, use the internal system account:

User name: **system**

Password: **cOntent@ccess**

Important: It is highly recommended to change this internal system account after the first login immediately.

For more information how to enable further external login providers, please refer to section [Login providers](#).

Note: Central administration remembers the last accessed page of the user and will automatically navigate back when logged on again. The same rule applies to tenant settings. Central Administration will log in under the tenant which was last selected.



contentACCESS Automated single sign on

Third-party login providers can be set for automatic login. Automated login providers sign in the user into contentACCESS Central Administration (also into contentWEB) without any further interaction with the selected provider. The following login providers can be automatized: Office 365, Google, Windows and any other third-party authentication providers. Datengut and Forms providers cannot be set to automatic. (Read more about login providers [here](#).)

To automatize one of the above mentioned login providers, select it in the **Auto login** column on the **Login providers** page (**System** tab → **Security** group → **Login providers** button)

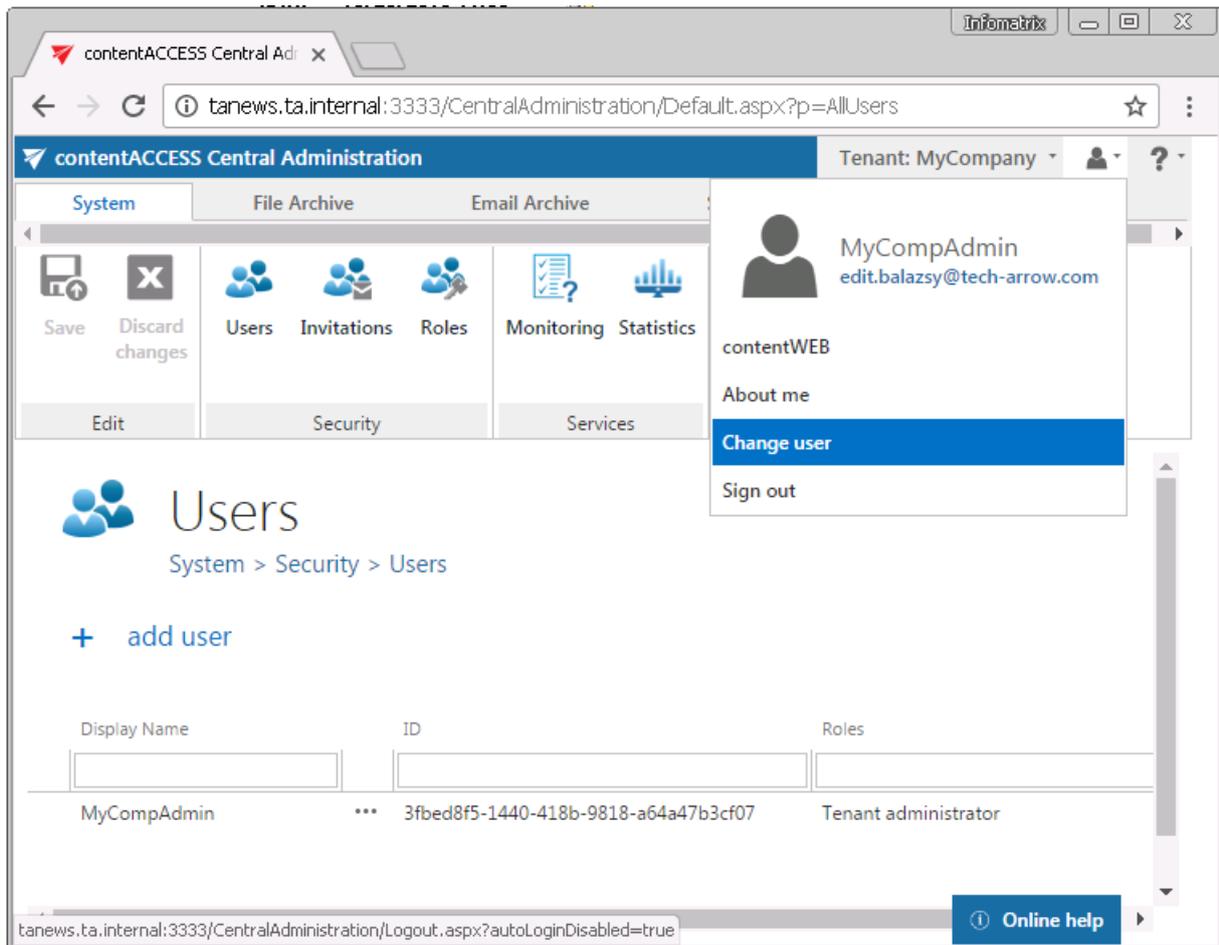
 Login providers
System > Security > Login providers

[+ new](#)

Provider name	Provider type	Provider availability	Create user	Is enabled	Auto login
Forms	*** Forms	All applications	False	Yes	<input type="checkbox"/>
Windows	*** Windows	All applications	False	Yes	<input type="checkbox"/>
External AD	*** ExternalAD	All applications	False	Yes	<input type="checkbox"/>
Office 365	*** Office 365	All applications	False	Yes	<input checked="" type="checkbox"/> 
Google	*** Google	All applications	False	Yes	<input type="checkbox"/>

Please note, that only one login provider can be selected at the same time.

To change the user who is logged in with his auto login provider (e.g. edit.balazsy@tech-arrow.com in this use case), open the user menu in the upper right corner and click option “Change user”.



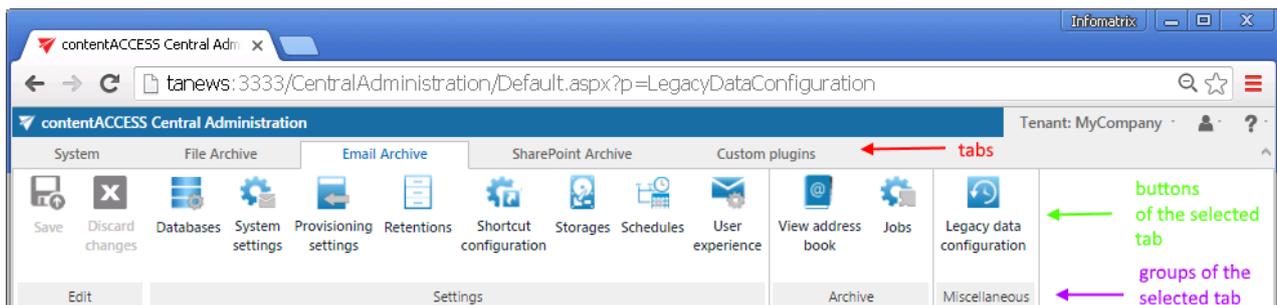
Central Administration logout

The user who is logged in to the Central Administration can log out from the application using the User menu in the upper right corner of the user interface:

- Option **“Sign out”**
 - a) if auto login provider is NOT used: the user is signed out from the application, and then he is redirected to the central login page, where he can log in again;
 - b) if auto login provider is used: the user is signed out from the application, he is redirected to the login page of the respective third-party provider and he is automatically logged in again with the login provider selected for auto login.
- Option **“Change user”** –the user is signed out from the application, and then he is redirected to the central login page, where he can log in (also with another user) again.

contentACCESS Central Administration user interface

After you have successfully logged in, the Central administration of contentACCESS page will load. The ribbon is divided into 5 main tabs: **System**, **File archive**, **Email Archive**, **SharePoint Archive** and **Custom plugins**. Each tab is divided into several groups, which also have several buttons.

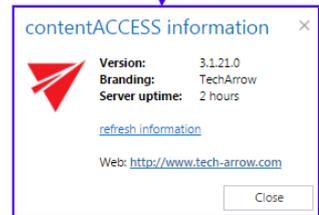
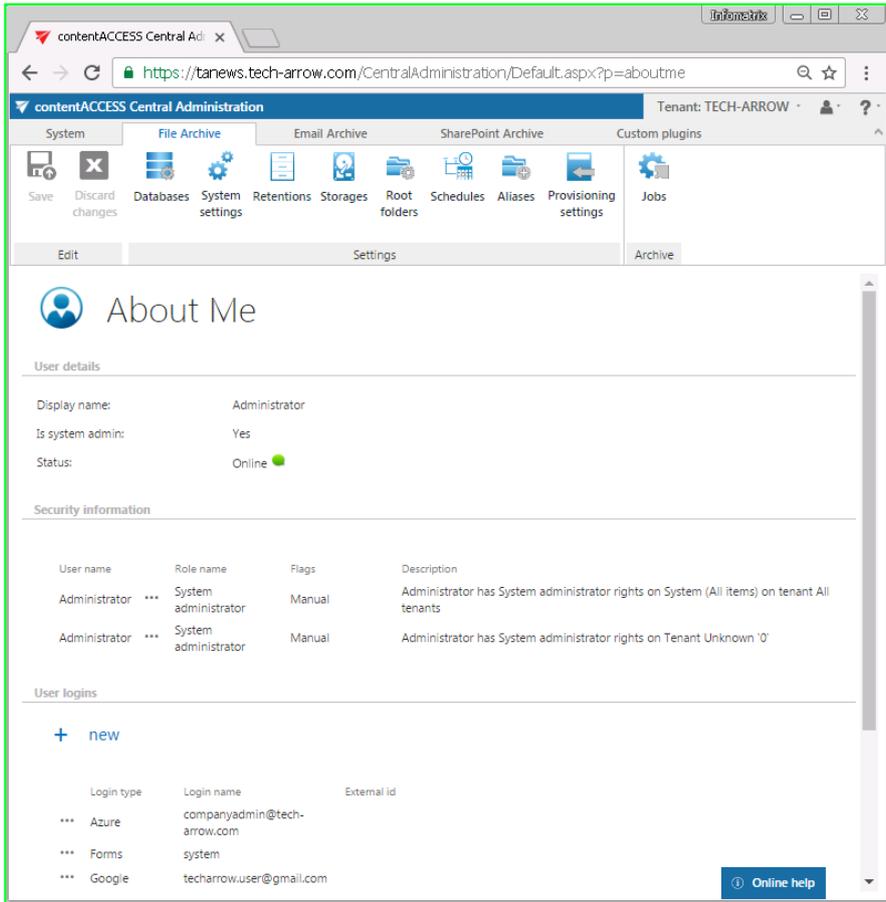
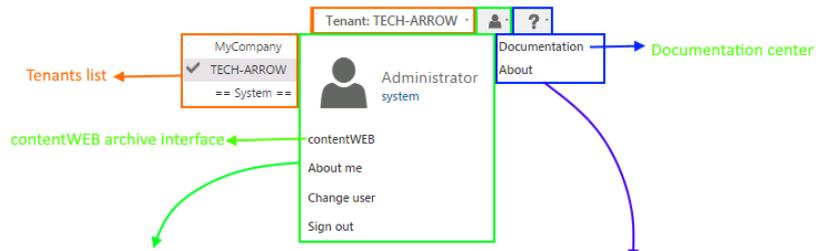


General system settings (application settings, security settings, system database settings, external accessibility, license activation, clusters, statistics, setting up new databases etc.) are accessible under **System** tab (marked with red frame on the screenshot above). Configurations of File Archive, Email Archive, SharePoint Archive and Custom plugins can be adjusted on the **File Archive**, **Email Archive**, **SharePoint Archive** and **Custom plugins** tabs on the ribbon.

You can **switch between the tenants** in the right upper menu of the Central Administration user interface.

In the **user menu** you can see the signed in user, the detailed information about the signed in user (**About me**), or you can **change the already logged in user**. Also here you can **sign out from the Central Administration** and **log in to the contentWEB archive interface**.

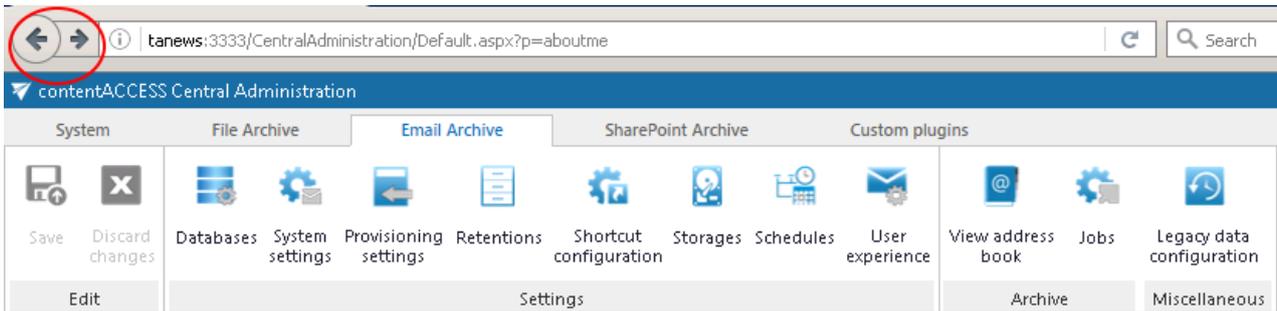
Click on the “?” question mark to roll down the **help** menu. Under **About** menu point you will find the information about the contentACCESS **version** that you have installed, here you can check the system uptime, and it also contains a link pointing to the company’s website. Under **Documentation** menu point you can **access all documentations** related to contentACCESS software.



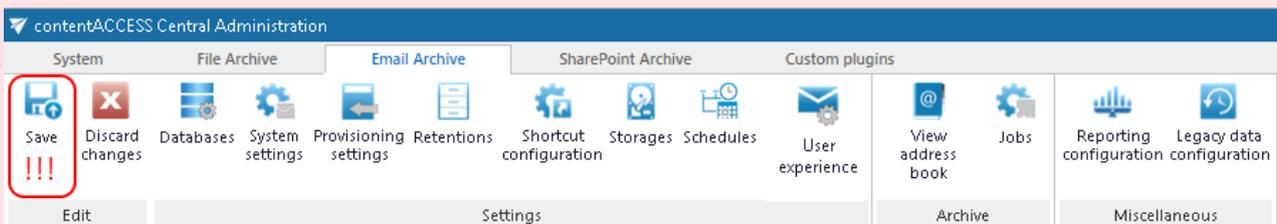
Note: In the **About me** menu under the **Security information** in the **Role name** column you can see the role assignment(s) of the signed in user. The **Flags** show whether the rights were given by provisioning job (flag name is **Automatic**) or manually (flag name is **Manual**).



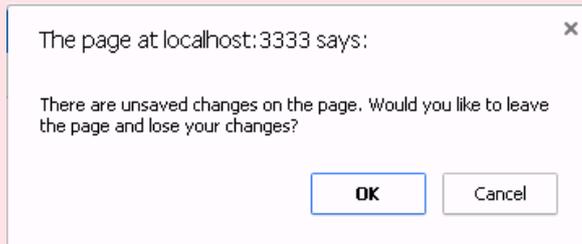
In contentACCESS, the back/forward button is also supported:



Important!!! Any changes made in the Central Administration must be saved via “Save” button, which is accessible in the left upper corner of the ribbon.



If the user has any unsaved settings, the system will warn him about it:



When you open contentACCESS Central Administration for the very first time, you need to create a tenant first (check section [Tenants in contentACCESS](#)). Further you need to adjust the system settings (refer to section [General system configurations](#)).



contentWEB

What is contentWEB? contentWEB is a web user interface for the contentACCESS archive, which ensures an over-simple read-only or full access to any items (files and emails), which have been previously archived/processed by contentACCESS. For the end user these items are also accessible from any mobile device. The searching, item listing, recovery and export functions of contentWEB make the work with these archive items more comfortable and intuitive.

The only condition to access the content of mailboxes/folders is that the end user must have access permissions to them. Such permissions must be granted by the system administrator. Email archive access permissions can be granted in the contentACCESS address book (on page View address book, more information [here](#)), File archive access permissions can be granted in the File archive's provisioning settings according to the steps described in [this](#) chapter.

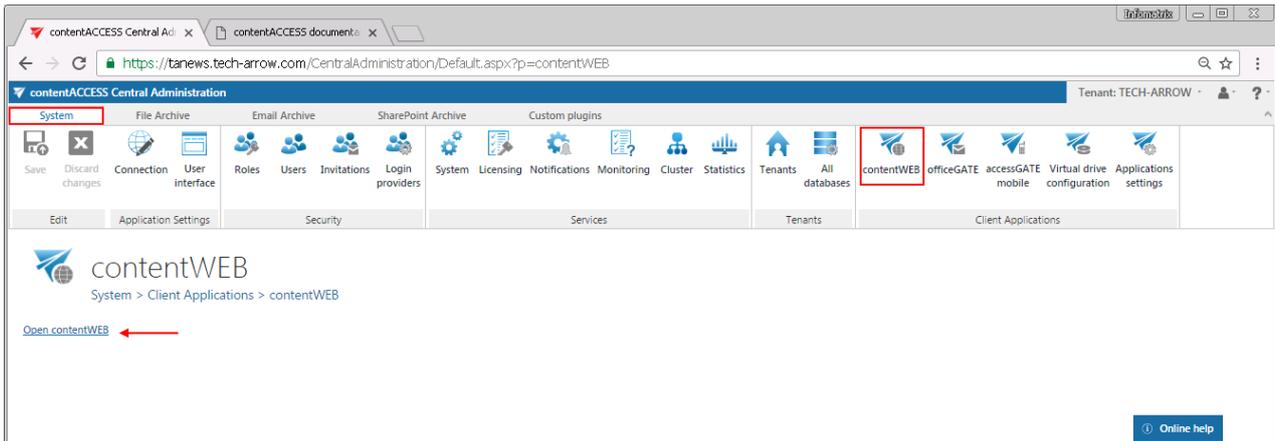
The main advantages of using contentWEB are as follows:

- ✓ Quick and easy access to the archived documents with the help of mobile devices.
- ✓ Ability to search between the archived items according to the certain parameters of an archived item (To, From, Modified by, Subject).
- ✓ Searching in the full text contents of the documents across multiple shares, using File Content Extractor plugin.
- ✓ Easy item sorting, item listing.
- ✓ Zero term search, advanced search.
- ✓ Active/inactive document view.
- ✓ Option to view document versions in the file archive.
- ✓ Recovery option in file archive.
- ✓ Export function to PST and ZIP format.
- ✓ One-click login with the help of external providers.
- ✓ Saving the last view of the logged in user.
- ✓ Ability to grant access to the archived documents for an explicit user.

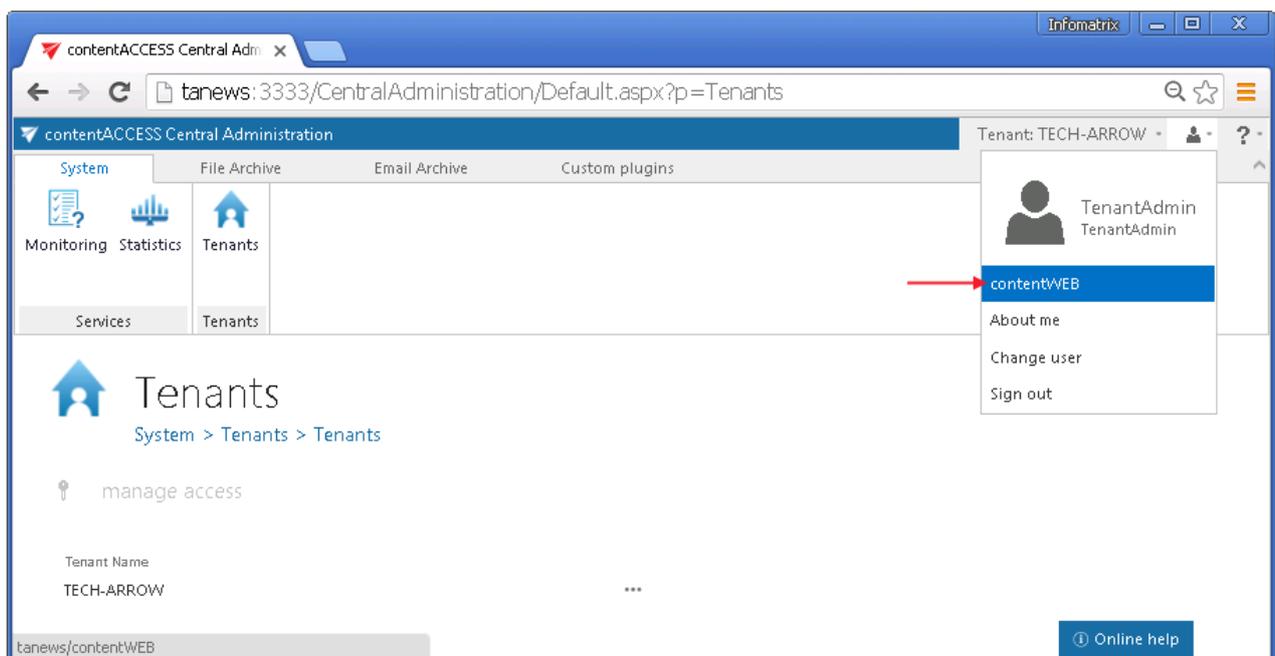


Logging in to contentWEB

System administrators can log in to contentWEB directly from the Central Administration using the “Open contentWEB option” on the “contentWEB” page (**System tab**→ **Client Applications group**→ **contentWEB button**). By clicking on “Open contentWEB” the login page opens. Enter your credentials and log in.



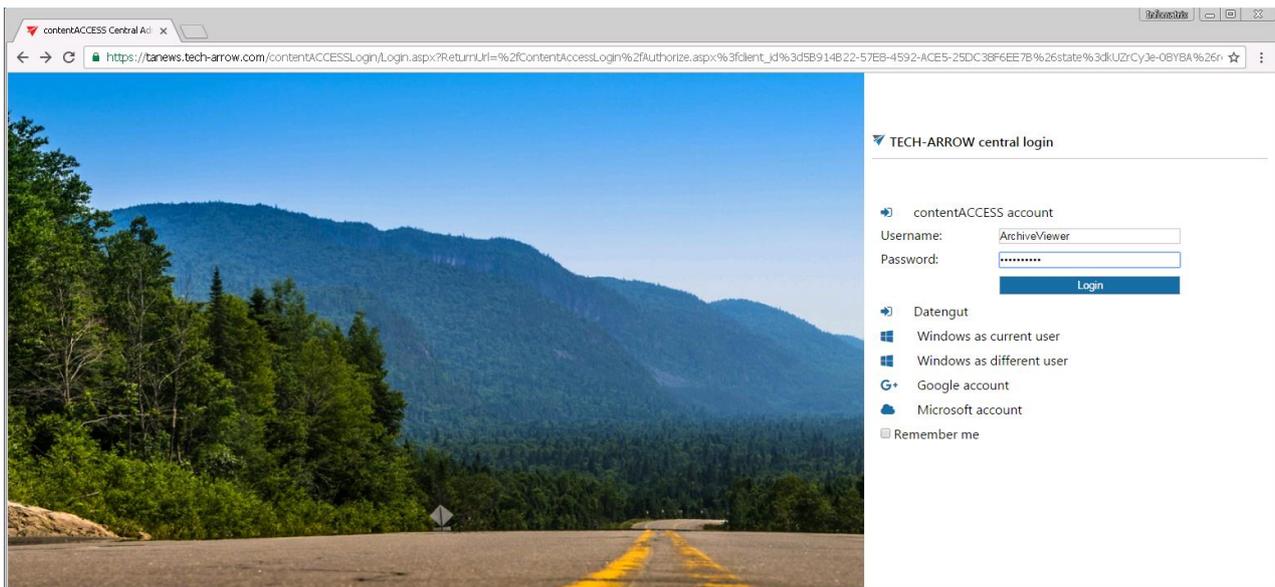
Tenant administrators (and also **system administrators**) can log in to contentWEB directly from the Central Administration using the login menu in the upper right corner of the interface. Open the menu, select “contentWEB” and the login page opens.



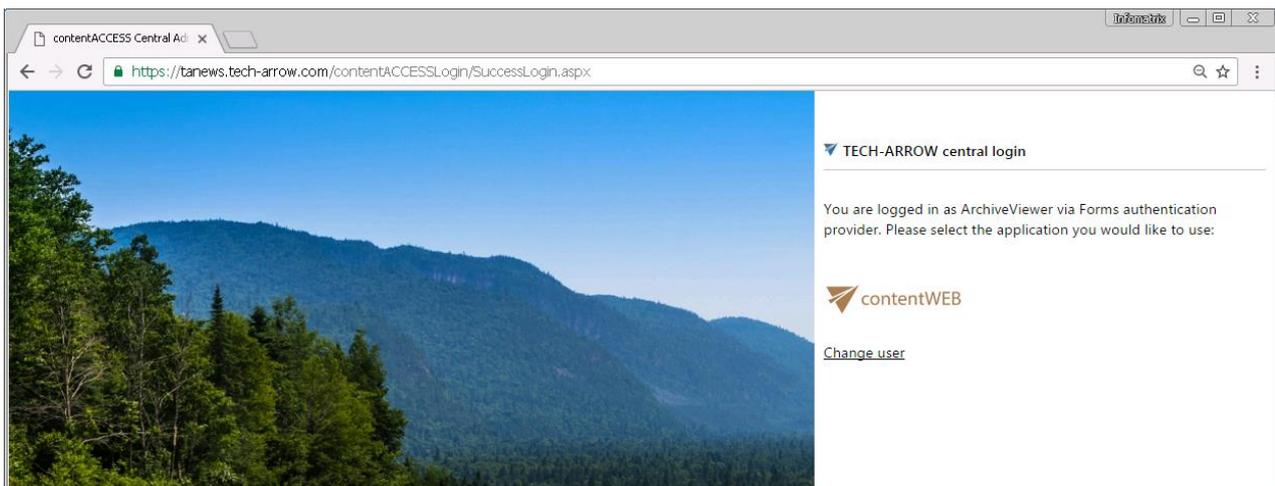


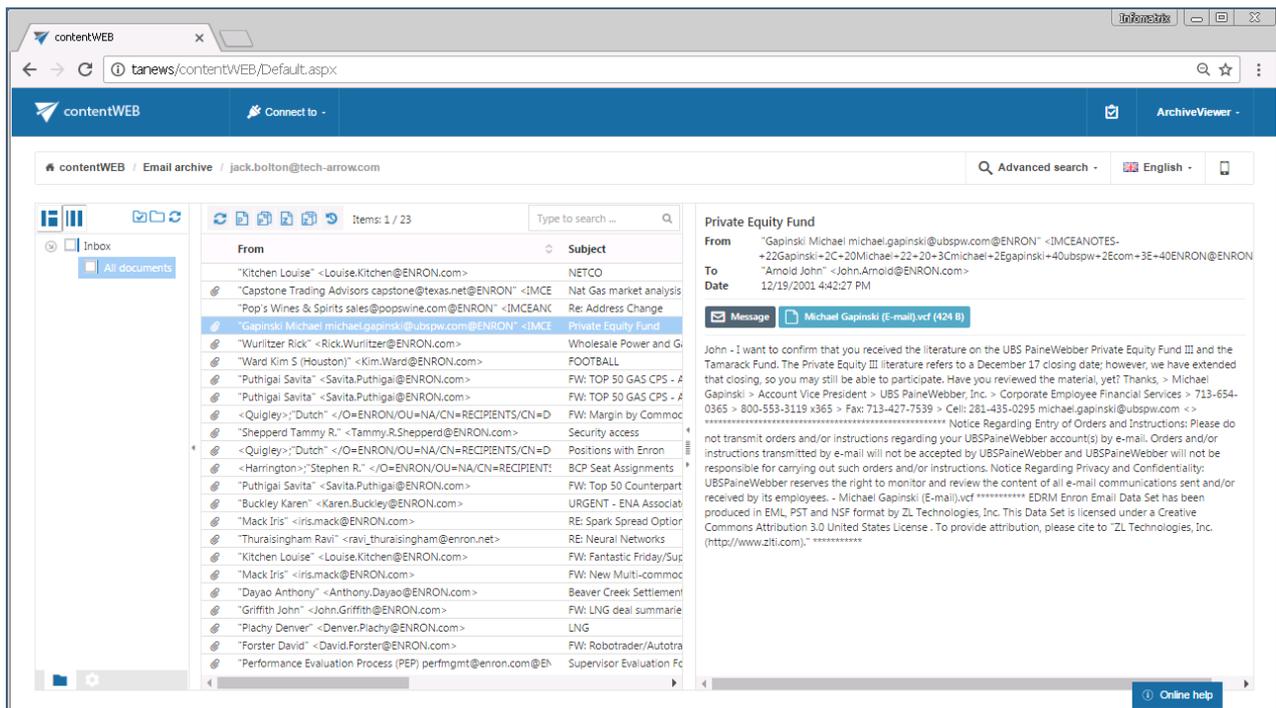
The **end users**, who do not have an access to the contentACCESS Central Administration page, and also the **system and tenant administrators** can log in to contentWEB using the **central login page**. From this central login page the user with the necessary permissions (roles) is further redirected to the contentWEB application:

Central login URL: [https://\[ServerName\]/contentACCESSLogin/Login.aspx](https://[ServerName]/contentACCESSLogin/Login.aspx)



Once you are logged in centrally, click “contentWEB” to open the desired application:





To be able to log in to contentWEB and to access the desired content on this interface, the user must have the necessary permissions. These must be granted for a user either

- in the Email archive/File archive settings (earlier described), or
- on the Users page, by assigning the necessary role to the user (Standard user role, with "Specific" rights in the archive)

Note: A system or tenant administrator can also create roles with specific permissions for a given user. E.g. it is possible to create a role, which allows for the assigned user to view the archived emails of [x@domain.com](#), but the emails of [y@domain.com](#) won't be available for the user in the archive.

contentWEB Automated single sign on

Third-party login providers can be set for automatic login. Automated login providers sign in the user into the contentWEB archive interface without any further interaction with the selected provider. The following login providers can be automatized: Office 365, Google, Windows and any other third-party authentication providers. Datengut and Forms providers cannot be automatized. (Read more about login providers [here](#).)

To automatize one of the above mentioned login providers, select it in the **Auto login** column on the **Login providers** page (**System** tab → **Security** group → **Login providers** button in the Central Administration).



Login providers

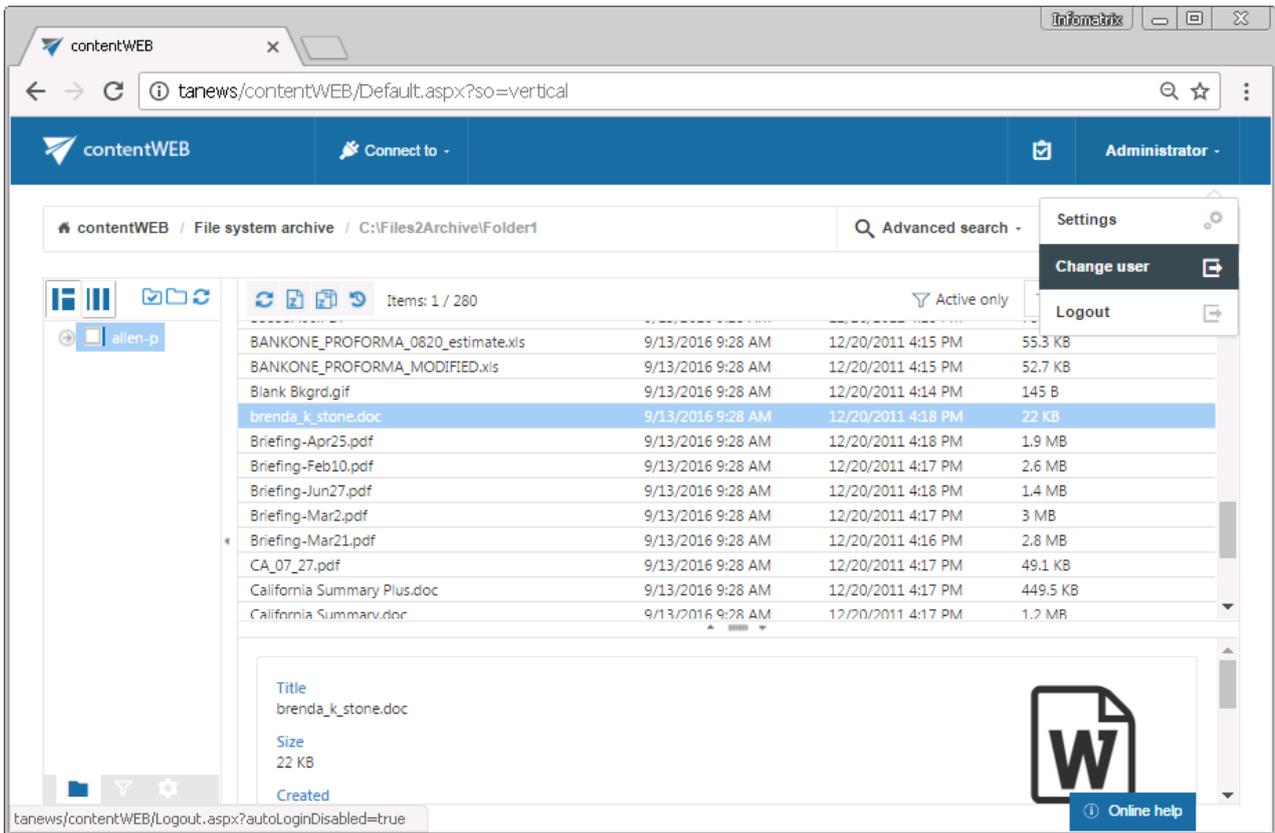
System > Security > Login providers

+ new

Provider name	Provider type	Provider availability	Create user	Is enabled	Auto login
Forms	*** Forms	All applications	False	Yes	<input type="checkbox"/>
Windows	*** Windows	All applications	False	Yes	<input type="checkbox"/>
External AD	*** ExternalAD	All applications	False	Yes	<input type="checkbox"/>
Office 365	*** Office 365	All applications	False	Yes	<input checked="" type="checkbox"/>
Google	*** Google	All applications	False	Yes	<input type="checkbox"/>

Please note, that only one login provider can be selected at the same time.

To change the user who is logged in to contentWEB with his auto login provider (e.g. with Offie 365 in this use case) open the user menu in the upper right corner and click option “Change user”.



Logout from contentWEB works the same way as the logout from the contentACCESS Central Administration.



Virtual Drive

What is a virtual drive? It is a virtual file system that presents/virtualizes any data (files and folders of an actual disk) to the end-user. Virtual drive is a non-existing drive that does not physically exist in the computer, but it contains the exact structure of the items that have been processed by contentACCESS.

The contentACCESS Virtual Drive was developed by TECH-ARROW and serves as a key access point between the end user and the **contentACCESS File Archive**. **Virtual Drive is a must have-tool for customers who have contentACCESS File system archive, as it is used to retrieve the archived files from the shortcuts.**

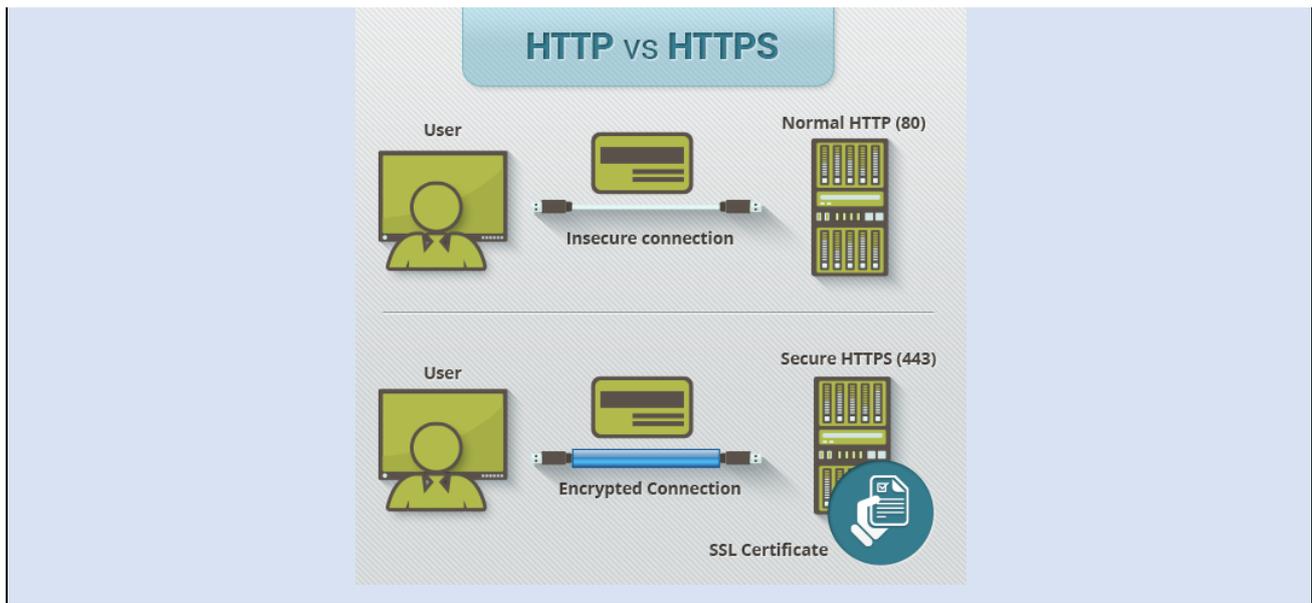
The archived items can be also viewed from this drive by the end users.

The Virtual drive configurations are accessible on the [Virtual drive configurations](#) page of Central Administration.

contentACCESS Web Services (Proxy)

Most companies understand that sensitive information/data should be transmitted using a secure connection. TECH-ARROW also reacted on this demand and offers a secure connection, i.e. HTTPS connection to enable communication between the user and the contentACCESS server. To use the HTTPS security, it is required to install a proxy server, which will enable for the user to communicate with the contentACCESS server. The contentACCESS Proxy is one of the contentACCESS components that are included in the contentACCESS setup package.

Note: Hyper Text Transfer Protocol Secure (HTTPS) is the secure version of HTTP the protocol over which data are sent between client (as in our case the Outlook form) and the contentACCESS server that you are connected to. The “S” at the end of HTTPS stands for “Secure”. It means all communications between the client and the server are encrypted. HTTPS is often used to protect highly confidential online transactions. HTTPS pages use one of two secure protocols to encrypt communications – SSL (Secure Socket Layer) or TLS (Transport Layer Security)(proxy that we will install uses SSL). Both of these protocols use what is known as asymmetric Public Key infrastructure (PKI) system. This PKI system uses two “keys” to encrypt communications, a “public key”, and a “private key”. Anything encrypted by the public key can only be decrypted by the private key and vica-versa.

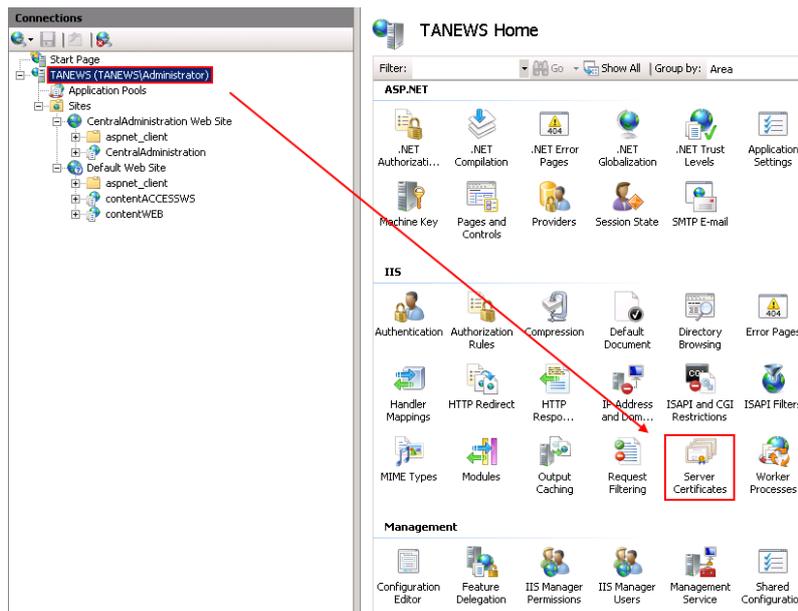


How to allow HTTPS secure connection between the proxy server and the contentACCESS in case of need?

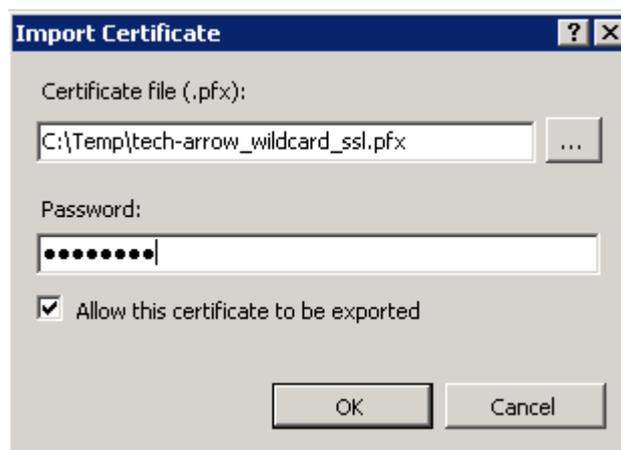
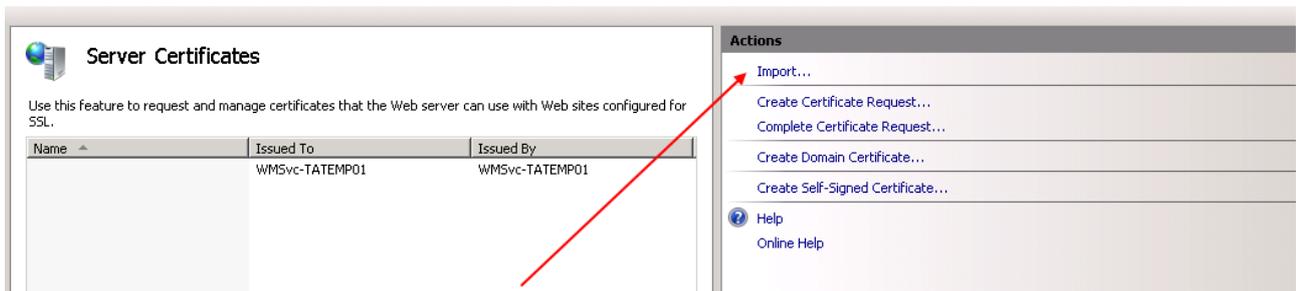
The contentACCESS setup package cannot configure the contentACCESS Proxy to use https on the Internet Information Services (IIS), therefore this must be set manually. It is also necessary to mention that the proxy server must be installed with the “https” connection from the contentACCESS package, otherwise it is not possible to establish HTTPS connection between the proxy server and contentACCESS.

Once the contentACCESS Proxy is installed, continue according to the next steps:

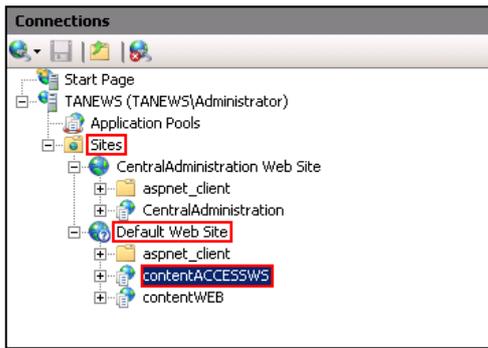
1. Open Internet Information Services (IIS) Manager on the computer where the proxy server is installed.
2. Import the company’s SSL Certificate
 - a) Click on the server name – “TANEWS(TANEWS\Administrator)” in our case – and under section **IIS** double click on **Server Certificates**:



b) **Import the certificate.** In the upper right corner of the Actions pane click on **Import** and in the **Import certificate** window browse for the company’s certificate, open it, then enter the password to it and click on **OK**:



c) **Bindings configuration.** Now enable the access to the proxy from HTTPS. Search for the node contentACCESSWS in the **Connections** pane. Double click on the **Default Web Site** in the pane, and in the upper right corner of the **Actions** pane click on **Bindings** option.



Screenshot A



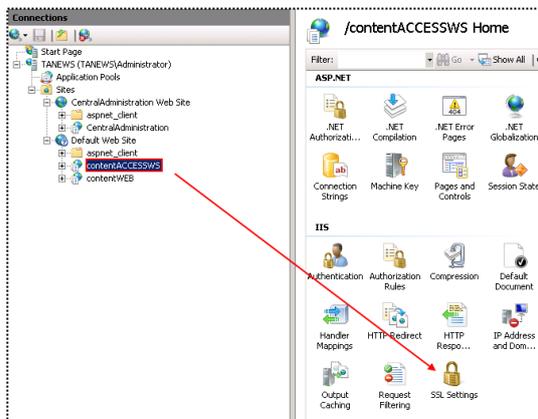
Screenshot B

In the **Site Bindings** window, click on **Add**. In the **Add site binding** window, under **Type** select “**https**” from the dropdown list, enter the Host name and select the SSL certificate from the dropdown list. Then click on **OK**.

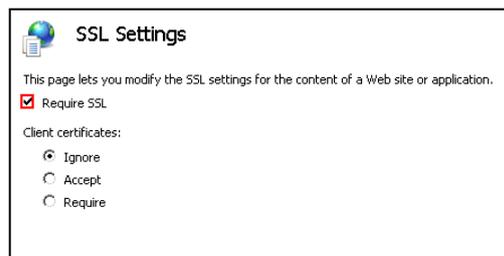


Cancellation of HTTP-allowance

- a) If you would like to stop using the HTTP connection, unfold the appropriate site in the **Connections** pane and click on the proxy (contentACCESSWS), then double click on **SSL Settings** option under **IIS** section (Screenshot A). The **SSL Settings** page will open. Here check checkbox **Require SSL** (Screenshot B).



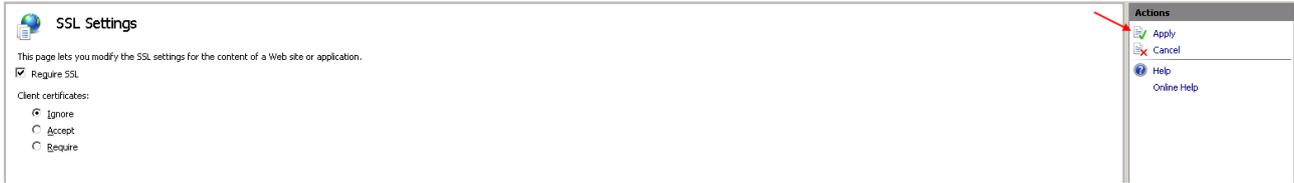
Screenshot A



Screenshot B



b) In the right hand corner click on **Apply** to save these changes.



To check, if the communication between the proxy and the contentACCESS is well established, enter the following URL into the browser:

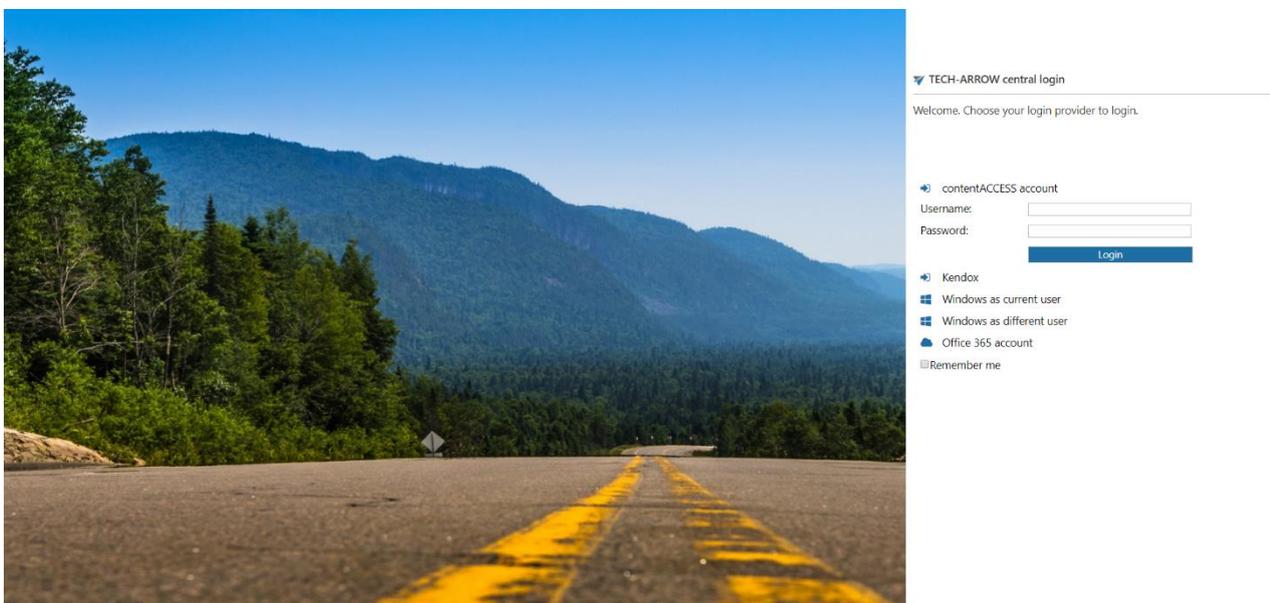
[https://\[HostName\]/contentACCESSWS/MobilityService.svc/ping](https://[HostName]/contentACCESSWS/MobilityService.svc/ping).

If the connection was well established, then the ping result will show **OK**.

Central login page

The Central login page is a separate component that's also a part of the contentACCESS installation package. It can be deployed on the machine where the contentACCESS server is deployed, or also on any other server, separately from other components.

The Central login page is a must-to component that enables to use the third-party login providers and also social login providers like Windows, Google, Office 365 etc. – i.e. the user can log in to the respective application using his Google, Office 365, Windows etc. account only from this page:



The component is using a standard OAUTH protocol, i.e. any other client application, which is able to authorize through the OAUTH, can be also authorized by contentACCESS.

Central login page features:

- **Long term login:** using option “**Remember me**” the logged in user is remembered in the next 3 months – this ensures that the user is not forced to log in to the application every time
- **Disabling application(s)** by disabling login to contentACCESS from that/those application(s) – e.g. by disabling officeGATE but leaving contentWEB enabled the company allows for the end user to browse the contentACCESS archive through contentWEB only, but in officeGATE the connection with contentACCESS will be disabled for that contentACCESS installation (read more in section [Application settings](#))



- **Social authentication support** (Google, Facebook, O365/Live – **Important!**: You still need to register yourself on these social providers; read more in [External login provider configuration](#))
- **Automatic login provider (single sign on)** –the central login page first tries to authenticate the user who tries to log in with login provider which is set to automatic; the user is automatically redirected to the desired application if the authentication was successful (read more in [contentACCESS Automated single sign on](#))
- **User invitation support**

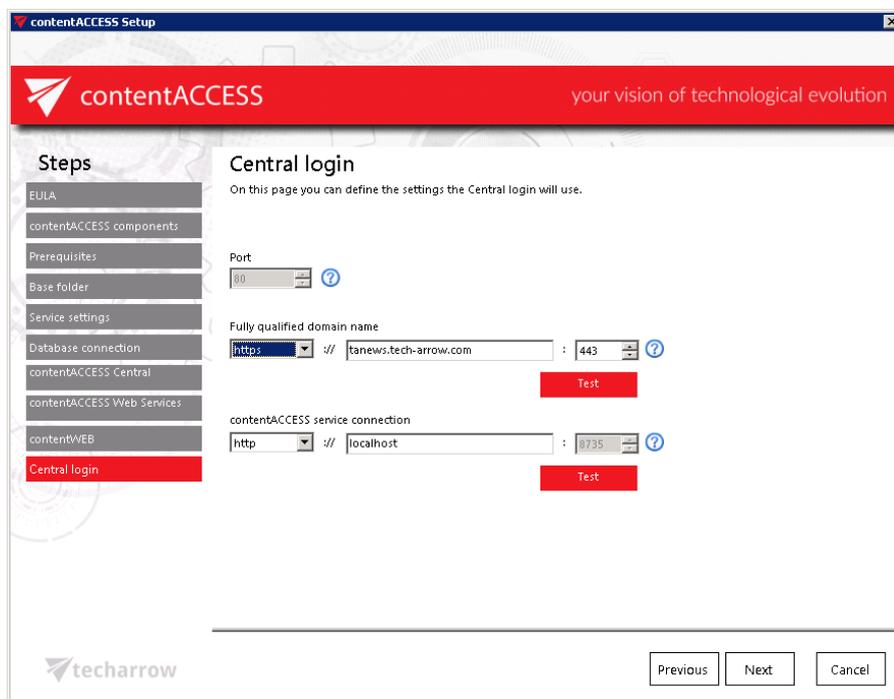
Central login configuration

The Central login page is accessible at the following address:

[http://\[CentralLoginUrl\]/contentACCESSLogin](http://[CentralLoginUrl]/contentACCESSLogin)

The physical port of the page in IIS, the application URL settings of the Central login page and the connection settings between the Central login page and the contentACCESS server are configured at the first install of the product, and are written to the database by the setup package. These values can be changed:

- by **updating** the product;



- on the **System** page of the Central Administration;



 **System**
 System > Services > System

General settings

Is system configured:
 Plugins directory: C:\Program Files\TECH-ARROW\contentACCESS\G

User search settings

Disable user searching:

Database settings

Database type: MSSQL
 Server name: TANEWS
 Database: CONTENTACCESSDB
 Schema: dbo
 User: sa

Proxy settings

Do not use proxy
 Use system default proxy settings
 Use explicit proxy server settings

Proxy server URL:
 Username:
 Password:

External accessibility settings

Retrieve server FQDN: :
 Enter an externally accessible alias for the contentACCESS server. This value is used for shortcut links too.

Central login: :
 Provide necessary information, where central login is deployed.

Connection successful!

When configuring the application URL for the Central login page, it is highly recommended to create an alias and to specify it in FQDN form to ensure a trouble free access from everywhere.

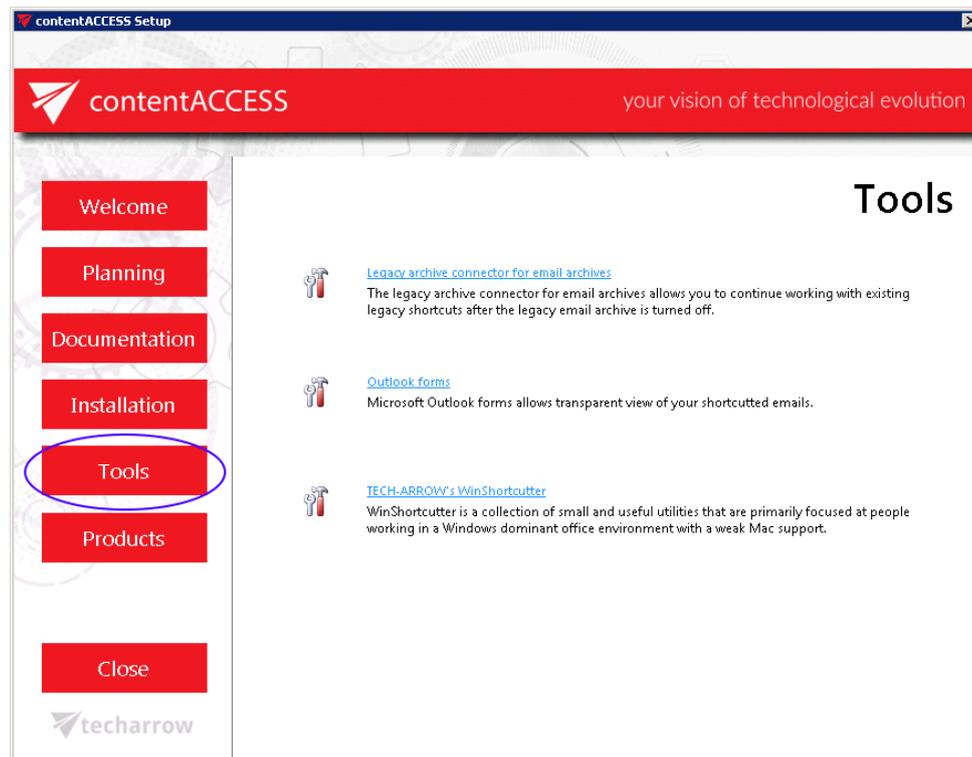
The **Applications settings** allow to configure certain Central login page settings as well, but the Application URL cannot be changed from here. The URL is written here by the setup package as well, but it can be changed only on the **System** page (System → Services → System):

contentACCESS Tools

The contentACCESS setup package is extended with the following tools:

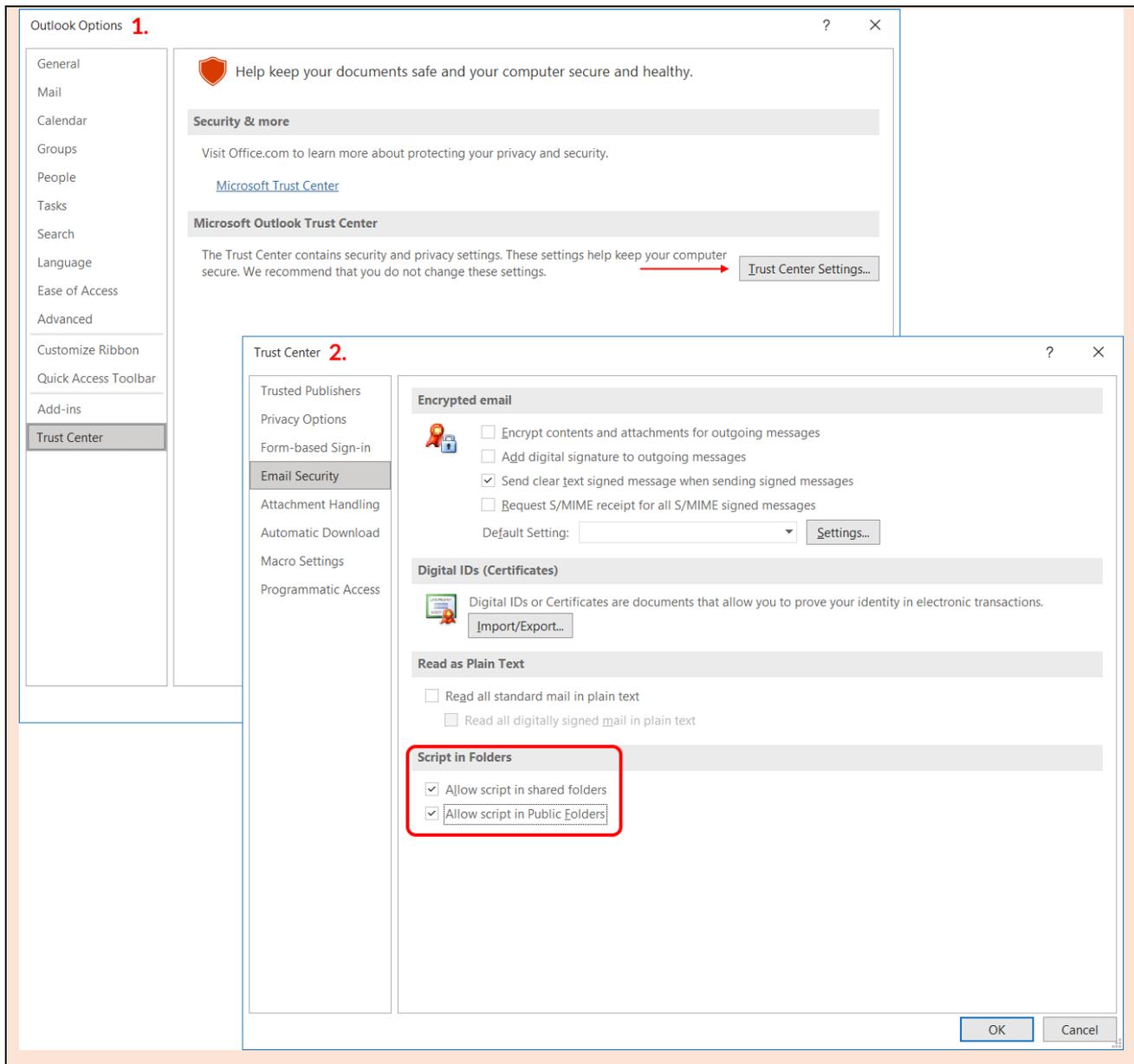
- **Legacy archive connectors** (used to access the legacy email archives [MAM EE and ELM]; for more information check section [Legacy email archive connectors](#)),
- **MS Outlook Forms** (further mentioned in section [Email Archive](#))
- **TECH-ARROW's Winshortcutter** (For more information click [here](#).)

Here you can also read a short description about these extensions of the contentACCESS setup:



Installing Outlook forms

Important: For Outlook forms to work correctly also for In-Place Archive mailboxes, **Allow script** options must be enabled in **Trust Center** settings in **Outlook**.



In Microsoft Outlook, each of the windows where you enter content — for example, a new email message or a new calendar appointment—is called an Outlook form. These default forms are stored in the Standard Forms Library for Outlook. There are additional libraries as well, including Personal Forms and Organizational Forms if you have an Exchange Account. Each folder within the Outlook hierarchy has a default Outlook form associated with it. As you would expect, a mail folder such as your Inbox has the Message form as the default, and the Contacts folder opens the Contact form as its default.

When archiving MS Exchange content, the contentACCESS MS Outlook forms are used to open an HTML shortcut – which replaces the archived email message – transparently with the original email message. If



the forms are installed, then the end user will not notice any change between the original email and the archived (shortcutted) one.

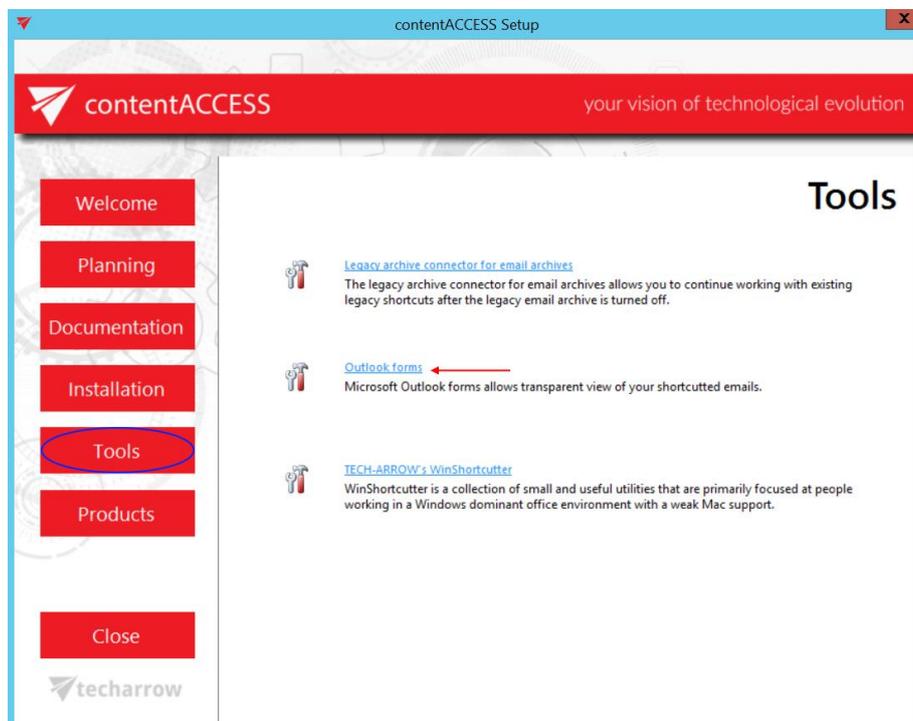
There are 3 contentACCESS Outlook forms available. For the correct functionality all these forms must be installed.

- CA_techarrow.oft – is used to transparently open the standard archive messages
- CA_R_techarrow.oft – is used to transparently open the replied archive messages
- CA_F_techarrow.oft – is used to transparently open the forwarded archive messages from the mailbox.

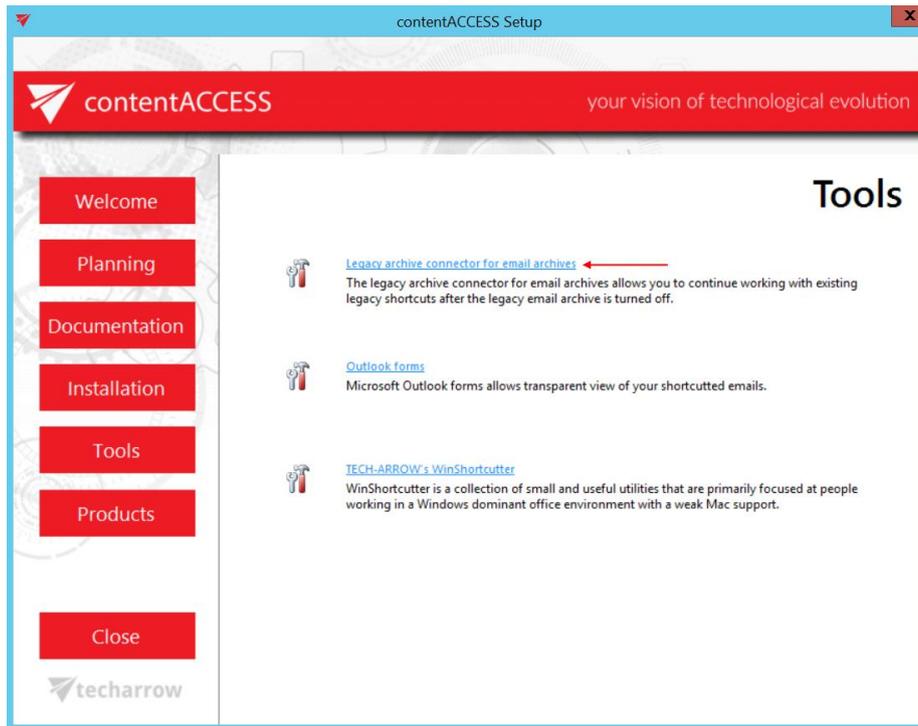
There are also available **contentACCESS Outlook forms for legacy archives** (both MAM and ELM).

Installations of **Outlook forms** and **Outlook forms for legacy archives** are very similar, differences are explained below.

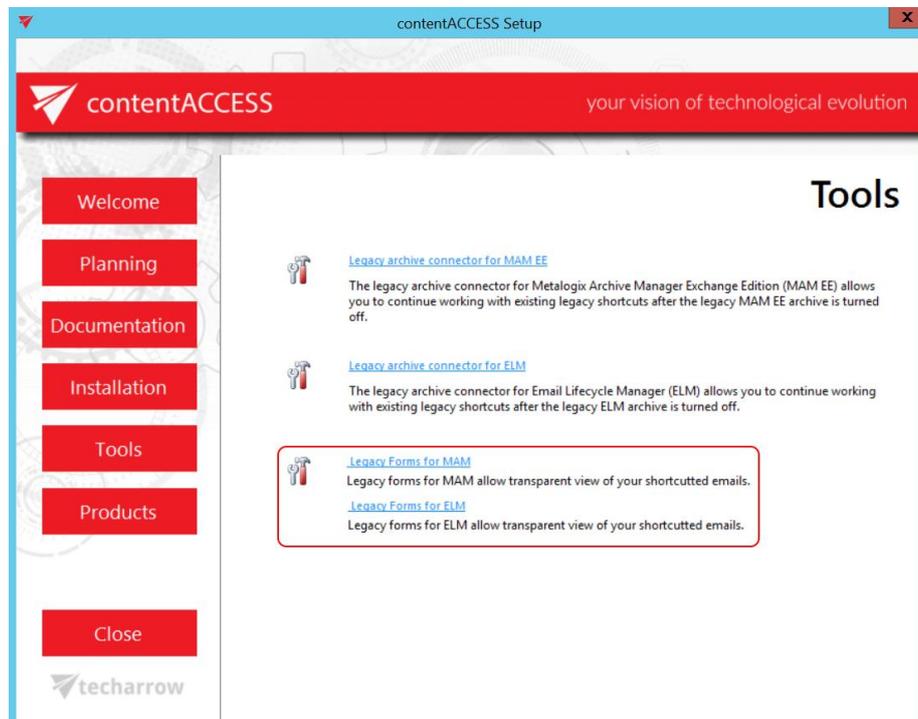
To install Outlook forms, open the **Tools** section in the contentACCESS installation wizard → click **Outlook forms** option.



To install Outlook forms for legacy archives, open the **Tools** section in the contentACCESS installation wizard → click **Legacy archive connector for email archives** option.



Then click on **Legacy forms for MAM** or **Legacy forms for ELM** (depends on what you are using).



By clicking the selected option the **Install Outlook forms, Install Outlook forms (Legacy MAM) or Install Outlook forms (Legacy ELM)** window opens:



Install Outlook forms

Server Url:
https://tanews.tech-arrow.com : 443
Test

 Publish to the whole organization

 Publish to mailbox only

 Publish manually

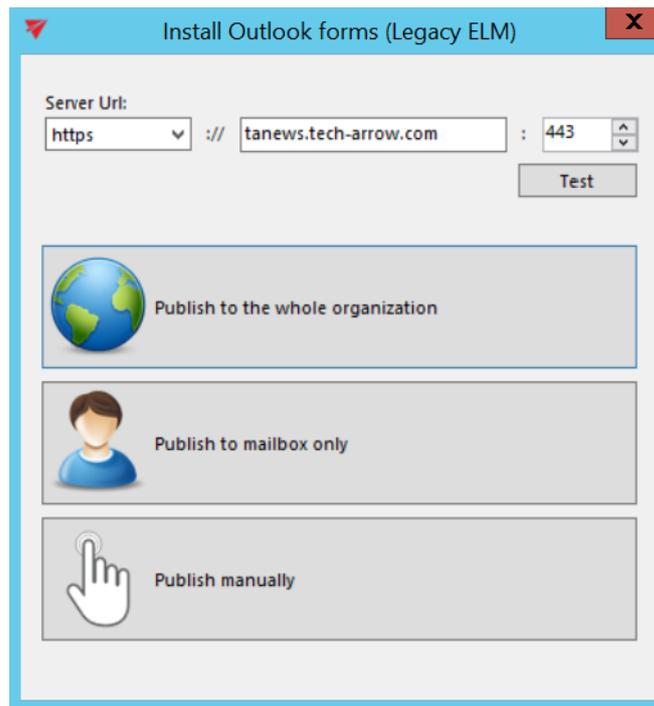
Install Outlook forms (Legacy MAM)

Server Url:
https://tanews.tech-arrow.com : 443
Test

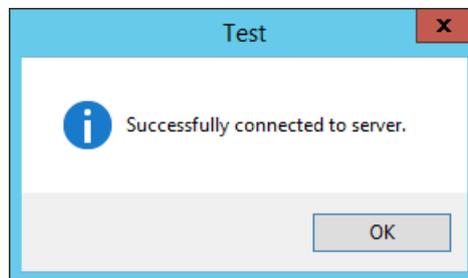
 Publish to the whole organization

 Publish to mailbox only

 Publish manually



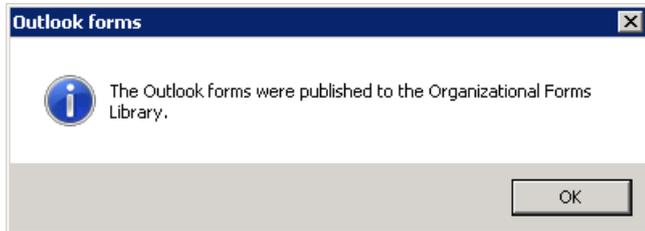
First the administrator needs to set the contentACCESS retrieve server (contentACCESS Proxy) URL. This option allows to install the forms for HTTP and HTTPS Proxy, too. It is also recommended to test the connection with the server.



The application simplifies the Outlook form publishing by providing an automated way for publishing. The application allows automatic publishing of the forms to the Organization forms library but also publishing the forms into the user's Personal forms library.

- **Publish to the whole organization** (Organizational forms library) – this is the recommended method, because the forms must be published once and will be available for the whole organization.
- **Publish to mailbox only** (Personal forms library) – if it's not allowed to publish to Organizational forms library (Office 365 doesn't have Organizational forms library), then this option is used.

By publishing to Organizational and/or personal forms library, Outlook starts automatically. If forms were published successfully, the user is warned about this:

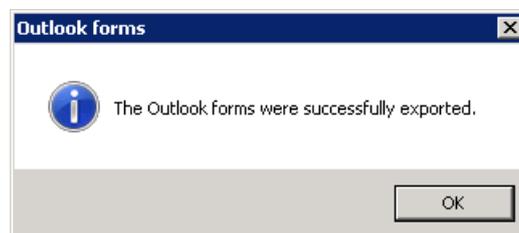


Requirements for automatic publishing are the following:

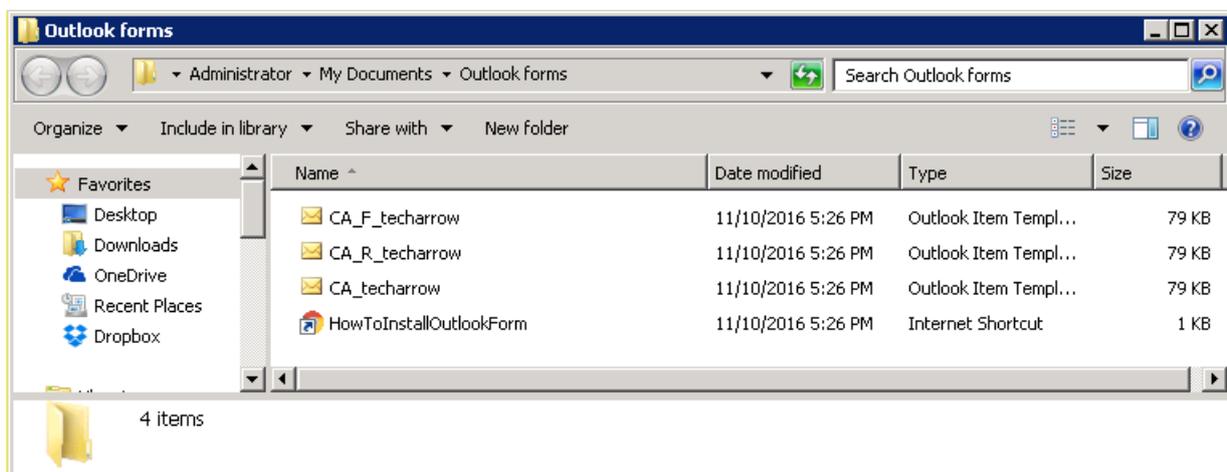
- Outlook x64 2013 and higher
- The user account running the application must have the necessary permissions

If the **requirements for automatic publishing are not fulfilled**, manual publishing is used:

- **Publish manually:** you need to select a folder, where the forms will be exported together with the link pointing to the Outlook forms installation manual.



Once exported, the folder will be opened and you can deploy the forms using the steps described in the manual ([click](#) to get the link to the manual).



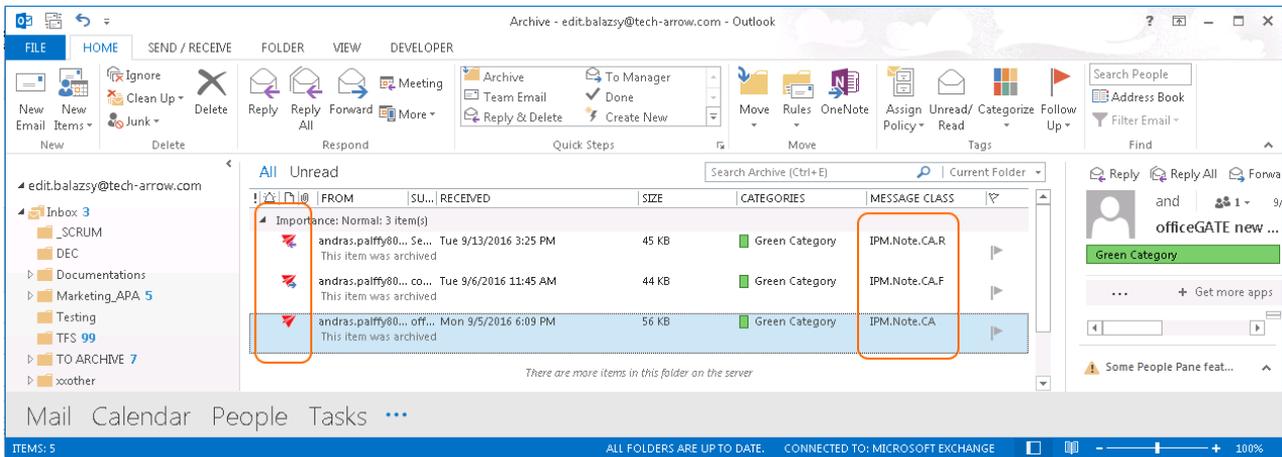


During the email archive process, the archive job changes the message class of the email messages:

- Standard messages – get the IPM.Note.CA message class
- Replied messages – get the IPM.Note.CA.R message class
- Forwarded messages – get the IMP.Note.CA.F message class

Based on these message classes, the Outlook forms mark the archived emails with the following icons:

- Standard messages – 
- Replied messages – 
- Forwarded messages – 



Important!!! Outlook 2013 users will have access to the Organizational forms library but cannot publish to it using Publish custom forms.

There are 2 possible ways how to solve this:

- a) Use an **earlier version** of MS Outlook to publish the Outlook Forms;
- b) Publish the Forms to your **Personal Forms Library** and then use the **Outlook Options** → **Advanced** → **Developers group** → **Custom Forms...** → **Manage Forms** functionality to copy the form from **Personal Forms** to **Organizational Forms**.



Legacy email archive connectors

Legacy retrieve services bring for the user the advantages of mixed archiving (connection to the legacy archive and the new archive through contentACCESS).

With installing the given retrieve service and configuring it in the contentACCESS Central Administration and on the legacy server, you will be able to **retrieve the old email archive shortcuts** and to **check your legacy archive using contentWEB**. It is recommended to install the retrieve service on the legacy archive server.

To be able to work with the existing legacy shortcuts, the legacy email archive should be turned off. contentACCESS has two legacy archive connectors:

- Legacy archive connector for **Metalogix Archive Manager Exchange Edition (MAM EE)**
- Legacy archive connector for **Email Lifecycle Manager (ELM)**

In the following subchapters we will learn how to install the MAM EE and ELM retrieve services and how to do necessary configurations in contentACCESS.

Legacy archive connector for Metalogix Archive Manager Exchange Edition (MAM EE)

Legacy MAM retrieve service is a replacement of the original Metalogix Archive Manager Exchange Edition (MAM EE) retrieve service. This service is used to access archived files over the legacy shortcuts, if you have uninstalled Metalogix Archive Manager (and Archive Web) from your computer, and you need to access the archive contents.

Important! Do not uninstall HSM from the server. It will be needed to access the MAM shortcuts and to retrieve the archived items.

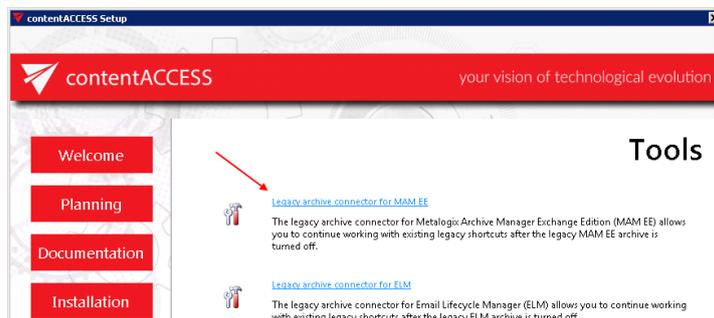
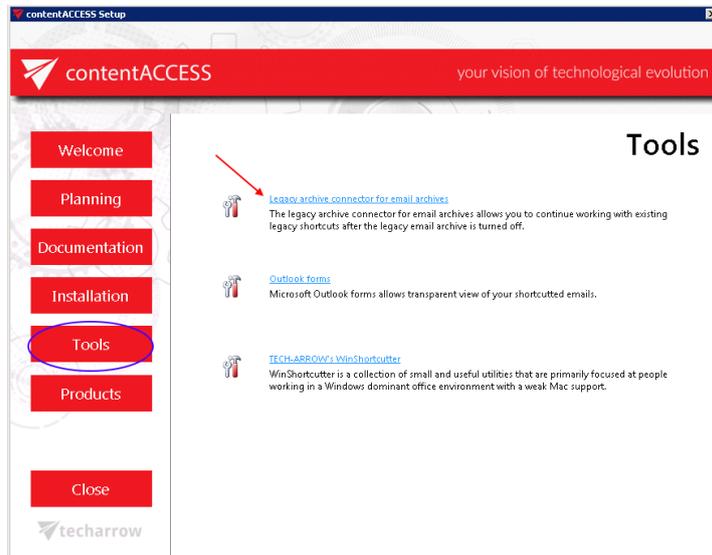
The configuration will be explained in two parts:

1. [Installation](#)
2. [Configuration](#)

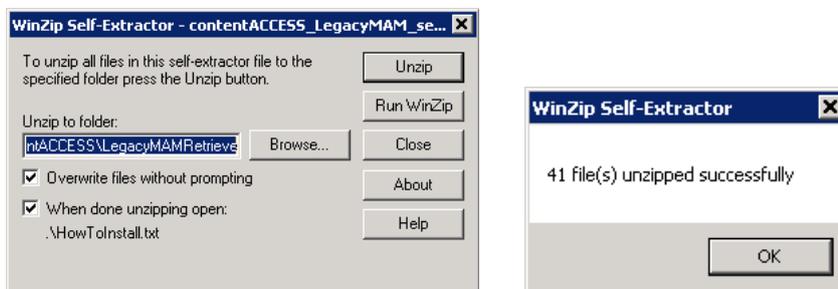


Installing Legacy MAM retrieve service and its configuration on the MAM server

1. In the **Tools** of the contentACCESS setup package click on **Legacy archive connector for email archives/Legacy archive connector for MAM EE** and run the setup package.

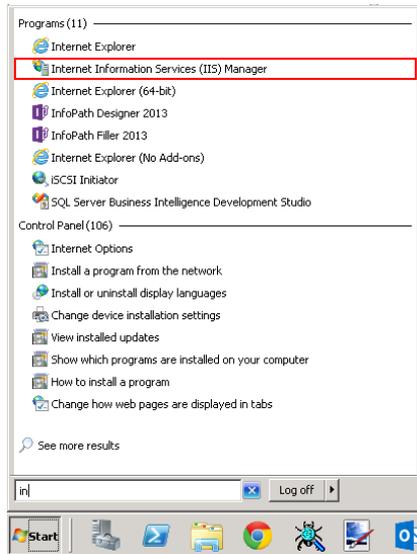


By default it unzips to C:\Program Files\TECH-ARROW\contentACCESS\LegacyMAMRetrieve folder. Click "Unzip". After the files have been successfully unzipped click "OK".

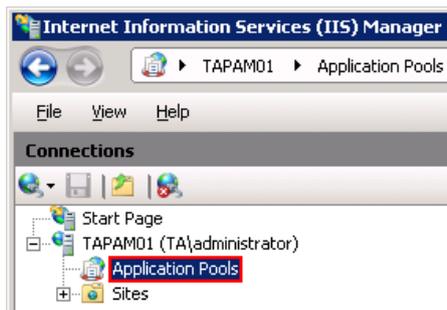


2. A short **HowToInstall** manual will automatically open to help you with installing the server. Follow the next steps of this short step-by-step manual:

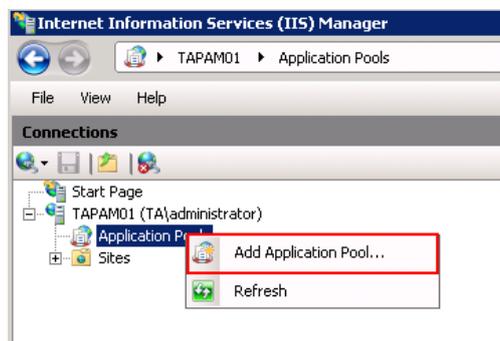
3. Open **Internet Information Services (IIS) manager** from the **Start** menu:



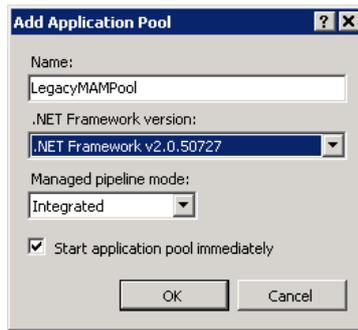
4. Navigate to the following node in the tree on the left side: [SERVER_NAME]\Application Pools:



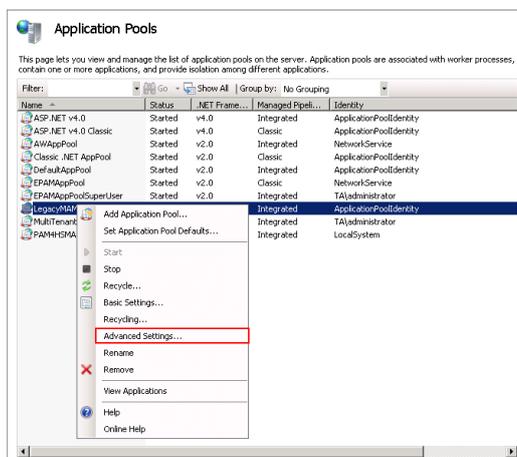
5. Right click on the node **“Application Pools”** and select **“Add Application Pool”**:



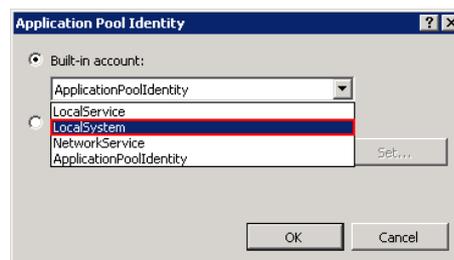
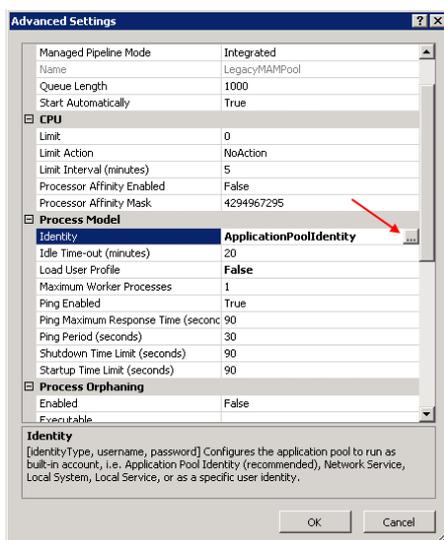
6. The **“Add Application Pool”** window will open. Enter "LegacyMAMPool" as name and select the .NET Framework version from the **.NET Framework version** dropdown list, then click **OK**.



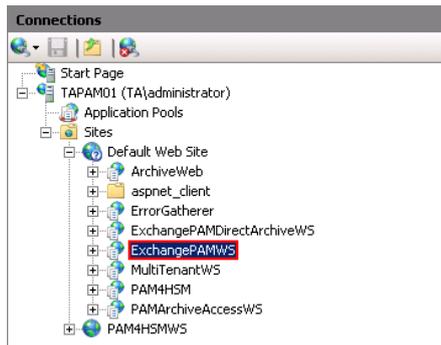
7. Right click on the newly created "LegacyMAMPool" in the grid, and select "Advanced Settings" from its context menu.



8. Change "Identity" to "Local system" built in account in the "Application Pool identity" window, then click "OK".

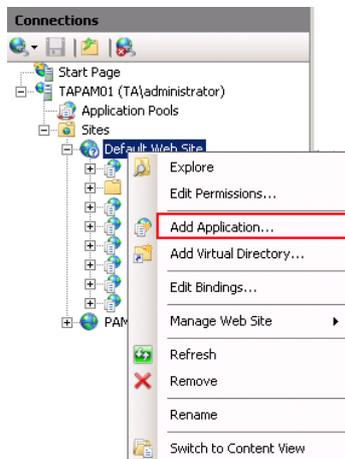


9. Navigate to the following node in the tree on the left side: [SERVER_NAME]\Sites\Default Web Site\ExchangePAMWS:



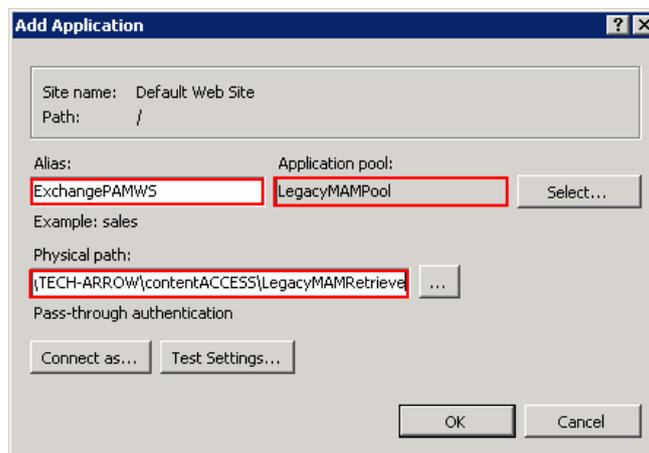
If the ExchangePAMWS is **NOT** found, then:

a) Right click on the “Default Web Site” and click on the "Add Application".



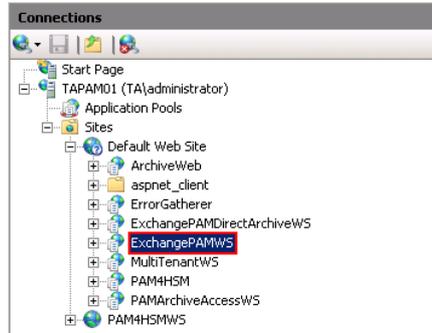
b) Enter “ExchangePAMWS” into alias and “C:\Program files\TECH-ARROW\contentACCESS\LegacyMAMRetrieve” as **Physical path**. Select the “LegacyMAMPool” by clicking the “Select” button.

c) Click “OK”.

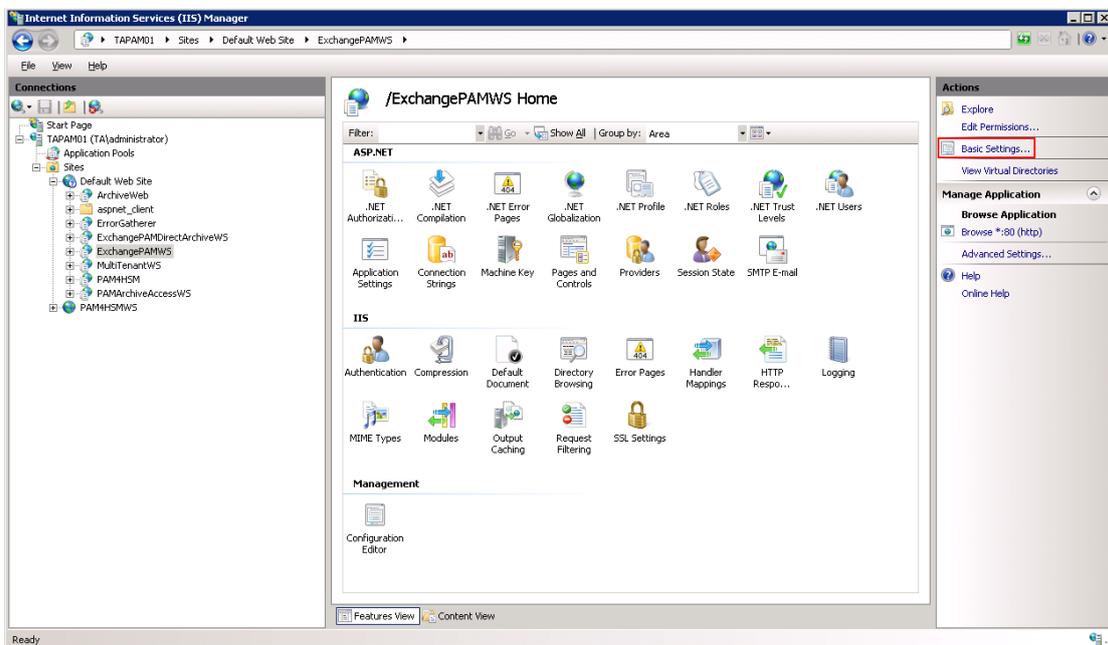


If the ExchangePAMWS is found, then:

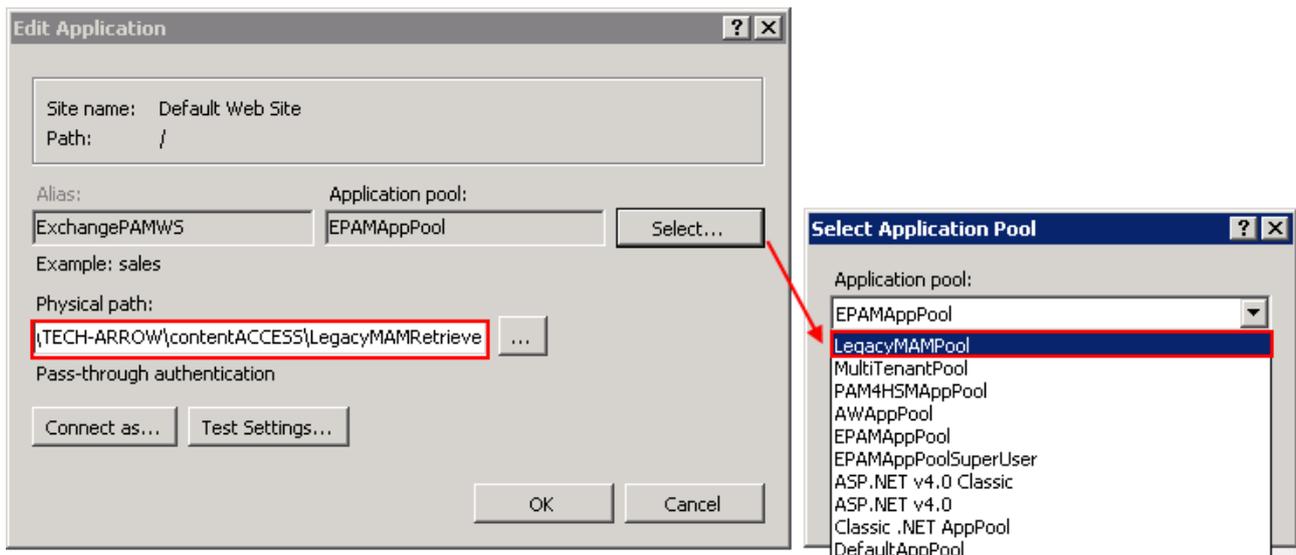
a) Select the "ExchangePAMWS" node by clicking on it.



b) Click "Basic Settings..." in the Actions pane (right side of the IIS Manager).



c) In the "Edit Application" dialog, select the "LegacyMAMPool" by clicking the "Select" button and enter "C:\Program Files\TECH-ARROW\contentACCESS\LegacyMAMRetrieve" into the Physical path textbox.



10. Continue with setting up the MAM server in contentACCESS, which will be explained in the [next section](#).

Configuration of the MAM server in contentACCESS Central Administration:

Configuration in contentACCESS can have 2 forms, based on what you need the system to do:

- 1) In-place replacement of MAM
- 2) Post-migration MAM support

We will explain both forms in this section.

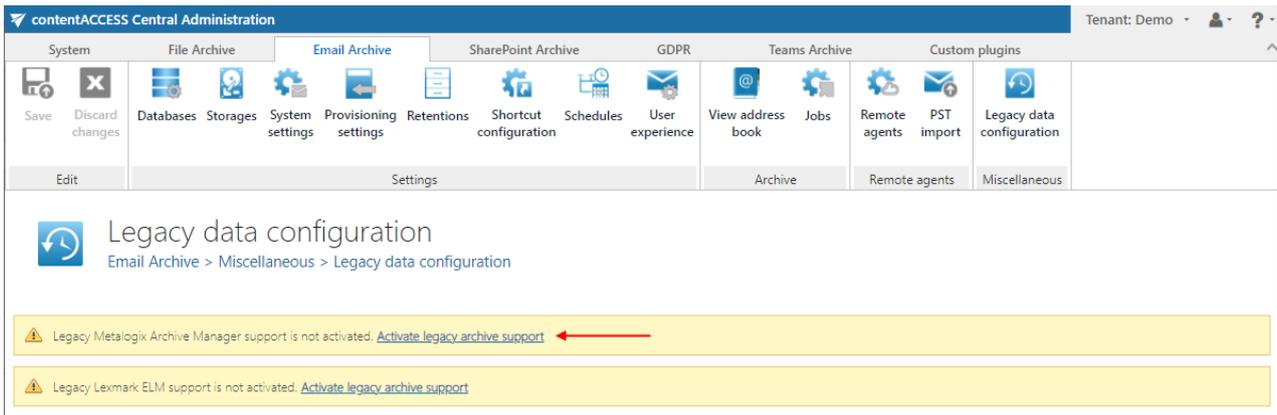
In-place replacement of MAM

- a) Open contentACCESS Central Administration from your browser:

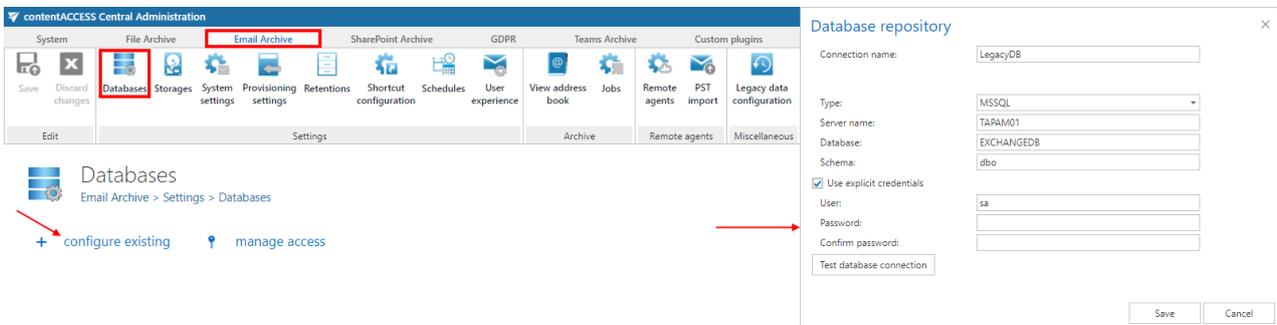
http://[contentACCESSServerName]:3333/CentralAdministration

- b) Navigate to **Email Archive** → **Miscellaneous** → **Legacy data configuration** on the ribbon:

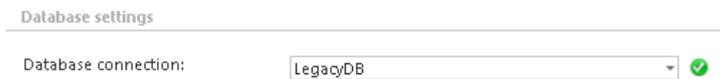
- c) Activate legacy archive support with clicking on the “Activate legacy archive support” option in the warning box.



d) **Database settings:** go to **Email Archive** → **Settings** → **Databases** button on the ribbon, and configure the connection with the old Metalogix database on the MAM server.



e) Navigate back to the **Legacy data configuration** page on the ribbon and select that database connection from the database dropdown list.



Now you can configure the URLs for the MAM retrieve server.

f) **HSM server settings:** Enter the HSM server name into the text field using the following sample:

http://[HSMServerName]/PAM4HSM/PAM4HSMWS.asmx



g) Under **Retrieve settings**, enter the **correct MAM retrieve service URL** using the server name (in our case "test-cd-01.tech-arrow.com"), where the Legacy MAM retrieve service was installed.



Use the following sample: [http://\[MAMServerName\]/exchangePAMWS](http://[MAMServerName]/exchangePAMWS)

Click **“Configure”**. In this step, the contentACCESS will configure the retrieve proxy with the correct parameters.

Retrieve settings

MAM retrieve service url:

✔ Retrieve service successfully configured.

h) **Additional settings:** For this type of configuration, you can leave out these settings.

Additional settings

Require user authentication:

Enable extended support:

i) **The last step is to publish the forms:** use the "FormsInstaller.exe mam" command to publish the legacy forms. Make sure the correct Outlook security registry keys were also applied.

Once the retrieve service installation and its configuration is ready, it will be possible to retrieve the old MAM shortcuts from Outlook/OWA and browse the legacy archive through contentWEB.

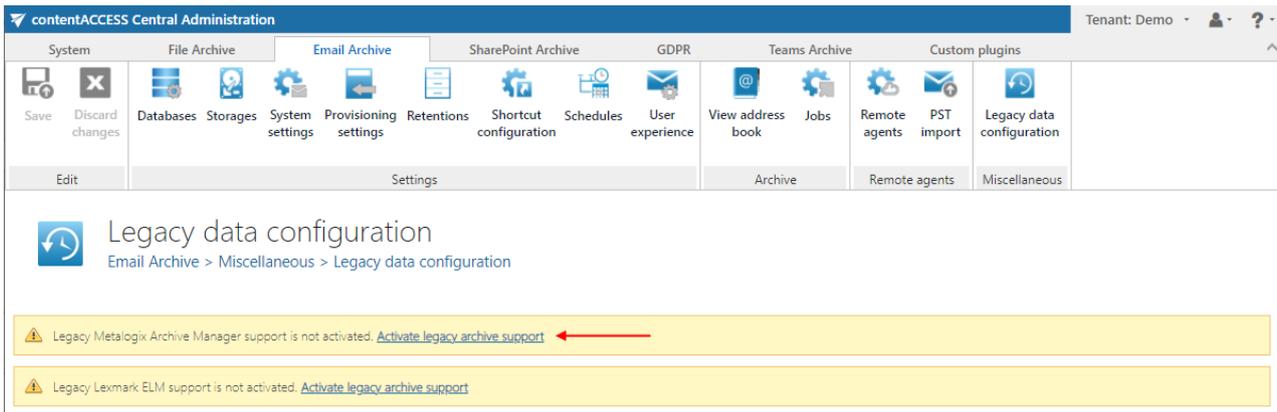
Post-migration MAM support

a) Open contentACCESS Central Administration from your browser:

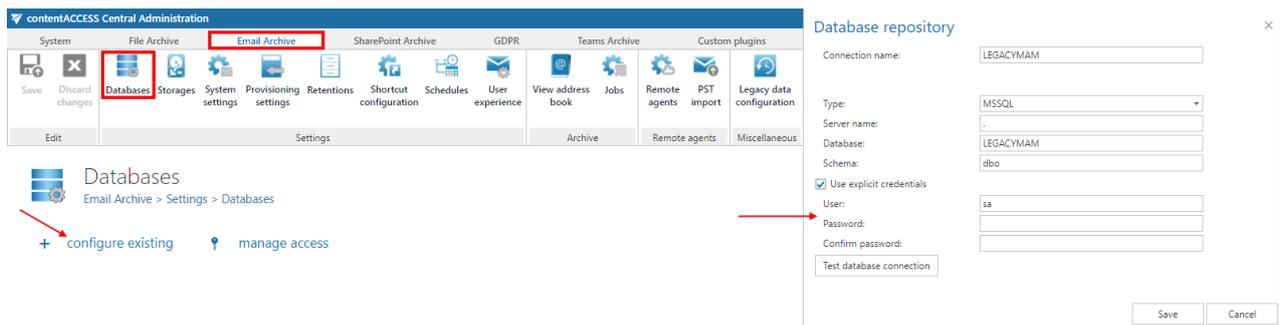
[http://\[contentACCESSServerName\]:3333/CentralAdministration](http://[contentACCESSServerName]:3333/CentralAdministration)

b) Navigate to **Email Archive** → **Miscellaneous** → **Legacy data configuration** on the ribbon:

c) Activate legacy archive support with clicking on the “Activate legacy archive support” option in the warning box.

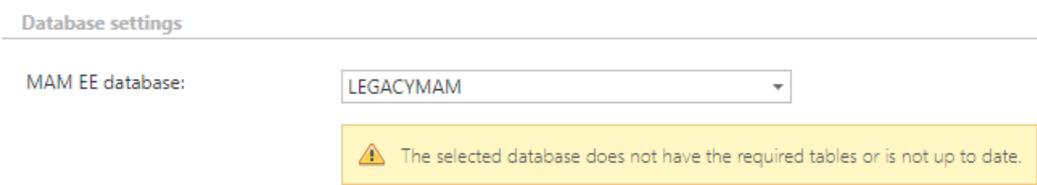


d) **Database settings:** Create a new SQL database, which will hold the information about mapping of MAM documents to contentACCESS databases. Go to **Email Archive** → **Settings** → **Databases** button on the ribbon, and configure the previously created SQL database here.



Important: This database needs to be filled with the mentioned mapping information: ask for professional services to extract the mapping information from the migration database (contentGATE) and import it into the SQL database.

e) Navigate back to the **Legacy data configuration** page on the ribbon and select that database connection from the database dropdown list. It does not necessarily need to work, but it **must be selected here**. The error that you may receive here is expected and OK.





Now you can configure the URLs for the MAM retrieve server.

- f) **HSM server settings:** Enter the HSM server name into the text field using the following sample:

http://[HSMServerName]/PAM4HSM/PAM4HSMWS.asmx

This URL does not need to work but **must be specified here**. The error that you may receive here is expected and OK.

HSM server settings

HSM Server name:

http://test-cd-01.tech-internal/PAM4HSM/PAM4HSI

Failed to connect: The remote name could not be resolved: 'test-cd-01.tech-internal'

Test

- g) Under **Retrieve settings**, enter the **correct MAM retrieve service URL** using the server name (in our case "test-cd-01.tech-arrow.com"), where the Legacy MAM retrieve service was installed.

Use the following sample: [http://\[MAMServerName\]/exchangePAMWS](http://[MAMServerName]/exchangePAMWS)

Click **"Configure"**. In this step, the contentACCESS will configure the retrieve proxy with the correct parameters.

Retrieve settings

MAM EE legacy retrieve service url:

https://test-cd-01.tech-arrow.com/exchangePAMW'

Retrieve service successfully configured.

Configure

- h) **Additional settings:** The **Require user authentication** option should be turned **OFF**. Check the **Enable extended support** checkbox. This enables the possibility to open MAM shortcuts from .msg files after the MAM servers were shut down and migrated to contentACCESS. A database will be required – select the same database you selected in the first step; in our case it is "LEGACYMAM".

Note: When you first select the database here, the control asks you to deploy the database - do so. The version is 5.0.



Additional settings

Require user authentication:

Enable extended support:

Mapping database:

LEGACYMAM

Change



Connection successful!

Test

- i) **The last step is to publish the forms:** use the "FormsInstaller.exe mam" command to publish the legacy forms. The setup can be found in **C:\TECH-ARROW5.0.5\contentACCESS_Package\Setups\Forms\GATE.FormsSetup.exe**. Make sure the correct Outlook security registry keys were also applied.

After this installation, if you click on any MAM shortcut, it will open the correct contentACCESS email. It will also be possible to retrieve the old MAM shortcuts from Outlook/OWA and browse the legacy archive through contentWEB.



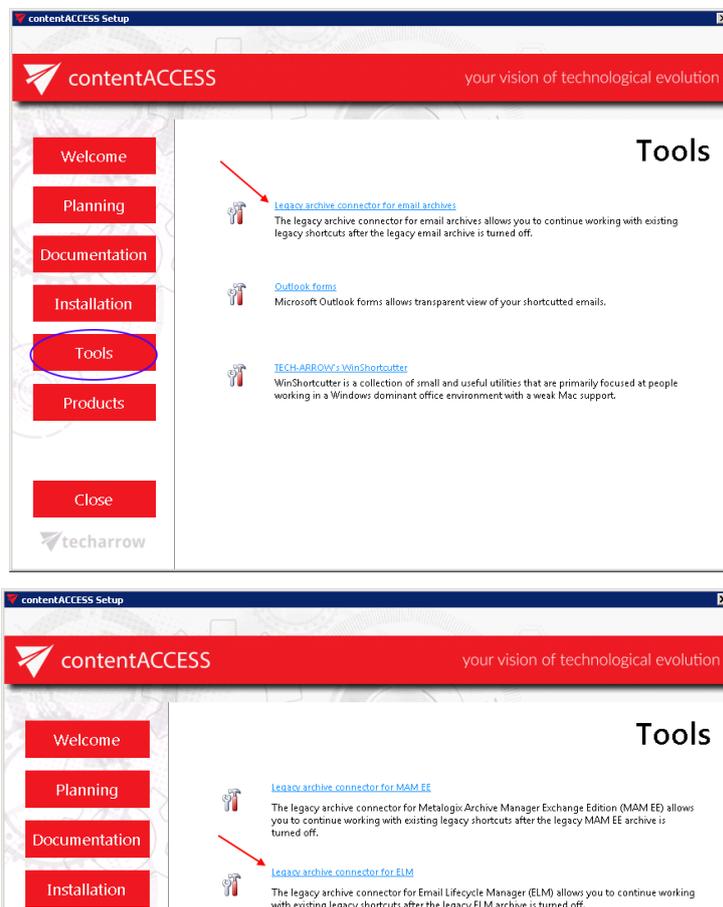
Legacy archive connector for Email Lifecycle Manager (ELM)

This service is used to access archived files from the legacy ELM shortcuts, if you have uninstalled Email Lifecycle Manager from your computer, and you need to check the archive contents.

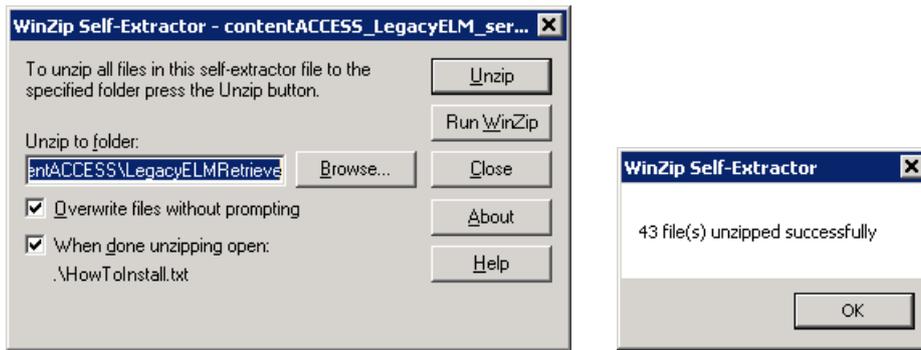
Installing Legacy ELM retrieve service on the ELM server and its configuration

In this use case the ELM is installed on server *taelm01*. The retrieve service will be installed on the same server as it is recommended by us.

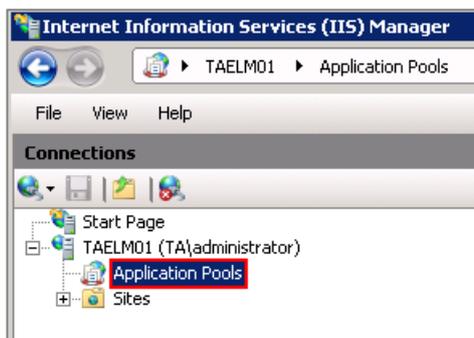
1. In the **Tools** of the contentACCESS setup package click on **Legacy archive connector for email archives/Legacy archive connector for ELM** and run the setup package.



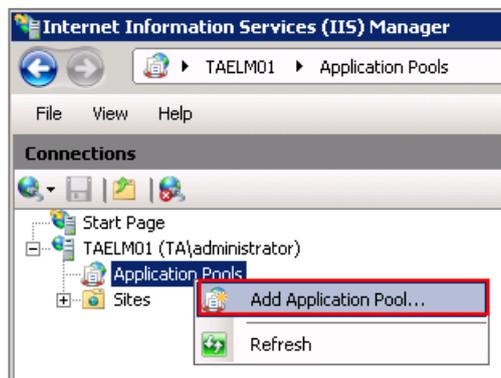
By default it unzips to C:\Program Files\TECH-ARROW\contentACCESS\LegacyELMRetrieve folder. Click "Unzip". After the files have been successfully unzipped click "OK".



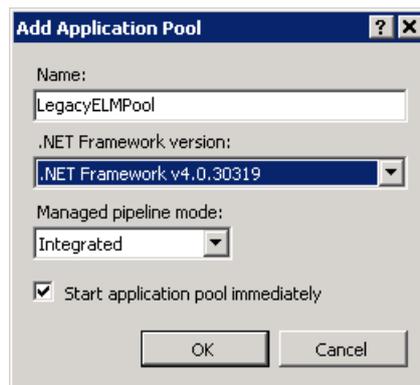
2. A short **HowToInstall** manual will automatically open to help you with installing the server. Follow the next steps of this short step-by-step manual:
3. Open **Internet Information Services (IIS) manager** from the **Start** menu:
4. Navigate to the following node in the tree on the left side: [SERVER_NAME]\Application Pools:



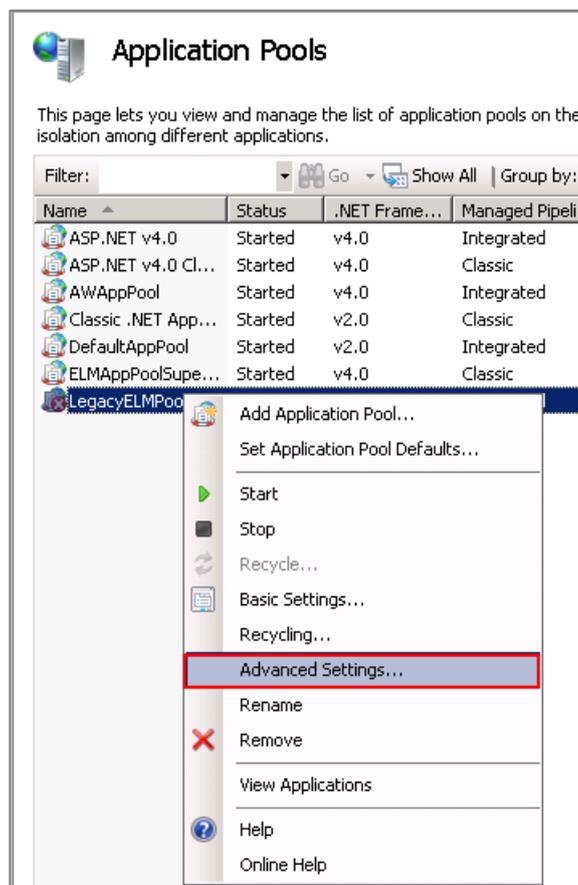
5. Right click on the node “**Application Pools**” and select “**Add Application Pool**”:



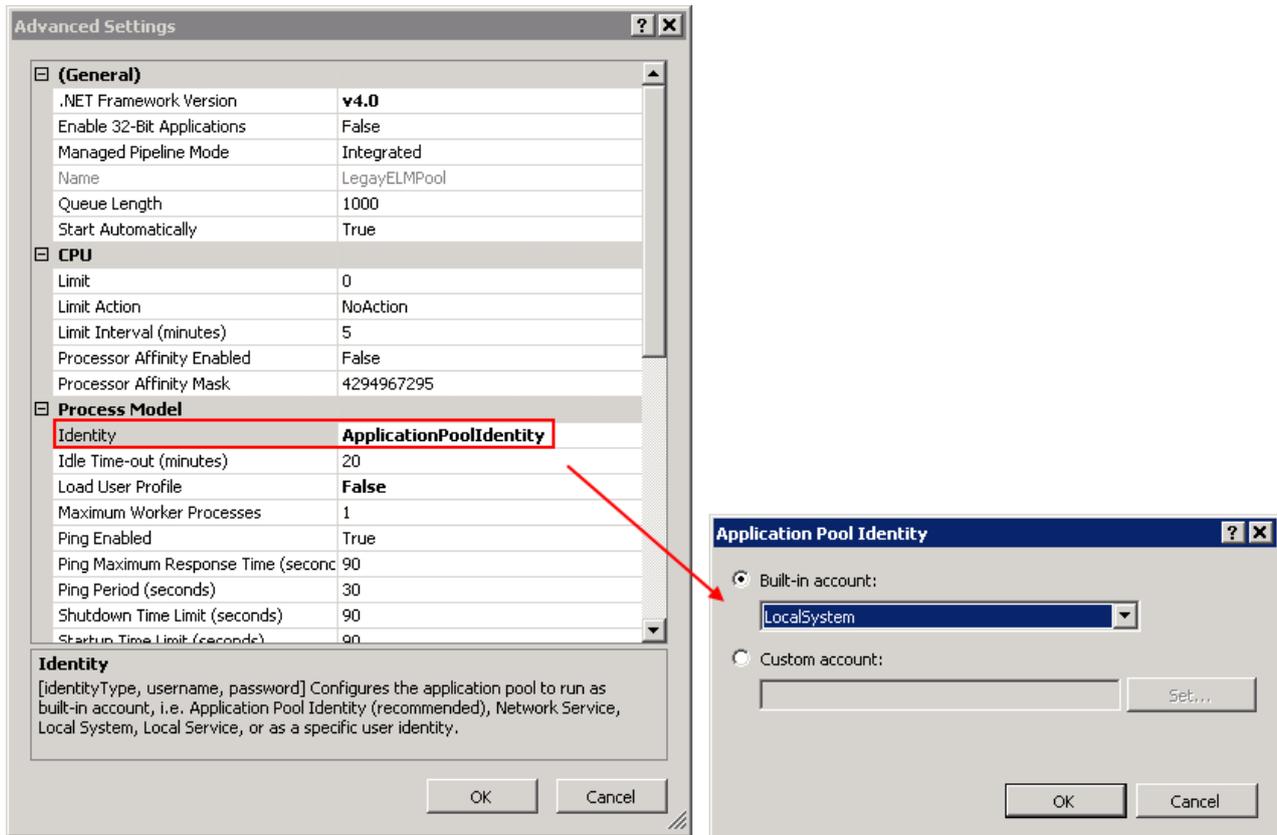
6. The “**Add Application Pool**” window will open. Enter "LegacyELMPool" as name and select the .NET Framework version from the **.NET Framework version** dropdown list, then click **OK**.



- Right click on the newly created "**LegacyELMPool**" in the grid, and select "**Advanced Settings**" from its context menu.



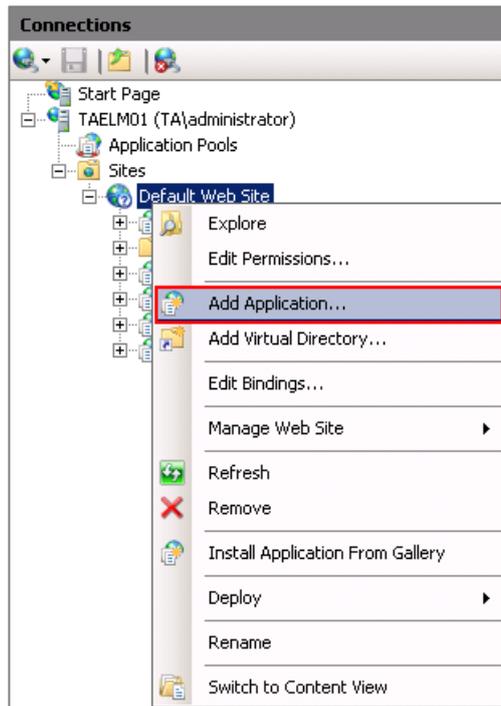
- Change "**Identity**" to "**Local system**" built in account in the "**Application Pool identity**" window, then click "**OK**".



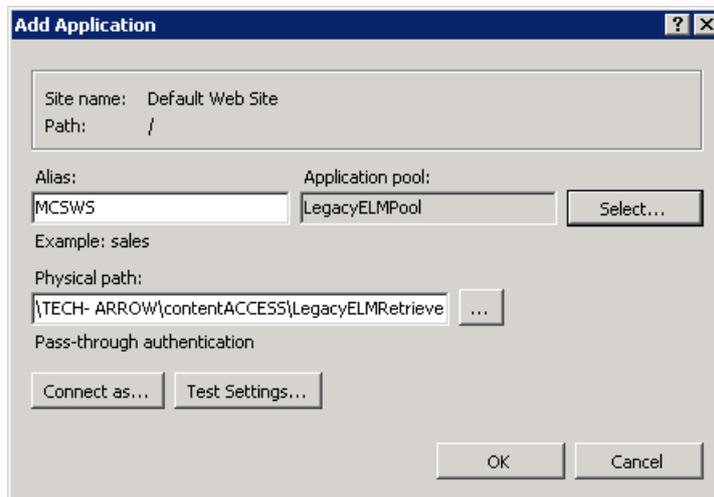
9. Navigate to the following node in the tree on the left side: [SERVER_NAME]\Sites\Default Web Site\MCSWS:

If the MCSWS is **NOT** found, then:

- a) Right click on the “**Default Web Site**” and click on the “**Add Application**”.

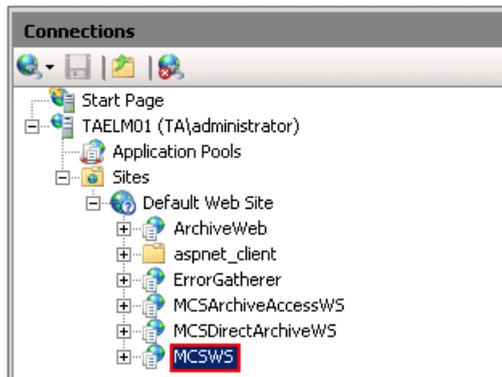


- b) Enter "MCSWS" into alias and "C:\Program files\TECH- ARROW\contentACCESS\LegacyELMRetrieve" as **Physical path**. Select the "**LegacyELMPool**" by clicking the "**Select**" button.
- c) Click "**OK**".

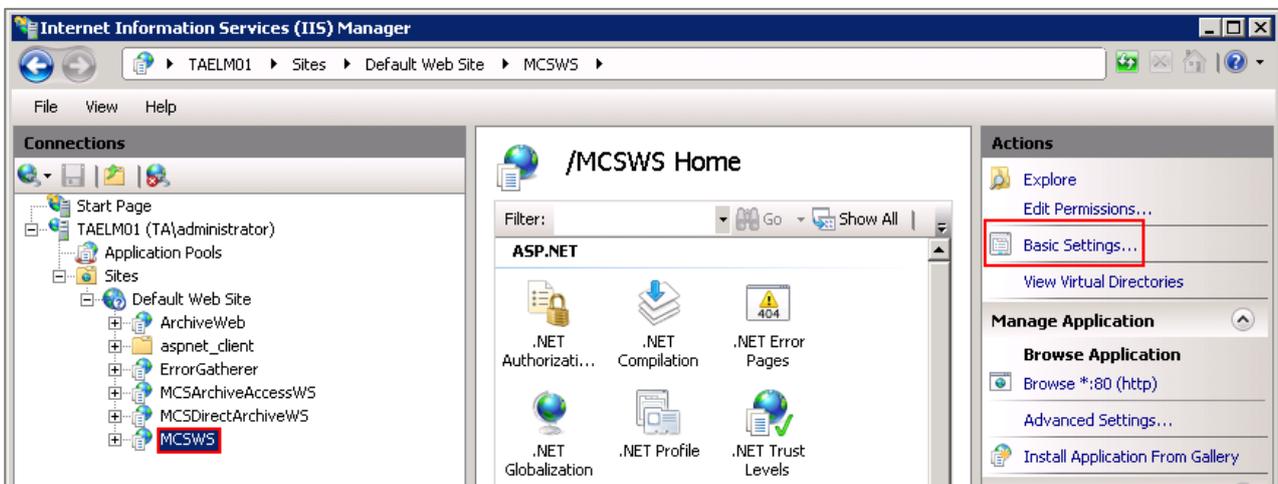


If the MCSWS is found, then:

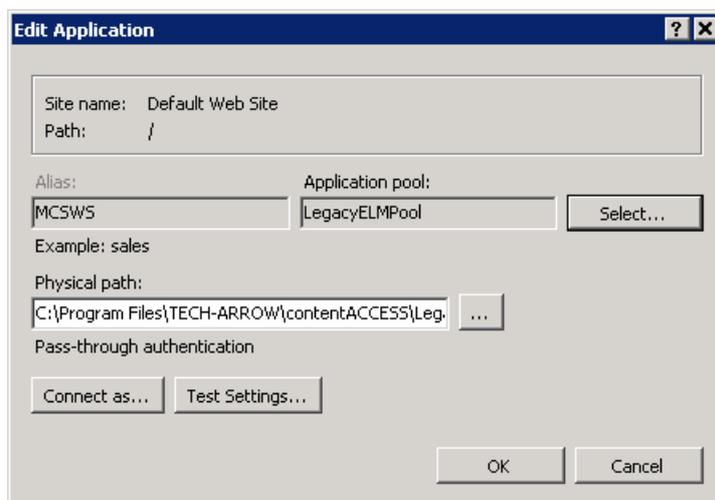
- a) Select the "**MCSWS**" node by clicking on it.



b) Click "Basic Settings..." in the Actions pane (right side of the IIS Manager).



c) In the "Edit Application" dialog, select the "LegacyELMPool" by clicking the "Select" button and enter "C:\Program Files\TECH-ARROW\contentACCESS\LegacyELMRetrieve" into the Physical path textbox.

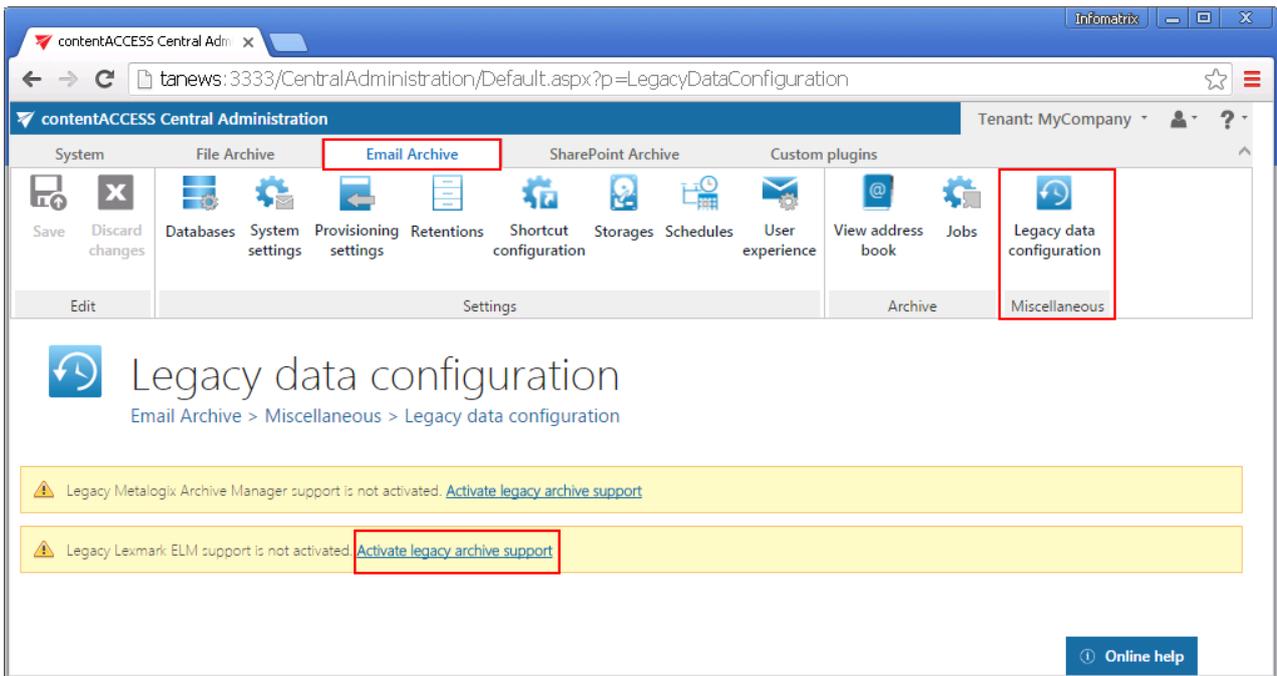


10. Continue with setting up the ELM server in contentACCESS:

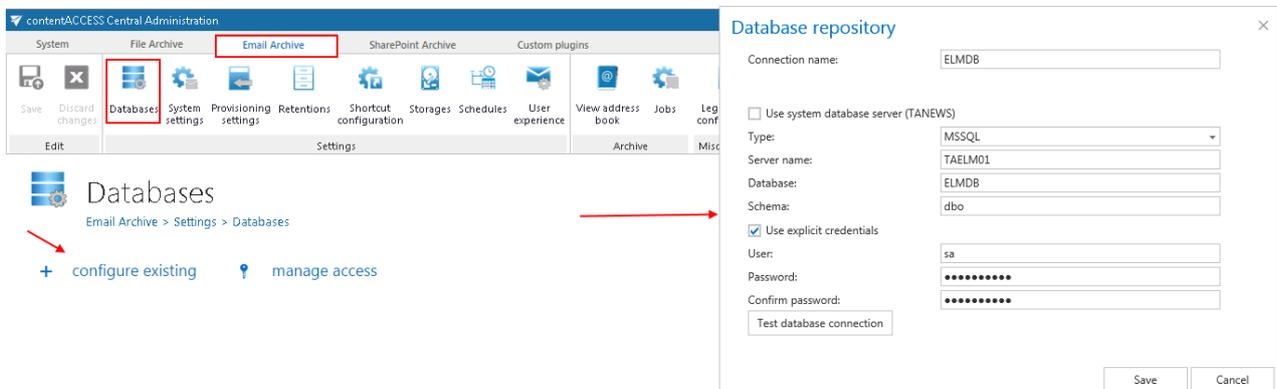


Configuration of the ELM server in contentACCESS Central Administration:

- a. Open contentACCESS Central Administration from your browser:
[ServerName]:3333/CentralAdministration
- b. Navigate to **Email Archive** → **Miscellaneous** → **Legacy data configuration** on the ribbon:
- c. Activate legacy ELM archive support with clicking on the “Activate legacy archive support” option in the warnings box.



- d. **Database settings:** go to **Email Archive** → **Settings** → **Databases** button on the ribbon, and configure the connection with the old ELM database on the ELM server (in our case with *taelm01*).

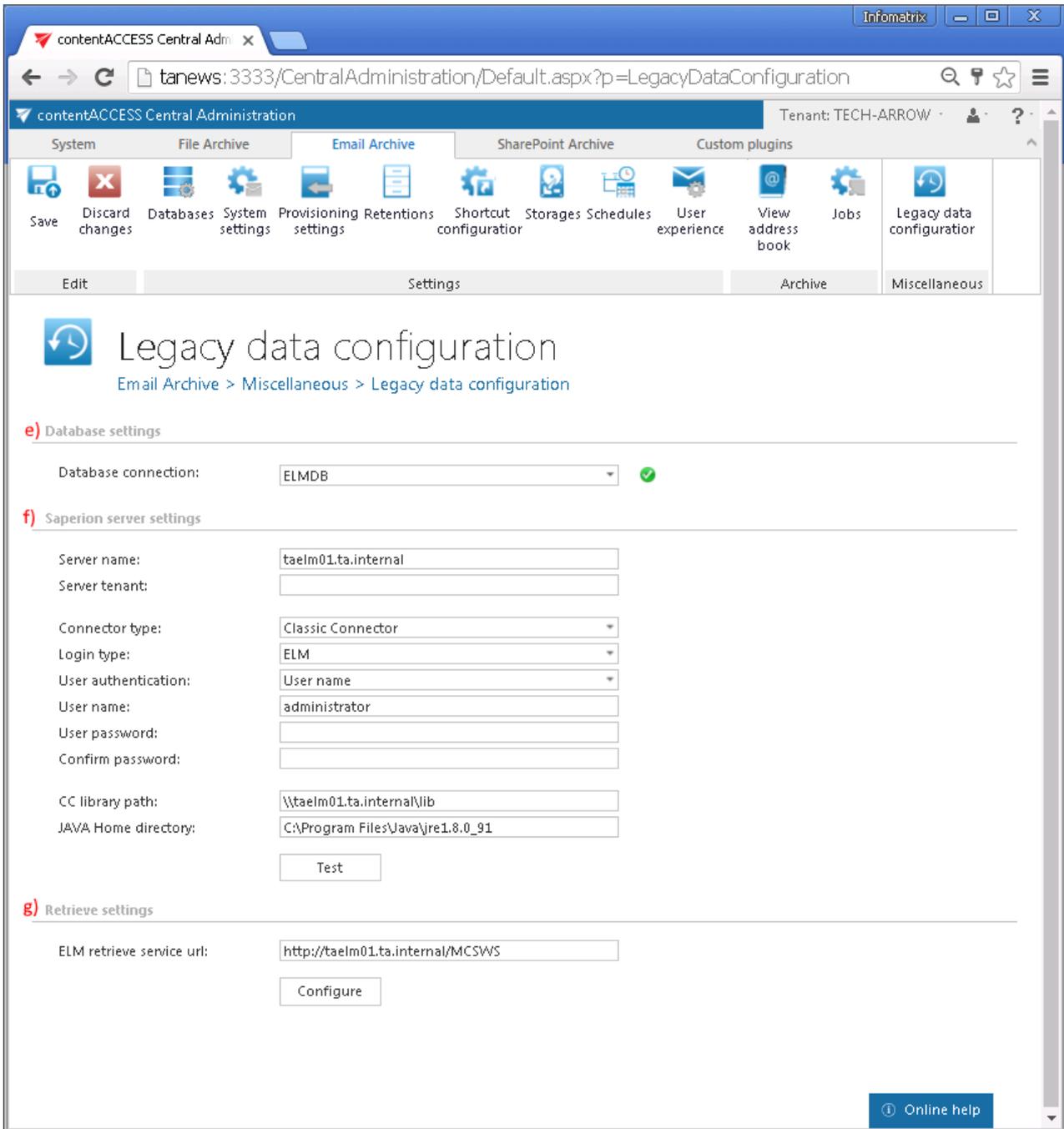




- e. Go back to the **Legacy data configuration** page on the ribbon, and set the connection with the ELM database (ELMDB from step *d*) above) in the **Database settings** section.
- f. In section **Saperion server settings** set the connection with the Saperion server. Set the values based on your configurations on the Saperion server. The connector has some prerequisites:
 - JRE x64 on the contentACCESS server (Check if folder exists: "C:\Program Files\Java\jre X.X") – to be configured in section **JAVA Home directory**
 - Need the ELM references, but it could be also referenced directly from the ELM machine. This is the path on which the Classic Connector jar files can be reached, e.g. *c:\Program Files\SAPERION\Application\scr\scr-classicconnector\lib* – to be configured in section **CC library path**.

Also run a test connection to verify the connection with the Saperion server.

- g. In section **Retrieve settings** enter the ELM retrieve service URL using the following sample: [http://\[ELMServerName/MCSWS\]/](http://[ELMServerName/MCSWS]/) and click on **Configure**.



The screenshot shows the 'Legacy data configuration' page in the contentACCESS Central Administration interface. The page is titled 'Legacy data configuration' and is part of the 'Email Archive > Miscellaneous > Legacy data configuration' path. It contains three main sections for configuration:

- e) Database settings:** A dropdown menu for 'Database connection' is set to 'ELMDB' with a green checkmark next to it.
- f) Saperion server settings:** A form with the following fields:
 - Server name:
 - Server tenant:
 - Connector type:
 - Login type:
 - User authentication:
 - User name:
 - User password:
 - Confirm password:
 - CC library path:
 - JAVA Home directory:
 A 'Test' button is located below the JAVA Home directory field.
- g) Retrieve settings:** A text input field for 'ELM retrieve service url' is set to 'http://taelm01.ta.internal/MCSWS'. A 'Configure' button is located below the field.

An 'Online help' button is visible in the bottom right corner of the interface.

Once the installation of the service and its configuration is ready, it will be possible to

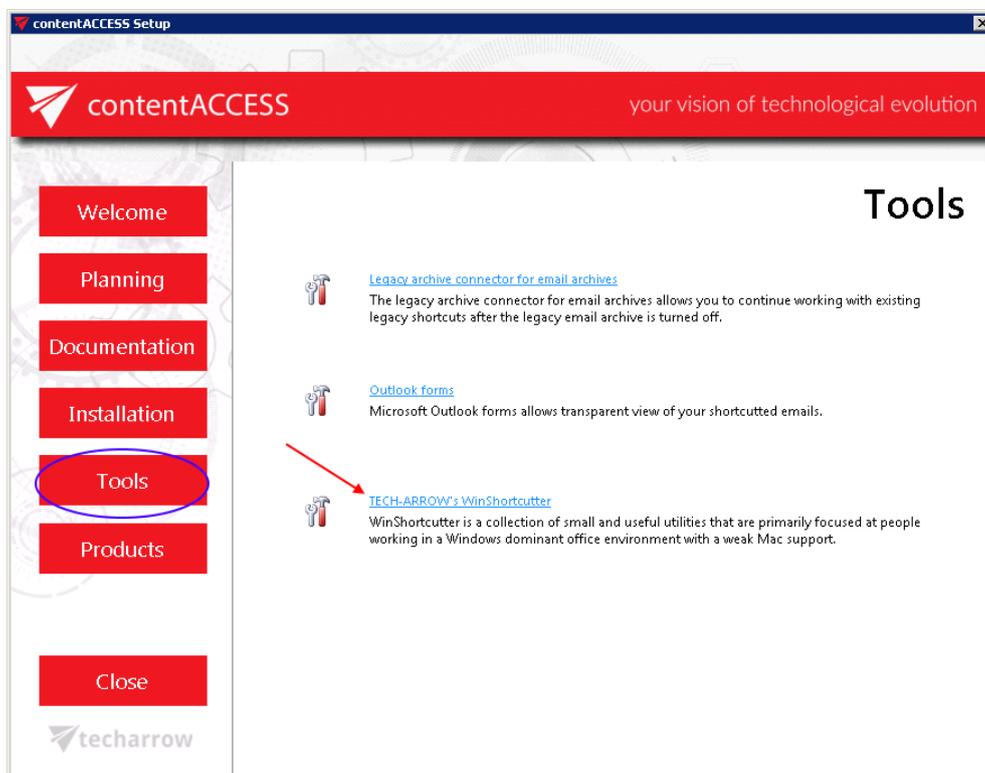
- retrieve the old ELM shortcuts in Outlook/OWA (necessary MS Outlook/OWA integration need to be also installed, see more [here](#)) and
- browse the legacy archive using contentWEB.



Installing TECH-ARROW's WinShortcutter

What is TECH-ARROW's WinShortcutter? It is a collection of small and useful utilities that are primarily focused on people working in a Windows dominant office environment with a weak MAC support. With this application you can open Windows shortcut files (.lnk files) on Apple OS X operating system and also shortcut files created by contentACCESS File Archive.

To install it, open the **Tools** in the contentACCESS setup window, and click on option WinShortcutter.



For further information **about the application please** refer to the TECH-ARROW's WinShortcutter Manual [here](#).



contentACCESS Outlook add-in

What is contentACCESS Outlook add-in? Outlook add-in is an application that allows the user to retrieve items from the archive, to capture actions as forwarding or replying to retrieved items, and update changes in the archive database and in the shortcut item. Currently there are supported only message class changes when retrieved item is sent away (forward or reply).

Note: Add-ins are **not supported** by In-Place Archive mailboxes in Outlook.

There are some terms which may need further explanation:

- **Message class** – type of the item in the mailbox. The message class defines which kind of form will be used to render the item in Outlook, OWA and other clients
- **Outlook form** – each message in Outlook is rendered using a form. There are standard forms (Note, Post, etc.) and there are custom forms. The custom forms are derived from the standard ones and are extending the standard functionality
- **contentACCESS Outlook form** – custom Outlook form belonging to contentACCESS
- **Standard shortcut** – type of archiving when the message class of the item is changed by contentACCESS
- **Primary mailbox** – the main mailbox in the Outlook profile
- **Additional mailbox** – the user can load additional mailboxes to Outlook profile next to the primary mailbox. Select Account settings in Outlook, change existing profile and add the next mailbox to the profile (you need to have permission to access the selected mailbox)
- **Shared Folder** – one Exchange account can share folders in his account with other people on the same Exchange server

Installation of contentACCESS Outlook add-in

First, follow [this](#) guide to help you with installing contentACCESS.

Note: To use the add-in, the user must install the [Outlook forms](#) as well.



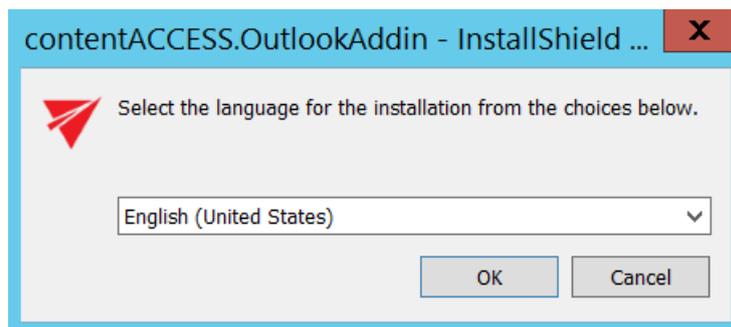
The following prerequisites should be present on the machine(s) where you want to use the Outlook add-in to make it work correctly:

- .NET 4.8
- Visual Studio 2010 Tools for Office Runtime 10.0.60724 (can be downloaded [here](#))

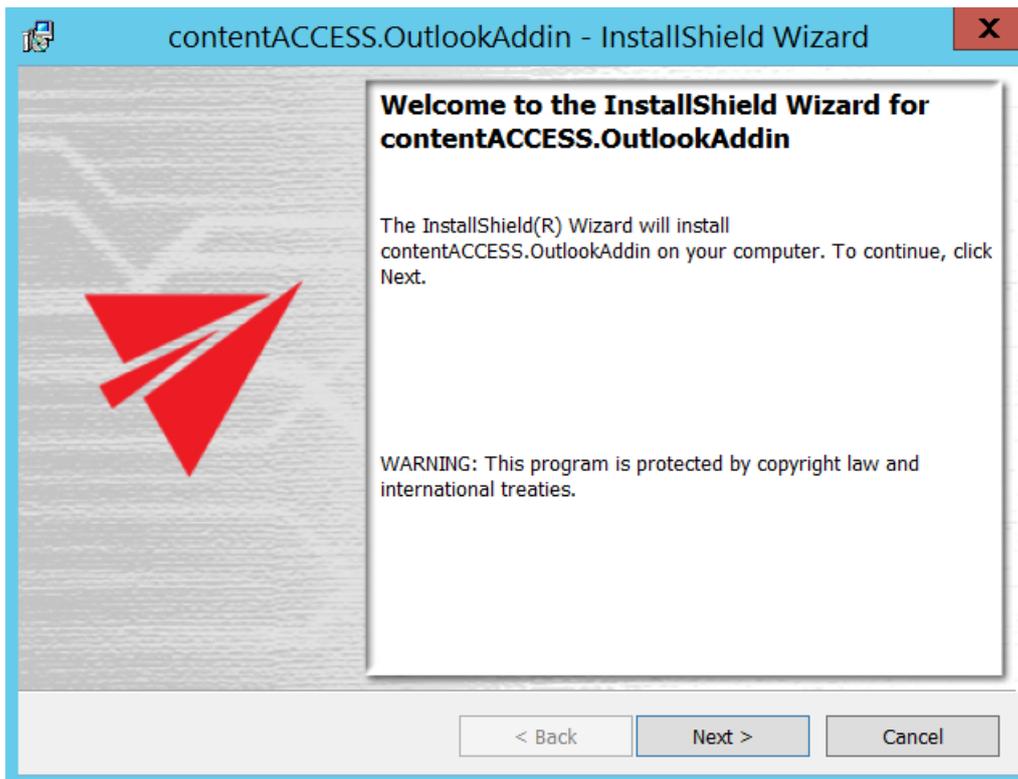
Next, you need to go to **C:\TECH-ARROW\contentACCESS_Package\Setups** or locate the folder to which you unzipped **contentACCESS_Package** when installing contentACCESS. Find and run the file with name **contentACCESS.OutlookAddin_x64** (if using 64bit Outlook) or **contentACCESS.OutlookAddin_x86** (if using 86bit Outlook).

Note: Outlook add-in is installed using an Administrator account and doesn't have to be installed for every user profile separately.

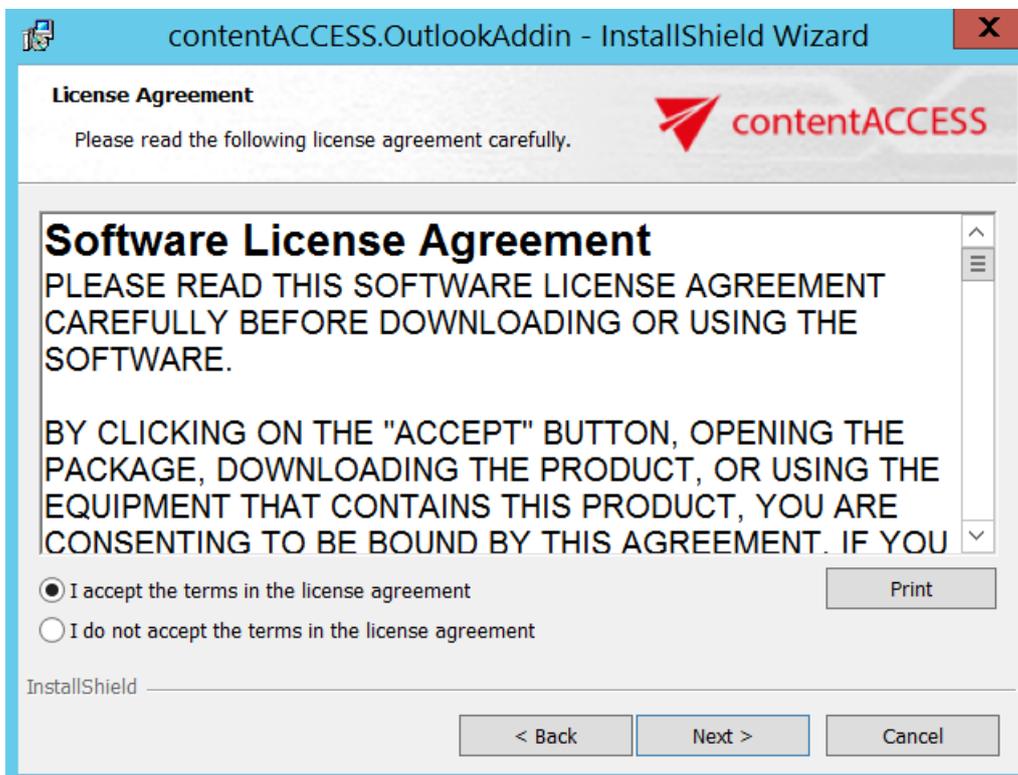
1. Choose the language that you will be using - English or German.



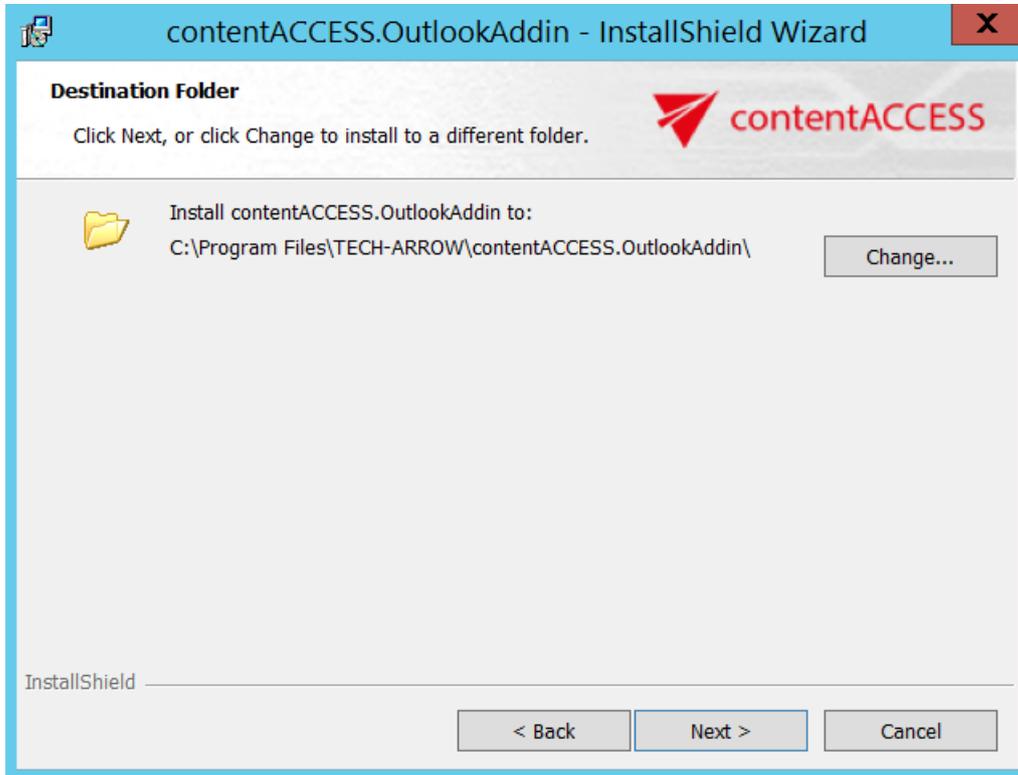
2. Click **Next**.



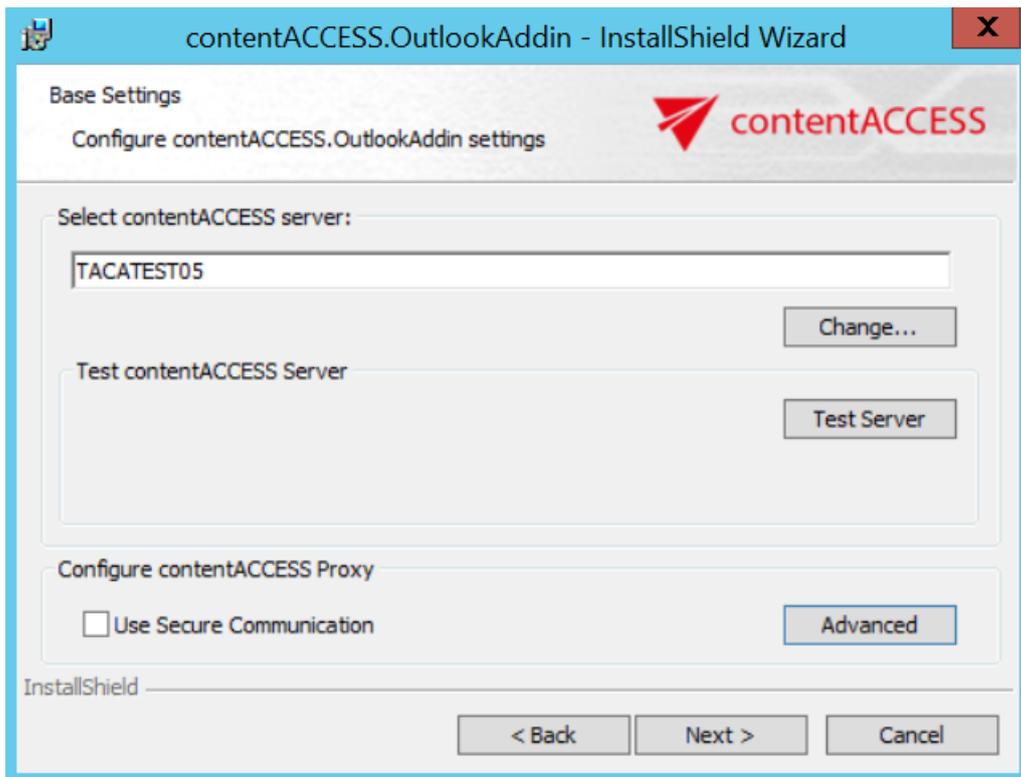
3. Choose **I accept the terms in the license agreement** and click **Next**.



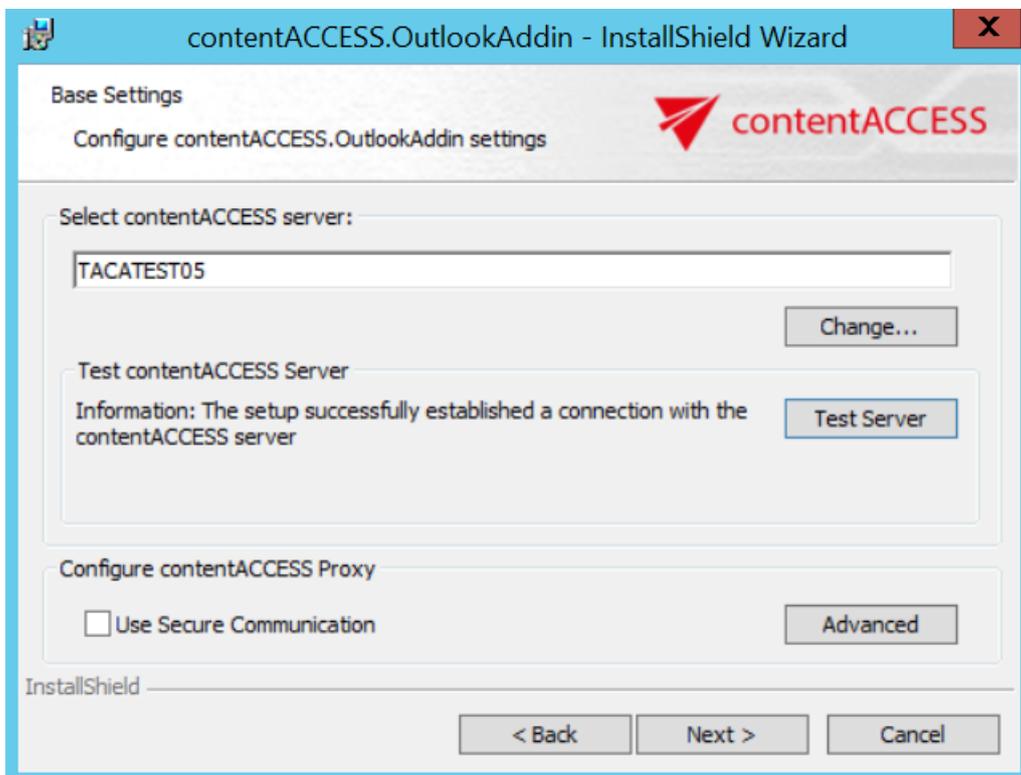
- Here you can choose the folder, to which Outlook add-in will be installed. We recommend to leave it like this. Click **Next**.



- Type the name of contentACCESS server you are using (in this case we used TACATEST05).



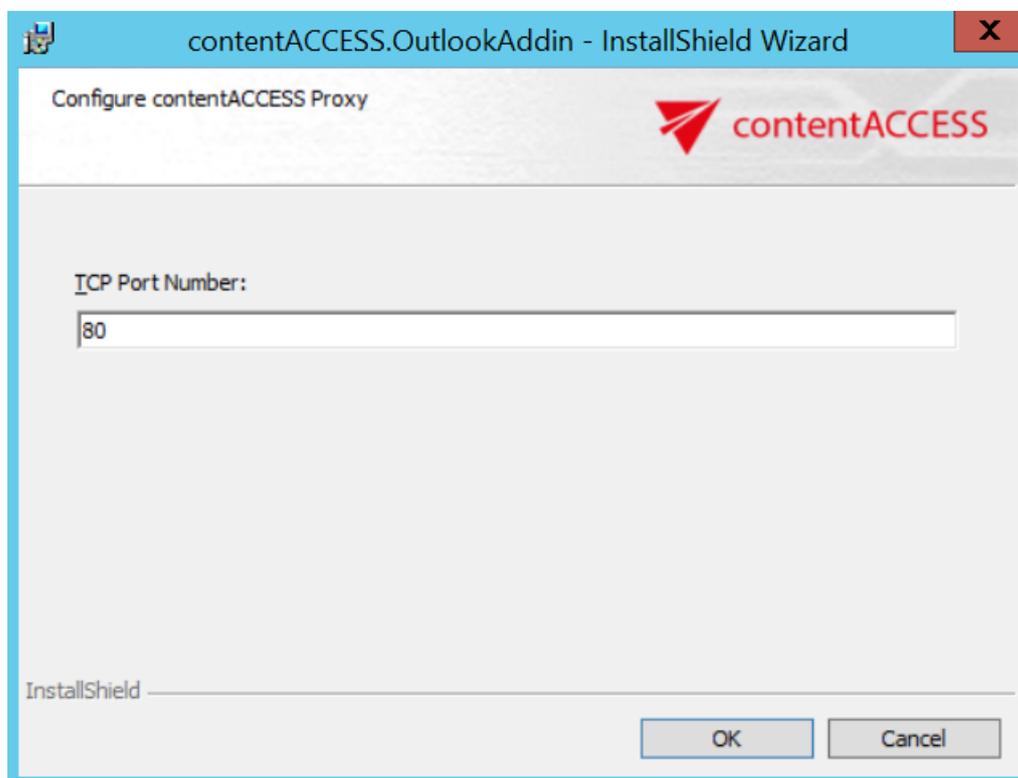
Click on **Test Server**. This will show you if the connection with contentACCESS server was established.



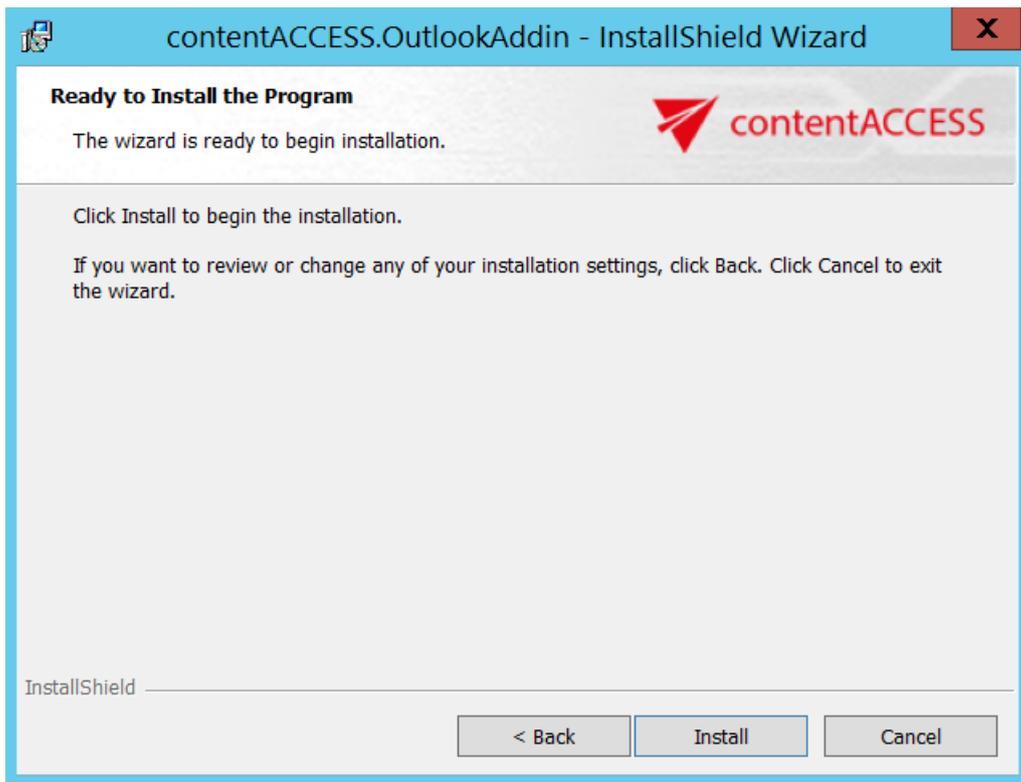


When clicking on **Advanced**, you can specify the TCP port number. If you check the **Use Secure Communication** option, the port number will be 443, if not, the port number will be 80. You can also specify a custom port number. Click on **OK** and then **Next**.

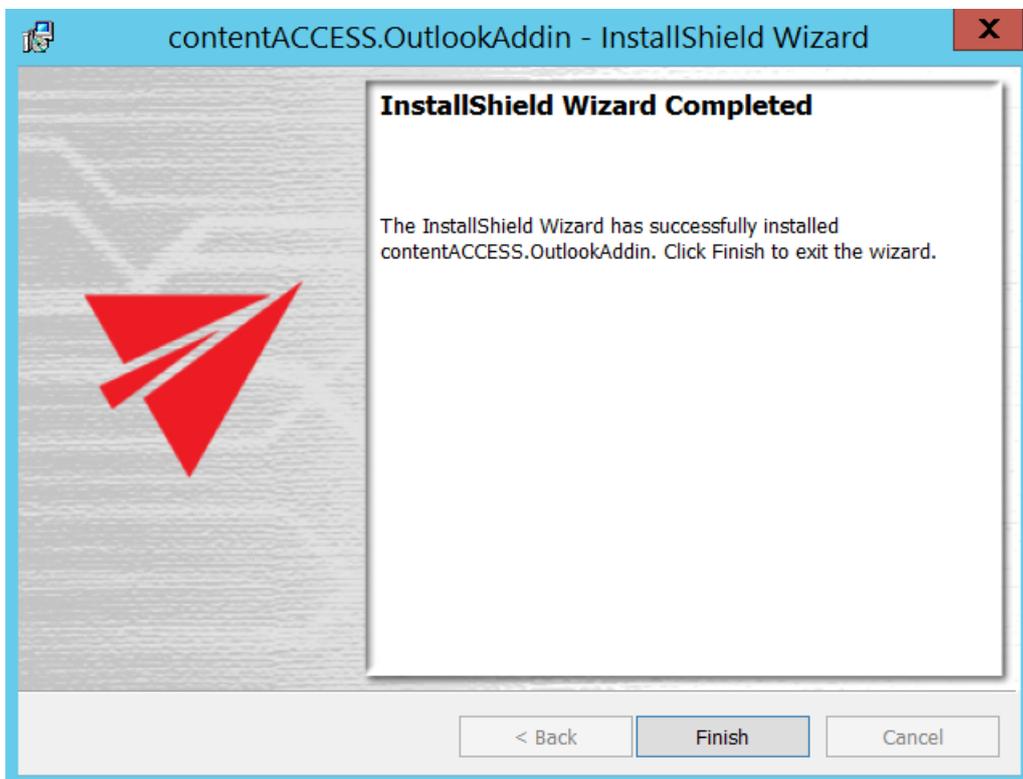
Note: These settings must match the settings that you used when configuring [contentACCESS Proxy settings](#). So if you used HTTPS, then the option **Use Secure Communication** must be checked. If you specify a custom port number here, you also have to change it in **System** settings (**System** tab → **Services** group → **System** page, section **External accessibility settings: Retrieve server FQDN**) in the Central Administration, otherwise contentACCESS Outlook add-in won't work.



6. Click on **Install**.



7. Click on **Finish** to complete the installation process.





Note: If you have repaired or updated the contentACCESS Outlook add-in, always restart Outlook under each profile. The new features will be available only after Outlook restart.

Note: contentACCESS Outlook add-in can be also installed via silent installation. The **silent installation command** is:

```
contentACCESS.OutlookAddin.exe /v"USESECURE=1 CASERVER="[SERVERNAME]"  
CASERVERPORT="[CUSTOMNUMBER]" /l*v log.txt /qn
```

Parameters:

- USESECURE - with or without SSL
- CASERVER - contentACCESS server name
- CASERVERPORT - not mandatory, the defaults are the 80 (if USESECURE = 0) or 443 (USESECURE = 1) ports
- /qn is for the silent installation
- /l*v log.tx – logging

If nothing is defined, then setup will be installed with default values.

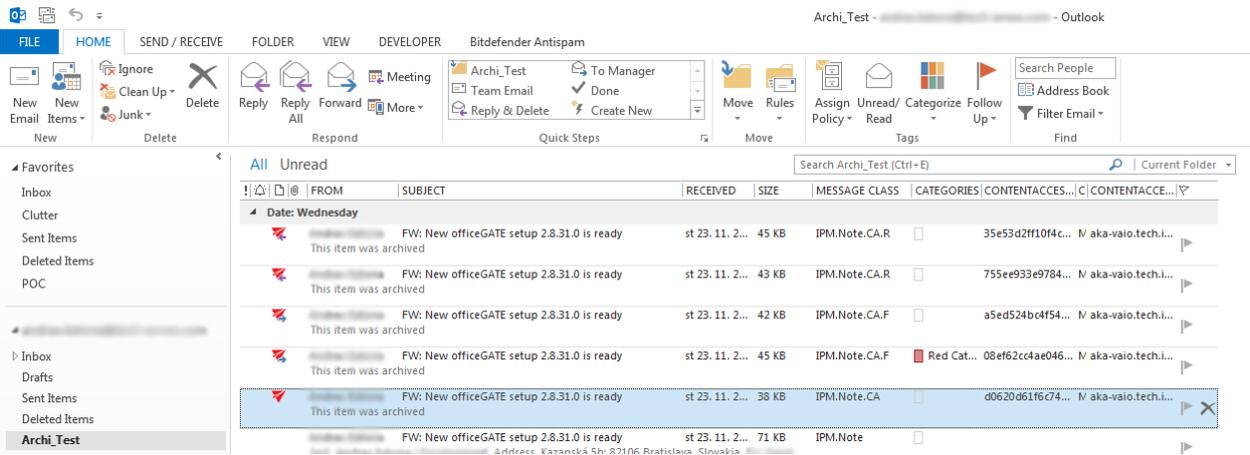
How to use contentACCESS Outlook add-in

Important: For now, contentACCESS Outlook add-in works only with [Windows authentication](#). It means that Windows authentication should be set up correctly and Windows user should be present in contentACCESS.

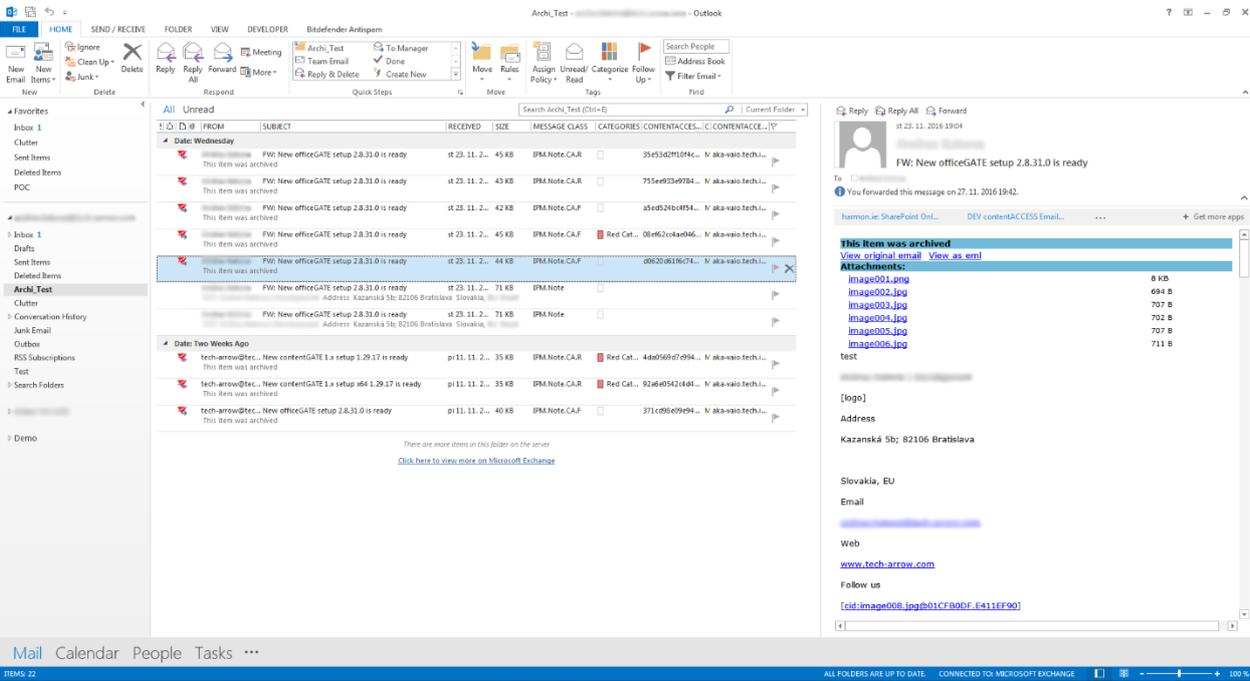
When a user forwards or replies a message archived using HTML or Normal shortcut, the records are updated in the archive database with the appropriate changes, and also the shortcuts are updated in the owner's mailbox.

Some possible scenarios are:

1. **Shortcut is in the primary mailbox** – add-in updates shortcut in the primary mailbox

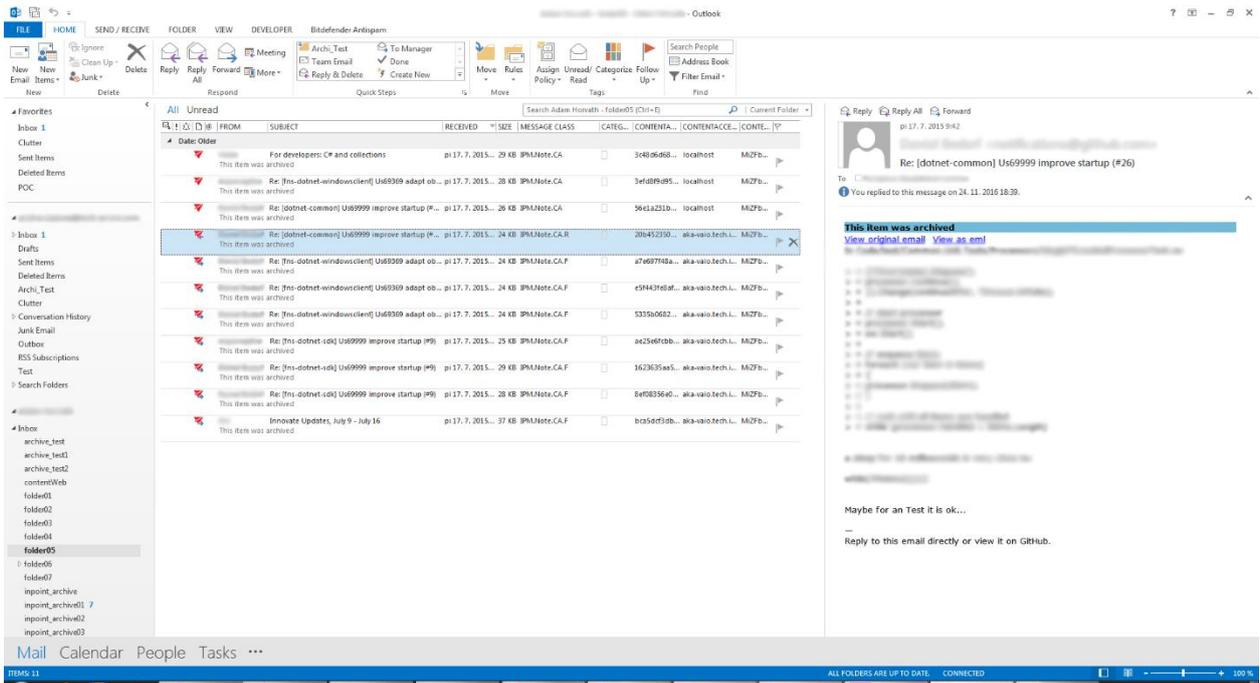


Screenshot.1. Shortcut in primary mailbox (message class IPM.Note.CA)

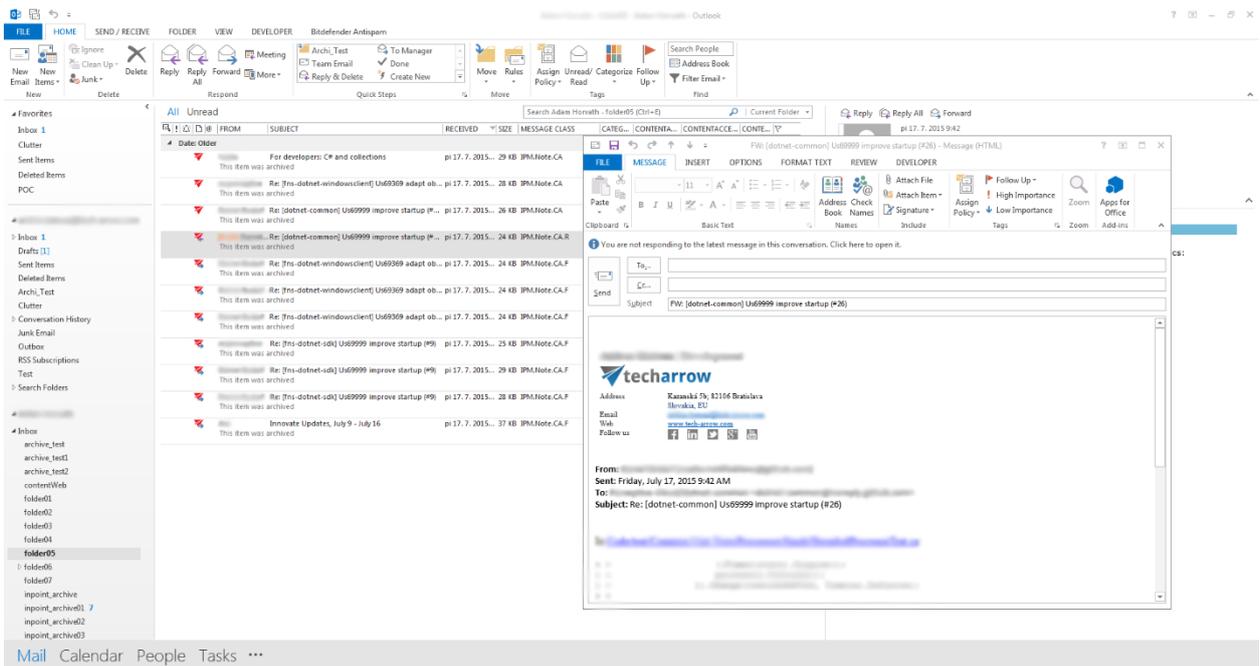


Screenshot.2. Shortcut in primary mailbox after retrieve and forward (message class IPM.Note.CA.F)

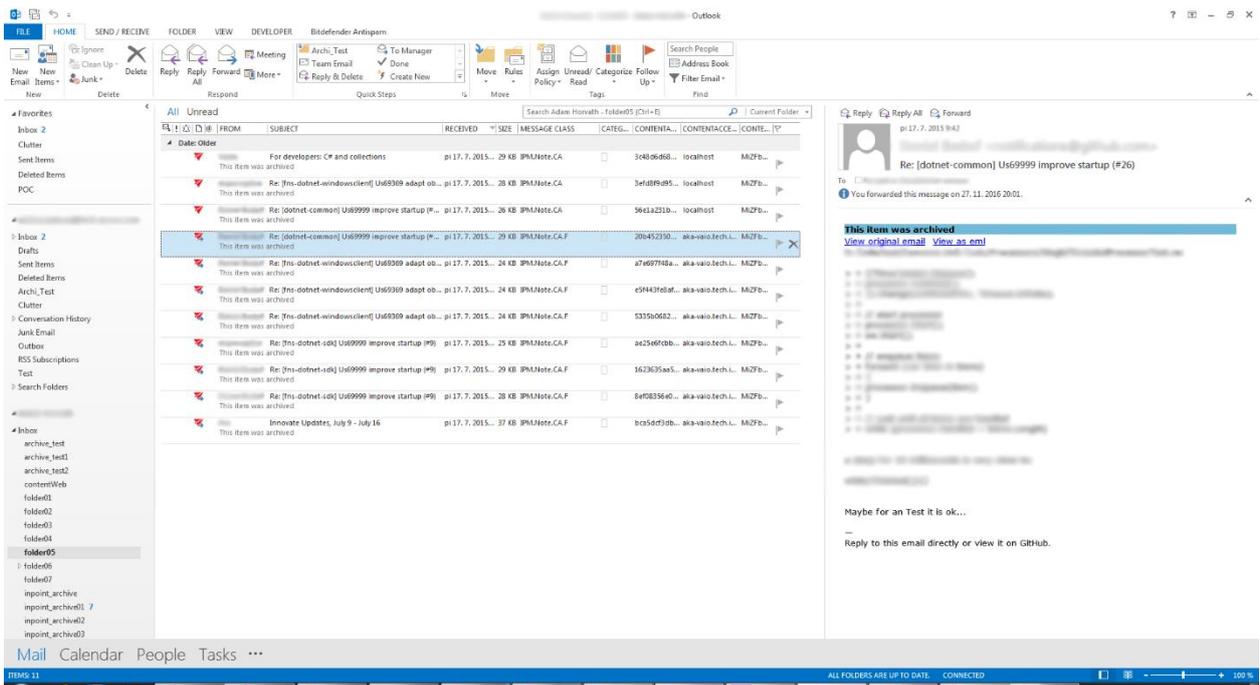
2. Shortcut is in the additional mailbox or shared folder – add-in updates shortcut in the shortcut’s owner mailbox



Screenshot.3 Shortcut is in additional mailbox (org. message class is IPM.Note.CA.R)

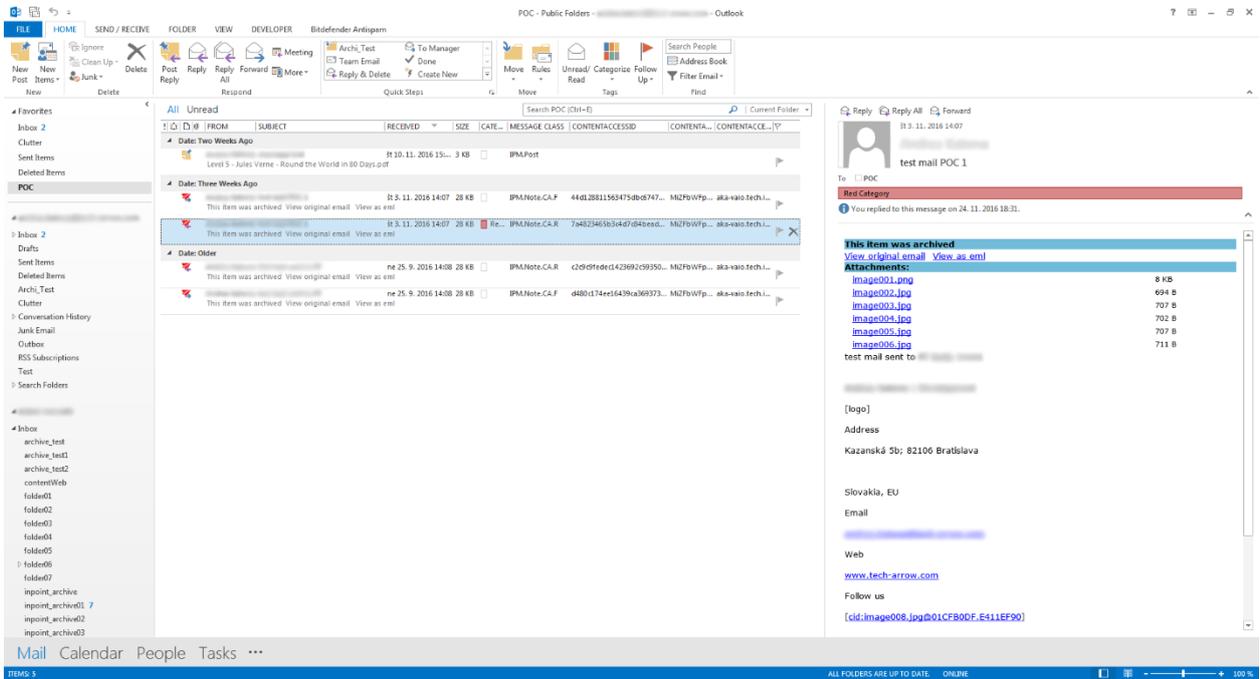


Screenshot.4. Call forward straightaway on the shortcut item, the Forward inspector is shown

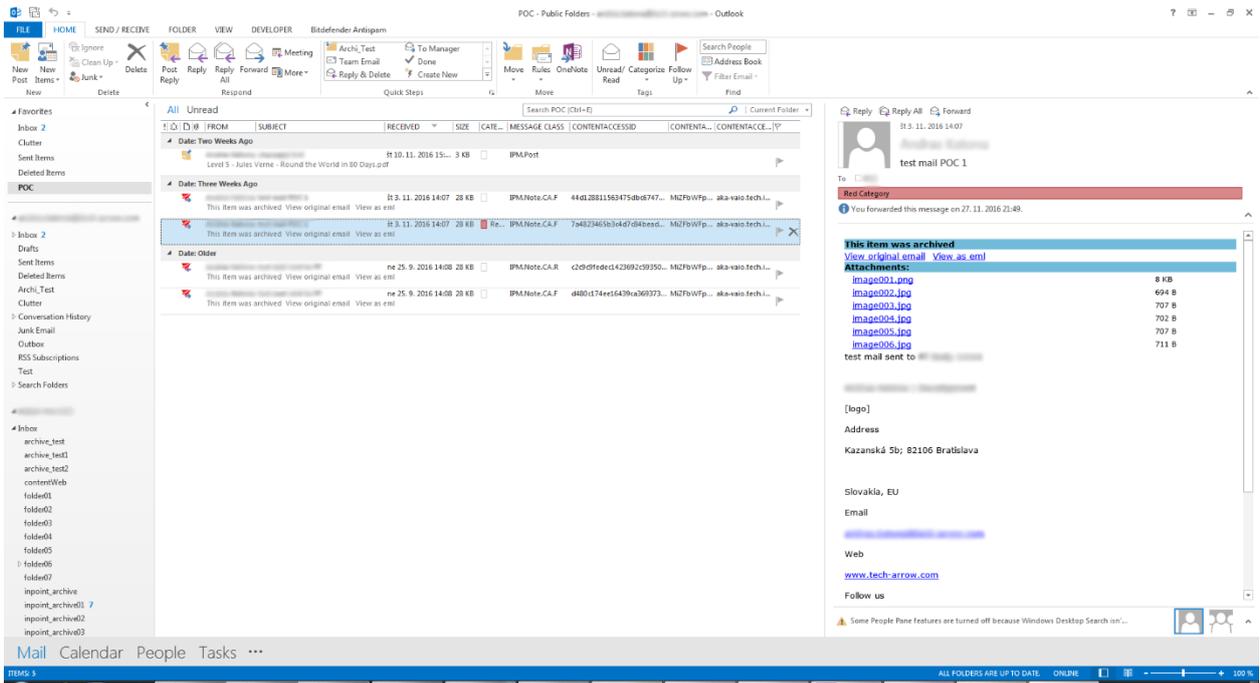


Screenshot.5. Shortcut in the additional mailbox after forwarding (message class is IPM.Note.CA.F)

3. Shortcut is in the public folder – add-in updates shortcut in the Public Folder



Screenshot.6. Shortcut is in Public Folders (original message class is IPM.Note.CA.R)



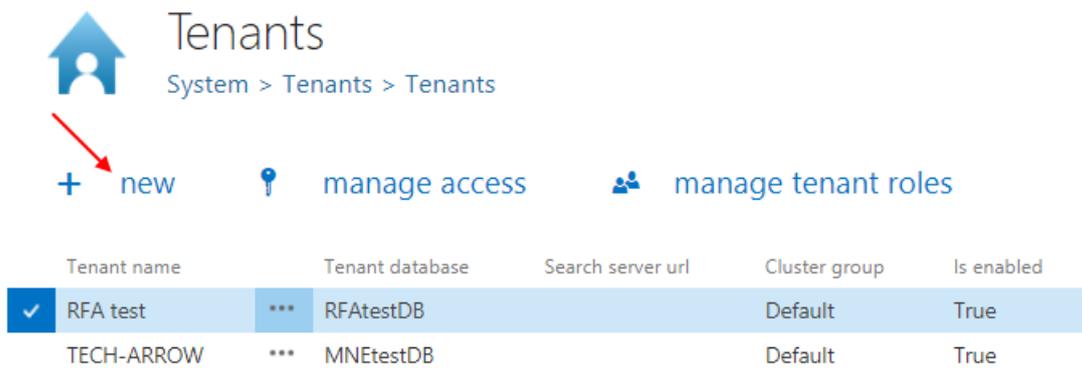
Screenshot.7. Shortcut's changed message class to IPM.Note.CA.F

Tenants in contentACCESS

contentACCESS supports multi-tenancy. This section will provide you with information about how to create a new tenant in contentACCESS. If you have a single tenant license, then your default tenant is already created and you can skip this section.

How to create a new tenant

In contentACCESS, only a user with **Manage tenant and Manage system permissions** has the right to create a new tenant. If these permissions are not granted, the **+ new** option (i.e. to create a tenant) is unavailable for the logged on user. The default system administrator role contains both these permissions. To create a new tenant, open the **Tenants** page in the Central Administration (**System** → **Tenants** → **Tenants** button). On this page you see the list of all tenants, which are present in contentACCESS. If you have not added a tenant to contentACCESS yet, the list is obviously empty. To add a new tenant to the list, click on **+ new**. The **Add new tenant** dialog will open.



Tenant name	Tenant database	Search server url	Cluster group	Is enabled
✓ RFA test	*** RFAtestDB		Default	True
TECH-ARROW	*** MNEtestDB		Default	True

In this window you need to name your tenant. Pick a **Cluster group** from the dropdown list, to which this tenant will belong. Set the **Time zone** and **Date format**. The time zone can be picked from the dropdown list; the date format can be picked from the dropdown list or specified manually – **Custom date format** option. These settings are on tenant level. Click **Next**.

Note: If a tenant doesn't have a configuration or if the user's default tenant is the **System tenant**, then the **System's globalization settings** will be used.

Create new tenant ✕

Tenant information

Tenant name:

Cluster group:

Globalization settings

Time zone:

Date format:

When you are creating a new tenant, you need to assign a user as tenant administrator to it. You have now multiple choices how to create a tenant administrator:

A) With selecting **Use existing user as an administrator for this tenant** radio button — select an existing contentACCESS user from the **Select user** dropdown list and click **Next**. This user already has contentACCESS credentials which he will use to log into contentACCESS Central Administration;

Create new tenant ✕

Administrator role:*

Use existing user as an administrator for this tenant
 Create new tenant administrator

User information

Select user:

B) If you choose option **Create new tenant administrator** radio button:

Select a login provider configuration from the **Login provider** dropdown list (Forms, Windows etc.). Only a provider configured in [Login providers](#) control (System tab → Security → Login providers) can be selected here. **Forms** and **Windows** are enabled by default. **Login name** and **Login password** are needed only in case



that the **Forms** type has been selected from the list. In case of **Windows**, only the login name must be filled in. Click **Next**.

Create new tenant

Administrator role:*

Use existing user as an administrator for this tenant

Create new tenant administrator

Display name:

Login provider:

Login name:

Login password:

Confirm password:

Next

Select if you want to create a new database or use an existing one. Click **Next**.

Create new tenant

Tenant database connection parameters

Create new database Use existing database

Next

Specify the required database parameters, test the connection and if everything is alright, click **Create**.

Create new tenant ✕

Connection name:

Use system database server (TACATEST)

Type:

Server name:

Database:

Schema:

Use explicit credentials

User:

Password:

Confirm password:

✓ Database connection is successful!

The already created tenant will appear in the tenant list on the **Tenants** page. With a left click on the ellipsis (...) the tenant context menu can be opened. The menu allows to edit the tenant name or tenant license, to delete the tenant, disable it, manage access to it (manage access = create new tenant administrator), manage the roles of the tenant (manage roles of tenant = add custom roles that will be available for the selected tenant; see more in chapter [Roles](#)) and specify the search server URL.



Tenants

System > Tenants > Tenants

+ new

🔑 manage access

👥 manage tenant roles

Tenant name	Tenant database	Search server url	Cluster group	Is enabled
ART&MIS	*** Default		Default	True
✓ DemoDE	*** DemoDE		Default	True
EA_ABAL	Edit tenant		Default	True
EA_Demo	Edit tenant license		Default	True
EA_LBA	Delete		Default	True
EA_SKE	Disable		Default	True
EA_TRA	Manage access to tenant		Default	True
EA_TEST	Manage roles of tenant		Default	True
EA_Test	Set search server url		Default	True

How to edit and disable a tenant

Edit a tenant

To edit a tenant, click on the ellipses and the context menu will open. Select **Edit tenant**.



Tenants

System > Tenants > Tenants

🔑 manage access

👥 manage tenant roles

Tenant name	Tenant database	Search server url	Cluster group	Is enabled
✓ EA_Test	*** EA_Test		Default	True
	Edit tenant			
	Edit tenant license			
	Delete			
	Disable			
	Manage access to tenant			
	Manage roles of tenant			
	Set search server url			

The **Update tenant** window will open. Here it is possible to change the tenant name, cluster group, database, time zone and date format.



Update tenant ✕

Tenant name:

Cluster group: ✎ Change

Database connection: ✎ Change ✔

Globalization settings

Time zone:

Date format:

If the user tries to change the cluster group and/or database, a warning pop-up window will open.

tacatest:3333 says

Are you sure you want to change the cluster group?

Warning: The changes will be applied on next task schedules.

Screenshot: Cluster group change warning

tacatest:3333 says

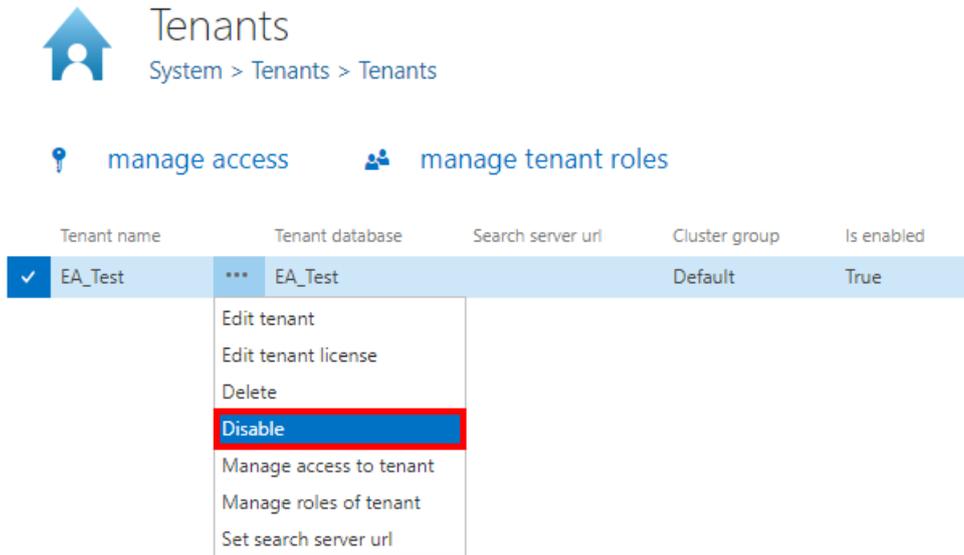
Are you sure you want to change the database?

Warning: Changing the database might lead to retrieve problems for the already archived items.

Screenshot: Database change warning

Disable a tenant

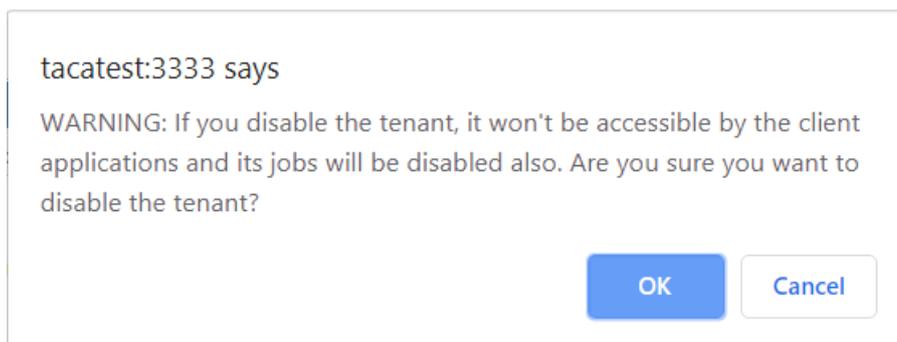
To disable a tenant, click on the ellipses and the context menu will open. Select **Disable**.



The screenshot shows the 'Tenants' management page. The breadcrumb trail is 'System > Tenants > Tenants'. There are two main actions: 'manage access' and 'manage tenant roles'. A table lists tenants with columns: Tenant name, Tenant database, Search server url, Cluster group, and Is enabled. The first row is 'EA_Test' with database 'EA_Test', search server url, 'Default' cluster group, and 'True' status. A context menu is open over the 'EA_Test' row, listing actions: Edit tenant, Edit tenant license, Delete, **Disable** (highlighted in red), Manage access to tenant, Manage roles of tenant, and Set search server url.

Tenant name	Tenant database	Search server url	Cluster group	Is enabled
EA_Test	EA_Test		Default	True

A warning window will pop up, saying that the tenant won't be accessible by client applications and its jobs will be disabled, too. If you agree, click **OK**.



Note: If you want to enable the tenant again, you can do it by selecting **Enable** from its context menu.

Tenant limitations

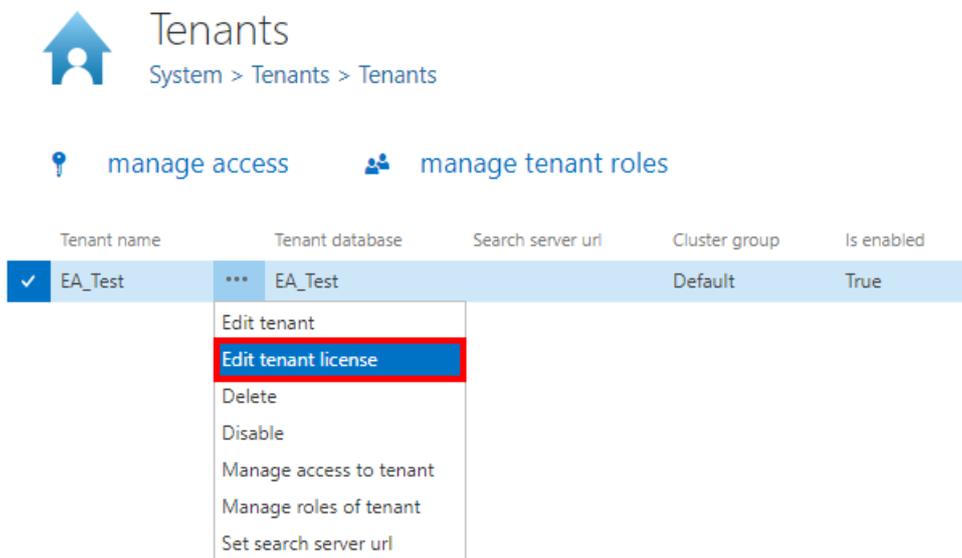
Each tenant in contentACCESS can manage only processes to which he has got the necessary rights. E.g. while one tenant has the right to archive emails only, another tenant can archive both files and emails using contentACCESS. The tenant rights can be restricted/extended on the **Tenant limitations** page of the



respective tenant. Only a system administrator has the necessary right to manage tenant limitations. The administrator may set on this page the:

- **System limitations** – plugins and stores that the given tenant will be able to use
- **Limitations related to the allowed plugins** – e.g. if Email archive plugin is allowed, then the maximum email count, mailbox count and email size that the given plugin can process can be defined

The **Tenant limitations** page can be opened from the context menu of the given tenant. Open the context menu and select “Edit tenant license”:



The **Tenant limitation** page is divided into 6 sections:

- **System limitations** – Plugins and stores available for the given tenant may be limited in this section.

By unchecking the “**Unlimited**” checkbox you open the list of plugins/stores. Check the plugins/stores that the tenant should be allowed to use.





- **Tenant limitations** – The administrator may limit the maximum number of jobs processed by the tenant at a time.

Tenant limitations

Job count:

- **Email archive limitations** – If the **Email archive** plugin is allowed, the administrator may limit the active/deactivated mailbox count, email(s) size, email(s) count that the given tenant will be able to archive. It is also possible to allow public folders here, by checking the **Public Folders allowed** checkbox and select if deactivated mailboxes should be hidden.

Email archive limitations

Active mailbox count: <input type="text"/>	Email(s) size in archive: <input type="text"/> B
Deactivated mailbox count: <input type="text"/>	Email(s) count in archive: <input type="text"/>
Public Folders allowed: <input checked="" type="checkbox"/>	Hide deactivated mailboxes: <input checked="" type="checkbox"/>

- **PST import limitations** – If the **PST import** is allowed, the administrator may limit the count of mailboxes with imported PSTs and the size of emails imported from PSTs.

PST import limitations

PST import allowed: <input checked="" type="checkbox"/>	Imported email(s) size from PST: <input type="text"/> B
Mailboxes with imported PSTs: <input type="text"/>	

- **File archive limitations** – If the **File archive** plugin is allowed, the administrator may limit the root folder count, file(s) count, file(s) size that the given tenant will be able to archive.

File archive limitations

Root count: <input type="text"/>	File(s) size: <input type="text"/> B
File(s) count: <input type="text"/>	

- **GDPR for File system limitations** – The administrator may limit here the number of file system roots and file system items.

GDPR for File system limitations

File system roots: <input type="text"/> unlimited (0 used)	File system items: <input type="text"/> unlimited (0 used)
--	--

- **GDPR for Exchange limitations** - The administrator may limit here the mailbox count and email count the tenant will be able to archive.

GDPR for Exchange limitations

Mailbox count: <input type="text"/> unlimited (0 used)	Email count: <input type="text"/> unlimited (0 used)
--	--

- **GDPR for applications limitations** – The administrator may limit here the application count and the number of application records.



GDPR for applications limitations

Application count:	<input type="text" value="unlimited (0 used)"/>	Applications records:	<input type="text" value="unlimited (0 used)"/>
--------------------	---	-----------------------	---

- **SharePoint archive limitations** – If the **SharePoint archive** plugin is allowed, the administrator may limit the count of connections, file(s) and the size of processed file(s).

SharePoint archive limitations

Connection count:	<input type="text"/>	File(s) size:	<input type="text"/> B
File(s) count:	<input type="text"/>		

- **Teams archive limitations** – The administrator may limit here the user count, team count, size of archived items, deactivated user count, deactivated team count, item count.

Teams archive limitations

User count:	<input type="text"/>	Deactivated user count:	<input type="text"/>
Team count:	<input type="text"/>	Deactivated team count:	<input type="text"/>
Size:	<input type="text"/> B	Item count:	<input type="text"/>

If the limitations text boxes are empty, this means that the allowed count and size is unlimited.

The tenant administrator may see his own limitations only in **read only** view.

How to provide access to a tenant (adding new tenant administrators)

A tenant can have one or more tenant administrators. If you want to provide access to a tenant for one or more users except of the tenant administrator, open the **Tenants** page (**System** → **Tenants** → **Tenants**), select the tenant from the list, with a left click on ellipsis (...) open the context menu and choose option **Manage access to tenant**.

It is also possible to manage access to the tenant with clicking on the **manage access** option on the same page. The button is active if the tenant is selected in the grid.



Tenants

System > Tenants > Tenants

manage access

manage tenant roles

Tenant name	Tenant database	Search server url	Cluster group	Is enabled
✓ EA_Test	EA_Test		Default	True

- Edit tenant
- Edit tenant license
- Delete
- Disable
- Manage access to tenant
- Manage roles of tenant
- Set search server url

With this action you will be redirected to the manage access page of the selected tenant. All currently existing tenant administrators of this selected tenant can be seen on this page. To add a new tenant administrator to the list, click on **+ new** on this page.

contentACCESS Central Administration | Tenant: TA Documentation

System > Tenants > tenant: TA Documentation > Manage access

+ new

User name	Role name	Flags	Description
Administrator	Tenant configuration administrator	Manual	Administrator has Tenant configuration administrator rights on Tenant TA Documentation

[Go back](#)

The **Create new role association** window will open. There are multiple options how to add a new tenant administrator.



Create new role association ✕

Tenant information

Role ▼
Tenant configuration administrator

Invitation type ▼
Invitation

E-mail address* ▼
mne@tech-arrow.com

Additional message
Please, accept this invitation.

OK
Cancel

Tenant administrator invitation types

There are multiple options how to add a new tenant administrator in the **Create new role association** window. You can **Create new** user, you can **Search for existing** worker from the company or you can also **Send an invitation** to somebody who is not a contentACCESS user yet. Select the **Tenant administrator** role type from the **Role** dropdown list.

➤ Create new

If you select **Create new**, insert a **Display name** into the dialog first. Select the default tenant from the **Default tenant** dropdown list. From **Login type** list select the authentication provider configuration that this user will use when logging in to the system. Then fill the credentials (if **Forms** type was chosen then both Login name and Password) and click **OK**.

Create new role association ✕

Tenant information

Role:

Invitation type:

Create new user

Display name:

Default tenant:

Login type:

- Office 365
- Google
- Forms
- Windows
- External AD

Note: Only a provider configuration set up in [Login providers](#) control (System tab → Security → Login providers) can be selected from the list of login types. **Forms** and **Windows** are enabled by default.

➤ Search for existing/Assign to existing user

To the **Search for existing user*** field fill in part of name of the person you want to find. After you have selected the user click **OK**. This user will use his already existing credentials to log into Central Administration.

Note: The invitation type can be used if user searching is enabled in the User search settings (more information [here](#)).

Create new role association ✕

Tenant information

Role:

Invitation type:

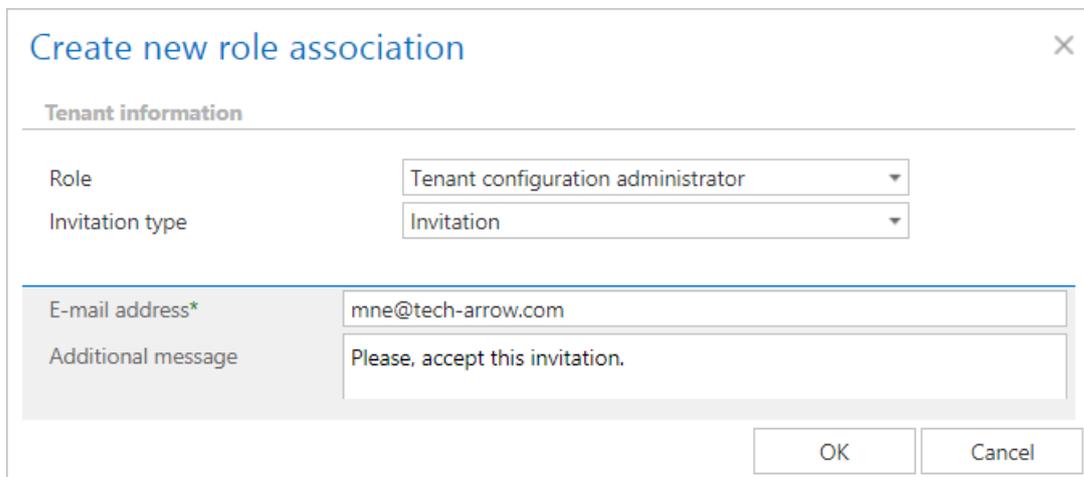
Search for existing user*

- ana ZNE. [redacted]
- An** ANE. [redacted]
- ana ZNE. [redacted]

Screenshot: Granting tenant administrator rights if user searching is **enabled**

➤ Send invitation

This option enables you to invite a person (who is not a contentACCESS user yet) to be a tenant administrator on your tenant. Select the **Tenant administrator** role type, enter the **E-mail address*** of the new user you wish to invite, and fill the **Additional message*** textbox which will be included in the email message that the invited user will receive from you. Then click **OK**.



The invited person will get an invitation message from you. If the user accepts your invitation, he/she will be redirected automatically to the login page of contentACCESS. Here he can configure his authentication provider that he prefers to use for future logins into the system (this can be adjusted with navigating to **System → Security → Login providers**).

Tenant associations

Tenant – database association

The [Task runner](#) plugin and [Indexing](#) plugin use the tenant database. This database is associated with the tenant on the tenant creation.

First, the tenant name must be specified. Pick a **Cluster group** from the dropdown list, to which this tenant will belong. Set the **Time zone** and **Date format**. The time zone can be picked from the dropdown list; the date format can be picked from the dropdown list or specified manually – **Custom date format** option. These settings are on tenant level. Click **Next**.



Create new tenant ✕

Tenant information

Tenant name:

Cluster group:

Globalization settings

Time zone:

Date format:

Then the tenant administrator must be added:

Create new tenant ✕

Administrator role:*

Use existing user as an administrator for this tenant

Create new tenant administrator

User information

Select user:

The user has to select then if he wants to create a new database on the SQL server or if he wants to use an existing one:

Create new tenant ✕

Tenant database connection parameters

Create new database Use existing database

Database parameters must be specified:

Create new tenant ✕

Connection name:

Use system database server (TACATEST05\SQLEXPRESS)

Type:

Server name:

Database:

Schema:

Database user

Use explicit user

New or existing user:

Password:

Confirm password:

Connect with user

Use explicit credentials

User:

Password:

Confirm password:

After tenant creation, the database scripts create tables for the [Task runner](#) and [Indexing](#) jobs. The tenant database column can be seen in the table of the tenants:



Tenants

System > Tenants > Tenants

+ new

🔑 manage access

👤 manage tenant roles

Tenant name	Tenant database	Search server url	Cluster group	Is enabled
RFA test	RFAtestDB		Default	True
TA Documentation	MNEtestDB		Default	True
TECH-ARROW	MNEtestDB		Default	True
✓ Arrow	MNEdatabase		Default	True

The user can change the tenant database from the context menu:



Tenants

System > Tenants > Tenants

🔑 manage access

👤 manage tenant roles

Tenant name	Tenant database	Search server url	Cluster group	Is enabled
✓ EA_Test	EA_Test		Default	True

- Edit tenant
- Edit tenant license
- Delete
- Disable
- Manage access to tenant
- Manage roles of tenant
- Set search server url



Update tenant ✕

Tenant name:

Cluster group:  Change

Database connection:  Change 

Globalization settings

Time zone:

Date format:

For the existing tenants, the update will run the necessary database scripts on the default database and set it as tenant database.

Tenant – user association

Every user belongs to at least one tenant. When creating or inviting a user, a tenant must also be selected. The default tenant here is the same tenant as selected in the upper right corner in [Central Administration](#).



Create / Invite a user ✕

Create new user
 Invite user

Display name:

Default tenant:

Login type:

Assign role

Role:

Tenant:

Globally allowed permissions of the selected role **will be assigned** to the user on the selected tenant.

[Show details](#)

* Note: If you select a tenant and the role has specific permissions, you will be redirected to the **Specific permission assignment** page.

Create / Invite a user ✕

Create new user
 Invite user

Tenant:

E-mail address*

Additional message

Assign role

Role:

Tenant:

Globally allowed permissions of the selected role **will be assigned** to the user on the selected tenant.

[Show details](#)

* Note: If you select a tenant and the role has specific permissions, you will be redirected to the **Specific permission assignment** page.

Show users

From the dropdown list on the **Users** page (after clicking the **Users** button on the ribbon), the user can choose one of the following filters:

- 1) Show current tenant users – users with current tenant assigned as default
- 2) Show linked users – users who have a role associated with the current tenant
- 3) Show all users – users who have access to the selected tenant
- 4) Show global administrators – users with a role associated with all tenants (visible only for system administrators)
- 5) Show users without tenant – users associated with no tenants (visible only for system administrators)



Users

System > Security > Users

+ Create or invite user

- Show all users
- Show current tenant users
- Show linked users
- Show all users
- Show global administrators
- Show users without tenant



Display Name	Default tenant	Roles
admin		
Administrator		System administrator
aho		Standard user
David User		
davidkatest01		
		Standard user
		Standard user
MNE		Configuration administrator, Tenant administrator, Standard user, System administrator

Change the default tenant

Go to user details (User -> pick Edit from its context menu). If you have **manage tenant** permission on the default tenant of the user, you can change his tenant.



User details

System > Security > Users > User details

User details

Display name:

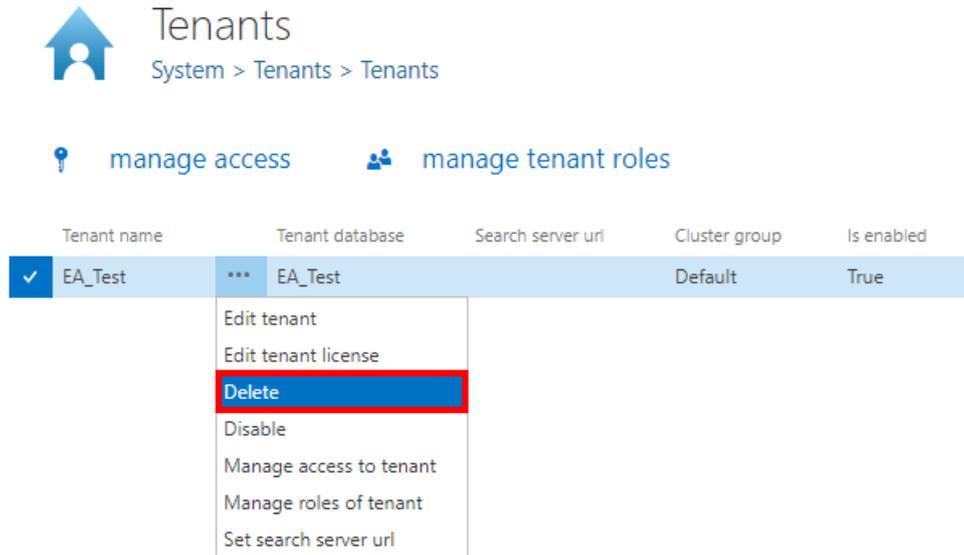
Tenant:

Is system admin: Yes

Status: Offline ●



Tenant deletion



The screenshot shows the 'Tenants' management page. At the top, there is a breadcrumb trail: System > Tenants > Tenants. Below this, there are two main action buttons: 'manage access' (with a key icon) and 'manage tenant roles' (with a group of people icon). The main content area displays a table of tenants. The first row is selected, and its context menu is open, showing several options. The 'Delete' option is highlighted with a red border.

Tenant name	Tenant database	Search server url	Cluster group	Is enabled
EA_Test	EA_Test		Default	True

- Edit tenant
- Edit tenant license
- Delete**
- Disable
- Manage access to tenant
- Manage roles of tenant
- Set search server url

If you want to delete a tenant, go to its context menu and choose the **Delete** option. All the plugins, settings, repository objects, [Schedulers](#), [Role](#) associations and [Users](#), who have no access to another tenant, will be deleted.

What happens with the existing users?

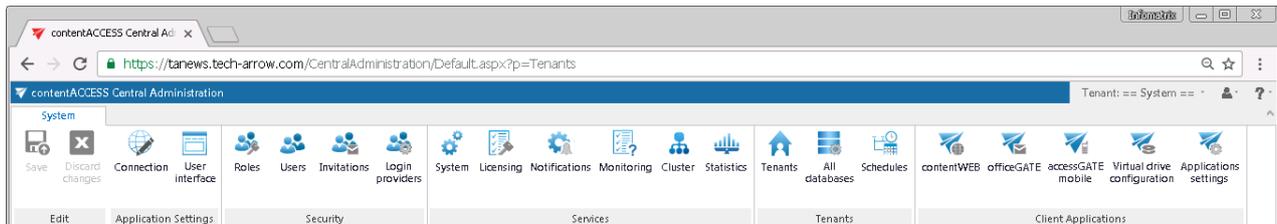
If the user had the permission to **manage system**, the system tenant was assigned.

If user had associated roles on the tenant, the first tenant found in role association was assigned.

If user had associated roles on **all tenants**, the first tenant found in the system was assigned.

General system configurations

General system settings of contentACCESS are available in the respective configuration groups under the **System** tab.



Only a user with Manage system permissions has the right to configure system settings. The user may find here all general system settings.

The **Application settings** are set by default, but can be changed (not recommended). Under **Security settings** the administrator can find all users of contentACCESS and the default system roles. He can also configure new custom roles for the users and new authentication providers from here. The list of invitations can be found here as well. Under **Services** it is possible to activate the license key, set up external accessibility settings, change system database connections, set default values for the clustering etc. Under **Tenants** the administrator may create new tenants and create databases for these tenants. The notification schedulers can be defined on the “Schedules” page, which is also accessible from here. Under **Client Applications** group the contentACCESS client applications are accessible. Virtual drive must be configured if File system archive is used.

Note: If you do not use Email Archive based plugins and also do not use accessGATE Mobile, the FQDN settings (accessible under **System** → **Services** → **System**) are irrelevant.

In the following subchapters we will go through each of these settings:

Connection

Navigate to **System** → **Application settings** →  **Connection** button. Here the service connection settings such as contentACCESS URL, plugins, plugin controls and storage controls directories can be found and edited. Plugins, plugin controls and storage controls directories are set by default as on the screenshot below, but in case you need to place them somewhere else on your computer, you can change the destinations right here (not recommended):



Plugins directory:	C:\Program Files\TECH-ARROW\contentACCESS\GATE.contentAccess\Plugins
Storage controls directory:	C:\Program Files\TECH-ARROW\contentACCESS\CentralAdministration\Storages
Plugin controls directory:	C:\Program Files\TECH-ARROW\contentACCESS\CentralAdministration\PluginControls

User interface

Navigate to **System** → **Application settings** →  **User interface** button. Here you can choose the Date-time format.



User interface

System > Application Settings > User interface

General settings

Date-time format:



Users in contentACCESS

All users of the current tenant are listed on the **Users** page (open it with navigating to **System** → **Security** → **Users** button).

This list is visible for users, who have **manage users and roles** permission on the selected tenant. Tenant administrator is able to see all **current tenant users** (default tenant of the user is the current tenant) and **linked users** - the users who have roles associated with the current tenant. System administrator can also see the list of **global administrators** – administrators who have roles associated on all tenants, and also list of **users without default tenant**. For more information about user filtering on the **Users** page, please check [this](#) section.

Note: If you remove a tenant, the users with roles only on this tenant will also be removed.

Note: Because of security reasons, it is highly recommended to change the above mentioned default system administrator’s login password after the very first login to the Central Administration. This can be done on the **User details** page of the **Administrator** user, in section **User logins**, **Forms** login provider’s context menu:

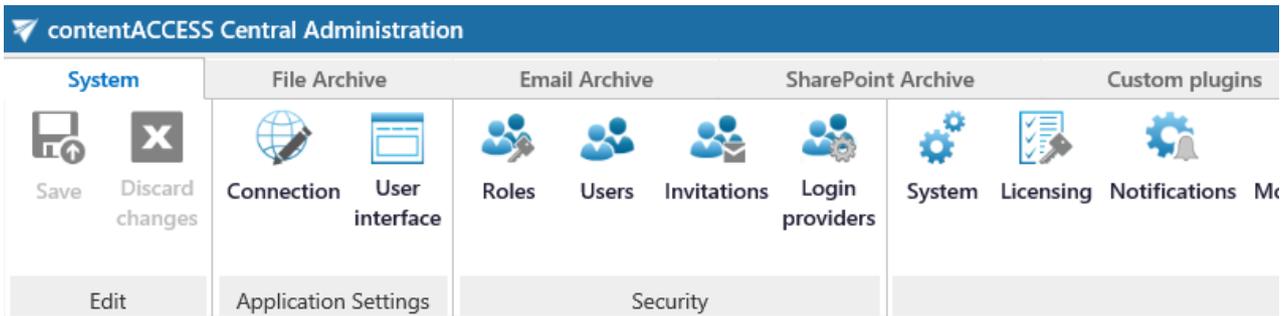
The screenshot shows the 'User details' page for the 'Administrator' user. The 'User logins' section is expanded to show the 'Forms' login provider. A context menu is open over the 'Forms' entry, with the 'Change password' option highlighted in red.

Login type	Login name	External id
Forms	*** system	

Login type	Login name	Last access date	Expiration	IP Address	User agent
Forms	*** system	12/9/2020 10:14:29 AM	12/9/2020 11:14:29 AM	135.181.50.162	SmtspServer
Forms	*** system	12/9/2020 9:58:07 AM	12/9/2020 10:58:07 AM	188.112.70.108	Platform Desktop; Browser: Chrome (87.0.4280.88); OS: Windows
Forms	*** system	12/9/2020 10:15:04 AM	12/9/2020 11:15:04 AM	91.127.142.124	Platform Desktop; Browser: Chrome (87.0.4280.88); OS: Windows
Forms	*** system	12/9/2020 10:12:17 AM	12/9/2020 11:12:17 AM	127.0.0.1	SYSTEM



Users' context menu



Users

System > Security > Users

+ Create or invite user

Show all users

Display Name	Default tenant	ID	Roles
Administrator	== System ==	A550E000-1588-423C-AD83-088D4CF07758	System administrator, Standard user
		ac44b546-04d0-4bea-8636-2a00f037e53b	Standard user
		f1f2bf4f-bb0c-4e5c-8e6f-f9f4223d27a0	Standard user
nev1	Default	92c26b29-2fff-4fed-b05c-c5b70b5a1cda	Standard user

The users' context menu allows the following operations:

- **Assign role** – assign a role to an already existing user; read more in section “Roles”

Note: If the logged on administrator has **specific** permissions on schedulers, repository items, jobs and/or to view the archive, he cannot assign roles containing these permissions for second users. E.g. If the logged user has specific permission to Edit job, then he cannot assign a role which contains Edit job permission. Read more about roles and permissions in chapter “Roles”.

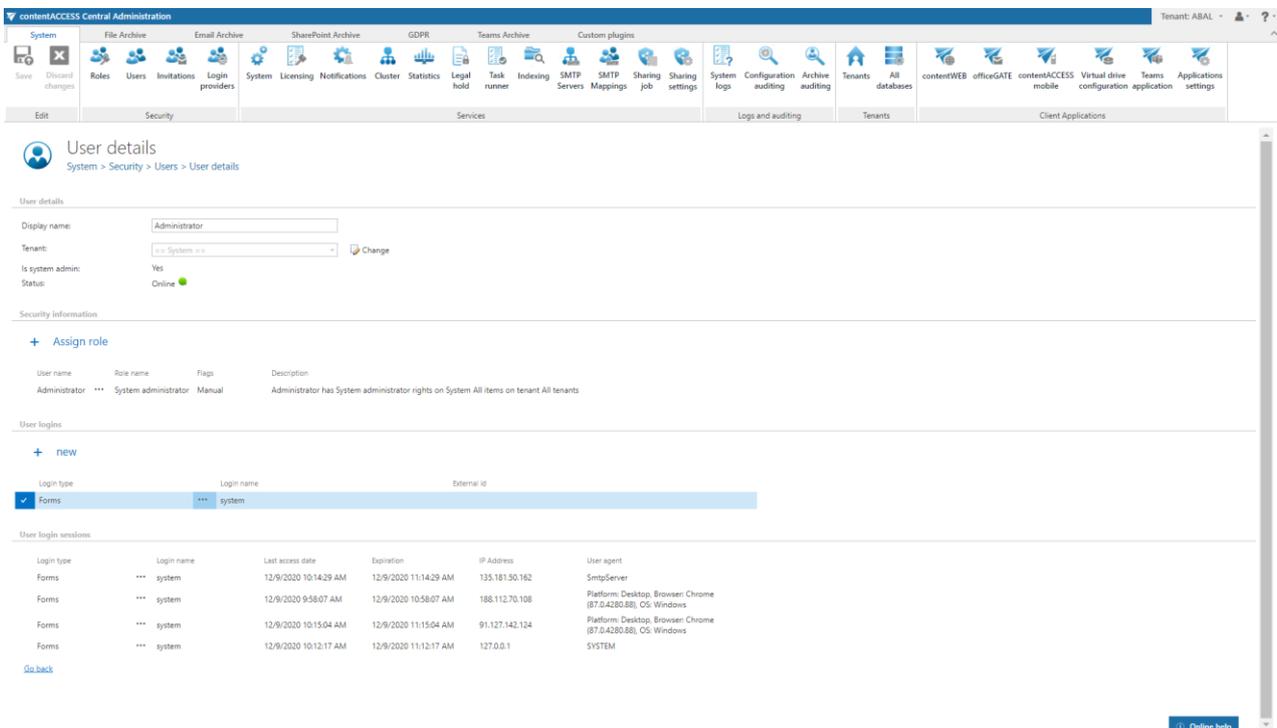
- **Edit role assignment** – edit permissions of the user's assigned role
- **Edit** – view the user details; add user logins; view user's login session(s); log off the user
- **Delete** – delete the user from the system



Note: It is good to know that for security reasons it is impossible to delete all system administrators from the list of users. It is possible to delete users with system admin permissions except of the default system administrator.

User details

The detailed user information can be accessed by selecting option “Edit” in the user’s context menu (the logged on user can access his own user details by clicking “About me” in the upper right user menu). With this option the **User details** (or **About me**) page opens.



Screenshot A: Details of the selected contentACCESS user



The screenshot shows the 'About Me' section for a user named 'Administrator'. The user details include:

- Display name: Administrator
- Tenant: == System ==
- Is system admin: Yes
- Status: Online

Below the user details, there is a table for 'User logins' and a table for 'User login sessions'.

Login type	Login name	Last access date	Expiration	IP Address	User agent
Forms	*** system	12/9/2020 10:48:29 AM	12/9/2020 11:48:29 AM	135.181.50.162	SmtspServer
Forms	*** system	12/9/2020 9:58:07 AM	12/9/2020 10:58:07 AM	188.112.70.108	Platform: Desktop; Browser: Chrome (87.0.4280.88); OS: Windows
Forms	*** system	12/9/2020 10:49:11 AM	12/9/2020 11:49:11 AM	91.127.142.124	Platform: Desktop; Browser: Chrome (87.0.4280.88); OS: Windows
Forms	*** system	12/9/2020 10:12:17 AM	12/9/2020 11:12:17 AM	127.0.0.1	SYSTEM

Screenshot B: Details of the logged in user

Section “User details”

In this section you can find the given user’s display name (i.e. his name in contentACCESS), and the information about the user’s status. To change the display name, rewrite the current **display name** and save your settings.

The image shows a close-up of the 'About Me' section. A red arrow points to the 'Display name' input field, which contains the text 'Administrator'. To the right of the 'Tenant' dropdown menu is a 'Change' button.

It is also possible to change the tenant of the selected user. To do so, click on the **Change** button.



User details

System > Security > Users > User details

User details

Display name:	<input type="text" value="aan"/>	
Tenant:	<input type="text" value="ABAL"/>	
Is system admin:	No	
Status:	Offline ●	

A warning window will pop-up. After you confirm the warning by clicking on the **OK** button, you will be able to change the tenant. The **retrieve problems** mentioned in this pop-up mean that you will not see your previously shared items in contentWEB.

Are you sure you want to change the tenant?

Warning: Changing the tenant might lead to retrieve problems.

The user's status signalizes if the user is:

- **Online (green):** means there was an interaction in the last 5 minutes
- **Away (yellow):** the user is logged in, but inactive in the last 5 minutes. If the user has clicked the Remember me when logging in, then he will be displayed as Away until his token expires
- **Offline (red):** the user does not have any login session

Section "Security information"

Here you find the user's display name, the role(s) assigned to the given user and a description about the user's rights. It is possible to assign a previously configured role for the user from here. After clicking on **+ Assign role**, a pop-up window, where the role can be specified, appears.

Role assignment ✕

User: Administrator

Role:

Tenant:

Globally allowed permissions of the selected role **will be assigned** to the user on the selected tenant.

[Show details](#)

* Note: If you select a tenant and the role has specific permissions, you will be redirected to the **Specific permission assignment** page.

Each role assignment has a flag. **Manual** flag means that the given role was assigned manually. Manual permissions are not changed/removed by the automatism. **Automatic** flag means that the role was assigned by the provisioning job. Automatic flag is marked with “(100)”.

Section “User logins”

New user logins can be assigned to a user in the **User logins** section. By clicking “+new” in this section the “Add new login” window opens.

Add new login ✕

Login provider:

Login name:

✔ User name is valid

In the **Add new login** window, select a provider configuration that the given user will use when logging into the given application. The providers, that were configured on the **Login providers** page (for more information check “[Login providers](#)”) can be selected here. **Windows** and **Forms** authentications are enabled by default. Multiple user logins are not enabled for Forms and Windows login providers.

Change password, Reset password context menu options:

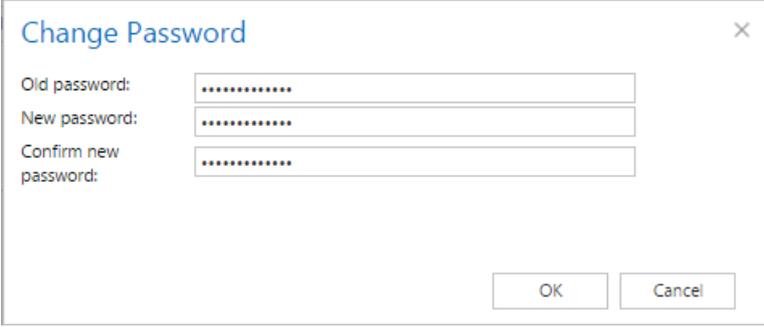
User logins

+ new

	Login type	Login name	External id
***	Azure	companyadmin@tech-arrow.com	
✓	Forms	system	
	Delete	techarrow.user@gmail.com	
	Change password	TA\Administrator	S-1-5-21-1454735840-2720631597-1747903052-500
	Reset password		

The administrator can change the user's password for the Forms type login. The administrator must have Manage tenant permissions to change, and/ or to reset the password of a user.

To change the password, just select this option and enter the old, new, and confirm the new, desired password in the pop-up window:



The dialog box titled "Change Password" contains three input fields for "Old password:", "New password:", and "Confirm new password:", each with a masked password field. At the bottom right, there are "OK" and "Cancel" buttons.

If the password has been lost or forgotten, use the **Reset password** option to create a new one. Enter the email address where the password should be sent.

Reset Password



Send email notification

Email address:

The new password will be sent to this email address.

Generate new password

Add new password manually

The user has now two options: to generate the password or to add the password manually. If the user selects **Generate new password**, he first needs to click on the **Generate password** button, then he will see the generated password in the textbox.

Reset Password



Send email notification

Email address:

The new password will be sent to this email address.

Generate new password

Add new password manually

Generated password:

If the user selects **Add new password manually**, he needs to type in two times his new password.

Reset Password



Send email notification

Email address:

The new password will be sent to this email address.

Generate new password

Add new password manually

New password:

Confirm password:



At the next notification job run the new password will be sent to the email address specified in the dialog.

Section “User login sessions”

At the bottom of the **User details** page, there is a list of active login sessions (if the user logged in in officeGATE, contentWEB etc., then all these apps will have a separate login session; if the user is logged in from different browsers, there will be separate login sessions for each browser as well). From that page, the administrator can also log off an existing user. Once the logoff is done, the user will be redirected to the login page on the next click in the given application.

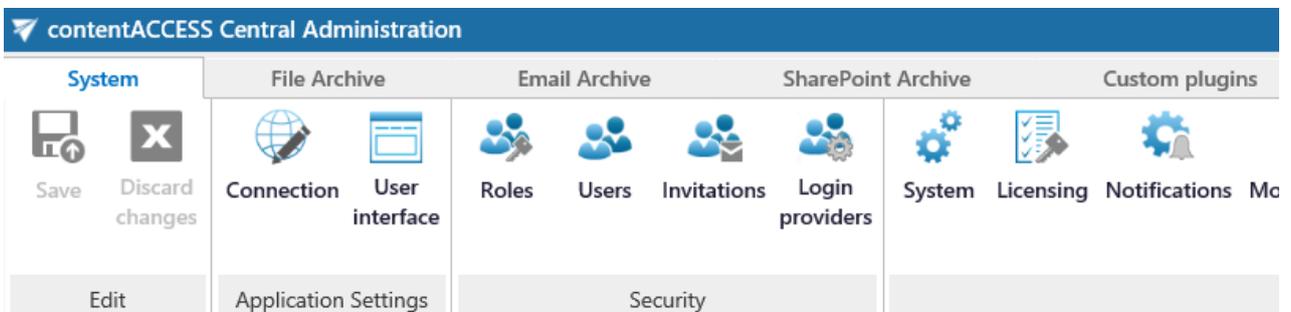
Creating/inviting contentACCESS users

When you create/invite user(s) in contentACCESS, always follow these steps:

- a) **Prepare a role** with the permissions that will be assigned to the user(s) – this step can be skipped if you want to assign an already existing, default global role to the user(s); more info in section “**Roles**”
- b) **Create/Invite the user(s) and assign the role** in the **Create/Invite a user** dialog
- c) **Edit the specific permissions of the assignment** – only if specific permissions were defined in the assigned role (read more in “**Roles**”)



Any new users/existing users (with new roles/permissions) can be added to contentACCESS on the **Users** page. To create/invite a user, click **“Create or invite user”** on the **Users** page (System tab → Security group → Users page).



Users

System > Security > Users

+ Create or invite user

Show all users

Display Name	Default tenant	ID	Roles
Administrator	***	== System ==	A550E000-1588-423C-AD83-088D4CF07758 System administrator, Standard user

The **Create/Invite user** dialog pops up, where you need to choose one of the user adding methods (Create new user/Invite user) and fill the necessary parameters into the dialog.

- “Create new user”** – use this option to add a new user (with the necessary roles) to contentACCESS without invitation. “Without invitation” means that the newly added user will not get a notification email message, that he was invited to contentACCESS.
- “Invite user”** – with this option a **new user and/or an already existing contentACCESS user** with the necessary role(s) can be **invited**. “Will be invited” means that the new/existing user will get a notification email, that he/she was invited into contentACCESS. Notification messages are sent by the notification job in specific time slots defined in the Notification settings. Read more about invitations in section [Invitations](#).



Create / Invite a user ✕

Create new user Invite user

Display name:

Default tenant:

Login provider:

Assign role

Role:

Tenant:

Globally allowed permissions of the selected role **will be assigned** to the user on the selected tenant.

[Show details](#)

* Note: If you select a tenant and the role has specific permissions, you will be redirected to the **Specific permission assignment** page.

Note: contentACCESS Email Archive/File archive standard users (and user permissions) can be automatically added to contentACCESS by the **File system archive provisioning job** and/or by the **Email archive provisioning job**. On the provisioning settings pages of Central Administration the administrator defines the role that the provisioning job will assign for the given Exchange user/group or for the users of the entire Exchange server. The provisioning job evaluates the user rights on the Exchange, creates the contentACCESS user(s) and assigns the permissions for these newly added contentACCESS user(s). Read more in [Provisioning settings and managing access to contentWEB](#) (File Archive) and [Email archive Provisioning settings](#) (Email Archive).

Option “Create new user”

Choose the “**Create user**” option in the **Create/Invite user** dialog and continue with the following settings:



Type in the user's name into the dialog box, and choose an authentication provider configuration from the **Login provider** dropdown list. **Forms** and **Windows** providers can be selected by default. (Other provider configurations need to be set on the [Login providers](#) page first.) If you select the **Forms** provider (as in this use case), then the login credentials must be also entered into the dialog. The current tenant will be selected as the **default tenant** for the user.

Further select a (default or predefined) role that will be assigned to the given user – in this use case we are creating a tenant administrator, so we select this role from the list. The globally allowed permissions of the selected role get displayed in the window. These can be shown/hidden.

Save your settings. In case that you have assigned a role containing at least one "Specific" permission, you will be automatically redirected to the **Assign specific permissions** page, where you can further specify these specific permissions of the role assignment. This will be described later in section "**Roles**".



Create / Invite a user



Create new user Invite user

Display name:	<input type="text" value="Jack Bolton"/>
Default tenant:	<input type="text" value="TECH-ARROW"/>
Login provider:	<input type="text" value="Forms"/>
Login name:	<input type="text" value="j.bolton"/>
Login password:	<input type="password" value="....."/>
Confirm password:	<input type="password" value="....."/>

Assign role

Role:	<input type="text" value="Tenant administrator"/>
Tenant:	<input type="text" value="TECH-ARROW"/>

Globally allowed permissions of the selected role **will be assigned** to the user on the selected tenant.

- Scheduler:** Edit scheduler, Remove scheduler, Add scheduler,
- EmailArchive:** Preview, View mailboxes, Manual restore, Manual recovery, Export, Manual archive,
- LegacyEmailArchive:** View mailboxes,
- Repository:** Remove repository item, Add repository item, Edit repository item,
- LegalHold:** Manage legal hold cases, View legal hold cases,
- BackMailz:** Use BackMailz Service,
- GradientFiles:** View folder,
- Categorization:** View mailboxes,
- EPOSAP:** View EPO SAP,
- Plugin:** Add job, Remove job, Edit job,
- DatengutDMS:** View Datengut DDCs,
- Data:** Customize GDPR search, Delete from archive,
- KendoxDMS:** View Kendox DDCs,
- AdvancedSharing:** View shared documents,
- Hierarchy:** View mailboxes, View mailboxes,
- FSArchive:** Manage remote file servers, View folders,
- System:** Manage users and roles,
- SharePointArchive:** View SharePoint sites, Manual recovery,
- Tenant:** Manage tenant,
- PerceptiveDMS:** View Perceptive DDCs,
- FCEFiles:** View folder,

[Hide details](#)

* Note: If you select a tenant and the role has specific permissions, you will be redirected to the **Specific permission assignment** page.

Create

Cancel

Note: If you **Create new user** login with **Microsoft Exchange** login provider, only tenants with licensed Email archive are listed.

Create / Invite a user ✕

Create new user Invite user

Display name:

Default tenant:

Login provider:

Email address:

Domain:

SAM account name:

Tenant:

Assign role

Role:

Tenant:

- TECH-ARROW
- Arrow
- RFA test
- TA Documentation
- TECH-ARROW

Globally allowed permissions of the selected tenant

Note: If you select a tenant and the role has specific permissions, you will be redirected to the **Specific permission assignment** page.

Option “Invite user”

[Invitation](#) is another way of how to

- a) create new users with a given role or
- b) **assign role to an existing user.**

To send an invitation for an already existing or potential contentACCESS user, click the “**Invite user**” option.

The pop up dialog requires to fill the email address, where the invitation will be sent and the role that should be assigned to this user. The tenant of the user is automatically filled in with the current tenant. If you are ready with the necessary configurations, click “Save”. In case that you have assigned a role having at least one “Specific” permission, you will be automatically redirected to the **Assign specific permissions** page,



where you can further specify these specific permissions of the role assignment. This will be described later in section “**Roles**”.

Create / Invite a user ✕

Create new user
 Invite user

Tenant:

E-mail address*

Additional message

Assign role

Role:

Tenant:

Globally allowed permissions of the selected role **will be assigned** to the user on the selected tenant.

[Show details](#)

* Note: If you select a tenant and the role has specific permissions, you will be redirected to the **Specific permission assignment** page.

The next running notification job (must be configured in **System** → **Services** → **Notifications**) will send the invitation for the respective user. You can start this job manually as well.

Invitations

Invitation is a way of how to add



- a) **new users** (with certain roles/permissions) and
- b) **already existing users** with new permissions to contentACCESS.

To send an invitation for an already existing or potential contentACCESS user, select the “**Invite user**” option in the **Create/Invite user** dialog. Further fill the email address, where the invitation will be sent and select the role that should be assigned to this user.

When a user is created with invitation:

- a) If the role does not contain specific permissions, the invitation is sent when the user clicks the **Invite** button

Create / Invite a user ×

Create new user Invite user

E-mail address*

Additional message

Assign role

Role:

Tenant:

Globally allowed permissions of the selected role **will be assigned** to the user on the selected tenant.

[Show details](#)

* Note: If you select a tenant and the role has specific permissions, you will be redirected to the **Specific permission assignment** page.

- b) If the role contains specific permissions (read more in section [Defining specific permissions of a role assignment](#)), the **Save** button is not active, but is replaced by the **Invite** button. The invitation is sent when the user clicks the **Send invitation** button.



contentACCESS Central Administration Tenant: MNETEST

System | File Archive | Email Archive | SharePoint Archive | Custom plugins

Save | Discard changes | Connection | User interface | Roles | Users | Invitations | Login providers | System | Licensing | Notifications | Monitoring | Cluster | Statistics | Tenants | All databases | contentWEB | officeGATE | accessGATE mobile | Virtual drive | Applications settings

Edit | Application Settings | Security | Services | Tenants | Client Applications

Invited person's permissions
System > Security > Users > Role assignment

Tenant: MNETEST
Role: Standard user
User: monika.nevicka@tech-arrow.com

Email archive

Assign the following permissions on the selected mailboxes: Manual restore, Export, Preview, Manual recovery, View mailboxes

<input type="checkbox"/>	Name	Type
<input type="checkbox"/>	monika@tech-arrow.com	Mailbox
<input type="checkbox"/>	monika@tech-arrow.com	Mailbox
<input type="checkbox"/>	monika@tech-arrow.com	Mailbox

Page 1 of 1 (7 items)

File Archive

Assign the following permissions on the whole tenant: View folders

Assign file archive permissions to the user.

To finish the invitation process click the button:

Send invitation

<< Go back to All users page

After clicking the **Send invitation** button, the user is notified that his invitation was successfully sent.



Invited person's permissions

System > Security > Users > Role assignment

Tenant: MNETEST

Role: Standard user

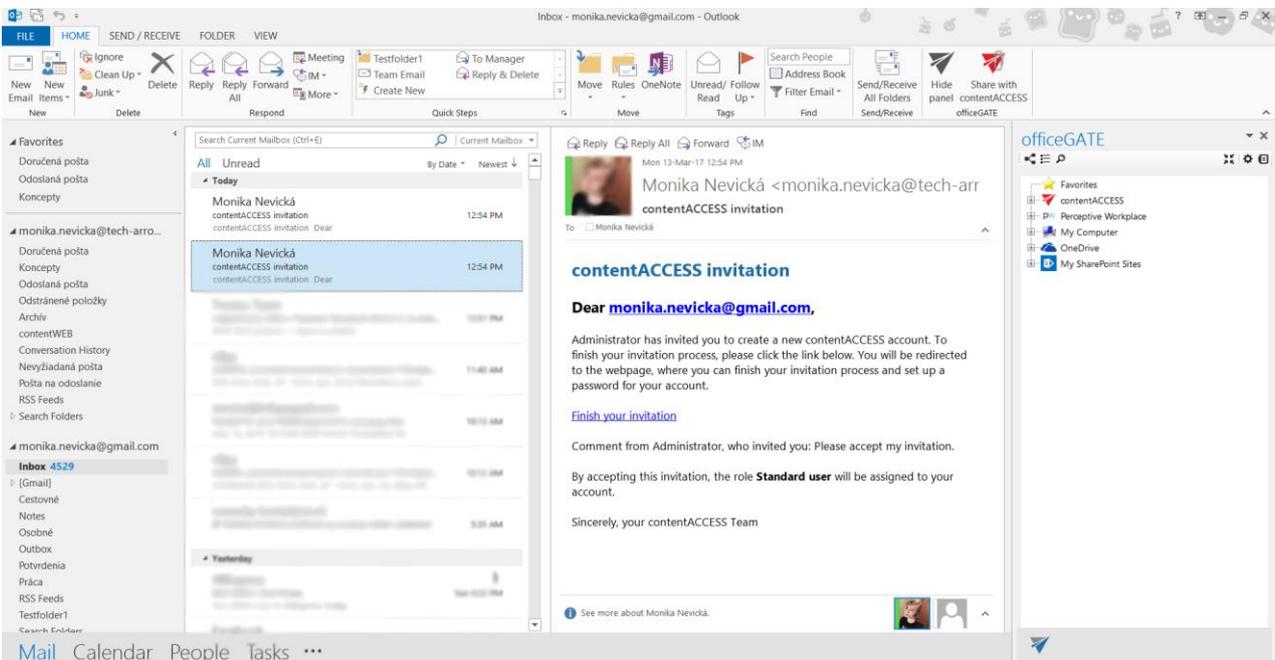
User: monika.nevicka@gmail.com

Your invitation was successfully sent.

To finish the invitation process click the button:



After the notification job has run, the invited user gets an invitation message, that he was invited to contentACCESS. To accept this invitation, he clicks “Finish your invitation”.



He is now redirected to the webpage where he can finish the invitation process. Depending on if the invited user already exists/doesn't exist in contentACCESS, or if the user is already signed in to contentACCESS, he has multiple options how to finish the invitation process. He can



- use **already signed in** user – as the user is already logged in, he is not required to log in again
- sign in with the **existing user, with the existing contentACCESS account**, if he has a contentACCESS account already, but currently he is not signed in to contentACCESS (option “Use another contentACCESS account”)
- sign up for a contentACCESS account, if he’s not a contentACCESS user yet (option “Sign up for contentACCESS account”) – the user logs in with any login provider to contentACCESS. He can either create his own contentACCESS account (**Forms** authentication) and sign in with it, or he can use any of his available authentication providers to sign in. After successful login the new user will be created and role will be assigned. The user login that he used at first will be saved in the **User details**



contentACCESS invitation

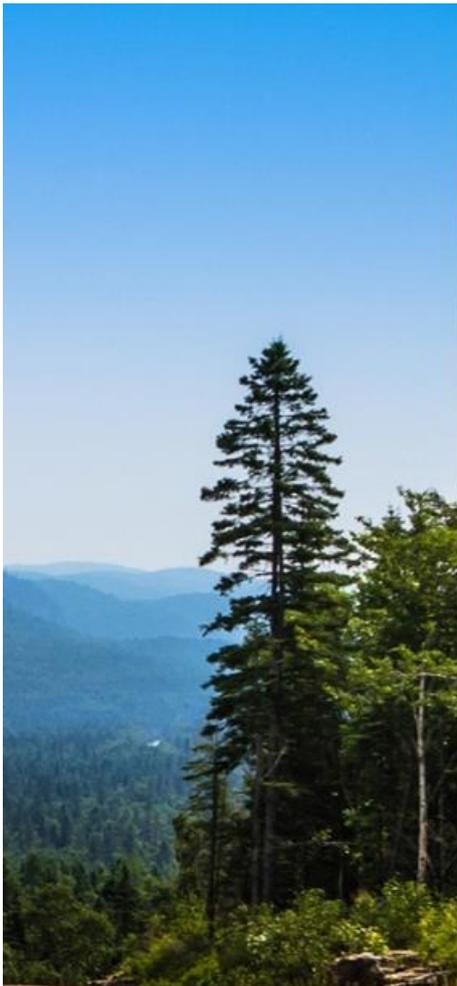
Use one of the following options to accept the invitation:

Continue as Administrator
(signed in)

I'm new to contentACCESS
(create a new account)

I already have a contentACCESS account
(let me sign in)

Screenshot: Finishing the invitation process as an already signed in user



contentACCESS invitation

Use one of the following options to accept the invitation:

I'm new to contentACCESS
(create a new account)

I already have a contentACCESS account
(let me sign in)

Screenshot: Finishing the invitation process as a new user or when not signed in

After successful login, the new user is created / the respective role defined in the invitation will be automatically assigned for the new/existing user.

The list of invitations, so the list of already invited users can be viewed on the **Invitations** page accessible at: **System** → **Security** → **Invitations**. The following columns are displayed in the grid:

- **Email:** the email address where the invitation was sent
- **Created:** the date when the invitation was sent to the user
- **State:** here can be viewed if the invitation was sent or not finished
- **Is accepted:** here can be viewed if the invited user has accepted the invitation, or it is still a pending invitation
- **Assigned user:** the user with the assigned role(s)



- **Accepted at:** the date when the invitation was accepted by the user



Invitations

System > Security > Invitations

Email	Created	State	Is Accepted	Assigned user	Accepted at
monika.nevicka@gmail.com	3/13/2017	Sent	No		

Delete
Send again

The context menu option of the respective invitation allows to delete it from the list or to resend it, if it was not accepted yet.

Roles

contentACCESS role(s) define the permissions that a certain contentACCESS user has in the entire system. Every contentACCESS user has an assigned role. The user roles can be extended, and a user can also have multiple roles assigned. There are 6 default (system level) roles in contentACCESS, but new roles with specific permissions can also be created. The default role types are visible for all tenants, on the system level. It is not possible to edit or delete them, and they have a different color on the user interface. These default roles are the following:

- A **system administrator** user has permissions to configure everything in contentACCESS Central Administration, and he has access to all processed data in contentWEB.
- A **tenant administrator** can configure his own tenant in Central Administrator and see all processed data of this tenant.
- A **standard user** is a client application user, who has specific permissions – from this reason, it is necessary to associate him with specific contentACCESS objects – e.g. with archived mailbox. Standard user role is typically created for end users, who have access to their assigned archives in contentWEB.
- A **repository editor** has the permissions to create/edit/delete repository items (i.e. databases, storages).



- A **configuration administrator** has the same permissions as the system administrator with one exception: he doesn't have the access to the archived data, so to contentWEB.
- A **tenant configuration administrator** has the same permissions as the tenant administrator with one exception: he doesn't have the access to the archived data, so to contentWEB.

Creating roles

It is possible to create

- **custom roles** in Central Administration on the **Roles** page (**System** tab → **Security** group → **Roles** page) – option “+ new role”:

Display name	Tenant name
Configuration administrator	*** All tenants
Repository editor	*** All tenants
Standard user	*** All tenants
System administrator	*** All tenants
Tenant administrator	*** All tenants
Tenant configuration administrator	*** All tenants
Limited user	*** All tenants
Full_EAUser	*** TECH-ARROW

- or you can create **tenant level roles** on the **Tenants** page (**System** tab → **Tenants** group → **Tenants** page) using the **Manage tenant roles** option, too.

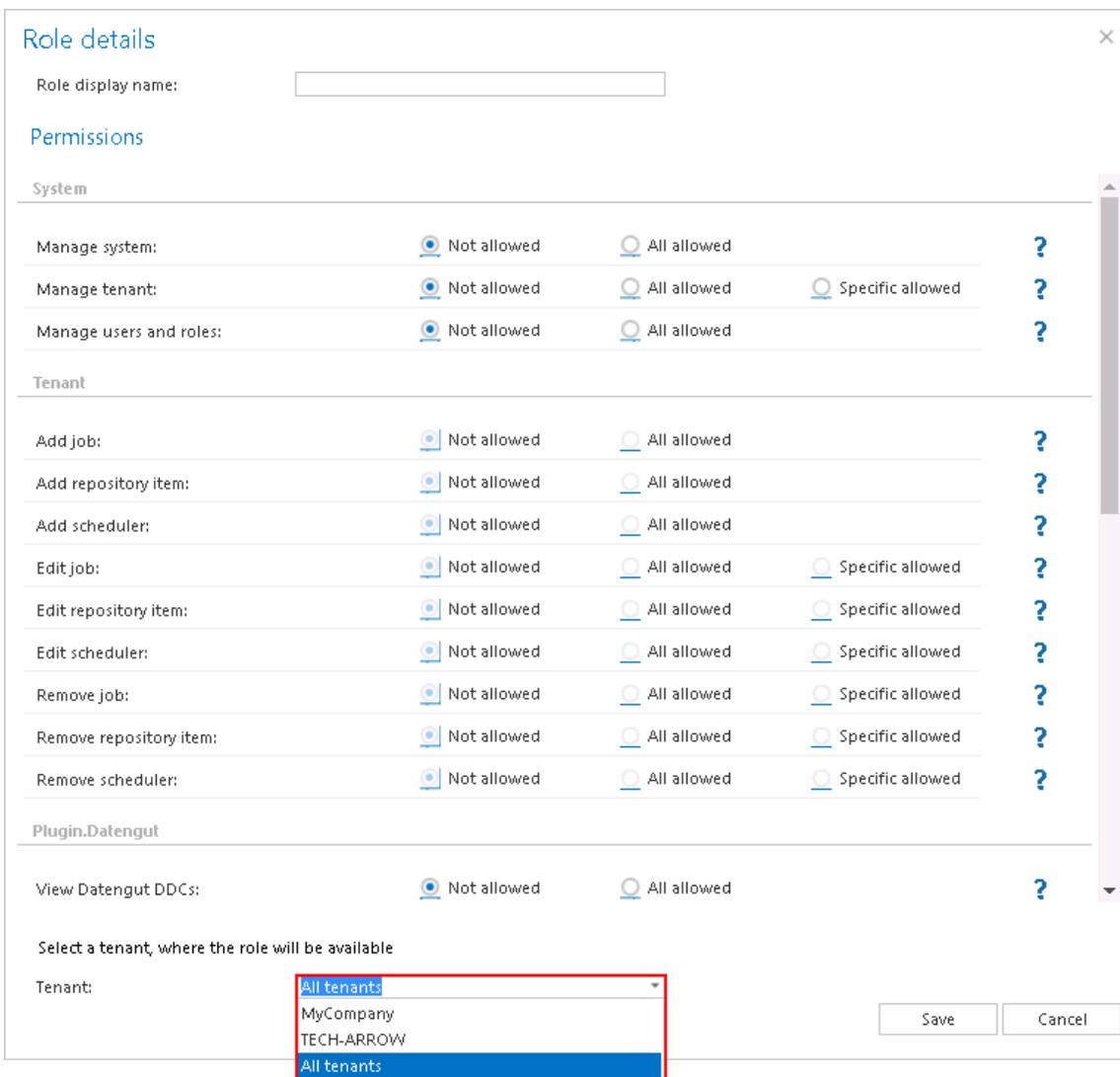
Tenant name	Tenant database	Search server url	Cluster group	Is enabled
<input checked="" type="checkbox"/> RFA test	*** RFAtestDB		Default	True
TECH-ARROW	*** MNEtestDB		Default	True

Role details

Based on availability, a role can be:

- **System level role** – which is **available for all tenants** in the system; the grid’s “Tenant name” column contains “All tenants”;
- **Tenant level role** – which is **available only for the selected tenant**; the grid’s “Tenant name” column contains the name of the selected tenant

The role’s availability is set in the **Role details** window, when creating it:



Role details [Close]

Role display name:

Permissions

System

Manage system:	<input checked="" type="radio"/> Not allowed	<input type="radio"/> All allowed	?	
Manage tenant:	<input checked="" type="radio"/> Not allowed	<input type="radio"/> All allowed	<input type="radio"/> Specific allowed	?
Manage users and roles:	<input checked="" type="radio"/> Not allowed	<input type="radio"/> All allowed	?	

Tenant

Add job:	<input checked="" type="radio"/> Not allowed	<input type="radio"/> All allowed	?	
Add repository item:	<input checked="" type="radio"/> Not allowed	<input type="radio"/> All allowed	?	
Add scheduler:	<input checked="" type="radio"/> Not allowed	<input type="radio"/> All allowed	?	
Edit job:	<input checked="" type="radio"/> Not allowed	<input type="radio"/> All allowed	<input type="radio"/> Specific allowed	?
Edit repository item:	<input checked="" type="radio"/> Not allowed	<input type="radio"/> All allowed	<input type="radio"/> Specific allowed	?
Edit scheduler:	<input checked="" type="radio"/> Not allowed	<input type="radio"/> All allowed	<input type="radio"/> Specific allowed	?
Remove job:	<input checked="" type="radio"/> Not allowed	<input type="radio"/> All allowed	<input type="radio"/> Specific allowed	?
Remove repository item:	<input checked="" type="radio"/> Not allowed	<input type="radio"/> All allowed	<input type="radio"/> Specific allowed	?
Remove scheduler:	<input checked="" type="radio"/> Not allowed	<input type="radio"/> All allowed	<input type="radio"/> Specific allowed	?

Plugin.Datengut

View Datengut DDCs:	<input checked="" type="radio"/> Not allowed	<input type="radio"/> All allowed	?
---------------------	--	-----------------------------------	---

Select a tenant, where the role will be available

Tenant:

Save Cancel

A role is a collection of permissions that will be assigned for the user when associating the given role with him.



The permissions can be divided into certain permission groups:

- **System level permissions** – Allow to manage the **system settings**, (Manage system: “All allowed”); **all tenants** (Manage tenant: “All allowed”) or **specific tenants** in the system (Manage tenant: “Specific allowed”), and to **manage users and roles** in the system. If the “Manage tenant” is specific in the role, then the given role will be available for a specific tenant only. Only a user with “Manage system” and/or “Manage tenant” permissions has the right to log in to the Central Administration.

Warning: Manage system permission does not allow to manage the entire system. A user with this permission has access to client applications settings, system-,license-,notification-, cluster-, login provider settings and to the notification scheduler. Such a user cannot create tenants or databases, this requires to have Manage tenants permission.

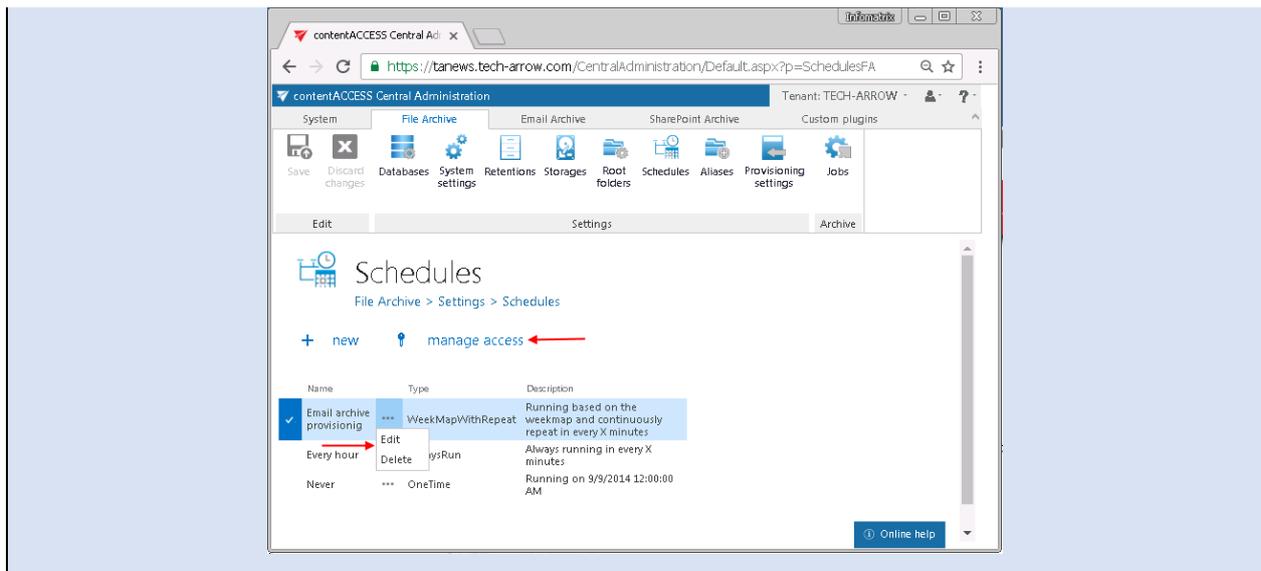
Note: Roles with Manage system and/or Manage tenant permissions cannot be assigned automatically (by contentACCESS email and file archive provisioning job).

Note: If the **Manage users and roles** permission is not assigned to a tenant administrator, then this tenant administrator will be able to view the roles only on the **Roles** page.

- **Tenant level permissions** – Allow to **manage all** jobs/repository items/schedulers (“All allowed”), and/or **to manage only specific** jobs/repository items/schedulers (“Specific allowed”) of the selected tenants.

Note: The **Edit**, **Delete** and **+ new** options on the Schedulers, Jobs, Storages, Databases, Aliases, Retentions, Shortcuts and Exchange connections pages/context menus are enabled based on the permissions defined in the **Role details**.

If the logged in user has got the Edit “All allowed” permission on the repository item and/or job and/or scheduler on the assigned tenant, and also has the **Manage users and roles** permission, then he can manage access to the selected object(s) on this tenant.



- Permissions to manage the **respective plugins of the selected tenant(s)** – Allow to **manage all or specific plugins** (email archive, file archive, SharePoint archive plugins etc.) **on all tenants** if Manage tenant is “All allowed” and you assign this role to user on all tenants.; allow to manage all or specific plugins **of the selected tenant** if Manage tenant is “Specific allowed”.

When you move your mouse over the question mark in the **Role details** dialog, the permission description gets displayed in a tooltip. Select the permissions that you want to assign for an already existing or for a newly created contentACCESS user, name your role, and save it.

Role assignment

Only user with "Manage users and roles" permissions can **assign roles** to users, edit role assignments and manage access to certain contentACCESS objects for second users on his own tenant. Otherwise the pages and options related to these settings (**Roles** and **Users** pages, and "**manage access to**" option on the respective pages) are not available for the logged on user in Central Administration.

The **logged on user's own permissions define, which roles this user will be able to assign, and which role assignments he will be able to edit.**

Note: In case that the logged on administrator has **specific** permissions on schedulers, repository items, jobs and/or to view the archive, he cannot assign roles containing these permissions for second users. E.g. If the logged user has specific permission to Edit job, then he cannot assign a role which contains Edit job permission.



The logged on user must have equivalent or more permissions on the tenant than the role to be assigned for the second user includes. E.g. if the logged on user has only "Edit all" repository items permission assigned on tenant "X", but he is not allowed to delete these repository items, then he is not allowed to assign a role for a second user with "Delete all" repository items permissions on this X tenant.

Or if the logged on user is tenant administrator on tenant "Y", but cannot view the archive mailboxes on his tenant (View mailboxes- not allowed), then he cannot assign a role (and also cannot edit a role assignment) containing permissions to view the archive mailboxes of this tenant.

The administrator can assign a role:

- **For a newly created/invited user** in the **Create/Invite user** dialog directly

Create / Invite a user

Create new user Invite user

Display name:

Login type:

Assign role

Role:

Tenant:

Globally allowed permissions of the selected role **will be assigned** to the user.

[Show details](#)

Save Cancel

- **for an already existing contentACCESS user** using the given user's "Assign role" context menu option

contentACCESS Central Administration

System File Archive Email Archive SharePoint Archive Custom plugins

Save Discard changes Connection User interface Roles Users Invitations Login providers System Licensing Notifications Monitoring Cluster

Edit Application Settings Security Services

Users

System > Security > Users

+ Create or invite user

Display Name	ID	Roles
Jack Bolton	3d5009b6-3b8b-4209-9b8f-8e0dc4723676	Tenant administrator
Administrator	3C-AD83-088D4CF07758	System administrator
BEEdit	04-bda7-787de96dc7c4	Standard user, Tenant administrator

Role assignment

Role:

Tenant:

Globally allowed permissions of the selected role **will be assigned** to the user.

[Show details](#)

Save Cancel

Important: If you are assigning a role containing both specific permissions and Manage tenant “All allowed” permissions and you have selected one specific tenant in the **Role assignment/Create /invite user** dialog, then every tenant will automatically get the Manage all tenants permission as it is defined in the role itself, and then you will be redirected to the **Assign specific permissions** page. If “All tenants” is selected in one of the above mentioned dialogs, then Manage all tenants permissions are assigned, but the user is not redirected to the **Assign specific permissions** page. These specific permissions can be assigned later using the user’s “Edit role assignment” context menu option.

Defining specific permissions of a role assignment

Definition of terms:

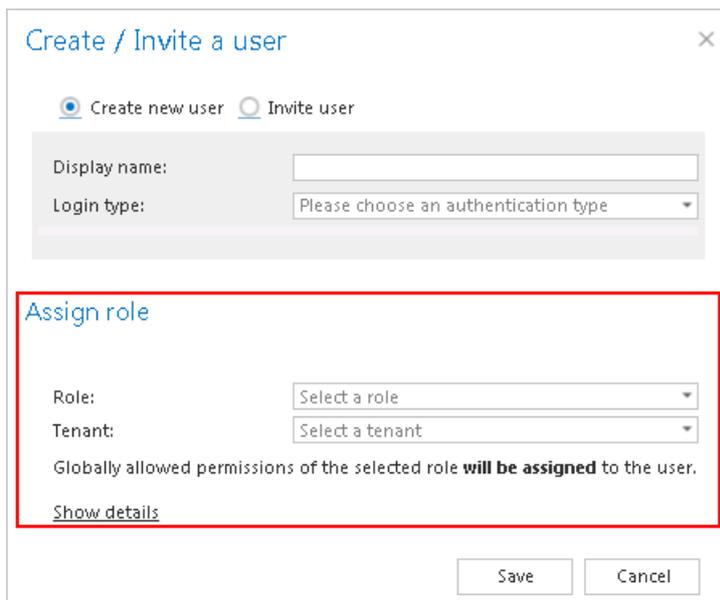
Specific permissions = user permissions which allow to manage only certain (specific) objects of the selected tenant (e.g. certain jobs of TECH-ARROW tenant only)

Objects = specific objects (databases, schedulers, jobs etc.) of the selected tenant

Specific permissions can be granted to various objects of the selected tenant(s): jobs, repository items (databases, storages, aliases, retentions, shortcuts and Exchange connections), schedulers and also to the processed contentACCESS data (e.g. permission to manage the archive mailbox). The administrator decides, which objects of which tenants will the user (with the given permissions) be able to manage. Specific permissions of a role assignment can be granted on the **Assign specific permissions** page. Only the objects with “Specific allowed” permissions are listed on this page (e.g. if TECH-ARROW tenant was selected, then TECH-ARROW’s jobs, repositories etc. with “Specific allowed” permissions are displayed).

To define specific permissions open the **Assign specific permissions** page. The page can be opened:

- From the **Create/invite user** dialog when creating/inviting a user;



- From the **Role assignment** dialog (user’s “Assign role” context menu option) when assigning a role to an already existing user.



Role assignment ✕

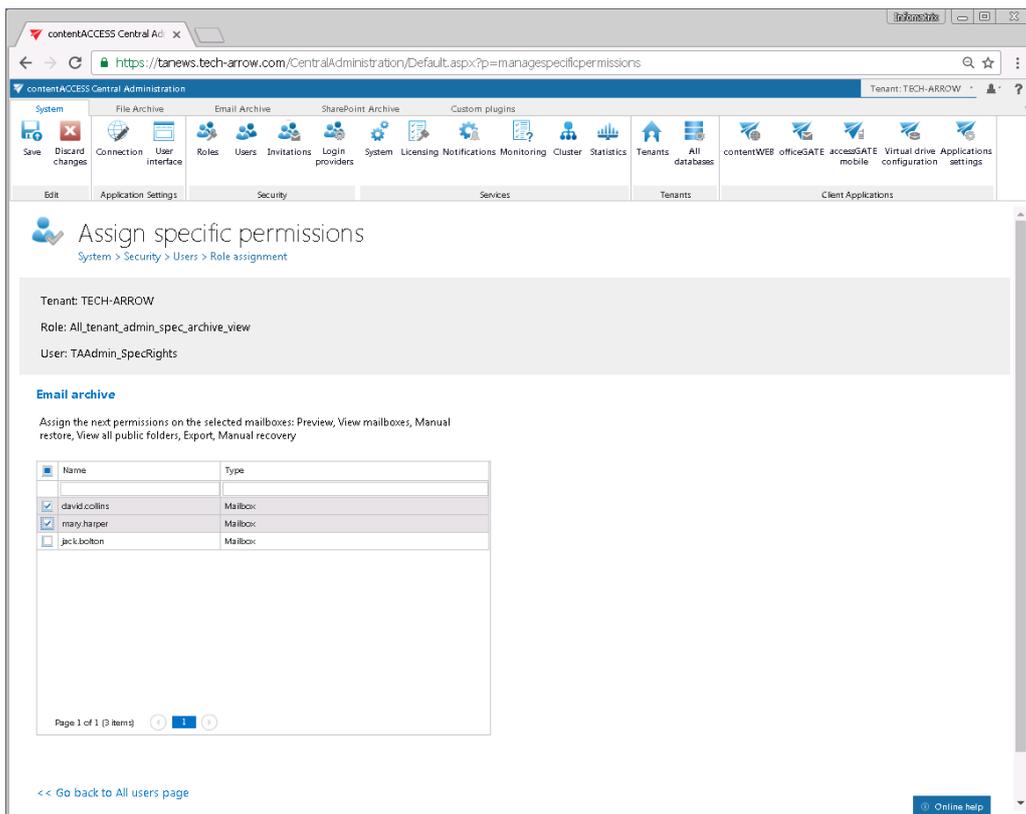
Role:

Tenant:

Globally allowed permissions of the selected role **will be assigned** to the user.

[Show details](#)

In one of the above mentioned dialogs, select the predefined role with the specific permissions, and then **select a tenant**, of which specific objects the user will be allowed to manage. When a given role is assigned to a user, the “All allowed” permissions and the manage tenant specific permission is assigned to the user. contentACCESS verifies, if there are any specific permissions defined in the respective role. If any specific permissions are found, the user is automatically redirected to the **Assign specific permissions** page (see below), where he can select the objects that the given user will be allowed to manage:

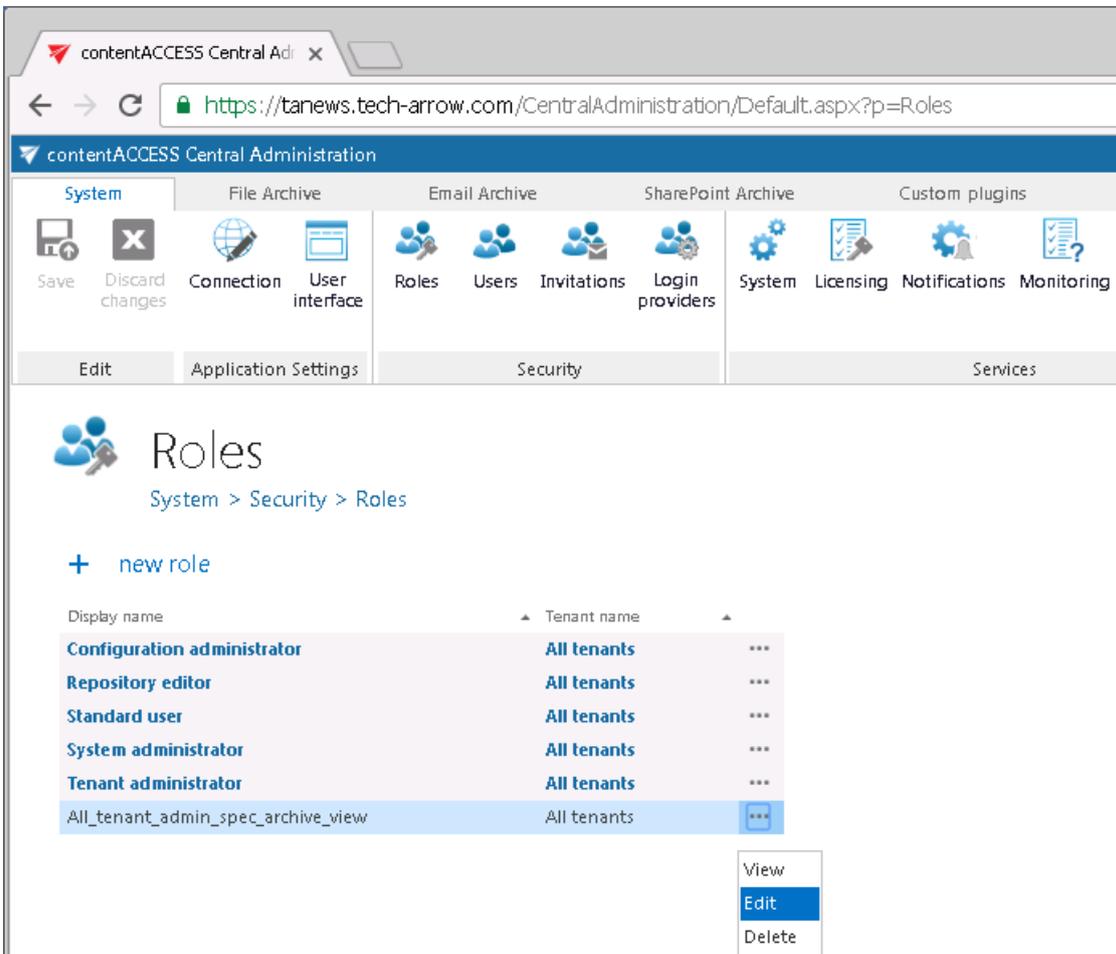


Tenant administrator role with specific permissions on the selected archive mailboxes

Important: If the user selects “All tenants” in the dialog (option is available if “Manage all tenants” permission is defined in the given role), then specific permissions page won’t be opened. The “All allowed” permissions (global permissions) will be granted to **All tenants** automatically.

Editing roles, editing role assignments

Roles can be edited in the **Role details** window. Open it using the given role’s context menu (option “Edit”).



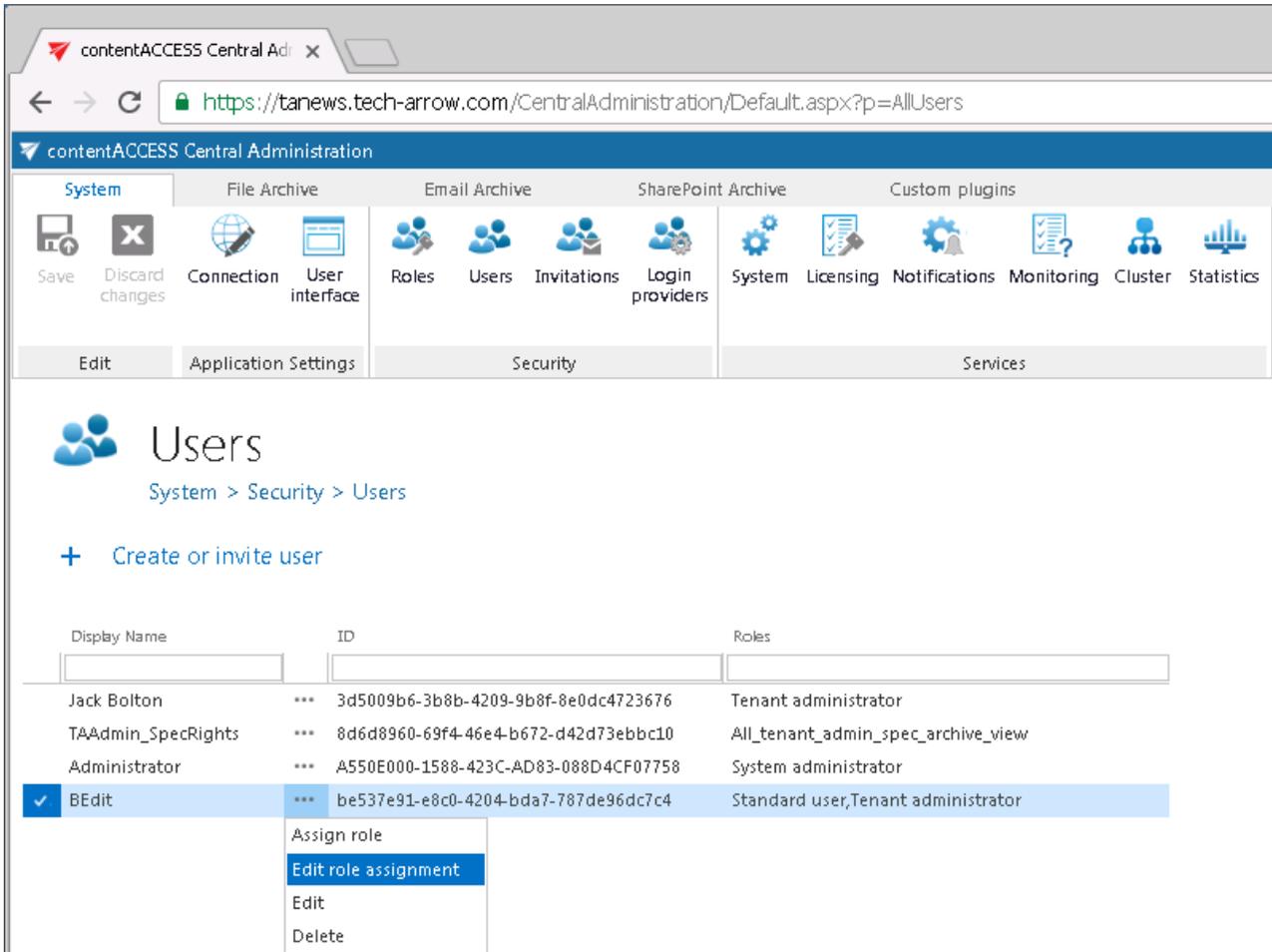
The screenshot shows the 'Roles' management page in the contentACCESS Central Administration. The breadcrumb trail is 'System > Security > Roles'. A table lists roles with their display names and tenant names. The 'All_tenant_admin_spec_archive_view' role is selected, and its context menu is open, showing 'View', 'Edit', and 'Delete' options.

Display name	Tenant name	
Configuration administrator	All tenants	...
Repository editor	All tenants	...
Standard user	All tenants	...
System administrator	All tenants	...
Tenant administrator	All tenants	...
All_tenant_admin_spec_archive_view	All tenants	...

The rule is that the logged on user cannot edit a role already assigned to himself, i.e. he cannot extend his rights.

Role assignments are roles already assigned to a given user, with or without specific permissions. These role assignments can be edited from the user’s context menu, using option “**Edit role assignment**”. The **Role assignment** window opens, where you select the role to be edited (you may have multiple roles

assigned). If the role has any specific permissions defined, the **Assign specific permissions** page opens, where you can change your settings.



The screenshot shows the 'Users' page in the contentACCESS Central Administration interface. The breadcrumb trail is 'System > Security > Users'. A table lists users with columns for Display Name, ID, and Roles. The 'BEdit' user is selected, and a context menu is open over it, showing options: Assign role, Edit role assignment, Edit, and Delete.

Display Name	ID	Roles
Jack Bolton	3d5009b6-3b8b-4209-9b8f-8e0dc4723676	Tenant administrator
TAAdmin_SpecRights	8d6d8960-69f4-46e4-b672-d42d73ebbc10	All_tenant_admin_spec_archive_view
Administrator	A550E000-1588-423C-AD83-088D4CF07758	System administrator
<input checked="" type="checkbox"/> BEdit	be537e91-e8c0-4204-bda7-787de96dc7c4	Standard user, Tenant administrator

Only users with "Manage users and roles" permissions can edit role assignments, otherwise the **Users** page is not available for them. It depends on the logged on user's own permissions, which role assignments he will be able to edit. **The logged on user must have equivalent or more permissions than the role assignment that he/she would like to edit has.** E.g. if the logged on user has no permissions to edit jobs of his associated tenant, then he cannot edit a role assignment with permissions to edit the jobs of this tenant.

Role cloning

With this feature it is easy to clone and customize (not only) the roles defined by the system. Click on the context menu of the selected role -> **Clone**.



Roles

System > Security > Roles

+ new role

Display name	Tenant name	
Configuration administrator	All tenants	...
Repository editor	All tenants	...
Standard user	All tenants	Clone
System administrator	All tenants	View
Tenant administrator	All tenants	Edit
Tenant configuration administrator	All tenants	Delete

Here you can add a role name, modify the permissions and select a tenant. After you made the desired changes, save your settings.



Role details ✕

Role display name:

Permissions

Manage tenant:	<input type="radio"/> Not allowed	<input type="radio"/> All allowed	<input checked="" type="radio"/> Specific allowed	?
Manage users and roles:	<input checked="" type="radio"/> Not allowed	<input type="radio"/> All allowed		?

Tenant

Add job:	<input checked="" type="radio"/> Not allowed	<input type="radio"/> All allowed		?
Add repository item:	<input type="radio"/> Not allowed	<input checked="" type="radio"/> All allowed		?
Add scheduler:	<input checked="" type="radio"/> Not allowed	<input type="radio"/> All allowed		?
Edit job:	<input checked="" type="radio"/> Not allowed	<input type="radio"/> All allowed	<input type="radio"/> Specific allowed	?
Edit repository item:	<input type="radio"/> Not allowed	<input checked="" type="radio"/> All allowed	<input type="radio"/> Specific allowed	?
Edit scheduler:	<input checked="" type="radio"/> Not allowed	<input type="radio"/> All allowed	<input type="radio"/> Specific allowed	?
Remove job:	<input checked="" type="radio"/> Not allowed	<input type="radio"/> All allowed	<input type="radio"/> Specific allowed	?
Remove repository item:	<input type="radio"/> Not allowed	<input checked="" type="radio"/> All allowed	<input type="radio"/> Specific allowed	?
Remove scheduler:	<input checked="" type="radio"/> Not allowed	<input type="radio"/> All allowed	<input type="radio"/> Specific allowed	?

Data

Select a tenant, where the role will be available

Tenant:

General use cases of how to create/assign roles

In this chapter we will demonstrate general use cases of how to work with roles. We will create 3 contentACCESS users with the following roles/permissions:

1. System administrator (name: "SysAdmin") **with the default "system administrator" role**
2. Tenant administrator (name: "TAAdmin") **of all tenants without** a right to edit/delete the jobs, repository items and schedulers and to manage the processed (archived) data.



- Email archive user (name: "EAUser") of TECH-ARROW tenants **with rights to view all** archive mailboxes, but with limited permissions to work with archive mailboxes (**recover, export allowed on specific mailboxes of the selected tenant only**).

A) Prepare roles for your future users first:

- For the System administrator the default role is already created, so here this step can be skipped.



- For the second user the role must be created so open the **Roles** page, click **+new** role and set the following in the **Role details** window:

Role display name: optional ("2nd_user_role" in this use case)

Manage system permission: "Not allowed"

Manage tenants: "All allowed" – so the associated user will have permissions to manage all tenants

Manage users and roles: "All allowed" – without this permissions user and role creation, association is not allowed

Under **section Tenants:** set the "Add job" "Add repository item" and "Add scheduler" to "All allowed" – the user will be able to create these objects for every tenant, but **set the Edit and Delete of the same objects to "Not allowed"** – the user won't be allowed to edit/delete these objects

Under **each Plugin section** select option **"Not allowed"** – the user won't be able to view and/or manage the processed data.

Save your changes and the role will be added to the **Roles** grid.



Role details

Select a tenant, where the role will be available

Tenant:

Role display name:

Enable ribbon filter:

Permissions

System	Not allowed	All allowed	Specific allowed	?
Assign user roles:	<input checked="" type="radio"/>	<input type="radio"/>		?
Manage system:	<input checked="" type="radio"/>	<input type="radio"/>		?
Manage tenant:	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	?
Manage users and roles:	<input type="radio"/>	<input checked="" type="radio"/>		?
View system auditing:	<input type="radio"/>	<input checked="" type="radio"/>		?
Tenant				
Add job:	<input type="radio"/>	<input checked="" type="radio"/>		?
Add repository item:	<input type="radio"/>	<input checked="" type="radio"/>		?
Add scheduler:	<input type="radio"/>	<input checked="" type="radio"/>		?
Edit job:	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	?
Edit repository item:	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	?
Edit scheduler:	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	?
Remove job:	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	?
Remove repository items:	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	?
Remove scheduler:	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	?
Data				
Customize GDPR search:	<input checked="" type="radio"/>	<input type="radio"/>		?
Delete from archive:	<input checked="" type="radio"/>	<input type="radio"/>		?
LegalHold				
Manage legal hold cases:	<input checked="" type="radio"/>	<input type="radio"/>		?
View legal hold cases:	<input checked="" type="radio"/>	<input type="radio"/>		?
PeriodicalSearch				
Create periodical searches:	<input checked="" type="radio"/>	<input type="radio"/>		?
Manage other user's periodical searches:	<input checked="" type="radio"/>	<input type="radio"/>		?
Plugin.EmailArchive				
View mailbox:	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	?
Export:	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	?
Manual archive:	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	?
Manual recovery:	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	?
Manual restore:	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	?
Preview:	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	?
View all public folders:	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	?
Plugin.FSArchive				
Manage remote file servers:	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	?
View File system folder:	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	?
Plugin.GDPR.Application				
View GDPR applications:	<input checked="" type="radio"/>	<input type="radio"/>		?
Plugin.GDPR.Exchange				
View GDPR mailboxes:	<input checked="" type="radio"/>	<input type="radio"/>		?
Plugin.GDPR.FileSystem				
View GDPR file system:	<input checked="" type="radio"/>	<input type="radio"/>		?
Plugin.Sharing				
View shared documents:	<input checked="" type="radio"/>	<input type="radio"/>		?
Plugin.SPArchive				
Manual recovery:	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	?
ViewSPSite:	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	?
Plugin.TeamsArchive				
View private channels:	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	?
View teams archive:	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	?



3. For the third user the role must be prepared, too. Create a new role and define the following settings in the **Role details** window:

Role display name: optional (“3rd_user_role” in this use case)

Tenant dropdown list at the bottom of the window: select “TECH-ARROW”

Everything must be set to “Not allowed” except of the **Plugin.EmailArchive** section, where:

View mailboxes, Preview and View all public folders are “All allowed”

Export, Manual recovery are “Specific allowed” – i.e. only specific mailboxes can be recovered and /or exported from contentWEB. The exact mailboxes will be set later on the **Assign specific permissions** page.

Save your changes.

Role details ✕

Select a tenant, where the role will be available

Tenant: ←

Role display name:

Enable ribbon filter:

Manage other user's periodical searches: Not allowed All allowed ?

Plugin.EmailArchive

View mailbox:	<input type="radio"/> Not allowed	<input checked="" type="radio"/> All allowed	<input type="radio"/> Specific allowed	?
Export:	<input type="radio"/> Not allowed	<input type="radio"/> All allowed	<input checked="" type="radio"/> Specific allowed	?
Manual archive:	<input type="radio"/> Not allowed	<input type="radio"/> All allowed	<input checked="" type="radio"/> Specific allowed	?
Manual recovery:	<input type="radio"/> Not allowed	<input type="radio"/> All allowed	<input checked="" type="radio"/> Specific allowed	?
Manual restore:	<input type="radio"/> Not allowed	<input type="radio"/> All allowed	<input checked="" type="radio"/> Specific allowed	?
Preview:	<input type="radio"/> Not allowed	<input checked="" type="radio"/> All allowed	<input type="radio"/> Specific allowed	?
View all public folders:	<input type="radio"/> Not allowed	<input checked="" type="radio"/> All allowed	<input type="radio"/> Specific allowed	?

Plugin.FSArchive

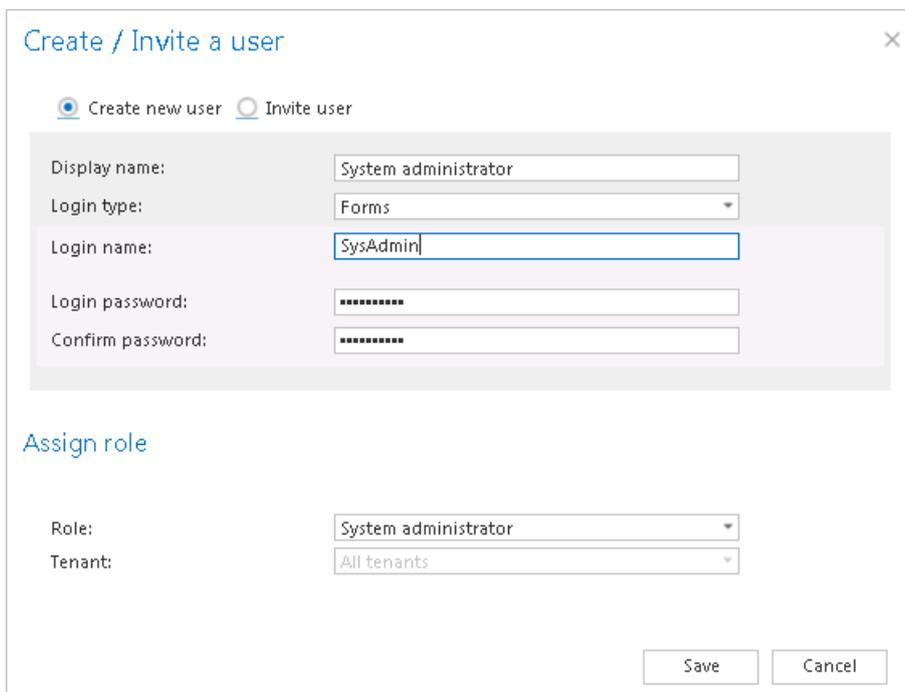
Manage remote file servers:	<input checked="" type="radio"/> Not allowed	<input type="radio"/> All allowed	<input type="radio"/> Specific allowed	?
View File system folder:	<input checked="" type="radio"/> Not allowed	<input type="radio"/> All allowed	<input type="radio"/> Specific allowed	?

Plugin.GDPR.Application

B) Create your users and assign roles to them

Now the roles for all three users are ready. We just have to create users and assign the roles to them, and to set specific permissions for our 3rd (Email Archive) user. In these use cases we will create users with Forms provider. Go to **Users** page (System → Security → Users) and click “**create or invite user**”.

1. Create a system administrator, set his credentials and assign the default “system administrator” role to him. Save the user.



Create / Invite a user ×

Create new user Invite user

Display name:

Login type:

Login name:

Login password:

Confirm password:

Assign role

Role:

Tenant:

2. Create your **TAAdmin** tenant administrator user and assign “**2nd_user_role**” to him. Select “All tenants” from the tenants dropdown list. The Add job, scheduler, repository item, Manage tenants and Manage users and roles permissions will be assigned for the user on all tenants. Other permissions that we set to not allowed won’t be granted for the user. Save your user and use it.

Create / Invite a user ✕

Create new user
 Invite user

Display name:

Login type:

Login name:

Login password:

Confirm password:

Assign role

Role:

Tenant:

Globally allowed permissions of the selected role **will be assigned** to the user on the selected tenant.

Plugin: Add job,
Scheduler: Add scheduler,
Repository: Add repository item,
Tenant: Manage tenant,
System: Manage users and roles,

[Hide details](#)

3. Create your **EAuser** email archive standard user and assign “**3rd_user_role**” to him. “TECH-ARROW” will be automatically selected in tenants dropdown list, as this role was created for this specific tenant only.

In the details part of the window you can see the global permissions allowed for the user on this TECH-ARROW tenant – the user is able to view all archive mailboxes and public folders and also to use the email archive’s preview function in contentWEB.

Create / Invite a user ✕

Create new user Invite user

Display name:	<input type="text" value="EAUser"/>
Login type:	<input type="text" value="Forms"/>
Login name:	<input type="text" value="EAUser"/>
Login password:	<input type="password" value="*****"/>
Confirm password:	<input type="password" value="*****"/>

Assign role

Role:

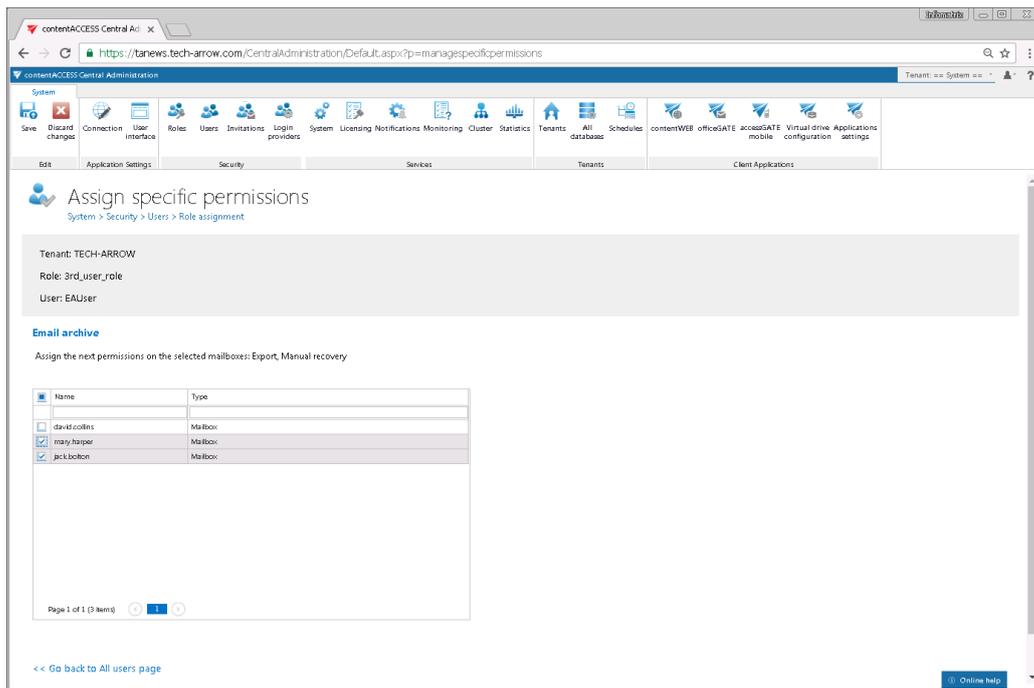
Tenant:

Globally allowed permissions of the selected role **will be assigned** to the user on the selected tenant.

EmailArchive: Preview, View all public folders, View mailboxes,

[Hide details](#)

The role assigned to the **EAUser** has also specific email archive recovery and export permissions on the TECH-ARROW tenant. As there are specific permissions defined in the role, the admin is automatically redirected to the **Assign specific permissions** page, where he can set the mailboxes that the EAUser will be able to recover and export. In this use case this permission is granted on mary.harper's and jack.bolton's mailboxes. Save your changes and use your EAUser.



Managing access to contentACCESS objects

Definition of terms:

Logged on user – the user logged in to the Central Administration, who has the permissions to manage access to contentACCESS objects;

Second user – the explicit user, who gets the rights (involved in the assigned role) to manage certain contentACCESS objects;

Tenant objects – objects like jobs, repositories, schedulers, archive mailboxes etc. of the given tenant;

Tenant repositories – databases, storages, retentions, shortcuts, Exchange connections, aliases of the tenant.

contentACCESS allows to manage access to the contentACCESS objects for second users. These objects are the following:

- **schedulers and repositories** of tenants (database, storage, retention, shortcut, Exchange connection, alias)
- **jobs** of tenants
- **archive mailboxes** of a given tenant
- **the file archive** of the tenant



- the **tenant** itself

In case of schedulers, repositories and jobs the “manage access” means that the logged on user (with the necessary permissions) assigns for a second user a role containing permissions to

- edit and/or
- delete

the assigned tenant’s

- schedules and/or
- repositories and/or
- jobs.

In case of tenants “manage access” means that the logged on user grants rights for a second user to manage the tenant assigned for him, i.e. he **gives tenant administrator permissions** for this user. The second user’s exact permissions on the given tenant are defined in the assigned role.

In case of **archive mailboxes** and **file archive** “manage access” means that the logged on user grants for the second user access rights to the archive mailboxes and file system archive on the assigned tenant.

The permissions of the role assignment define what the second user will be allowed to manage. E.g. if my user called “Job manager” has got “Edit job – All allowed” permission on the TECH-ARROW, but the “Delete job” permission is not allowed in his role assignment, then he will be able to edit the jobs of this tenant, but won’t be able to delete any jobs of the tenant.

The **user logged on to the Central Administration**, who is **able to give access e.g. to TECH-ARROW tenant’s objects for second users**, must have “**Manage users and roles**” permissions and “**Manage tenant**” permissions on the TECH-ARROW tenant and also

- **Edit repositories** – “**All allowed**” permission to be able to manage access to the repository items on the TECH-ARROW tenant;
- **Edit jobs** – “**All allowed**” permission to be able to manage access to the jobs of the TECH-ARROW tenant;
- **Edit schedules** – “**All allowed**” permission to be able to manage access to the schedules of the associated tenant
- **Manage tenant** –permission on the TECH-ARROW tenant to be able to add tenant administrator rights on the TECH-ARROW tenant for a second user



- **View mailboxes/View folders/View public folders** – “All allowed” permissions on the TECH-ARROW tenant to be able to give access to the archive mailboxes/file system root folders/public folders for second user(s) on the tenant.

The rule is that the logged on user must have equivalent or more permissions than the role to be assigned for a second explicit user. E.g. the logged on user is not allowed to assign a role for a second user containing permission “Delete job”, if this permission is not granted for him as well.

Manage access option is available for the logged on user on the respective pages of the Central Administration.

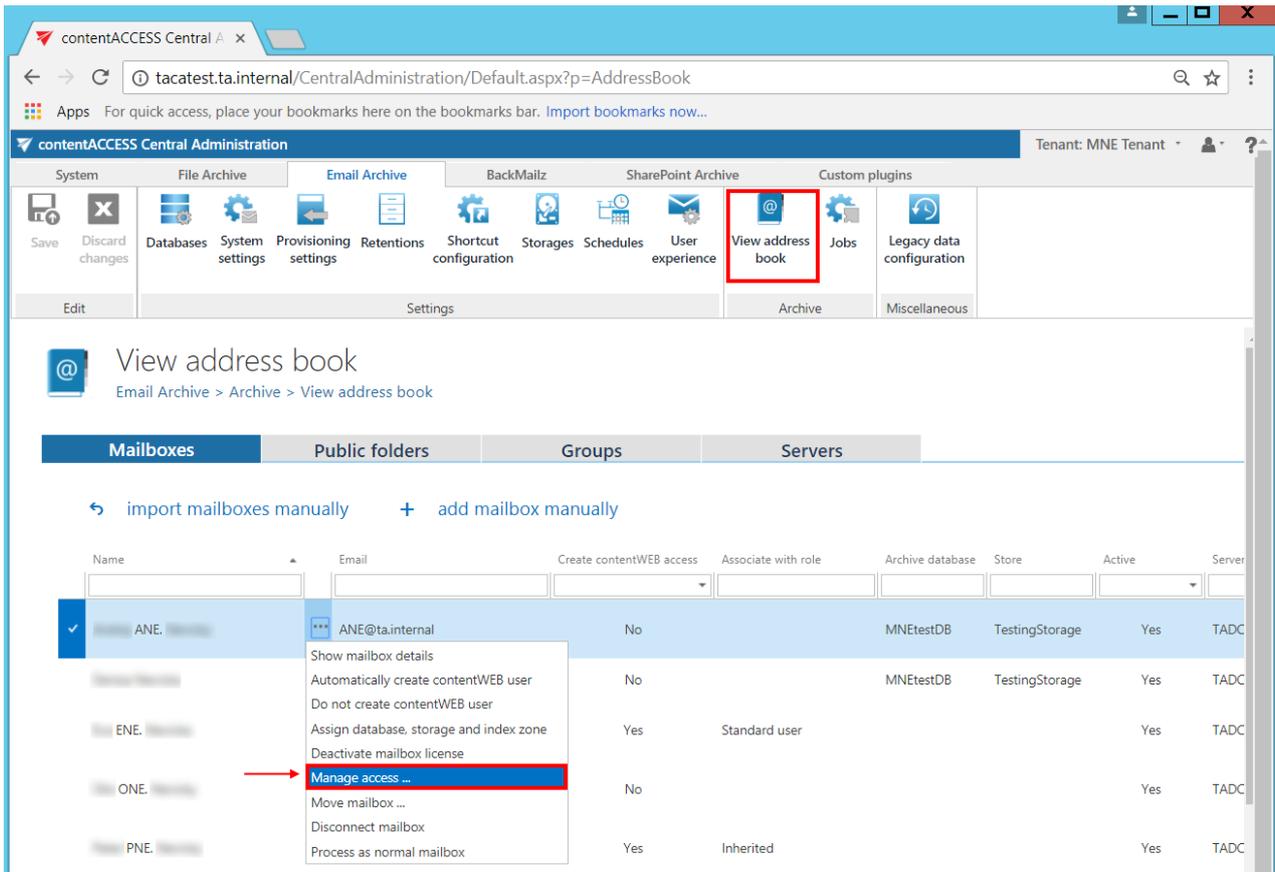
In case of repository items, schedules, jobs and tenants the option is available above the list of items:

The screenshot shows the 'Jobs' page in the contentACCESS Central Administration interface. The breadcrumb navigation is 'File Archive > Archive > Jobs'. The page includes a toolbar with buttons for '+ new', 'refresh', 'disable auto refresh', and 'manage access'. The 'manage access' button is circled in red. Below the toolbar is a table with columns: ID, Display Name, Type, Status, Last Start, Last Duration, Progress, Summary, Next Start, Is active, Cluster node, and Running on. The table contains one row for an 'Archive job'.

ID	Display Name	Type	Status	Last Start	Last Duration	Progress	Summary	Next Start	Is active	Cluster node	Running on
8	Archive job	File system archive	Idle	6 weeks ago	25 seconds	100 %	1 folders processed 185 documents processed (185 newly archived)	Never	Yes	Any available	-

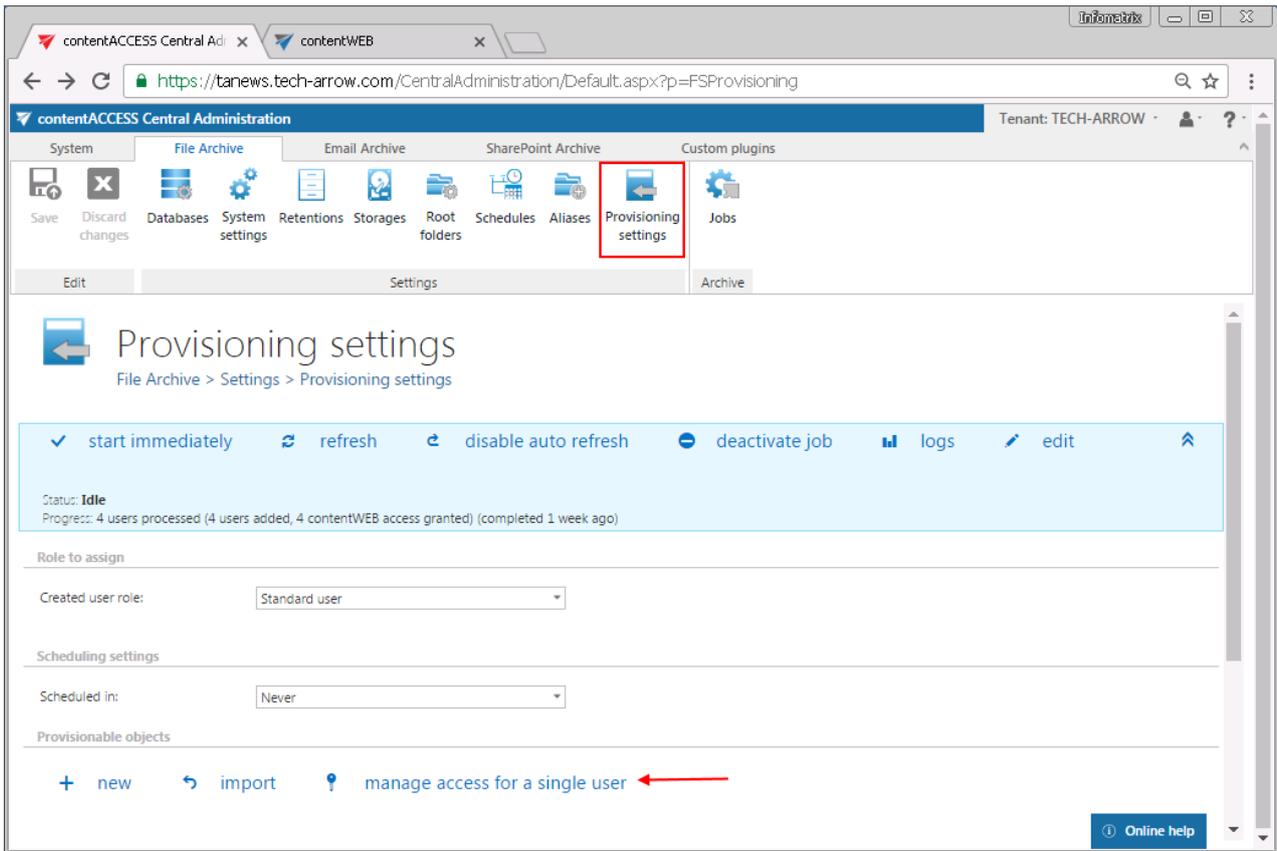
Screenshot A: Manage access to the TECH-ARROW tenant's file archive jobs

In case of archive mailboxes the option is available in the Address book, in the context menu of the given Exchange mailbox:



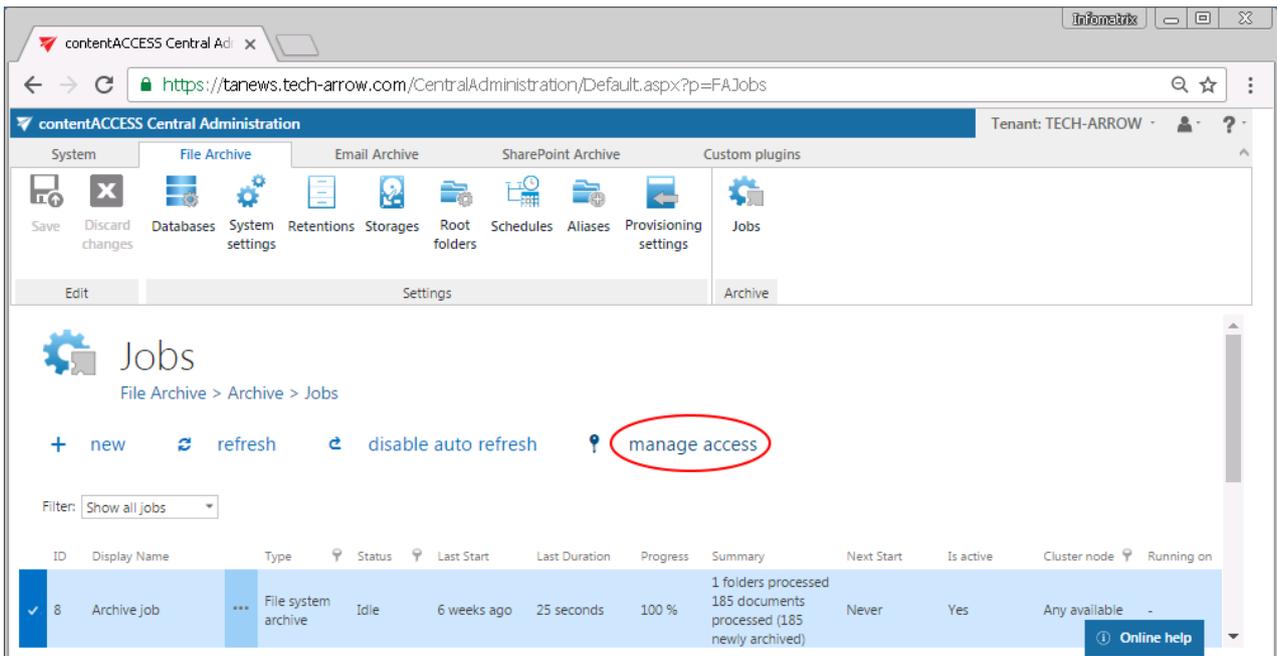
Screenshot B: Manage access to ane’s archive mailbox

In case of file system archive the option is available in the File archive’s Provisioning settings:



Screenshot C: Manage access to the file system archive folders

First, the user needs to select an item (a given job, database, retention, mailbox etc.) from the list.





In any case, by clicking the “manage access” option, the logged on user is redirected to the **Manage access to Object** page. Here he can manage access to the contentACCESS object. He clicks **+new** and the **Create role association** window opens.

The **Role** dropdown list lists only the roles that the logged on user is allowed to assign, and those that contain specific permissions on that object (in this case the object is the job). Roles containing “All allowed” permissions (e.g. “Edit job –All allowed” or “View mailboxes – All allowed”) cannot be granted on the “Manage access to Object page”. The user selects the role with the necessary permissions and assigns it to a new or an existing contentACCESS user.

In this use case we grant access for Jack Bolton to edit the Archive job of TECH-ARROW tenant.

The **TAAdmin_job_editor** role is already prepared and contains permission to edit specific job(s) of this tenant (“Edit job – Specific allowed”):

Role details

Role display name:

Permissions

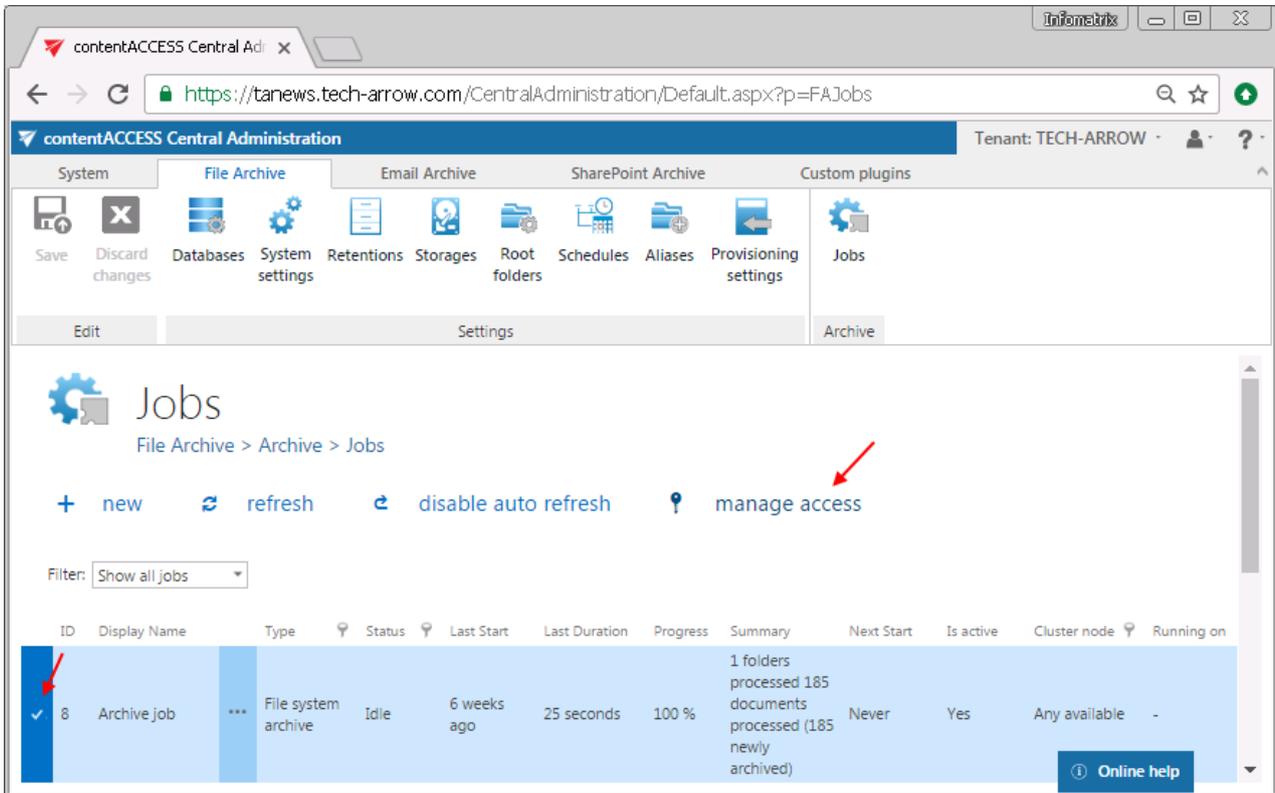
System	Not allowed	All allowed	Specific allowed	
Manage system:	<input checked="" type="radio"/>	<input type="radio"/>		?
Manage tenant:	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	?
Manage users and roles:	<input checked="" type="radio"/>	<input type="radio"/>		?
Tenant				
Add job:	<input checked="" type="radio"/>	<input type="radio"/>		?
Add repository item:	<input checked="" type="radio"/>	<input type="radio"/>		?
Add scheduler:	<input checked="" type="radio"/>	<input type="radio"/>		?
Edit job:	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	?
Edit repository item:	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	?
Edit scheduler:	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	?
Remove job:	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	?
Remove repository item:	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	?
Remove scheduler:	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	?
Plugin.Datengut				

Select a tenant, where the role will be available

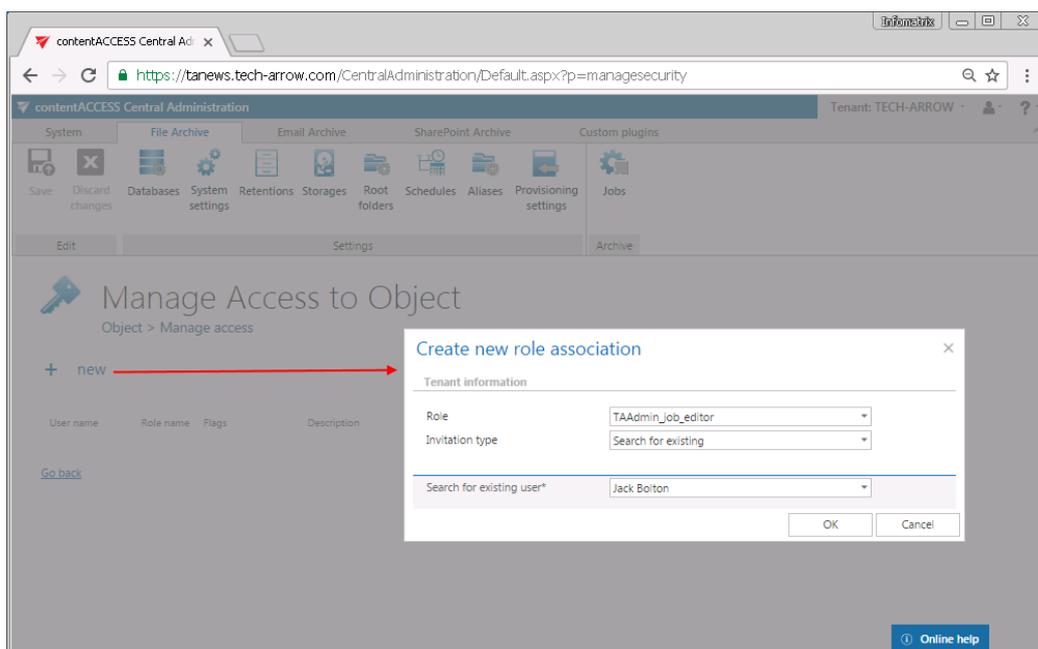
Tenant:



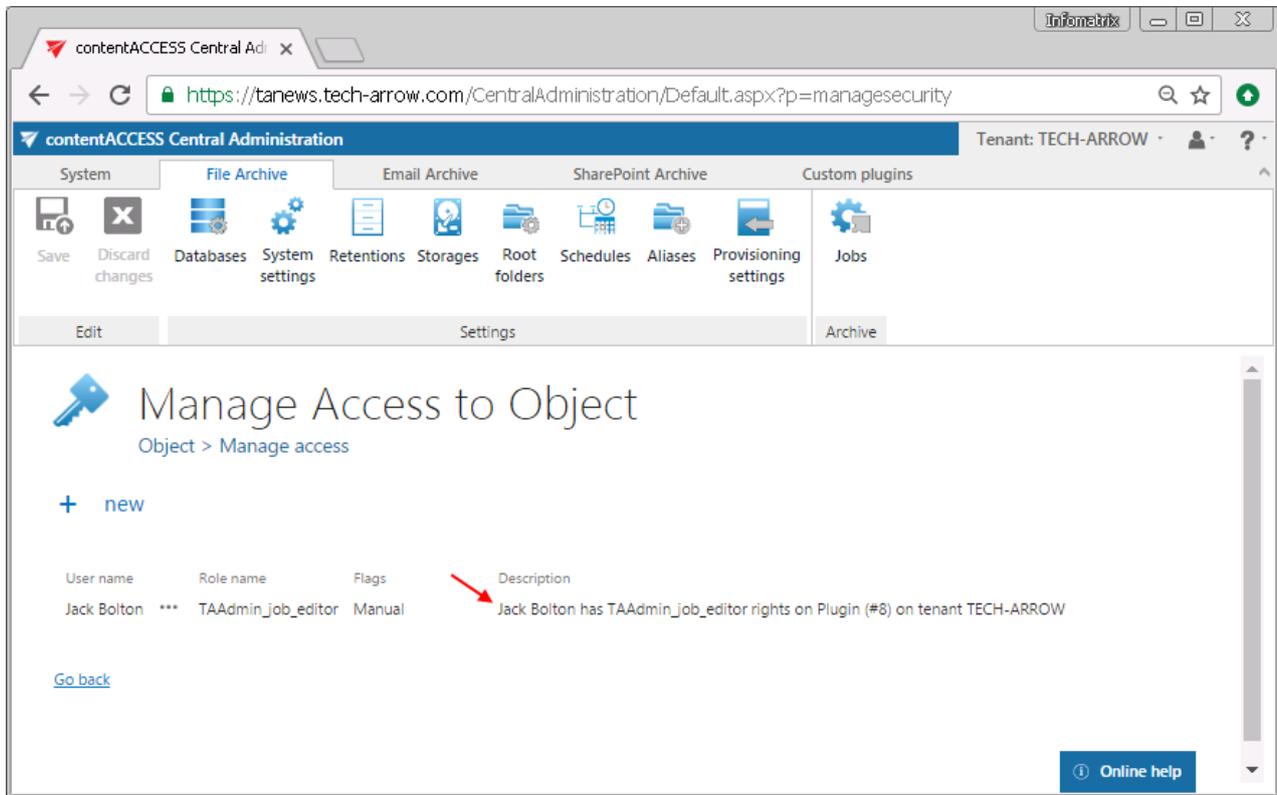
On the File Archive’s **Jobs** page of TECH-ARROW tenant we locate the **Archive job**, select it and click “manage access”.



On the “Manage access to Object” page, we select the “TAAdmin_job_editor” role, and assign it to our existing user, Jack Bolton:



Our Jack Bolton user has now rights to edit the “Archive job” on the TECH-ARROW tenant, but he cannot delete this job from the list.



Login providers

A contentACCESS user may log into contentACCESS (and/or into client application “contentWEB”) with an external user account (using third-party providers) or internal (“Forms” provider) user account.

The following external authentication providers are available in contentACCESS:

- Windows
- Office 365
- Google
- Datengut
- Perceptive
- Microsoft Exchange
- External AD

If you use a third party provider, then this third party authentication provider will authenticate you when logging into the system.



Note: When using **Microsoft Exchange** login provider, email address is used as username and Exchange password as password.

It's also possible to set Office 365, Google and Windows providers as automated single sign on providers (column option Auto login), and to use them as default providers to sign in to the Central Administration (read more [here](#)) and/or into contentWEB (read more [here](#)). The configuration steps required for third-party providers are detailed in the External login provider configuration chapter. The **Forms** type requires to enter credentials when logging in.

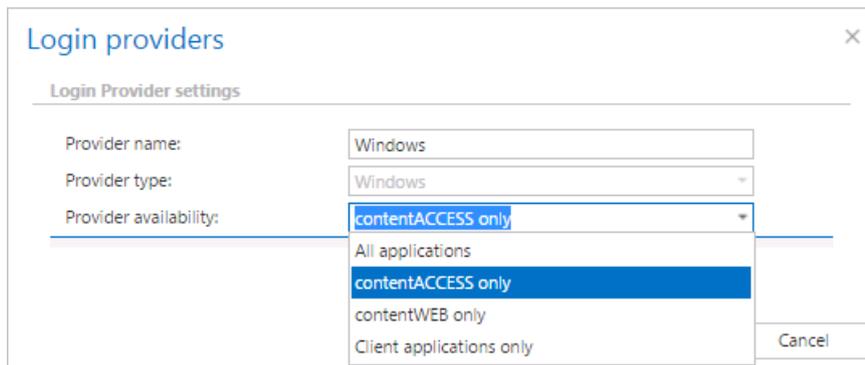
When setting up a user account, a login type must be always selected. Users can only use login types which have been enabled in "Login providers". "Windows" and "Forms" login providers are enabled by default. Other providers are available only after they have been configured. The configuration settings of a login provider allow to define, if the login provider can be used to log in to the contentACCESS Central Administration only, to contentWEB only, or to both of them.

Login providers' context menu options

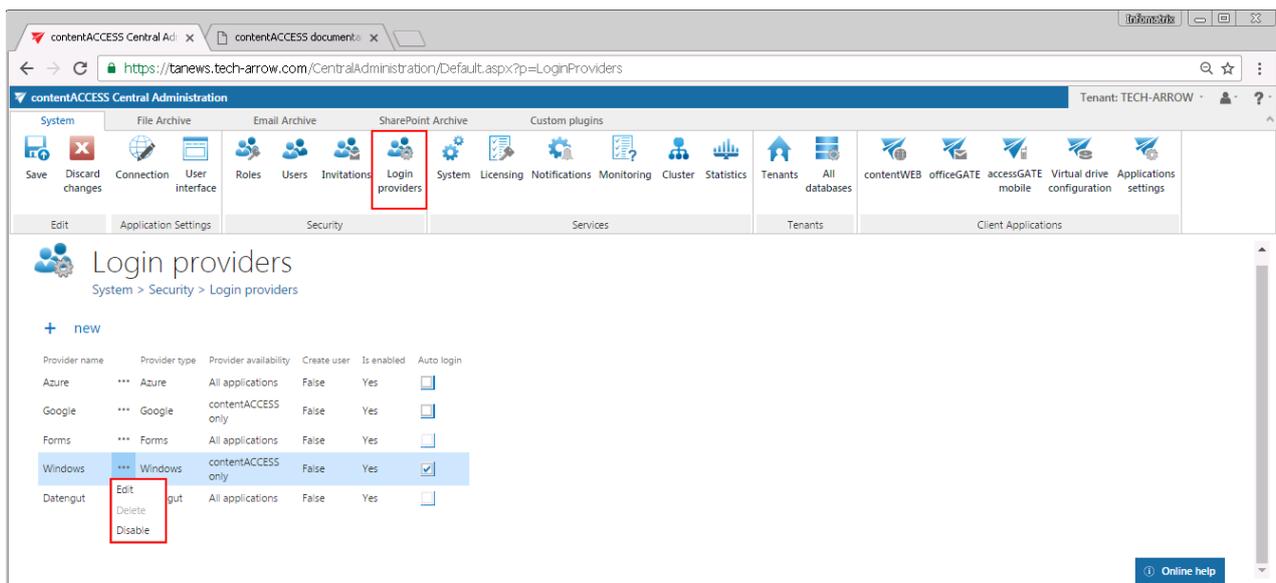
The list of enabled providers can be found on the **Login providers** page. To open it, navigate to the **System** tab → **Security** group on the ribbon and click on the **Login providers** button.

To edit or enable/disable/delete providers, open its context menu on the **Logins provider** page, and click on the desired item in the dropdown list.

- Option "edit": Use this option to edit/modify the current login provider configurations. Here you can set the provider availability, i.e. to define, if the appropriate login provider can be used to log in to:
 - contentACCESS Central administration only – option "contentACCESS only"
 - contentWEB only – option "contentWEB only"
 - both contentACCESS and contentWEB – option "All applications"



- Option “disable”: If a provider is disabled, it will not be possible to log in to contentACCESS with it. For security reasons, the user can't disable “Forms” authentication.
- Option “delete”: For security reasons, the user can't delete “Windows” and “Forms” login providers. Those login providers, which are already associated with a user login, also can't be deleted, only disabled.



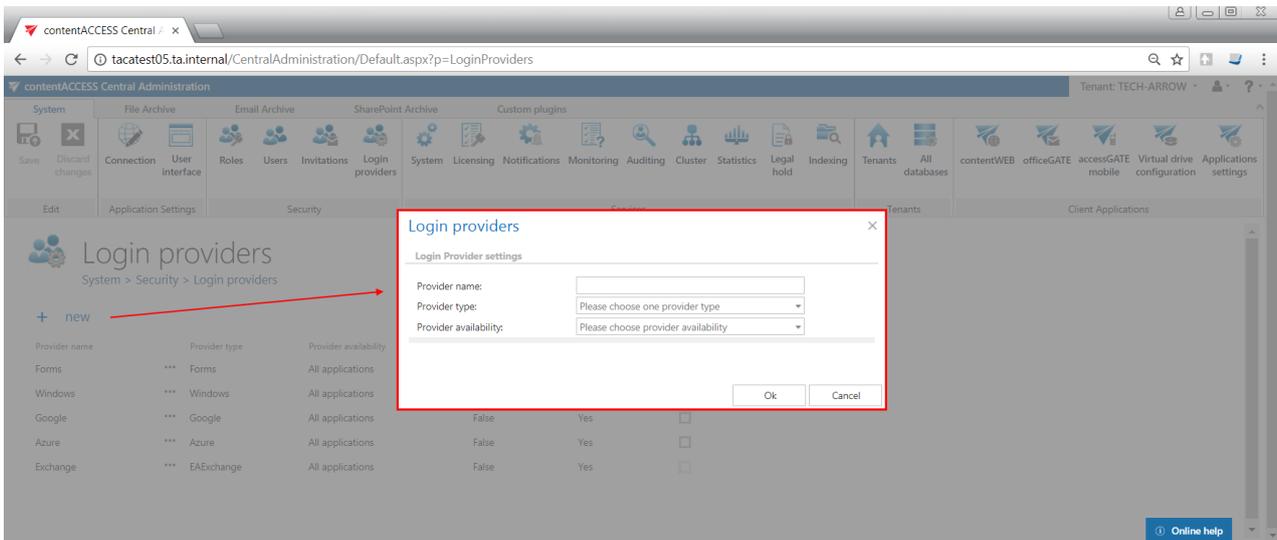
External login provider configuration

To configure a new login provider, click on **+new** on the **Logins provider** page. The **Login providers** dialog will open. It requires to:

- name the provider,
- choose a supported external provider from the **Provider type** list,
- set the provider availability – here you may set the applications that will use the given provider
- fill the required fields – detailed below for the provider types



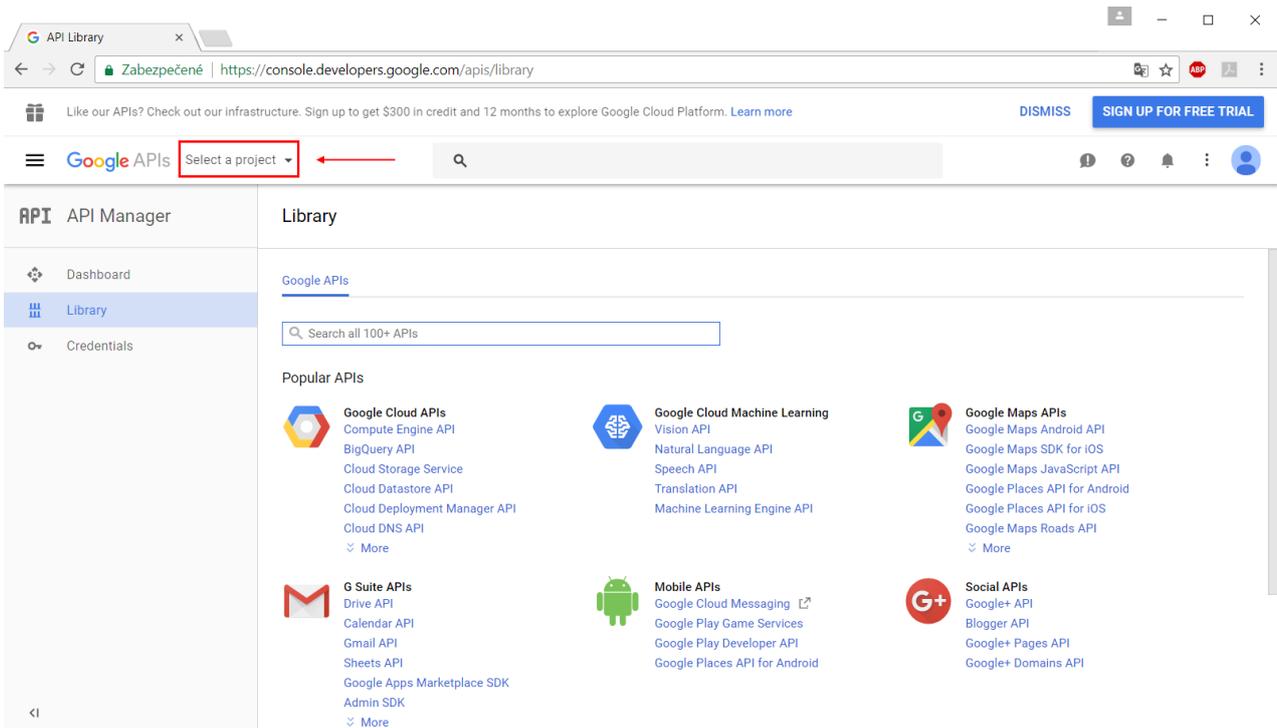
- and click on **OK** to save the settings.



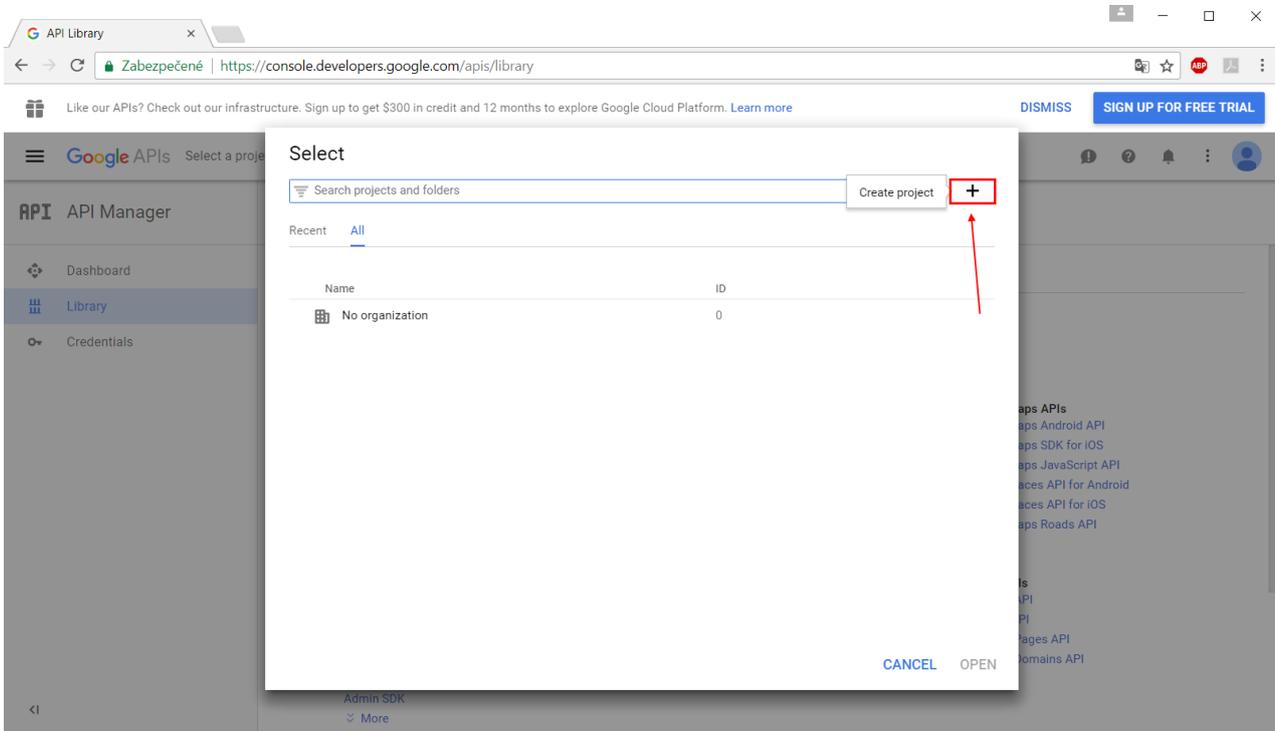
Configuring Google OAuth

contentACCESS supports Google authentication as well. If you would like to use it, you need to apply for a Client ID and Client Secret by registering the contentACCESS application on the **Google Developers Console** page first. Open the page, sign in with your Google account and follow these steps:

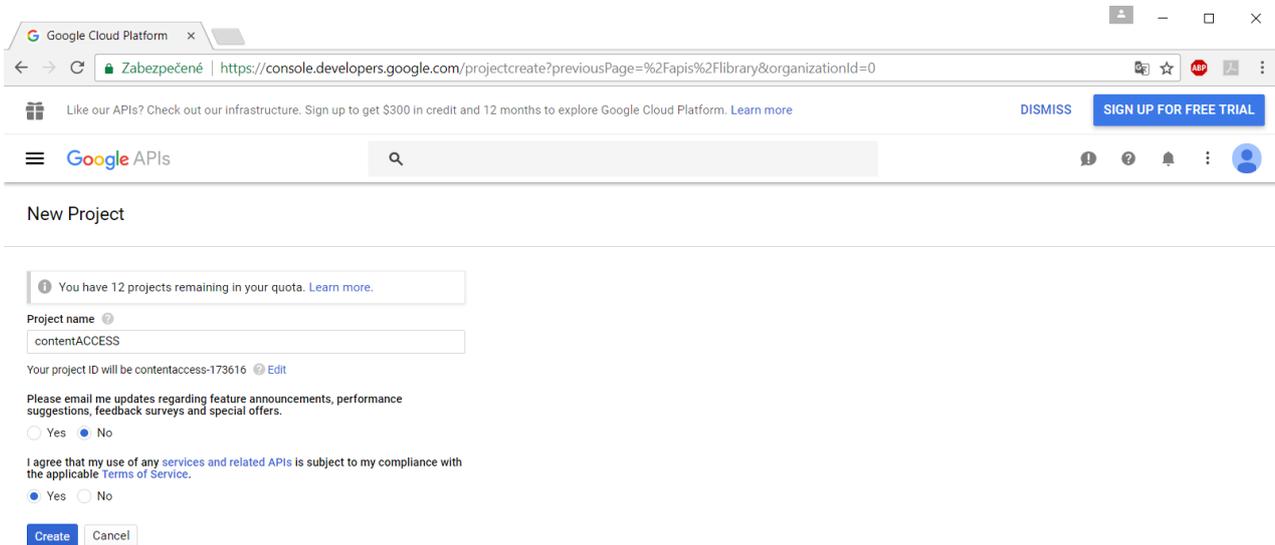
- 1) Click **Select a project** in the upper left corner of the menu:



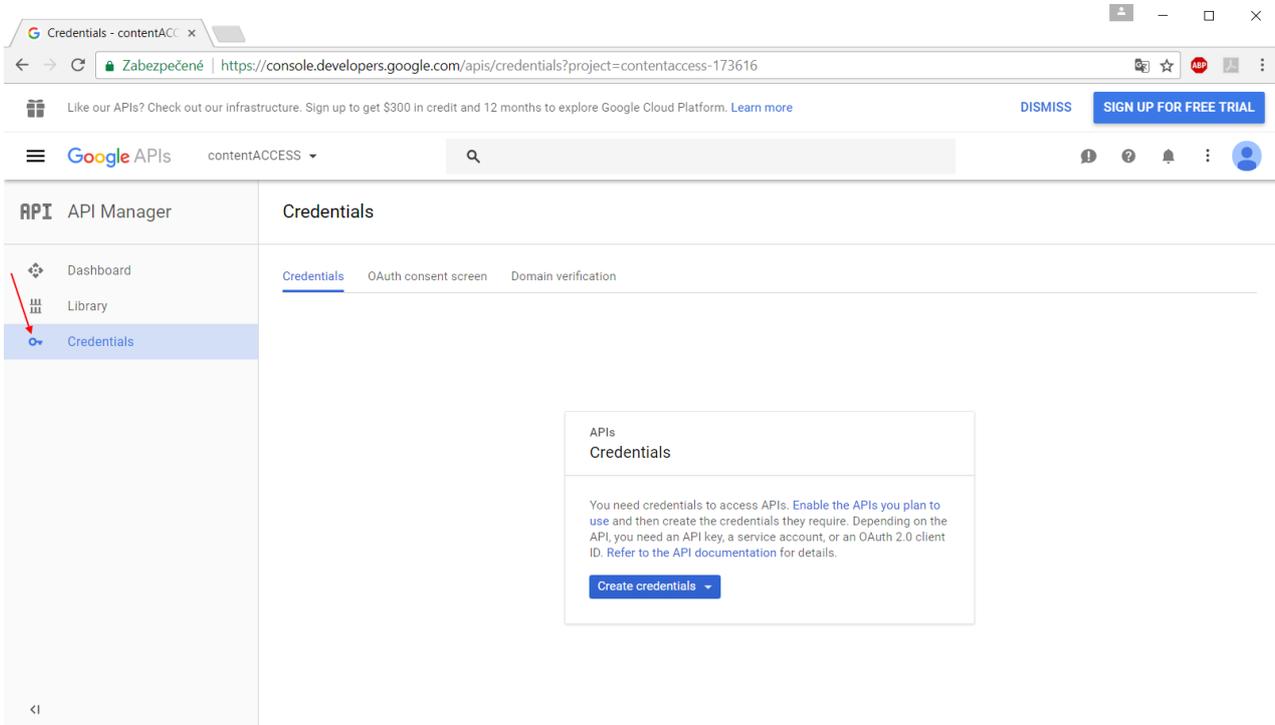
2) Click on **Create project** in the upper right corner:



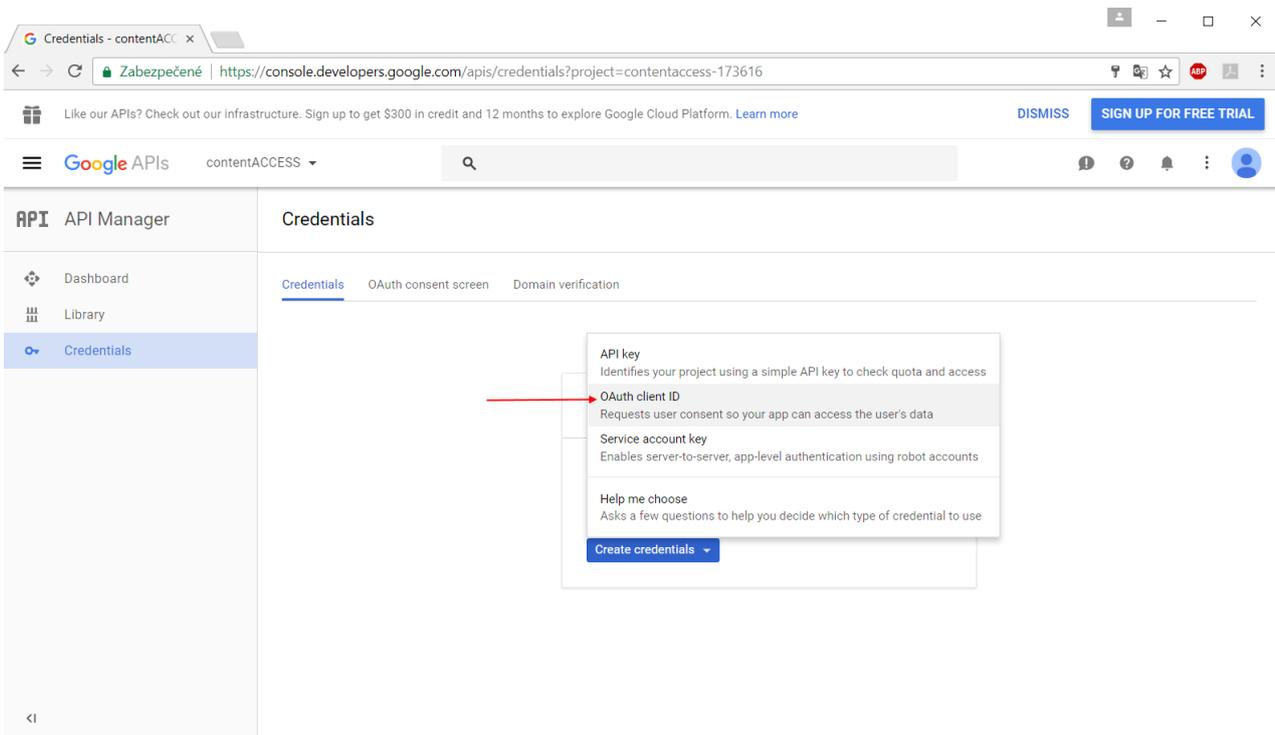
3) Name your project and create it:



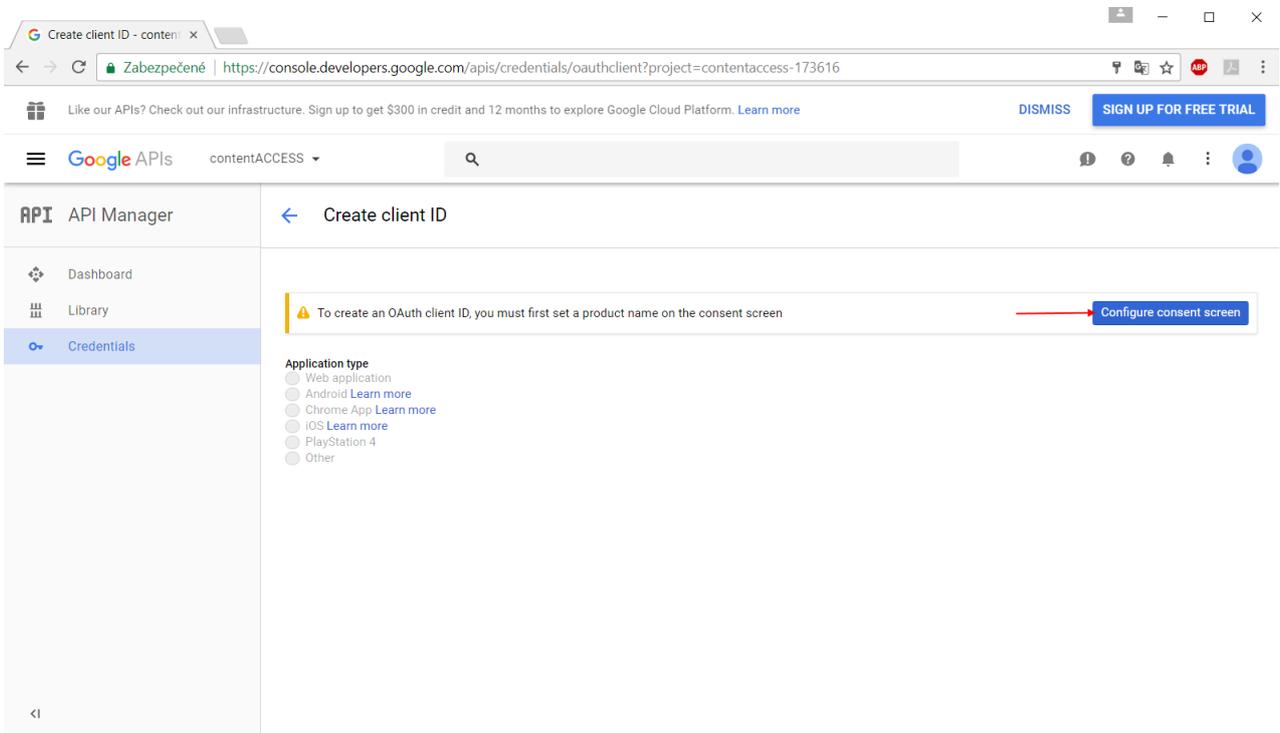
4) If the API Manager page isn't already open, open the console menu and select **“API manager”**. On the left, click **“Credentials”** and then select your project.



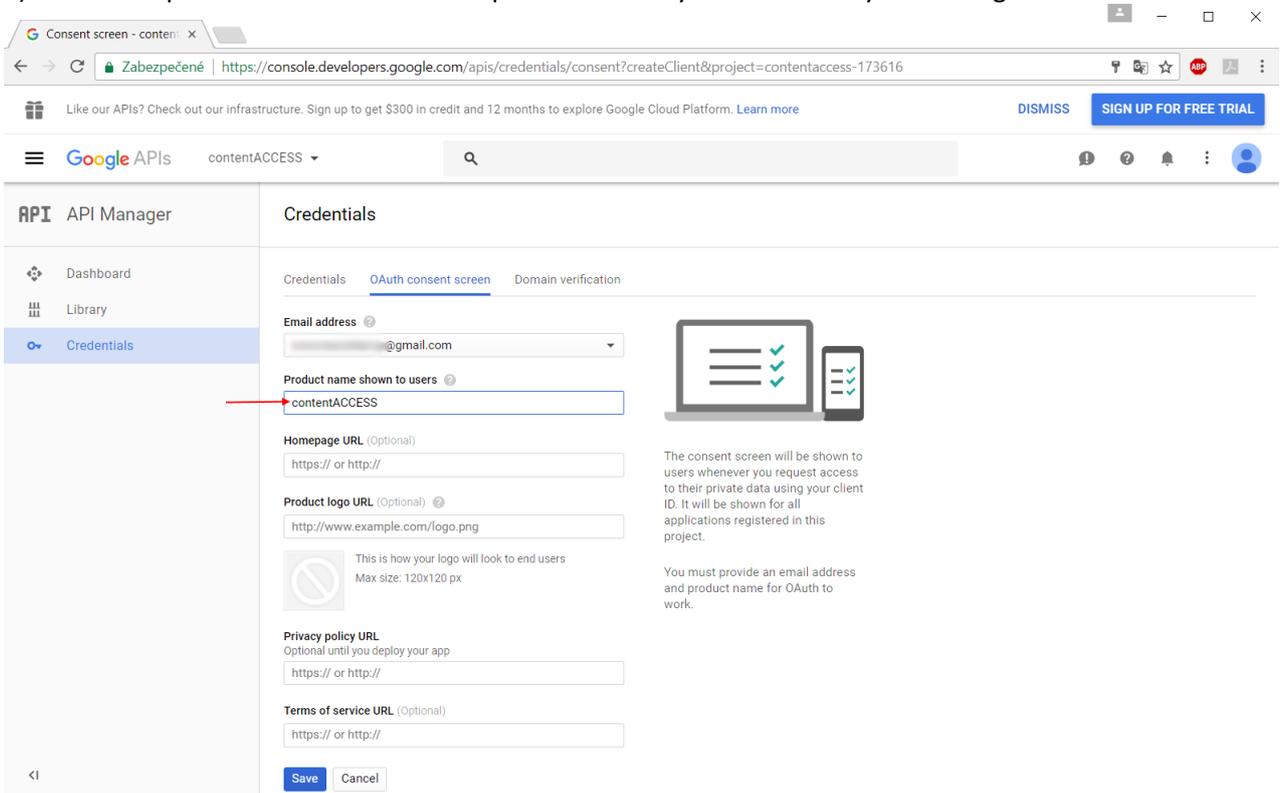
5) Click **“Create credentials”**, then select **“OAuth client ID”**.



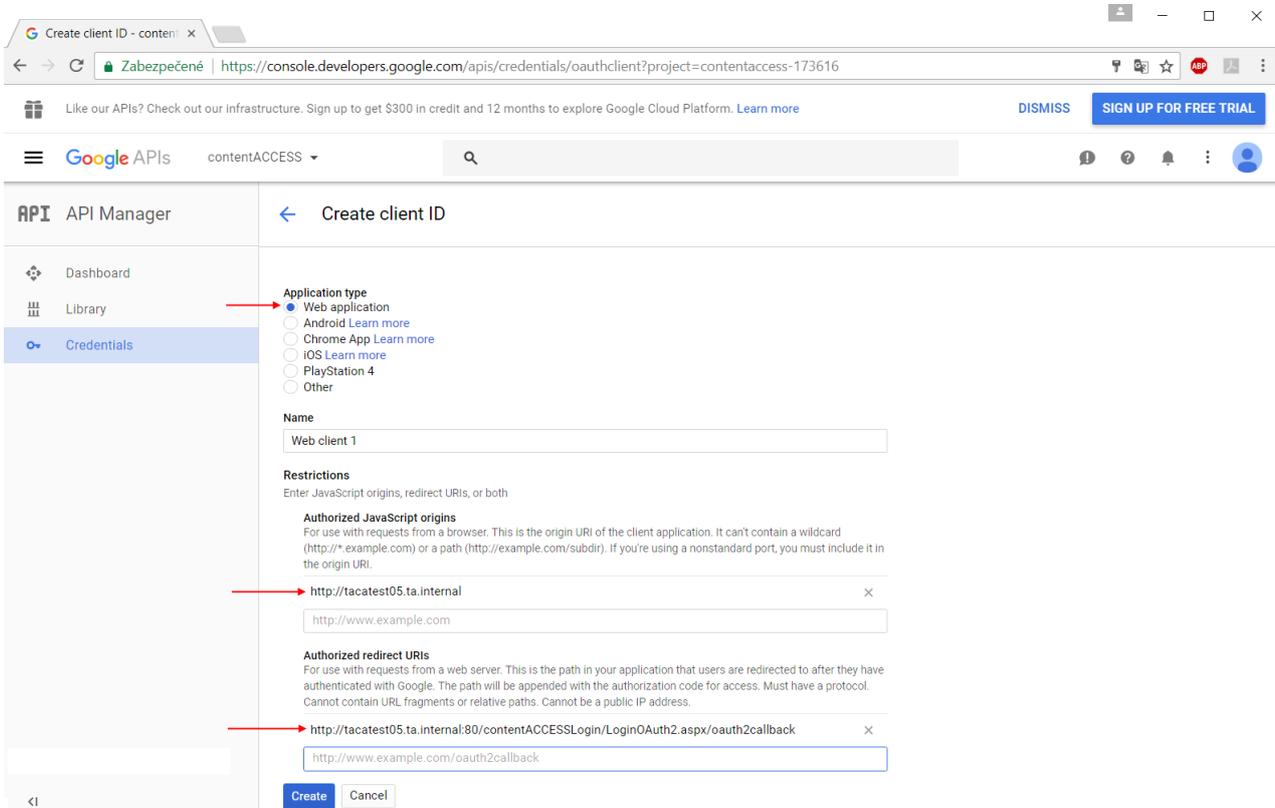
6) If this is your first time creating a client ID, configure your consent screen by clicking “**Configure consent screen**”.



7) Enter the product name and fill the optional fields if you want. Save your settings.

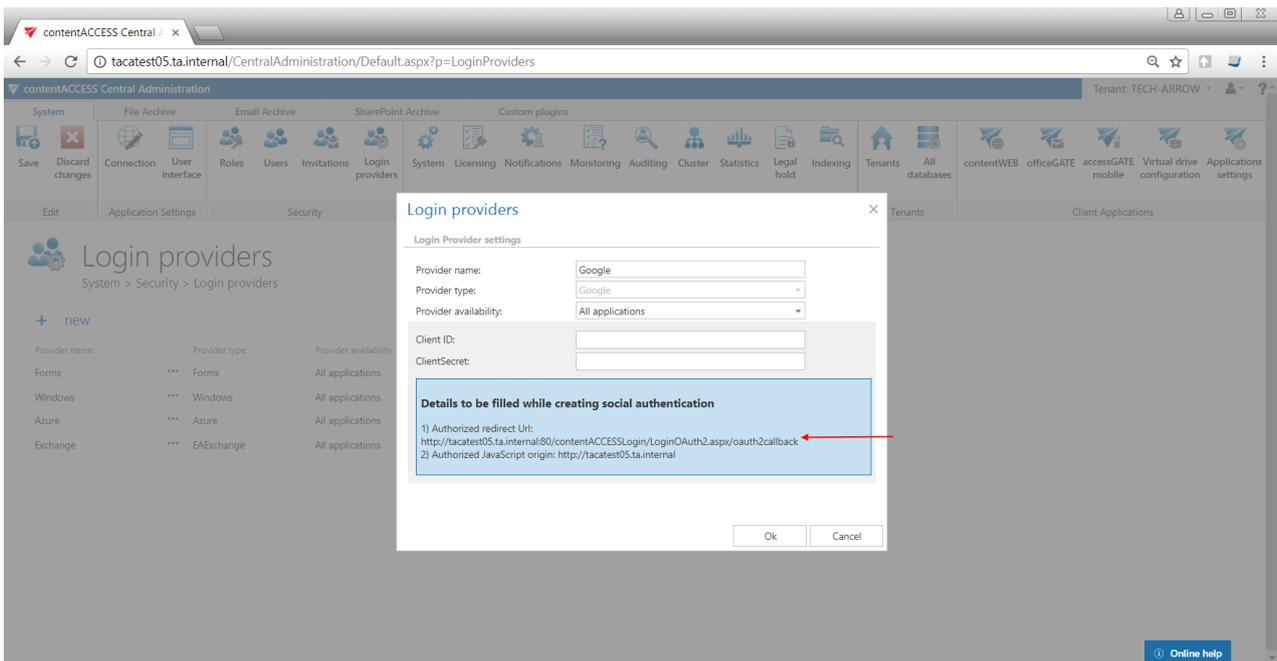


8) Select the WEB application type for your project and enter JavaScript Origins, redirect URLs or both to the appropriate text fields.

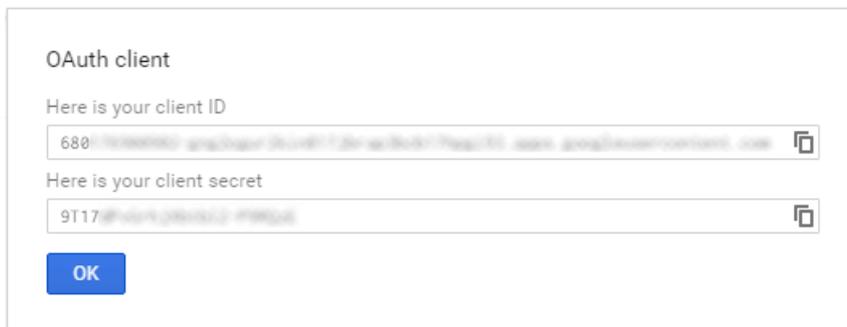


Use the URLs accessible in the Google login provider's window in contentACCESS Central Administration, like in the blue frame on the picture below.

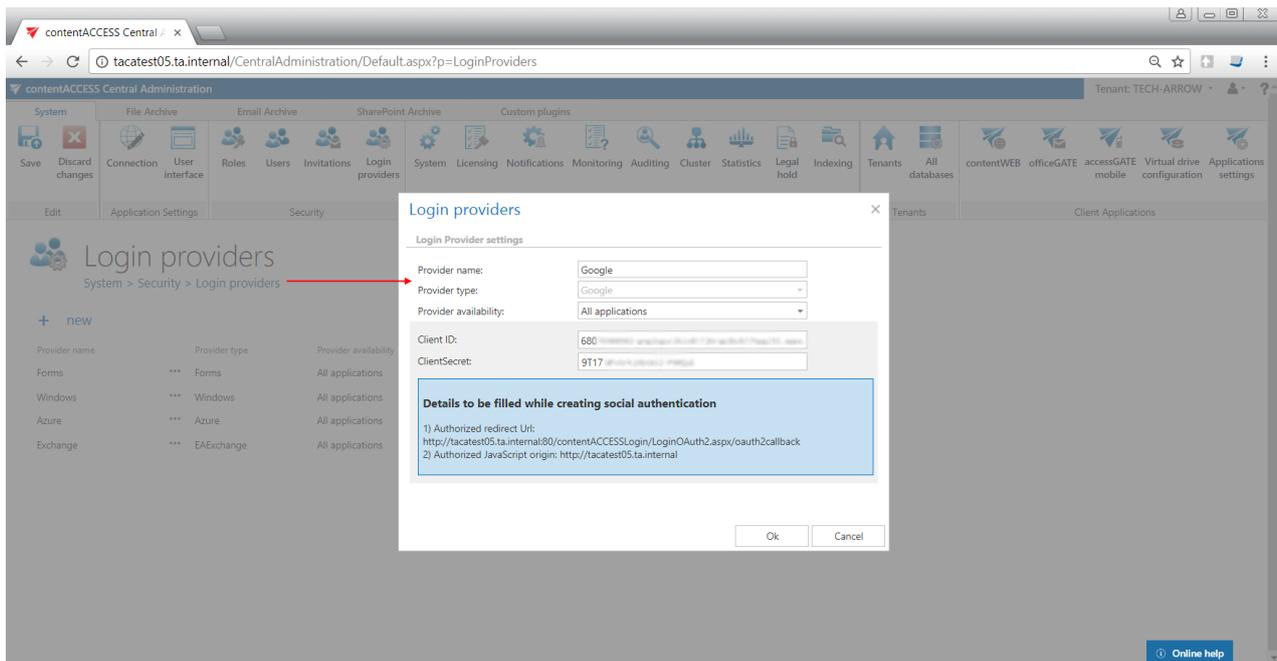
Important: The URLs are case sensitive!



9) Click “Create” on the Google developers console and the Client ID and Client Secret will be created automatically. Save these values somewhere on your computer:



Now configure your **Login provider** in contentACCESS Central Administration. Open the **Login providers** page (**System** → **Security** → **Login providers**), click here on “+new”. In the **Login providers** window name your provider, select **Google** provider type and choose the application that should use this authentication type. Further enter the **Client ID** and **Client Secret** from step 9) to the respective text fields, and click **OK**.



Configuring Office 365 login provider

The Office 365 login provider supports both API versions (v1.0 and v2.0). [German cloud](#) (dedicated and isolated Microsoft Azure version for Germany) unfortunately does not support v2.0, only v1.0. Here are the differences between versions:

- a) The login application for **API version 1.0** is registered through the Azure management portal (requires Microsoft Azure subscription) and does not support logins through Microsoft personal accounts, only Work and School accounts.

The login application for **API version 2.0** is registered through apps.dev.microsoft.com and supports all Microsoft logins (Personal, Work and School).

API version 1.0 registration

When configuring **Office 365** login provider, if **Germany** is selected in the **Region** dropdown list, version 1 is automatically preselected in the **API version** dropdown list. Do not change it, as the German cloud does not support API v2.0.

Login providers ✕

Login Provider settings

Provider name:

Provider type:

Provider availability:

Client ID:

ClientSecret:

Region:

API version:

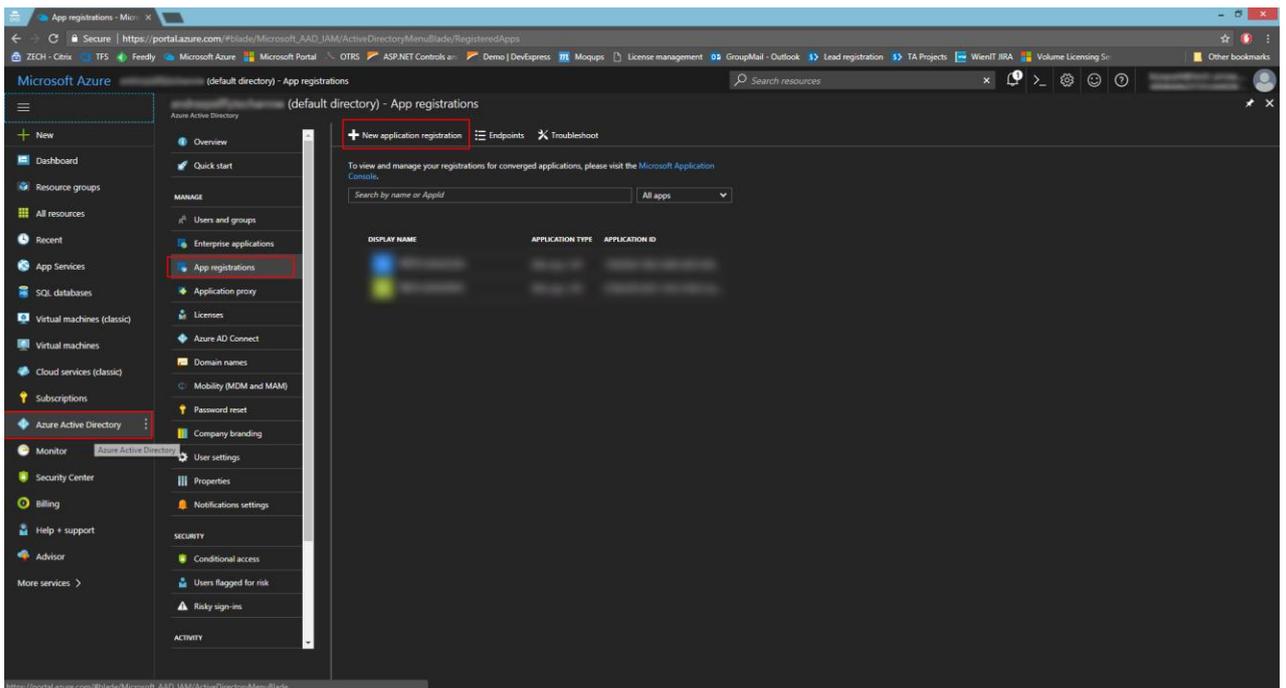
Details to be filled while creating social authentication

1) Authorized redirect Url:
http:///contentACCESSLogin/LoginOAuth2.aspx/oauth2callback

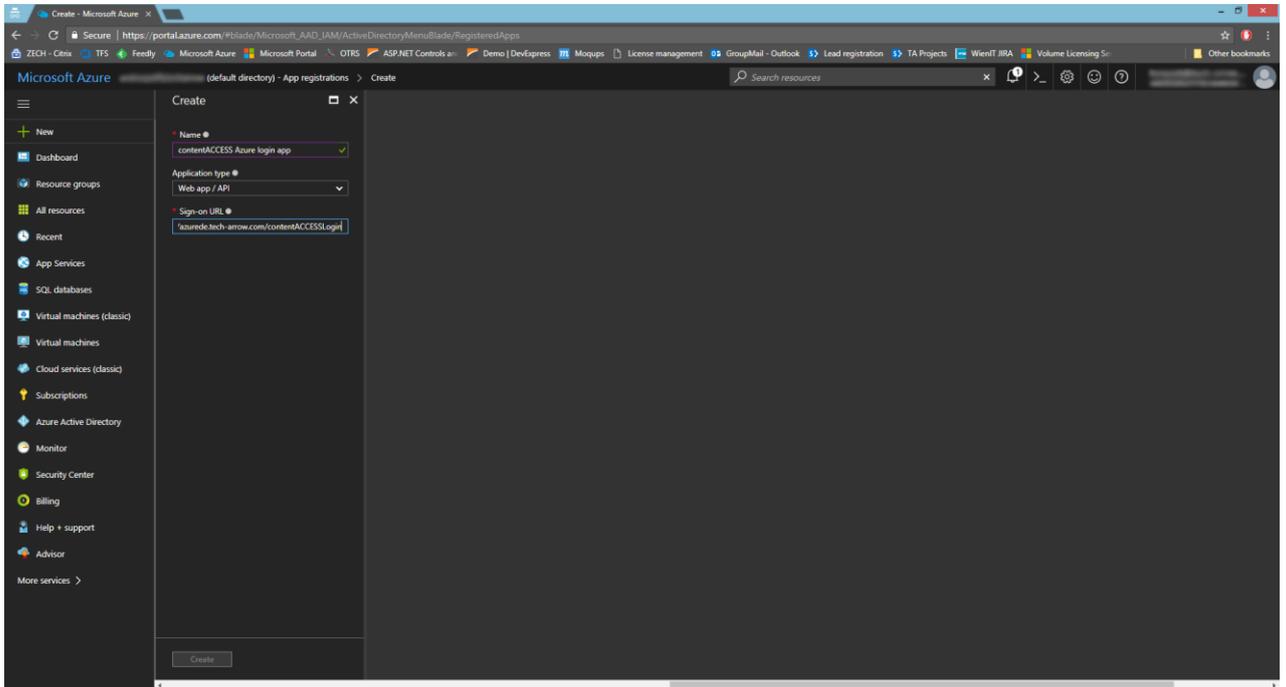
2) Authorized JavaScript origin: http://

Here is how to register the API version 1.0:

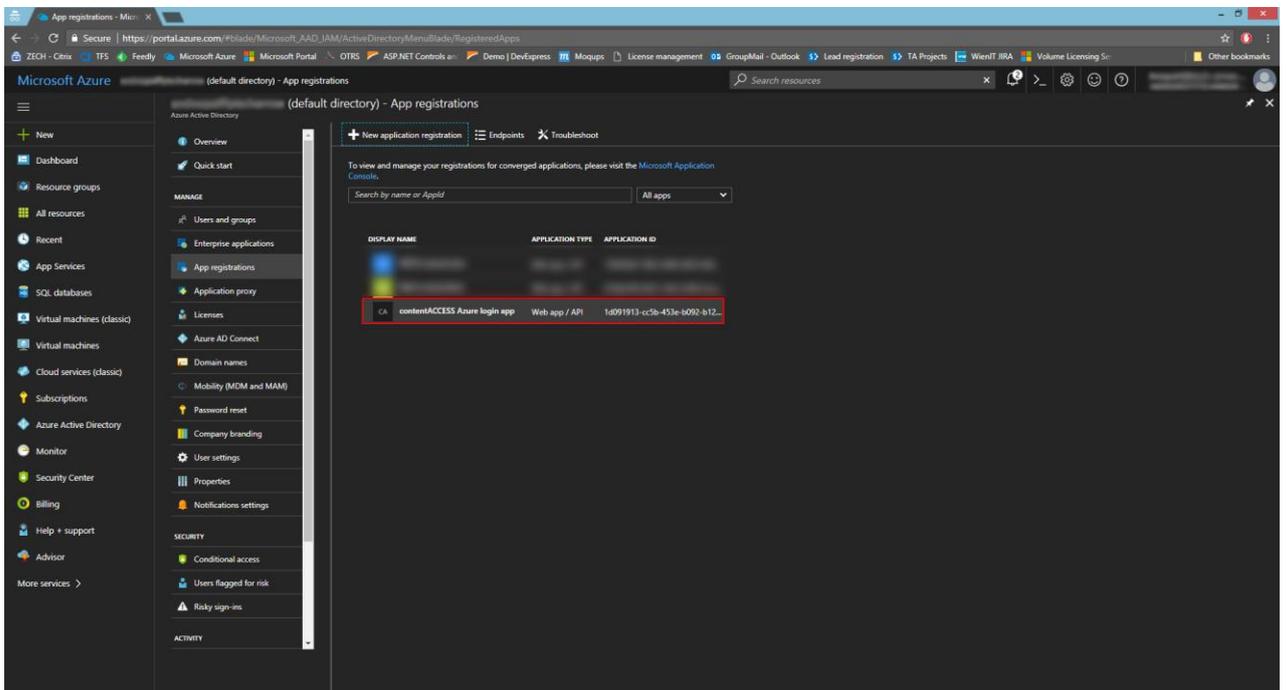
1. On the Microsoft Azure portal, click on Azure Active Directory -> App registrations -> New application registration.



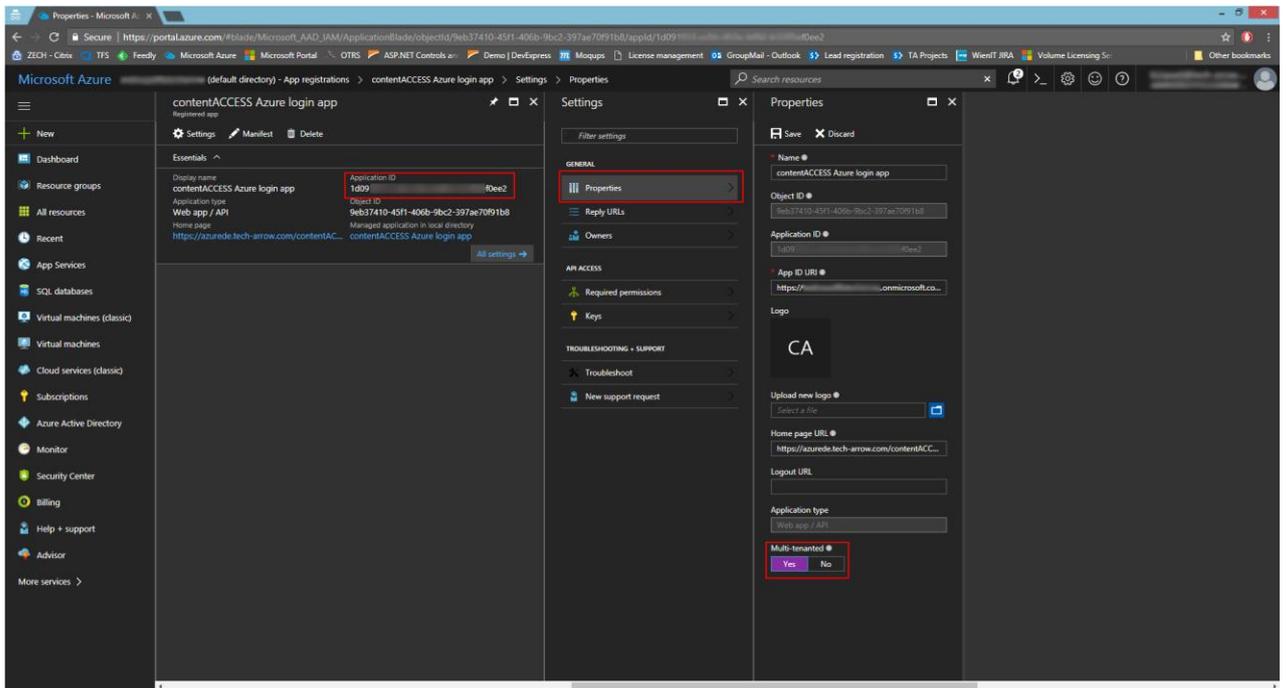
- Enter the name, application type (API) and sign-on URL (https://SERVER_NAME/contentACCESSLogin).



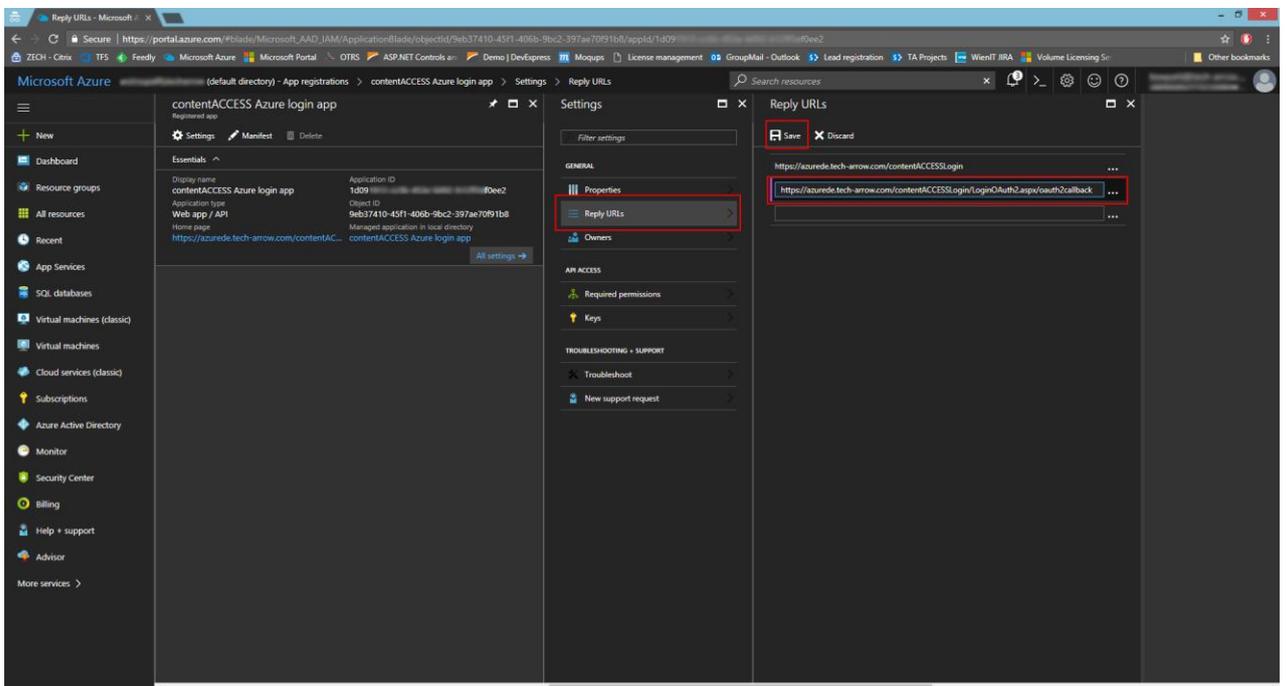
- Select the created app.



- Copy the necessary IDs and enter them to the respective fields in Settings -> Properties. Set the app as multi-tenanted.



- In Settings -> Reply URLs, enter the reply URL (https://SERVER_NAME/contentACCESSLogin/LoginOAuth2.aspx/oauth2callback). This URL can also be found in contentACCESS Central administration -> System -> Login providers -> Office 365 -> Authorized redirect URL.



Login providers ✕

Login Provider settings

Provider name:

Provider type:

Provider availability:

Client ID:

ClientSecret:

Region:

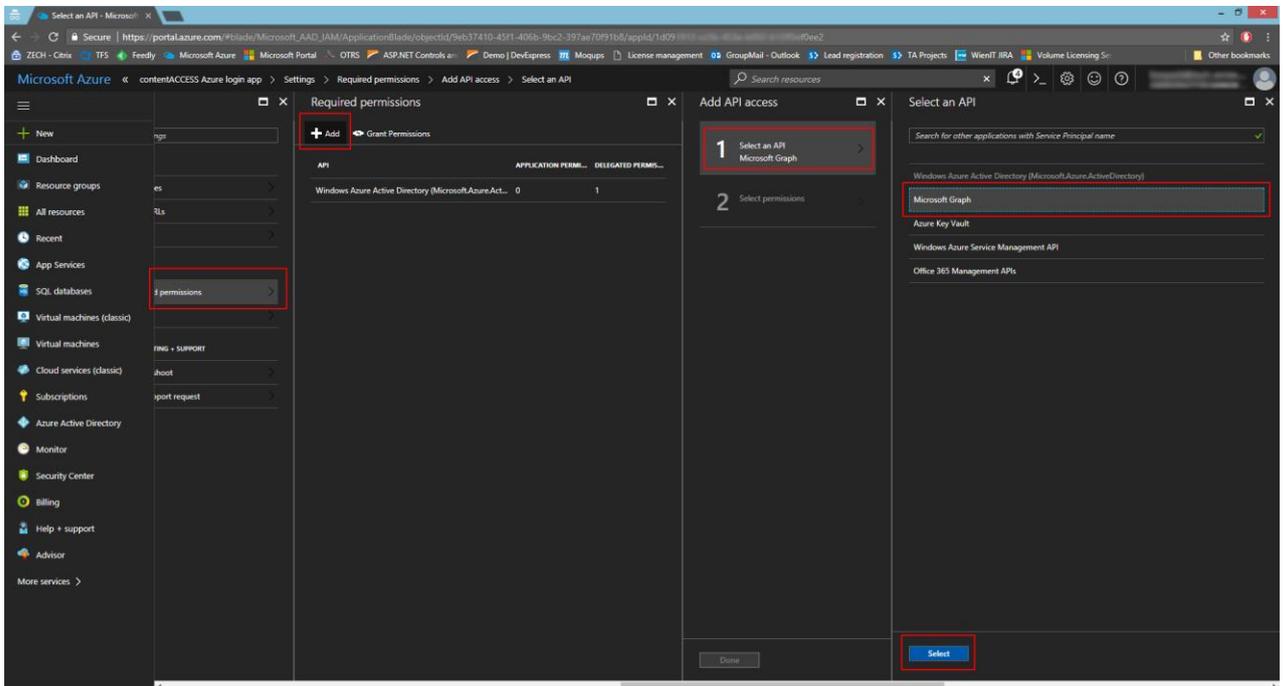
API version:

Details to be filled while creating social authentication

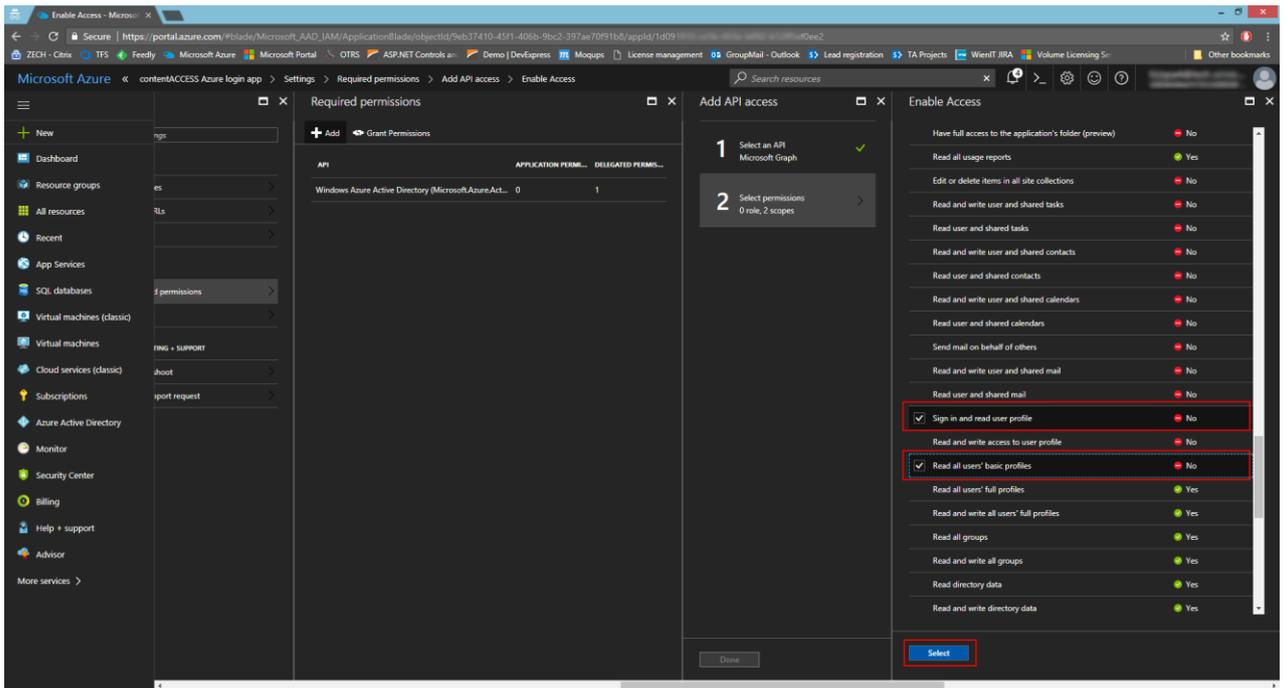
1) Authorized redirect Url:
 http:///contentACCESSLogin/LoginOAuth2.aspx/oauth2callback ←

2) Authorized JavaScript origin: http://

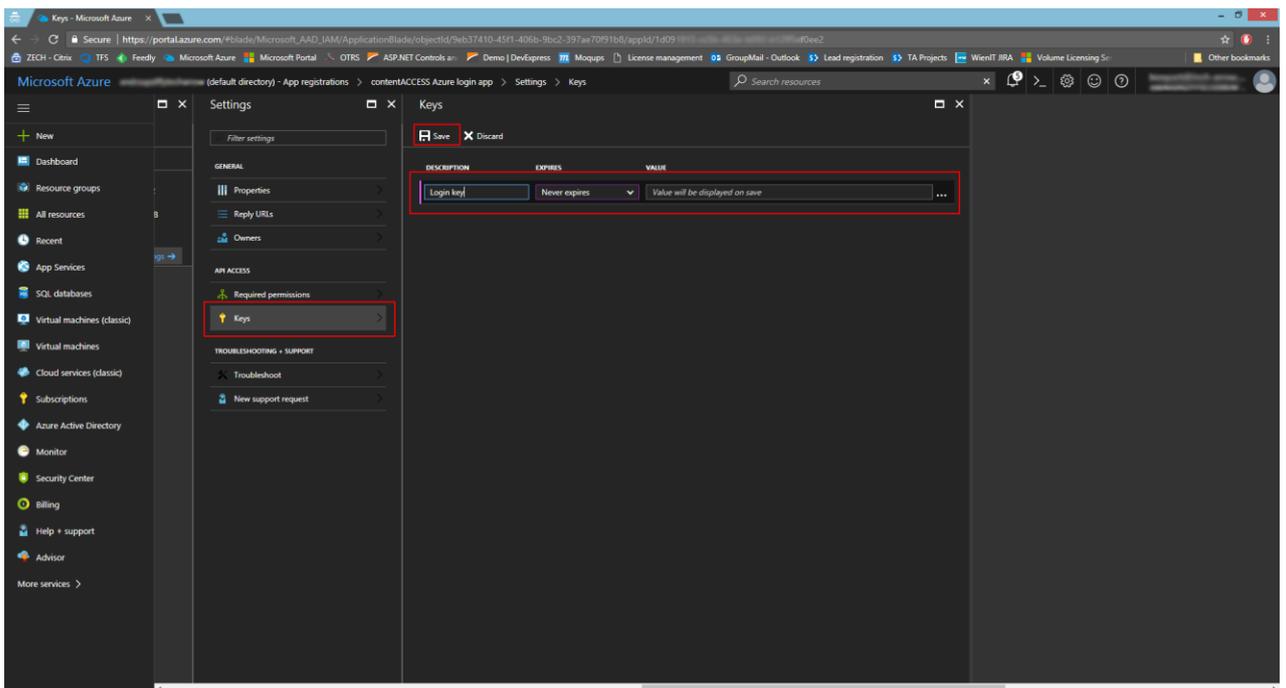
6. In **Required permissions**, click on +Add -> Select an API -> Microsoft Graph.



7. Click on **Select permissions** and check the options **Sign in and read user profile** and **Read all users' basic profiles**.



8. In Settings -> Keys, add the key name/description and select the option **Never expires**. Click **Save**.

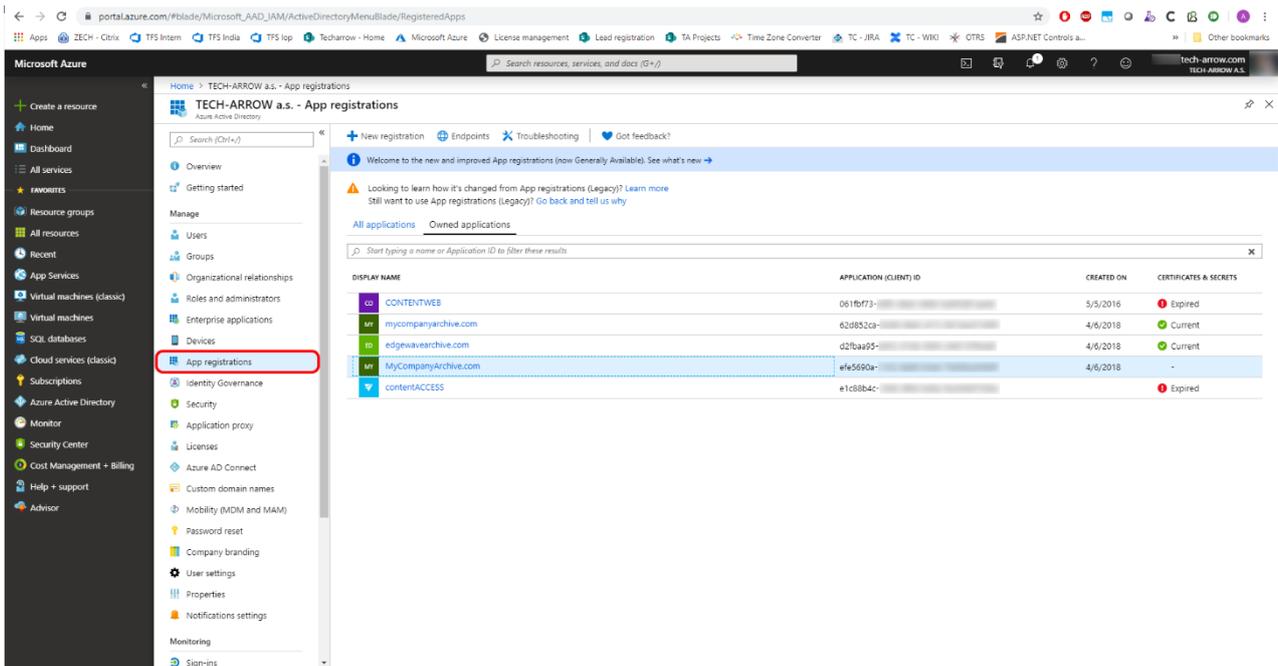


9. Copy the key value and save it somewhere, because you won't be able to retrieve it afterwards. This value must be entered in the Office 365 login provider as the **ClientSecret**.

API version 2.0 registration

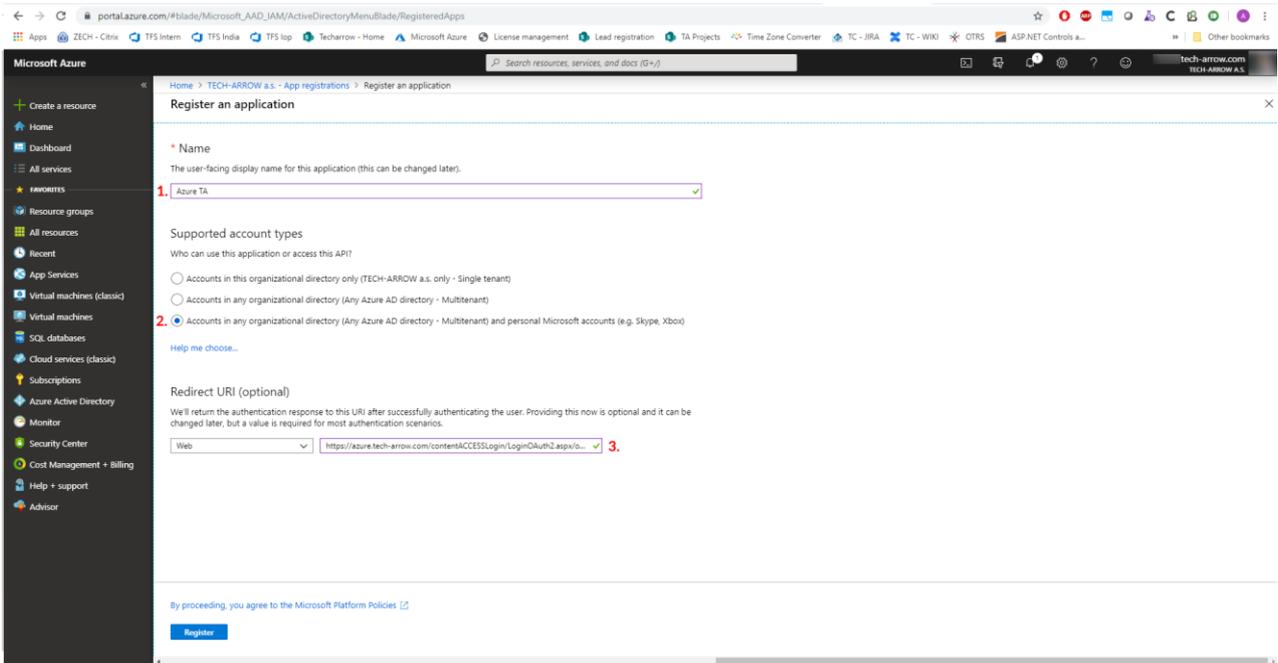
contentACCESS supports log in using your Microsoft account. The first thing you need to do is to register an application (contentACCESS) under your Microsoft account.

1. Log in to Azure portal: <https://portal.azure.com>
2. Go to **Azure Active Directory** -> App registrations

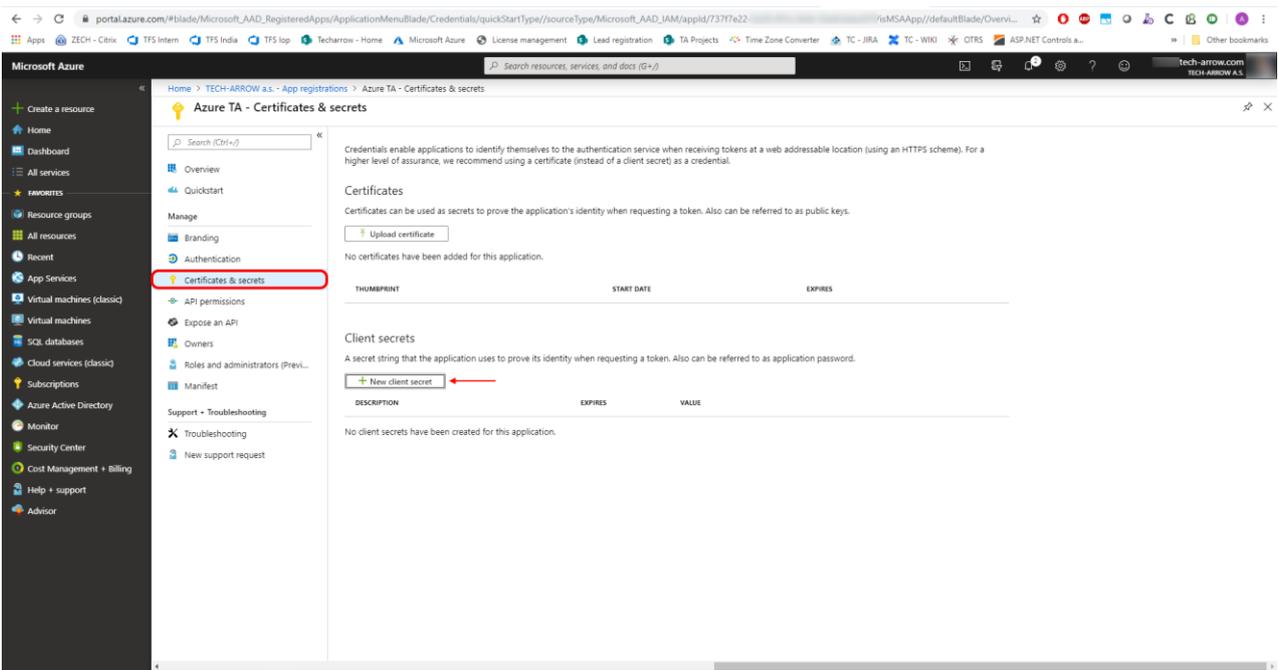


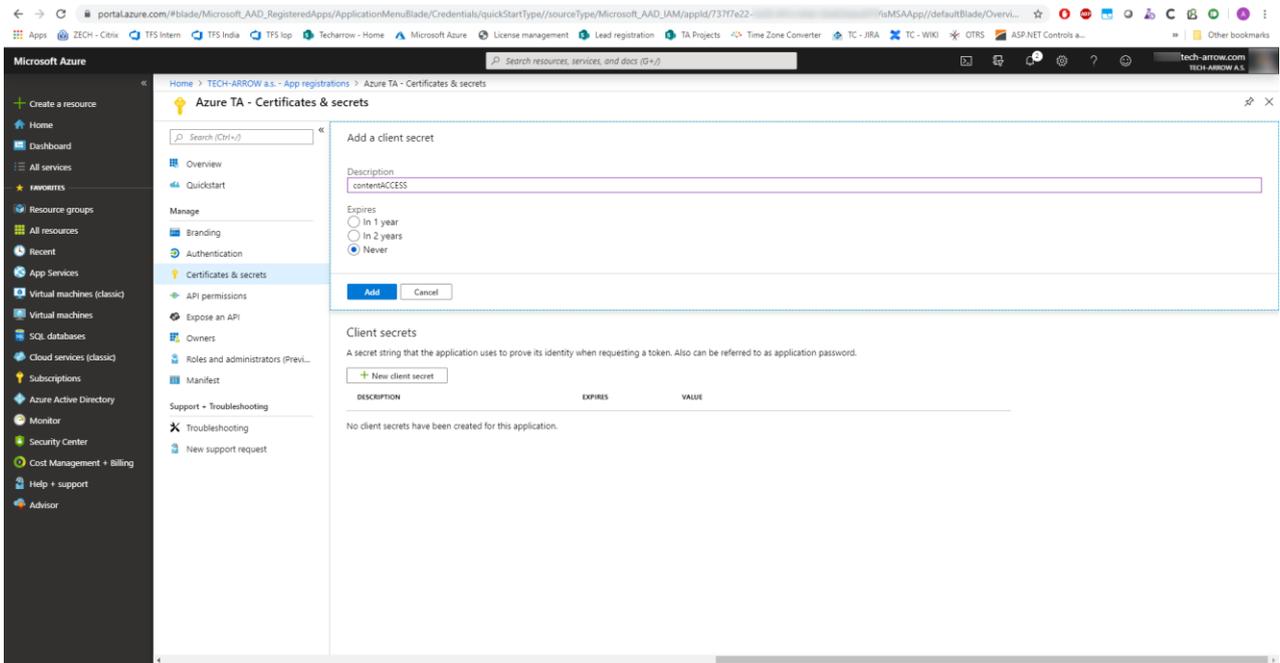
3. Create a new application registration

1. Name the application (this will be displayed for users while approving the access to their details on first login)
2. Select the preferred account types to allow logging in
3. Enter the redirect URL (this info is provided in contentACCESS in O365 login provider configuration)

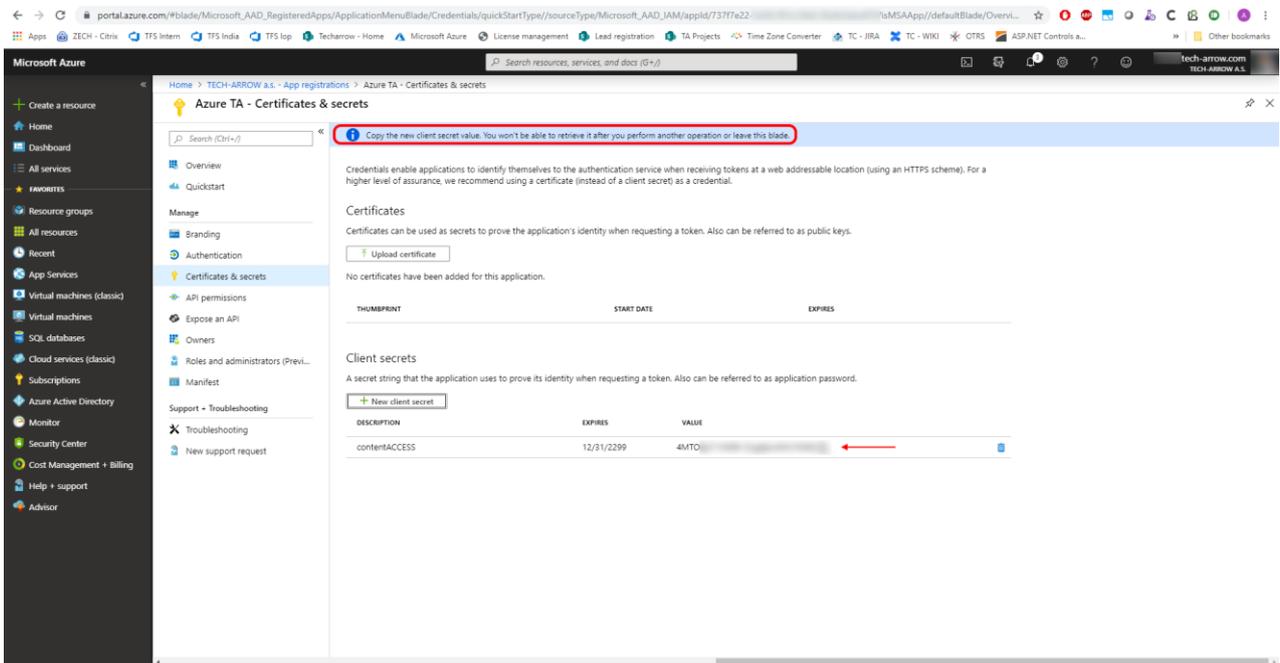


4. Go to Certificates & secrets and generate a new client secret

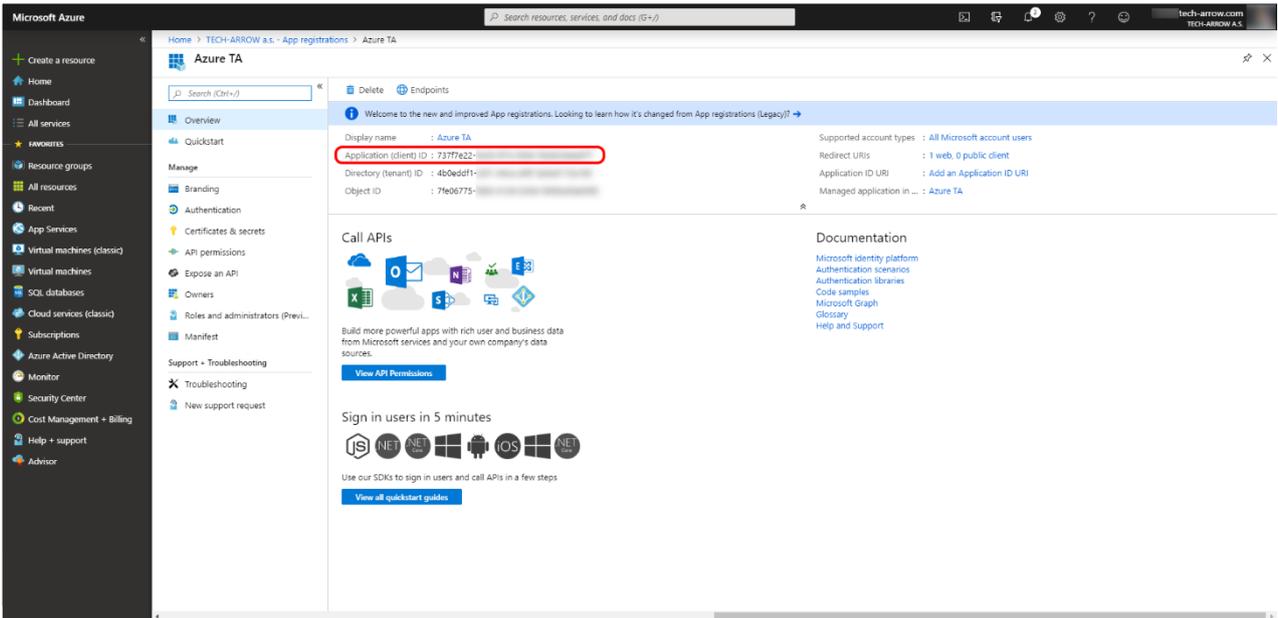




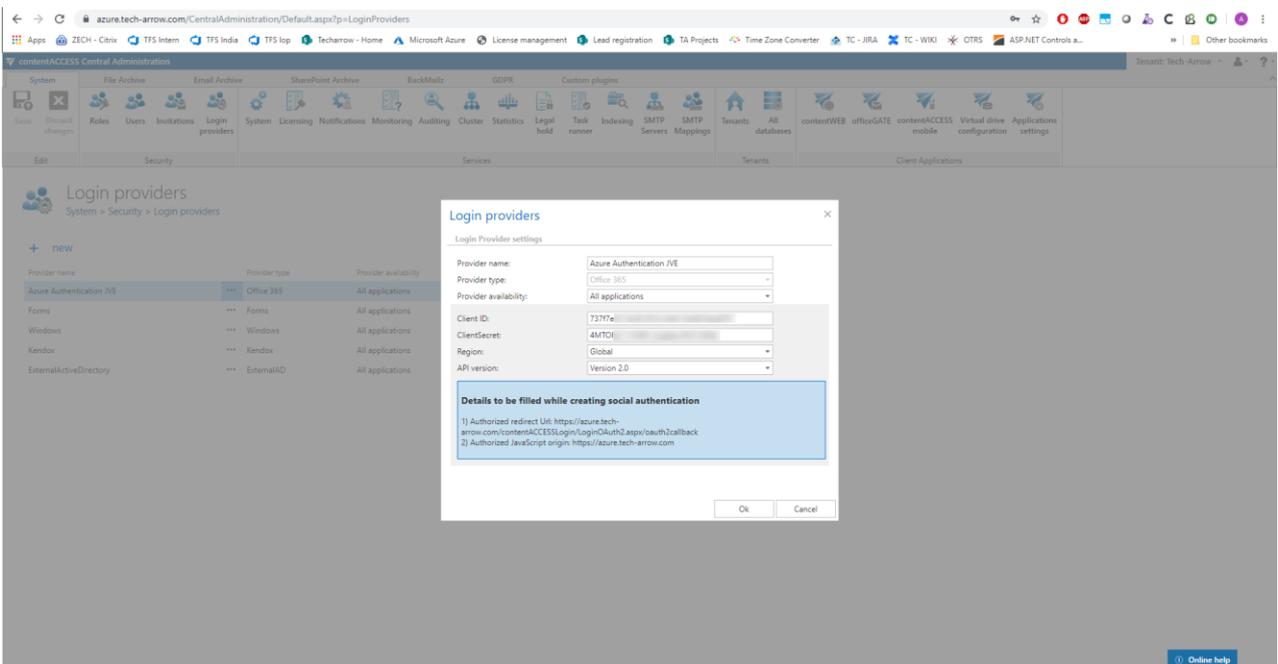
5. Copy the client secret



6. Go to **Overview** and copy the **Application ID**



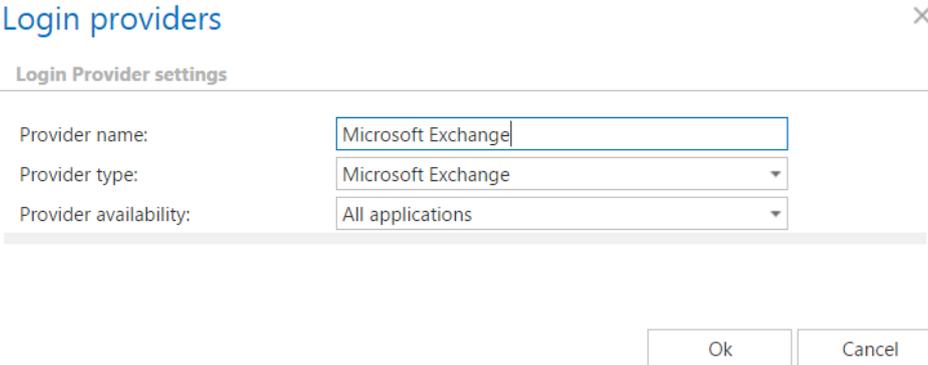
7. Enter the **Application ID** and **Client Secret** into **O365 login provider** configuration in Central Administration



Exchange login provider

The **Microsoft Exchange** login provider is one of the external authentication providers. It will allow the users to use their email address and mailbox password to log into contentACCESS. With this method, contentACCESS will use the entered credentials and will try to open the user's mailbox through Exchange Web Services (EWS). If it succeeds, then the user will be logged into contentACCESS. The user's password is not stored inside contentACCESS, it is managed only by **Exchange**. The only prerequisite for this login type is that there should be **Email archive** configured for a tenant. It is also possible to create users with **Microsoft Exchange** login types manually.

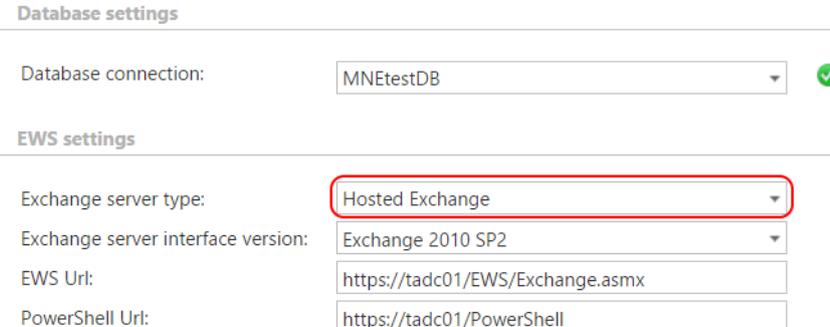
1. Creation of a **Microsoft Exchange** login provider (for more info please refer to section [Login providers](#))



2. Configuring the Exchange settings in [Email archive System settings](#)

System settings

Email Archive > Settings > System settings



If you want the **Email archive Provisioning job** to create contentWEB users with **Microsoft Exchange** login provider, **Hosted Exchange** needs to be selected in **Exchange server type**.



3. Automatic creation of contentWEB users with Microsoft Exchange login provider

Go to Address book and select **Automatically create contentWEB user**

View address book
 Email Archive > Archive > View address book

import servers manually | import groups manually | import mailboxes manually

Exchange servers

Name	EWS version	Server DN	Create contentWEB access	Associate with role
TADC01	*** Exchange2010_SP2	/o=First Organization/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Configuration/cn=Servers/cn=TADC01	No	

Exchange groups

Name	Group DN	Create contentWEB access	Associate with role	Active
Neveckí	*** CN=Neveckí,CN=Users,DC=ta.DC=internal	Yes	Inherited	Yes
Neveckí2	Automatically create contentWEB user	No		Yes
Neveckí3	Do not create contentWEB user	No		Yes
	Assign database and storage			
Public folders	Activate/Deactivate mailboxes			

contentWEB user role

The user will be created with Microsoft Exchange login provider.

- Use the role defined in the provisioning job
- Select a custom role you want to assign to the created user(s)

Save Cancel

4. Manual creation of contentWEB users with Microsoft Exchange login provider

Go to **System => Security => Users** and click on **Create or invite users** (read more in section [Users in contentACCESS](#))

Create / Invite a user ✕

Create new user Invite user

Display name:

Default tenant:

Login provider:

Email address:

Domain:

SAM account name:

Tenant:

Assign role

Role:

Tenant:

Globally allowed permissions of the selected role **will be assigned** to the user on the selected tenant.

[Show details](#)

* Note: If you select a tenant and the role has specific permissions, you will be redirected to the **Specific permission assignment** page.

External AD login provider

This provider is used for logging in with remote Active Directory credentials into the contentACCESS. It communicates with a WCF service, which is part of the contentACCESS proxy (Web/contentACCESSWS/ADService.svc). The proxy searches the Active directory for the user's name and allows him to log in to the contentACCESS it is connected with.

Note: The communication between the external active directory and contentACCESS will work correctly only if the contentACCESS proxy is installed on the same machine as the [Remote File archive](#) agent.



This provider can be assigned to the user by two ways: **1)** Running the provisioning in [Remote File archive](#) agent or **2)** manually adding it in Central Administration:

- click on **Edit** in the user's context menu

The screenshot shows the 'Users' management page in Central Administration. The breadcrumb path is 'System > Security > Users'. There is a '+ Create or invite user' button and a 'Show all users' dropdown. The user list has columns for Display Name, Default tenant, ID, and Roles. The user 'nev1' is selected, and a context menu is open over it, showing options: Assign role, Edit role assignment, Edit (highlighted with a red arrow), and Delete. The page footer indicates 'Page 1 of 1 (5 items)'.

Display Name	Default tenant	ID	Roles
Administrator	== System ==	A550E000-1588-423C-AD83-088D4CF07758	System administrator, Standard user
	Default	ac44b546-04d0-4bea-8636-2a00f037e53b	Standard user
	Default	f1f2bf4f-bb0c-4e5c-8e6f-f9f4223d27a0	Standard user
nev1	Default	92c26b29-2fff-4fed-b05c-c5b70b5a1cda	Standard user
	Default	5ae274a3-1ee9-494f-8451-206db1ef84a7	Standard user

- click on **+new**, choose **External AD** from the **Login provider** dropdown list and enter your credentials

The 'Add new login' dialog box is shown. It has a title bar with a close button (X). The 'Login provider' dropdown is set to 'External AD'. The 'User name' field contains 'TA\nev1'. The 'SID' field is empty. There are 'OK' and 'Cancel' buttons at the bottom right.

- click **OK**

How does the external AD login work?

- User provides his credentials on the login page.
- We find the user in our database by his login name.



3. We find all Remote agents on the users default tenant.
4. If the Remote agent has enabled Remote Active Directory (File archive -> Archive -> [Remote agents](#), Active directory in the agent's context menu), we call the ADService and try to login with the user's credentials to the remote Active Directory.



Remote agents

File Archive > Archive > Remote agents

[download agent](#)
[download proxy](#)

Status	Server name	Server IP	Enabled	Last ping	
Online	TACATEST	192.168.190.96	<ul style="list-style-type: none"> Enable Disable Create rule <li style="background-color: #0070c0; color: white;">Active directory 	Yes	11/7/2017 10:25:24 AM

Rule ID	Name	
1	Rule04	



Active Directory configuration

File Archive > Archive > Remote agent > TACATEST

Scheduling settings

Scheduled in:

Active Directory integration settings

LDAP Server name:

Enter the LDAP server name or IP address if you are out of the domain. This value is used for user name resolving.

Authentication type:

Use explicit credentials

User name:

Password:

Confirm password:

Remote Active Directory

Enabled:

Proxy FQDN: : :

[Online help](#)



- If the login to the Remote Active Directory was successful, we allow the user to log in to the contentACCESS. The content shown for him is evaluated based on SDDL permissions.

Associating an enabled provider with a user login:

It depends on the provider type if it supports multiple configurations or not. You can create only one **Windows** and **Forms** login provider configuration for a user login, but can create multiple e.g. for **Office 365**.

Once the desired provider is enabled and configured, you have to create a new user login for the user, who will use the provider. Navigate to **System** → **Security** → **Users** button on the ribbon. Click on it and the **Users** page will open. Select the desired user and double click on it.

The **User details** page will open. Click on **+new** under **User logins** section.

The screenshot shows the 'User details' page in the contentACCESS Central Administration interface. The breadcrumb trail is 'System > Security > Users > User details'. The user's display name is 'Administrator', and they are a system administrator who is currently online. The 'Security information' section lists two roles: 'System administrator' and 'System administrator' on 'Tenant Unknown'. The 'User logins' section has a '+ new' button highlighted with a red arrow. Below it, a table shows one login configuration: 'Forms' login type with 'system' as the login name. The 'User login sessions' table shows a single session for the 'Forms' login type on 'system' at 11/14/2016 2:50:30 PM, expiring at 11/14/2016 3:50:30 PM.



In the **Add new login** dialog select the desired provider configuration from the **Login provider:** dropdown list, fill in the required credentials and click **OK**.

The external provider gets available in the **login window of the selected applications**.

contentACCESS users in third party systems

Datengut Baueakte and Perceptive DMS can be interconnected with officeGATE, which is an MS Outlook add-in used for collaborating on documents residing in different data management systems (DMS). officeGATE is a client application of contentACCESS, and it requires a contentACCESS user to sign in to the particular data management system that is interconnected with contentACCESS. To simplify this login process into these third party systems (DMS like Datengut, Perceptive), it is possible to automatically create a contentACCESS user from the particular provider's configuration dialog, in contentACCESS Central Administration. This ensures single sign on into the particular DMS providers in officeGATE.

To achieve this, check the **“Create contentACCESS user automatically”** checkbox (and fill the required credentials). When you are logging in to Datengut or Perceptive DMS in officeGATE with your personal account, the contentACCESS user will be created automatically at the moment of logging in.



If the **“Create contentACCESS user automatically”** function is not enabled in the provider’s configuration dialog, then the administrator is forced to create contentACCESS users manually. Automated user creation helps to save much time for the administrator, as he does not need to create contentACCESS users for each user of the third party application **(like Datengut or Perceptive)**.



System

The **System** page (**System** → **Services** →  **System**) consists of 12 configuration sections: **General settings**, **Globalization settings**, **User search settings**, **Tenant level resource settings**, **Resource storage settings**, **Database settings**, **Proxy settings**, **Search server settings**, **Monitoring log storage settings**, **External accessibility settings**, **Active directory integration settings** and **Cluster settings**. The first two sections are configured by the setup by default.



contentACCESS Central Administration Tenant: TECH-ARROW

System > Services > System

General settings

Is system configured:

Plugins directory: C:\Program Files\TECH-ARROW\contentACCESS\GA

Globalization settings

Time zone: [UTC+01:00] Belgrade, Bratislava, Budapest, Ljubljana, Prague

Date format: 31/01/2019 5:50:50 (24h)

User search settings

Disable user searching:

Tenant level resource settings

Disable resource settings:

Resource storage settings

Storage path: C:\TestingStorage

Use explicit credentials:

User name:

Password:

Confirm password:

Test

Database settings

Database type: MSSQL

Server name: TACATEST

Database: MNEtestDB

Schema: dbo

User: sa

Configure

Proxy settings

Do not use proxy

Use system default proxy settings

Use explicit proxy server settings

Proxy server URL:

Username:

Password:

Search server settings

Search server url: net.tcp://localhost:8732

Test

Enable extended search results:

Enable search suggestions:

Enable hit highlighting:

Monitoring log storage settings

Use the system database

Use the default search server

Use a different search server

External accessibility settings

Retrieve server FQDN: https://tacatest.ta.internal:443

Enter an externally accessible alias for the contentACCESS server. This value is used for shortcut links too.

Test

Enable link security:

Central login: http://tacatest.ta.internal:80

Provide necessary information, where central login is deployed.

Test

Active Directory integration settings

LDAP Server name: LDAP://192.168.190.91

Enter the LDAP server name or IP address if you are out of the domain. This value is used for user name resolving.

Authentication type: None

Use explicit credentials

User name: ta/administrator

Password:

Confirm password:

Test

Cluster settings

Node update interval (sec): 30

Node auto logoff time (sec): 120

Events retention time (sec): 1800

Events distribution interval (sec): 60

Task auto disable time (sec): 30

Stop task after ping failures (count): 2

Node selection strategy: First wins

Default node role: Universal

Enabled by default:



▪ General settings

If the 1st checkbox is checked it means that the system is configured, thus connection to SQL Server database is well configured and the plugins directory is pointing to a correct folder. If this checkbox is not checked, the contentACCESS will run in a so called “zombie” mode.

Plugins directory textbox contains the path, where the processing plugins are stored on the server.

▪ Globalization settings

In this section, it is possible to set the **Time zone** and **Date format**. The time zone can be picked from the dropdown list; the date format can be picked from the dropdown list or specified manually - **Custom date format** option. These settings are on system level.

Note: If a tenant doesn't have a configuration or if the user's default tenant is the **System tenant**, then the **System's globalization settings** will be used.

Important: When updating from contentACCESS version 3.7 and older, default values are set here. It is possible to change them.

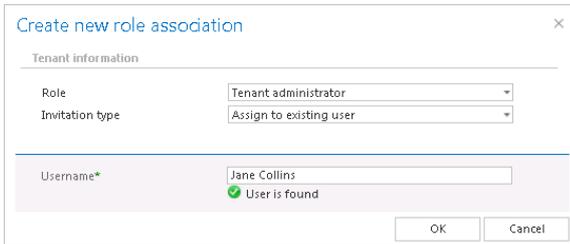
▪ User search settings

By default this option is turned off. The feature is used to disable / enable user searching when assigning

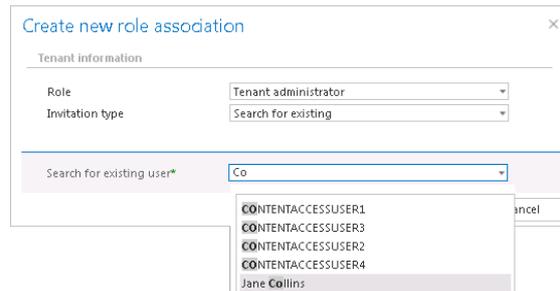
- tenant administrator rights,
- File Archive access rights
- access rights to a certain Exchange mailboxes
- access rights to jobs, schedulers, retentions, databases, root connections, email archive shortcuts, storages, file archive aliases

for a contentACCESS user **already existing** in contentACCESS.

If the option is **turned off**, all the existing contentACCESS users are listed in the respective dialog when assigning the access rights (like on Screenshot B below). If the option is turned on, then the rights can be granted only in case if the correct contentACCESS **User name** is manually entered in the dialog (like on Screenshot A below). This configuration option is used if you have contentACCESS in a hosted environment and you want to hide the users of one customer from the users of other customer.



Screenshot A: Granting tenant administrator rights for Jane Collins if user searching is **disabled**



Screenshot B: Granting tenant administrator rights for Jane Collins if user searching is **enabled**

▪ **Tenant level resource settings**

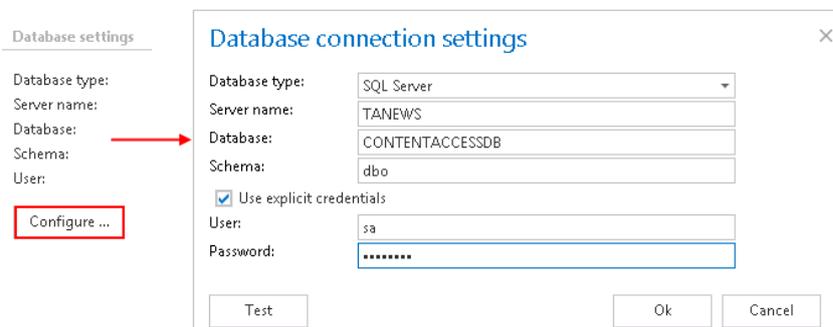
Resource settings can be disabled on tenant level by checking the checkbox in this section.

▪ **Resource storage settings**

The resource storage must be accessible from every contentACCESS node. Files created by contentACCESS that should be further accessible (for example files exported to PST or ZIP) are automatically stored in this folder. If more contentACCESS nodes are installed, a UNC path has to be set here, otherwise it can be any common folder as shown on screenshot.

▪ **Database settings**

Under **Database settings** the system database configurations, which are filled in by the setup by default, can be found. If you need to edit these settings (not recommended), click on the **Configure** button and fill the fields in the **Database connection settings** window:



By default contentACCESS is connected to the database with the credentials of the user, under whom contentACCESS is running. If you want to use SQL credentials which differ from these credentials data, then check checkbox **Use explicit credentials** and enter the **User** and **Password** that you want to use for



connecting to database. You can also run a test connection with the **Test** button in the left corner of the window.

▪ **Proxy settings**

In this section the user can configure (or change already configured) URL and user credentials to the proxy server. The licensing component will use this proxy in order to reach the licensing server. The user has multiple options. He can:

- **Use default proxy settings** – based on the Proxy settings on the contentACCESS server machine (**Control panel** → **Internet options** → **Connection tab** → **LAN settings** → **Proxy server** section) or
- **Use explicit proxy server settings** (explicit proxy server URL and user)
- **“Do not use proxy”** option is used to disable proxy usage.

▪ **Search server settings**

In this section the URL of the **Search server** can be specified. It is also possible to test the connection by clicking on the **Test** button.

By checking/unchecking the **Enable extended search results** checkbox, it is possible to switch between old and new search method:

Unchecked (new method)

- faster (works only from search engine – Elasticsearch)
- the first 200 characters from the email body are not displayed in contentACCESS Mobile and Teams App
- the icon for emails is always the same in contentACCESS Mobile and does not change for read/unread, forwarded and replied emails

Checked (old method)

- slower (works from search engine (Elasticsearch), from databases (email, file, ...), from store (for Email archive - body text))
- results are more detailed

Enable search suggestions

When you start a search in any client application of contentACCESS, search suggestions will help you find relevant information more quickly. Search suggestions are possible search terms related to what you are



looking for and are generated from the document contents, thus only those terms will be suggested, which are related to at least one of your documents.

To enable this feature, check the **Enable search suggestions** checkbox. After it is enabled, the suggestions won't appear immediately – the suggested terms are created during the **Indexing** process.

Important: The search suggestions will be created only from content of the items that were indexed when this option was **turned on**. If some items were already indexed without it and later the option is turned on, the search suggestions **won't be created** from their content.

The set of suggested terms depends on type of the archive the user is searching in:

Email archive

- Usernames and email addresses of senders and recipients
- Attachment filenames
- Email subjects

Filesystem archive

- File and directory names

SharePoint archive

- File and directory names
- Usernames

Teams archive

- Usernames
- Attachment filenames
- Team and channel names
- Message subjects
- Meeting topics

Teams chat archive

- Usernames



- Attachment filenames
- Meeting topics

GDPR Exchange

- Usernames and email addresses of senders and recipients
- Attachment filenames
- Email subjects

GDPR Filesystem

- File and directory names

Context sensitivity

Suggestions are also context-sensitive - if a user is searching for documents by specific property values, only values relevant for that property are suggested.

Examples:

1. For properties "sender", "from", "cc", "author" etc. only usernames will be suggested.
2. For properties "attachment", "subject", "title" etc. filenames and terms from document titles will be suggested.
3. If no search property is specified, both usernames and terms from document titles, filenames will be suggested, ordered by relevance.

Username suggestions

Usernames are suggested both by first and last name.

Example: the username "John Smith <john.smith@mail.com>" will be suggested if the user starts to type both John and Smith.

If the **Enable hit highlighting** checkbox is checked, contentWEB will highlight the located words in search results the following way:

- in the **item list** - highlights the title/subject, sender, recipient



- in the **email preview** - highlights the title/subject, sender, recipient, attachment name, email body
- in the **file preview** - highlights the title
- in the **SharePoint preview** - highlights any property

▪ **Monitoring log storage settings**

Here it's possible to set where the logs from **System logs** will be stored.

▪ **External accessibility settings**

Under **Retrieve server FQDN**: enter the externally accessible, fully qualified domain name for the contentACCESS proxy server into the Server FQDN textbox (in case the contentACCESS proxy is not installed, then the domain name of contentACCESS server needs to be entered here). The contentACCESS proxy server ensures the communication between the user and the contentACCESS, and forwards user requests to the contentACCESS server. These external accessibility settings are used by the shortcut links in the Email Archive system. **If you have contentACCESS Email Archive and/or accessGATE Mobile, then this setting is mandatory. In all other cases this setting is also highly recommended.**

Important: If the contentACCESS Server ID is changed, then the HTML shortcuts pointing to the archived mailbox items will not work. The solution is to update the contentACCESS Server ID in the Outlook forms, too. For more information refer to the [Outlook form installation manual](#).

Under **Retrieve server FQDN** is the option to enable link security:

External accessibility settings

Retrieve server FQDN: :// :
 Enter an externally accessible alias for the contentACCESS server. This value is used for shortcut links too.

Enable link security: ←

Central login: :// :
 Provide necessary information, where central login is deployed.



If you would like to protect the links in your mailbox pointing to archived items from unauthorized access, it is recommended to have this option turned on.

If this option is checked and you try to download some files, you will need to authenticate via CentralLogin. That means if you click on a link (download email, attachment, shared files), at first you will get to login page, then after successful login you can download your file.

The following parts are affected:

- MailApp for archivation
- [ShareApp](#) links
- Email shortcuts
- [contentACCESS Outlook add-in](#)
- All download links for files, emails, attachments

Under Central login: the Central login page URL and communication port configurations (previously specified in the setup package by installing the product) are accessible here. The package writes here/reads from here the Central login page URL if it's changed. Read more in [Installation of contentACCESS](#).

- **Active directory integration settings**

Some contentACCESS functionalities [like contentWEB access for mailboxes or Virtual Drive] require LDAP connection. Enter the required data and the user/administrator credentials into the user name and password textboxes over which you would like to connect to the active directory. It is not necessary to fill in these fields in case that you use an online Exchange server.

- **Cluster settings**

contentACCESS supports clustering, which enables to run contentACCESS and its jobs on multiple nodes, and thus improve performance. To adjust default cluster settings, scroll down on the **System** page. At the bottom of page, the following can be adjusted:

Node update interval (sec): in time intervals, which is set here (in our case in every 30 seconds) each node will "ping" the central database and will update his state in it.

Node auto logoff time (sec): if an input has not been received by a node during the time period set here, the node will automatically switch to offline.



Events retention time (sec): events (i.e. commands to run a job, added/changed/removed job configurations, changes in already set schedulers etc.) that are shared and distributed between nodes will be stored in the database during this retention time.

Events distribution interval (sec): events to be distributed between nodes are written into the system database. These events are periodically checked by each node in time periods, which are set here.

Task auto disable time (sec): if any failure occurred during the run of a node (server shutdown, hardware problems etc.), the task(s) performed by this specific node (job running, retrieving contents etc.) will be automatically disabled within the time set here.

Stop task after ping failures (count): the value which is set here will determine, after how many ping failures will be the task stopped. After the ping failure count reaches this value, all the tasks running on a node will be stopped.

Node selection strategy: the administrator can select here, how the nodes will be automatically selected for processing. A node that is picked up for a task can be selected according to one of these strategies:

“First wins” strategy – using this strategy the first running node will be picked for the task.

"Balanced" strategy – by this strategy type the CPU- and memory usage, and the number of running jobs will be considered before picking up the node for a task.

Default node role: the administrator can select here the default role type of a node added to the system. It is recommended to set here “Universal”, i.e. when the node can be used both for processing and retrieving data. Later on, the role type of a node can be adjusted with navigating to **System** → **Services** → **Cluster** on the Central Administration ribbon, in the nodes’ grid, from the nodes’ context menu.

Enabled by default: by default all nodes are enabled (the checkbox is checked), i.e. if contentACCESS service starts up, the nodes start the processing (to run jobs, publish models etc.), too. In case the user will install contentACCESS components on next nodes, it is recommended to disable the nodes (uncheck this checkbox). The reason for this is that a node must be fully configured before it picks up any job for processing. Enabled status of a node is marked with green color, disabled status is marked with yellow color in the nodes’ grid.

Licensing

A new license can be activated on the **Licensing** page, which is reachable with navigating to **System** → **Services** →  **Licensing** button on the ribbon. The administrator can also update the telemetry job (further described in chapter [Statistics](#)) on this page. The license restrictions and the current usage may be checked in the corresponding sections of the **Licensing** page.

The page is divided into the following sections:

- **General information** – the actually used license details are shown here. Here you can also check the date when your license has been activated and the expiration date.
- **Customer information** – displays information about the owner of the license
- **Contact information** – the contact person responsible for software-related issues, usually a contact person between the TECH-ARROW and the customer
- **System limitations** – in this section you may see the plugins and storages available in the activated license, and the maximally allowed tenant and node count (currently used count is in brackets), OEM version

The contentACCESS license system allows to set limits for the available plugins. The user will be allowed to archive items in the given range only, which is defined in the respective license. The currently archived item count and size is displayed in brackets.

- **Email archive limitations** – the maximally allowed and currently archived mailbox count (both active and deactivated mailboxes, read more [here](#)), email(s) count and size is displayed here, information about if Public folder archiving is allowed and if deactivated mailboxes should be hidden
- **PST import limitations** – information about if PST import is allowed, number of mailboxes with imported PSTs, size of emails imported from PSTs
- **File archive limitations** – the maximally allowed and currently archived root folder count, file(s) count and size is displayed here
- **GDPR for File system limitations** – number of file system roots, number of file system items
- **GDPR for Exchange limitations** – mailbox count, email count
- **GDPR for applications limitations** – application count, number of application records
- **SharePoint archive limitations** – connection count, file count, file size



- **Teams archive limitations** – user count, team count, size of archived items, deactivated user count, deactivated team count, item count

The screenshot shows the 'Licensing' page in the contentACCESS Central Administration interface. The breadcrumb trail is 'System > Services > Licensing'. Below the breadcrumbs, there are two buttons: 'activate license' and 'update telemetry'. The page is divided into several sections:

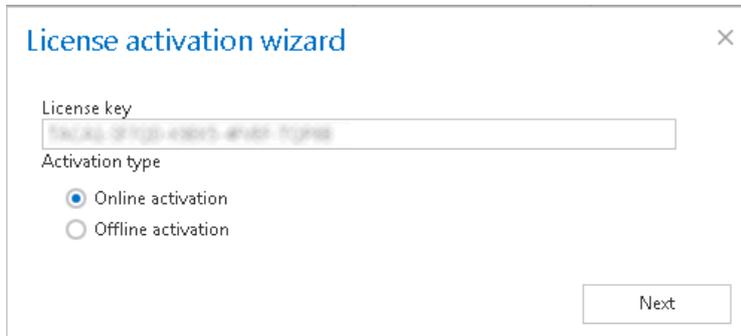
- General information:** Key, Status (Ok), Activation (10/6/2017), Expiration (unlimited).
- Customer information:** Name (Tezst Elek), State (Slovakia), Street (Kazanska), Zip.
- Contact information:** Name, Email, Phone.
- System limitations:** Includes a list of plugins (GDPR File system, GDPR Exchange, etc.) and a list of stores (AmazonS3, GoogleDrive, etc.).
- Tenant count:** 1000 (16 used), Node count: 1000 (3 used).
- Tenant limitations:** Job count: unlimited (132 used).
- Email archive limitations:** Active mailbox count: unlimited (33 used), Deactivated mailbox count: unlimited (0 used), Public Folders allowed: No.
- PST Import limitations:** PST import allowed: Yes, Mailboxes with imported PSTs: unlimited (1 used).
- File archive limitations:** Root count: unlimited (36 used), File(s) count: unlimited (3400 used).
- GDPR for File system limitations:** File system roots: unlimited (0 used).
- GDPR for Exchange limitations:** Mailbox count: unlimited (0 used).
- GDPR for applications limitations:** Application count: unlimited (0 used).
- SharePoint archive limitations:** Connection count: unlimited (1 used), File(s) count: unlimited (230 used).
- Teams archive limitations:** User count: unlimited (0 used), Team count: unlimited (0 used), Size: unlimited (0 used); Deactivated user count: unlimited (0 used), Deactivated team count: unlimited (0 used), Item count: unlimited (0 used).

How to activate your license key

If you want to activate a new license, click on option “**activate license**” below the breadcrumbs.

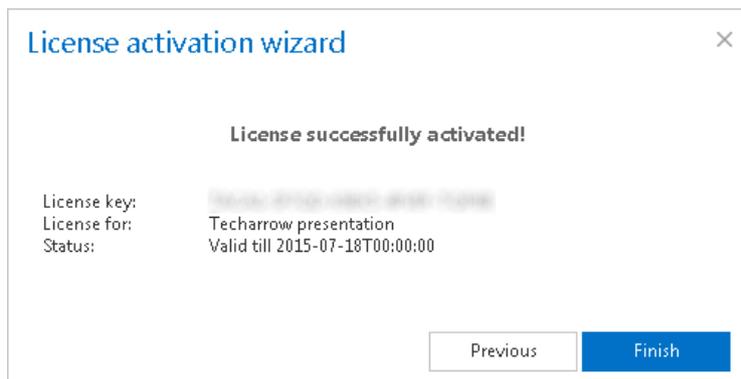
This image is a close-up of the 'Licensing' page breadcrumb and buttons. The breadcrumb trail is 'System > Services > Licensing'. Below the breadcrumbs, there are two buttons: 'activate license' and 'update telemetry'. The 'activate license' button is circled in red.

Insert your license key into the **License key** textbox of **License activation wizard** dialog and choose from 2 methods of license activation and follow the steps described below:



The dialog box is titled "License activation wizard" and contains a "License key" text input field with a placeholder license key. Below it, under "Activation type", there are two radio buttons: "Online activation" (which is selected) and "Offline activation". A "Next" button is located at the bottom right.

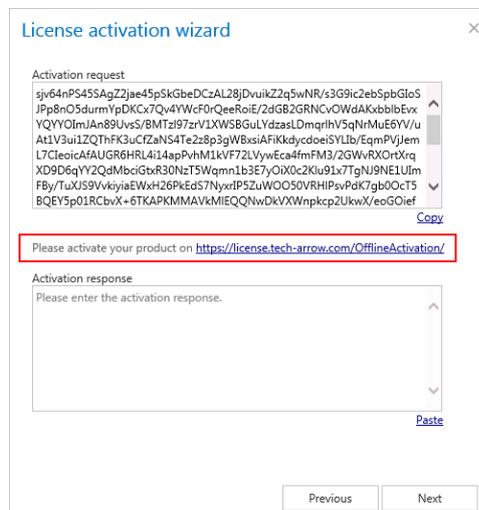
- 1) **Online activation** (requires internet access on the contentACCESS server) – click **Next** → **Finish** and your license will be activated automatically.



The dialog box is titled "License activation wizard" and displays the message "License successfully activated!". Below this, it shows the license key, the license for "Techarrow presentation", and the status "Valid till 2015-07-18T00:00:00". At the bottom, there are "Previous" and "Finish" buttons.

- 2) **Offline activation** (doesn't require internet access on the contentACCESS server)

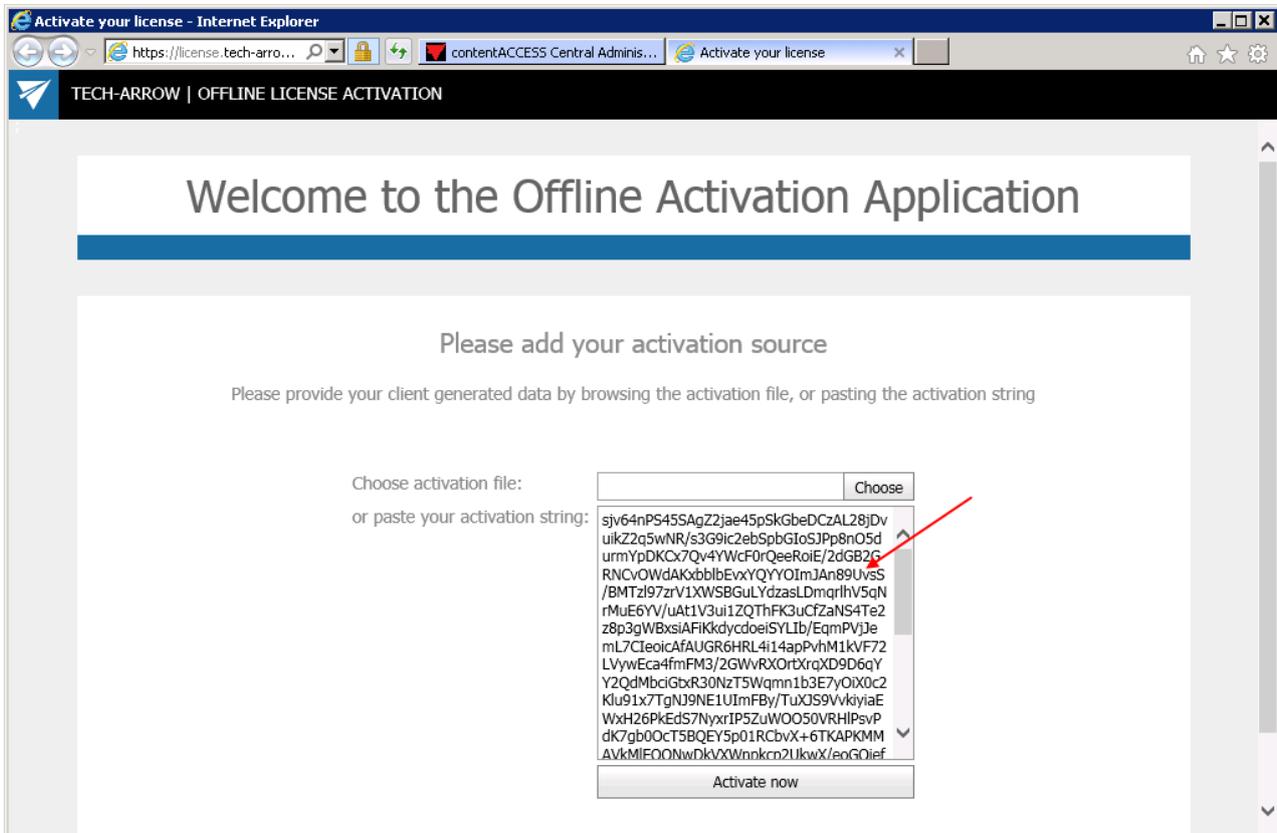
a) Open the offline license activation page of contentACCESS using the link in the dialog:



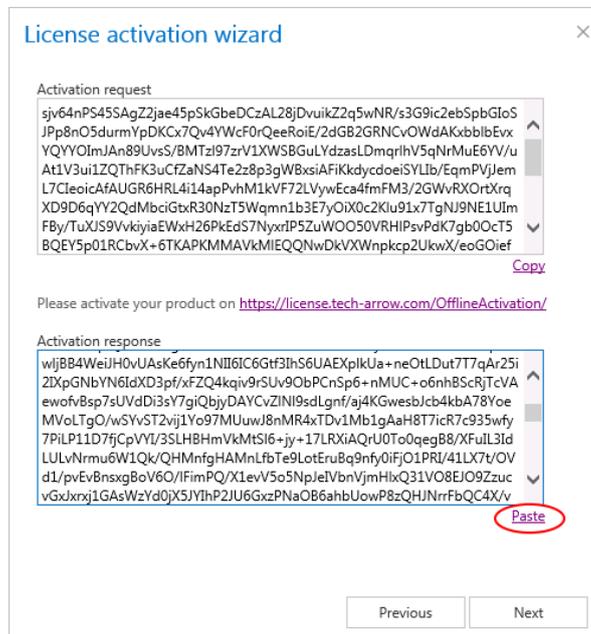
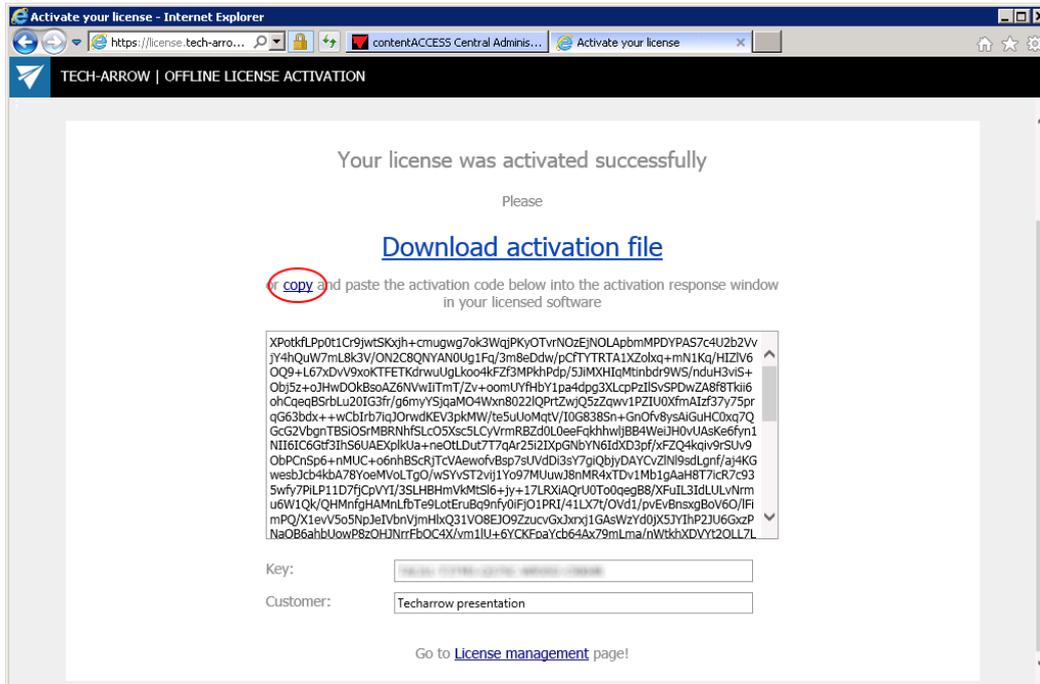
The dialog box is titled "License activation wizard" and shows an "Activation request" section with a long alphanumeric string. Below this, a red box highlights the instruction: "Please activate your product on <https://license.tech-arrow.com/OfflineActivation/>". Underneath is an "Activation response" section with a text input field and a "Paste" button. "Previous" and "Next" buttons are at the bottom.



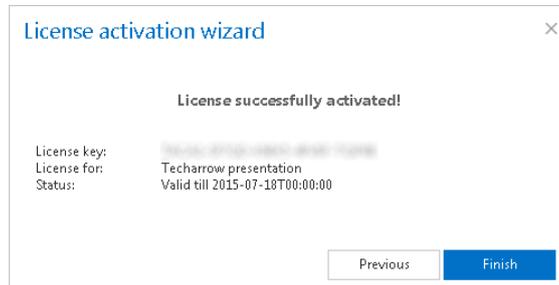
- b) Copy&paste the **Activation request** from the above dialog to the appropriate field and click **“Activate now”** to generate an activation response.



- c) Copy&paste the activation response from the web page (1st picture below) to the license activation dialog (2nd screenshot below).



d) Click **Next** and the license key will be successfully activated.

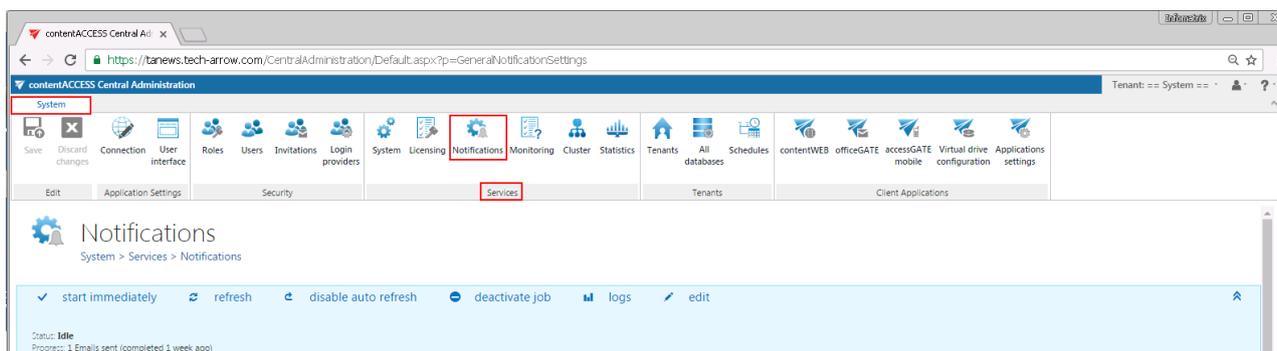


After successful license activation all **Allowed plugins, stores and limitations** within this license will be updated on the page.

Notifications

To increase efficiency of the troubleshooting process, contentACCESS uses notification plugins. These plugins are used to send notification emails to the user about the errors/warnings/misconfigurations or possible system or job failures in contentACCESS. Based on the settings in the Central Administration, the transport server of these notifications can be either an Exchange server, or an SMTP server. If the organization doesn't have Exchange Server, SMTP server can be used instead.

For Notification settings open the **Notifications** page (**System** tab → **Services** group →  **Notifications** button) on the Central Administration ribbon.



In the status bar of notifications there are 6 control buttons:

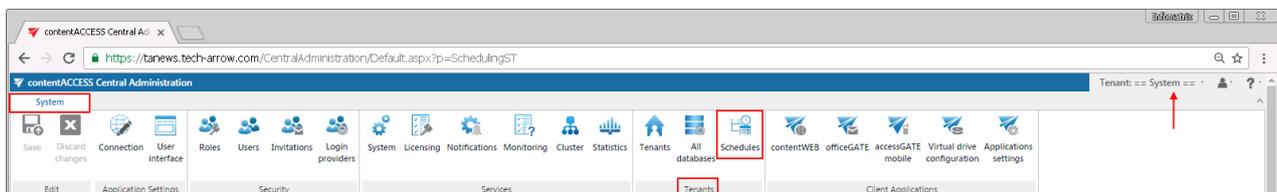
- With the “start immediately/stop” button it is possible to manually start/stop the sending of notification emails;



- “refresh” control button serves to reload (manually refresh) the current state of notification plugin;
- “enable auto refresh”/“disable auto refresh”: serves for activating/deactivating the auto refresh of notification plugin status information; if enabled, then the current state will be refreshed in every 5 seconds;
- “deactivate job/activate job” button is used to deactivate/activate the job if it should not run; a deactivated job will not be started automatically, nor can be started manually.
- “logs”: in case that you want to check the notifications plugin events, or if any problem occurred during the sending of notifications emails, click on this control button and you will be redirected to the corresponding monitoring page, where the last run of the plugin will be pre-selected, and the corresponding run events will be displayed.
- “edit” control button is used to change the name of the notification job and to specify the node where the job should run;
- With the arrows mark () at the right side of the status bar the user may collapse or expand the progress information about the job’s running. The status bar’s last state is always stored, and the last state will be opened by navigating to the page again.

Under the status bar the following sections are configured:

- **Scheduling settings:** This configuration option is common both for SMTP and Exchange server transport types. The administrator can choose here an already existing notification scheduler from the list, or create a new one. Notification emails will be sent at time, which is set here. New notification schedulers can be also created (or edited) by selecting the “system” tenant in the right upper menu of the Central Administration user interface, and configuring the schedulers on the **Schedules** page (**System** tab → **Tenants** group → option **Schedules** on the ribbon, refer to screenshot below).



- **Notification settings:** The administrator can choose right here, if the SMTP server or Exchange provider will be used to transfer notification emails.



Notification settings

Transport server type: Use Exchange Server
 Use SMTP server

From address:

Administrator addresses:

Test email was successfully sent

In both cases, the

From address – the email address of the real sender

Administrator addresses – the recipient addresses

text boxes must be filled. It is also possible to send notification emails on behalf of somebody else. The condition for that is to have on behalf permissions on the mailbox of this second user. It is recommended to send a test email via the “Send test email” button to check, if everything works correctly.

The page displays different configuration sections based on which transport type is selected in the Notification settings section. If “Use Exchange Server” is selected, then the **EWS settings** must be configured; if “Use SMTP server” is set, then the **SMTP server settings** must be configured. SMTP server is used if the organization doesn’t have Exchange Server.



contentACCESS Central Administration

Tenant: == System ==

System

Save Discard changes Roles Users Invitations Login providers System Licensing Notifications Cluster Statistics SMTP Servers System logs Configuration auditing Tenants All databases Schedules contentWEB officeGATE contentACCESS mobile Virtual drive configuration Teams Applications settings

Notifications

System > Services > Notifications

start immediately refresh disable auto refresh deactivate job logs edit

Status: Idle
Progress: 0 Emails sent (1 failed) (completed 2 days ago)

Notification settings

Transport server type: Use Exchange Server Use SMTP server

From address: @ta.internal

Administrator addresses: @ta.internal

Send test email

*Note: To send a test email, the connection to the selected transport server must be configured. Please fill in the EWS or SMTP server settings below.

Exchange connection settings

Exchange server type: Exchange Online (O365)

Region: Global

Exchange server interface version: Exchange 2016 or higher

EWS Uri: https://outlook.office365.com/EWS/Exchange.asmx

Use impersonation:

EWS authentication mode: Modern

OAuth application ID: 72c7-...

OAuth tenant ID: 4b0e-...

OAuth client secret:

Use explicit credentials:

User name: taadministrator
administrator@domain.com or domainadministrator

Password:

Test connection

Resource settings

Worker thread count: 2

Online help

Screenshot A: Exchange Server used

contentACCESS Central Administration

Tenant: == System ==

System

Save Discard changes Connection User interface Roles Users Invitations Login providers System Licensing Notifications Monitoring Cluster Statistics Tenants All databases Schedules contentWEB officeGATE accessGATE mobile configuration Applications settings

Notifications

System > Services > Notifications

start immediately refresh disable auto refresh deactivate job logs edit

Scheduling settings

Scheduled in: always

Notification settings

Transport server type: Use Exchange Server Use SMTP server

From address: @tech-arrow.com

Administrator addresses: companyadmin@tech-arrow.com

Test email was successfully sent

Send test email

SMTP server settings

Host: smtp.office365.com

Port: 587

Enable SSL:

User name: @tech-arrow.com

Password:

Confirm password:

Resource settings

Worker thread count: 2

Online help



Screenshot B: SMTP server used

- **EWS settings:** The following parameters are needed for EWS connection:

Exchange server type: the type of the Exchange provider which will send the notification emails.

Region:

In case of the user having/using a [German cloud](#) (dedicated and isolated Microsoft Azure version for Germany), **Germany** must be selected in the **Region** dropdown list.

In case that the predefined settings for **O365** don't match your expectation and/or needs, it is possible to select the **Custom** option from the **Region** dropdown list and specify your own values.

Exchange connection settings

Exchange server type:	Exchange Online (O365)	
Region:	Custom	
Exchange server interface version:	Exchange 2016 or higher	←
EWS Url:	https://outlook.office365.com/EWS/Exchange.asmx	←

Exchange server interface version: the version of the Exchange provider which will send the notification emails.

EWS URL (received from the Exchange provider)

Use impersonation: By default, this checkbox is turned off. If it is turned on, **Impersonation** will be used instead of **delegation** (more information in [this](#) section). Impersonation allows the superuser account to impersonate any other user's account and access their mailboxes.

Note: Only accounts with the **ApplicationImpersonation** role can use impersonation. For more information about how to configure impersonation for your account, please check [this](#) page.

If the O365 user has "desktopless" license, his account **can't be used** for impersonation. The problem is that EWS access is disabled for such user (he is unable to connect to EWS).

EWS authentication mode: Select one **EWS authentication mode** from the dropdown list. There are 2 options: **Basic** and **Modern**. **Basic** authentication method was used by default in previous versions and it wasn't possible to select another authentication type. **Modern** authentication is more secure and complex and requires the app to be registered on **Azure portal**. How to register it and gain the necessary **IDs** and **client secret** is described in [this](#) section.



EWS authentication mode:	Modern
OAuth application ID:	72c73
OAuth tenant ID:	4b0e
OAuth client secret:

Keep connection alive: If it is turned on, then the connection between contentACCESS and the Exchange server is cached, which increases the performance. If the Exchange is load balanced, some requests can land on another Exchange which causes errors in contentACCESS. In these cases unchecking the keep alive option will destroy the connection after each request and will rebuild it on the next request.

- If you are communicating with **one Exchange server: turn it on** to increase the performance
- If you have a **load balanced Exchange environment** and there are **communication problems** with the Exchange: it is recommended to **turn it off**

User name, Password: Finally enter the **User name** (email address) and **password** of the EWS user that can be applied to connect to the Exchange server.

➤ **SMTP server settings:** the following parameters are needed for the SMTP connection:

Host – name of the SMTP server (like: smtp.gmail.com, smtp.office365.com, ...)

Port – the SMTP port of the SMTP server. There are some recommendations and standards. Usually the port 25 is used for SMTP (or 2525). But because this protocol is vulnerable, the port is usually blocked by firewall. The secure SMTP port is either 465 or 587. The port 587 is usually using TLS (Transport layer security).

Enable SSL - based on the SMTP server it is possible to enable SSL (recommended)

User name, password: authenticated user on the SMTP server (required)

Use the **Send test email** button to verify if the notification emails are working properly.

➤ **Resource settings:** under worker thread count, at the bottom of the page you can set the count of simultaneously sent notifications.



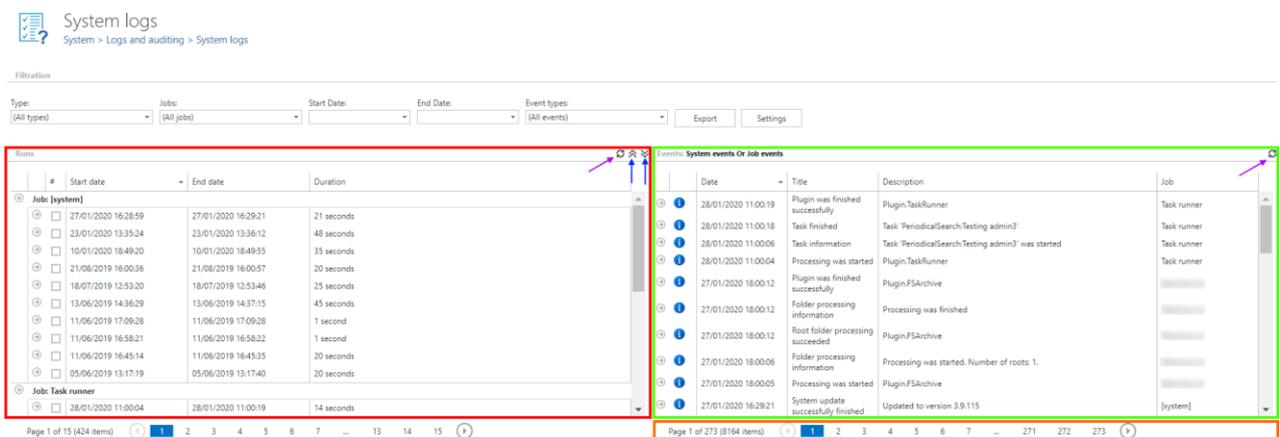
System logs — how to find out possible misconfigurations / reasons of potential system/job failures

Navigate to **System** → **Logs and auditing** → **System logs** button.



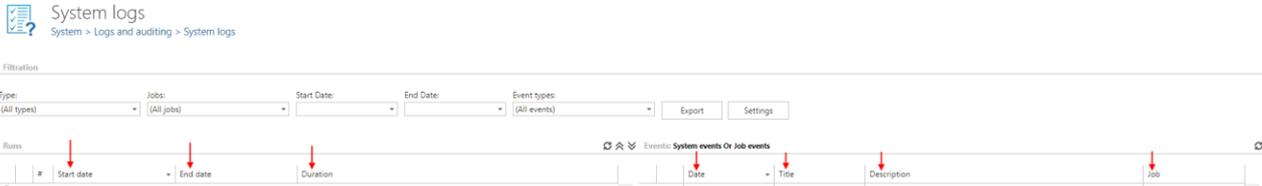
The **System logs** feature enables to check the currently running or in the past run system or job related events very easily. The user can check here all desired system events such as system updates, shutdowns, startups, system component updates, or possible system errors etc. In **System logs** feature, the user also has the chance to check all possible failure details that might happen during the running of the jobs, so it makes the troubleshooting easier.

If you first open **System logs**, you can see the following basic parts on the interface: **Runs** of the jobs or system on the left side (**red** frame); **system and job events** on the right side (**green** frame). With clicking on the **Refresh** button (**purple** arrow) you can also check the real-time running jobs. With this button it is possible to reload the current runs/event from the database. With a single click on the **collapse all/expand all** buttons (indicated with **blue** arrows) you can expand or collapse all sessions for all jobs. It is also enabled to list among the events at the bottom of the **System logs** page (**orange** frame).





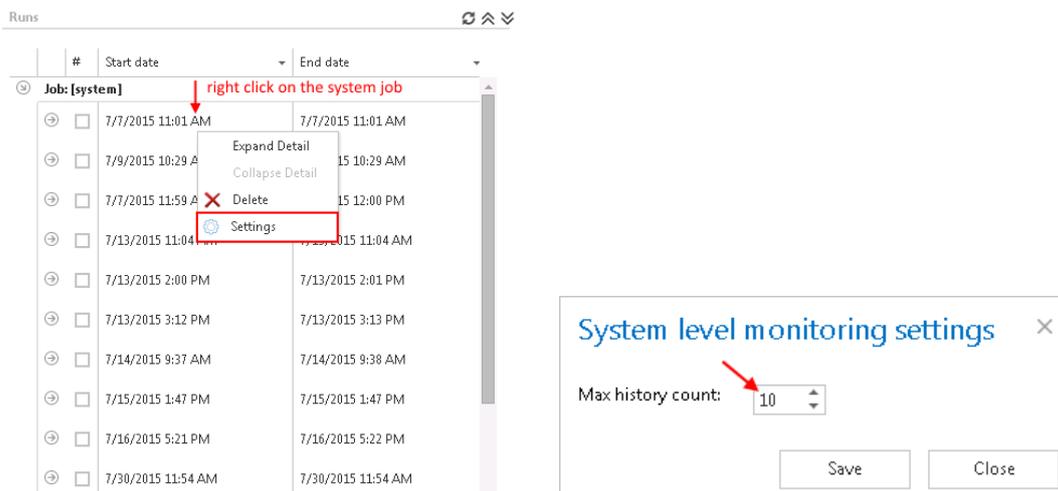
Sorting in System logs: sorting option is enabled both in the **Runs** and **Events** tables. Click on the particular column name (Start date, End date by the runs, Date, Title, Description, Job by the events), and the items will be displayed in the reverse order.



Setting of maximum history count of the runs: With this option it is possible to set, how many job runs the user would like to keep. If the value is set to 10 for example, and a job has run 20 times, then only the last 10 runs can be viewed, remaining 10 will be deleted and the user will not have an access to them. It is recommended to set a higher value here, if a job is running too often, or during the weekends, and the user needs to view the events retroactively.

This value is always inherited from the higher level. There are three levels altogether, where the history counter can be adjusted; the **system** is the highest level, the next is **tenant** level and the last one is the level of **jobs**.

- **System level settings** are accessible with right mouse click on a system related job in the column of **Runs**; here click on **Settings**, and adjust these settings in the **System level monitoring setting** dialog.



- **Tenant level monitoring settings** are inherited from the system, i.e. if maximum history count is set on "10" on system level, then the same value will apply for the tenant level monitoring settings, too. Nevertheless it is possible to configure the tenant level settings independently from the system settings. Click on the **Settings** button and set the required value into the **Tenant level monitoring settings** dialog.

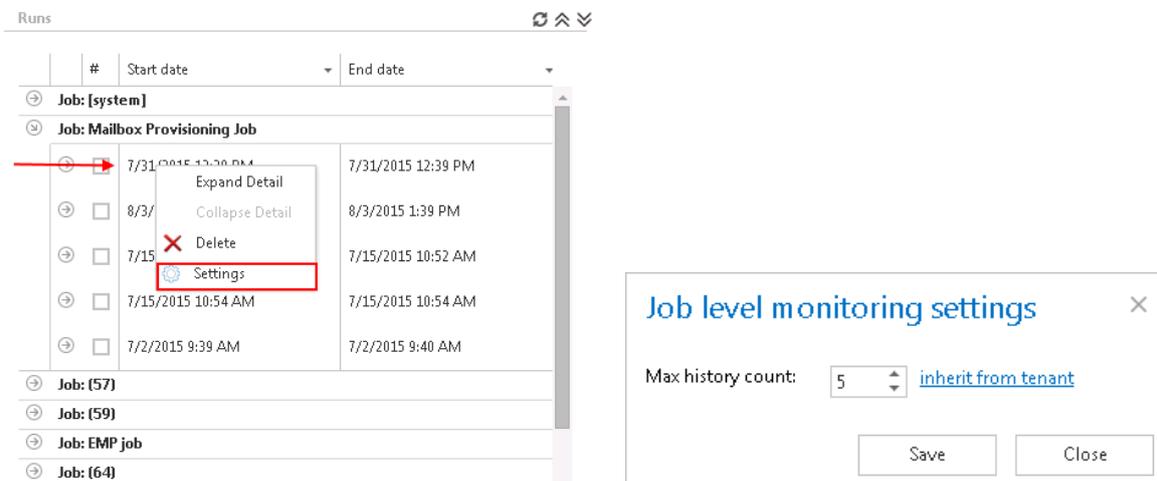


If the tenant level settings are set independently, it can be still adjusted to the system settings with a click on the “inherit from system” option in the **Tenant level monitoring settings** dialog.

System logs
System > Logs and auditing > System logs



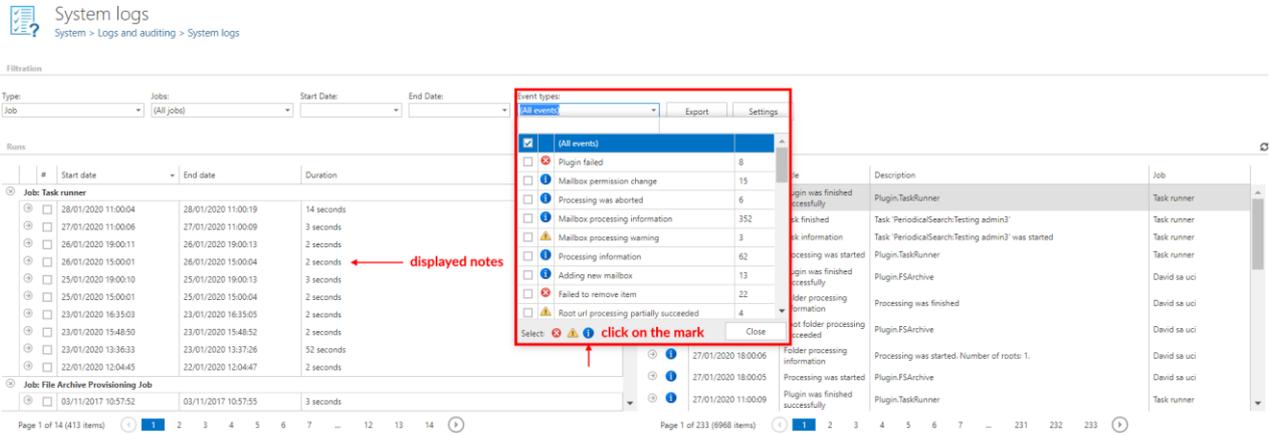
- **Job level monitoring settings** can be adjusted with clicking on the particular job running in the column of **Runs** and configuring these settings in the **Job level monitoring setting** dialog. These settings are inherited from the tenant by default. Nevertheless it is still possible to set another value with a right click on the particular job in the **Runs** column, select here **Settings** and set the maximum history count in the dialog. This value can be adjusted to the default value inherited from tenant with clicking on the “inherit from tenant” option in the same dialog.



Filtration in System logs: If the user would like to check details of a certain system/job running, then he can also filter among the jobs under **Filtration** → **Jobs:** dropdown list. If it is necessary to check the system/job events that run in a certain period of time, then it is possible to further filter among these items with setting the **Start date** and the **End date** under filtering options. Under **Event types** it is allowed to filter among event types occurred in the actually selected events. An event type filter is also available at the bottom of the Event types dropdown list. Using this filter it is possible to sort out all events which belong to one of the



3 event groups [1. error (❌), 2. warning (⚠️) or 3. note (ℹ️)]. Click on the mark of the particular event group next to “Select”, and the selected events will be displayed. On screenshot below, we sorted out all the notes (with a click on “ℹ️” mark).



Note: If the logged in user is a system administrator, then he will be allowed to see the system related events, if he has tenant administrator rights, then he will be allowed to check the tenant related events using monitoring feature.

The **Export** function makes it easy to save the reviewed events into XML, CVS or HTML. The report contains all necessary information (date, job ID, Message, Details) which enable to have a look at the desired information, and also identify possible failures very quickly. This enables a very quick access to the system/job processing information and also ensures a very quick troubleshooting in case of need.



On the below displayed screenshot we have filtered out **Mailbox Provisioning Job** and **TA_ Email Archive job** and set 1st of July 2015 as **Start date**, and 8th of July as **End date**. Among event types we have also set **All events**. This filter will find all the events related to these 2 jobs, which happened in this time interval.



System logs

System > Logs and auditing > System logs

Filtration

Type: Job

Jobs: visioning Job:TA_ Email archive job

Start Date: 7/1/2015 12:00 AM

End Date: 7/9/2015 12:00 AM

Event types: (All events)

Export

Runs

#	Start date	End date
Job: Mailbox Provisioning Job		
<input type="checkbox"/>	7/2/2015 9:39 AM	
Job: TA_ Email archive job		
<input type="checkbox"/>	7/2/2015 9:22 AM	
<input type="checkbox"/>	7/3/2015 10:56 AM	
<input type="checkbox"/>	7/3/2015 11:08 AM	
<input type="checkbox"/>	7/3/2015 11:15 AM	
<input type="checkbox"/>	7/3/2015 11:15 AM	
<input type="checkbox"/>	7/3/2015 11:19 AM	
<input type="checkbox"/>	7/7/2015 11:16 AM	
<input type="checkbox"/>	7/7/2015 12:16 PM	

Jobs list:

- (All jobs)
- Mailbox Provisioning Job
- TA_ Email archive job
- TA_EA 2
- FA job
- EMP job
- File content extractor
- Email archive new job
- restore
- New email archive job
- Email Archive

Events: Job is Mailbox Provisioning Job Or Job is TA_ Email archive job And (Date >= 7/1/2015 12:00:00 AM And Date <= 7/9/2015 12:00:00 AM)

Date	Title	Description
7/7/2015 12:17 PM	Plugin was finished successfully	Plugin.EmailArchive
7/7/2015 12:17 PM	Mailbox processing information	Processing was finished
7/7/2015 12:17 PM	Mailbox processing information	Mailbox processing finished
7/7/2015 12:17 PM	Mailbox processing succeeded	Plugin.EmailArchive
7/7/2015 12:16 PM	Mailbox processing information	Processing was started. Number of mailboxes: 1.
7/7/2015 11:18 AM	Plugin was finished successfully	Plugin.EmailArchive
7/7/2015 11:18 AM	Mailbox processing information	Mailbox processing finished
7/7/2015 11:18 AM	Mailbox processing information	Processing was finished
7/7/2015 11:18 AM	Mailbox processing succeeded	Plugin.EmailArchive
7/7/2015 11:16 AM	Mailbox processing information	Processing was started. Number of mailboxes: 1.
7/3/2015 11:19 AM	Plugin was finished successfully	Plugin.EmailArchive
7/3/2015 11:19 AM	Mailbox processing information	Processing was finished
7/3/2015 11:19 AM	Mailbox processing information	Mailbox processing finished
7/3/2015 11:19 AM	Mailbox processing succeeded	Plugin.EmailArchive
7/3/2015 11:19 AM	Mailbox processing information	Processing was started. Number of mailboxes: 1.

Under **Runs** section click on the arrow mark next to the job and the last run times will be opened. In the table of **Events** at the right side of the screenshot you can see all the events related to these 2 jobs, in time period 1st of July – 8th of July. With a click on the certain run of the job instance (for example with a click on the Mailbox Provisioning job that run at 7/2/2015 at 9:39-9:40) you can open further details about this run. In our case we can see that Mailbox provisioning job has processed in this time 98 mailboxes, of which 25 mailboxes added, 71 mailboxes skipped, 2 mailboxes updated etc. (red arrows).

If you check the checkbox next to this run of the job, then the right hand table will display all events, all event types related to this run at 9:39-9:40, on 2nd of July.

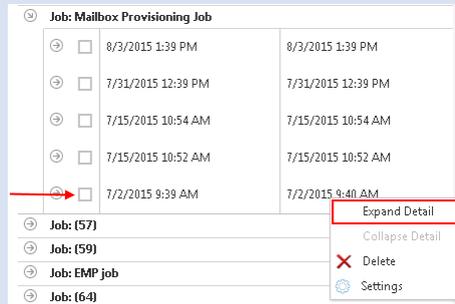
Runs

#	Start date	End date	Date	Title	Description	Job
Job: Mailbox Provisioning Job						
<input checked="" type="checkbox"/>	7/2/2015 9:39 AM	7/2/2015 9:40 AM	7/2/2015 9:40 AM	Plugin was finished successfully	Plugin.MailboxProvisioning	Mailbox Provisioning Job
<input type="checkbox"/>	7/2/2015 9:39 AM	7/2/2015 9:40 AM	7/2/2015 9:40 AM	contentACCESS user skipped from permission sync	User 'sa' permissions can't be set because the user [SID] could not be resolved.	Mailbox Provisioning Job
<input type="checkbox"/>	7/2/2015 9:39 AM	7/2/2015 9:40 AM	7/2/2015 9:40 AM	contentACCESS user skipped from permission sync	User 'new user' permissions can't be set because the user [SID] could not be resolved.	Mailbox Provisioning Job
<input type="checkbox"/>	7/2/2015 9:39 AM	7/2/2015 9:40 AM	7/2/2015 9:40 AM	contentACCESS user skipped from permission sync	User 'MA' permissions can't be set because the user [SID] could not be resolved.	Mailbox Provisioning Job
<input type="checkbox"/>	7/2/2015 9:39 AM	7/2/2015 9:40 AM	7/2/2015 9:40 AM	contentACCESS user skipped from permission sync	User 'administrator' permissions can't be set because the user [SID] could not be resolved.	Mailbox Provisioning Job
<input type="checkbox"/>	7/2/2015 9:22 AM	7/2/2015 9:24 AM	7/2/2015 9:40 AM	Updating mailbox	Updating mailbox '9 (@fab@tech-arrow.com)' in DB.	Mailbox Provisioning Job
<input type="checkbox"/>	7/3/2015 10:56 AM		7/2/2015 9:40 AM	Adding mailbox to group	Adding mailbox '9 (@fab@tech-arrow.com)' to group '1'.	Mailbox Provisioning Job
<input type="checkbox"/>	7/3/2015 11:08 AM	7/3/2015 11:08 AM	7/2/2015 9:40 AM	Mailbox permission change	Mailbox permission changed for '26 (@vladimir.werskov@tech-arrow.com)'.	Mailbox Provisioning Job
<input type="checkbox"/>	7/3/2015 11:15 AM	7/3/2015 11:15 AM	7/2/2015 9:40 AM	Adding new mailbox	Adding new mailbox '26 (@vladimir.werskov@tech-arrow.com)' to DB.	Mailbox Provisioning Job
<input type="checkbox"/>	7/3/2015 11:15 AM	7/3/2015 11:15 AM	7/2/2015 9:40 AM	Mailbox permission change	Mailbox permission changed for '25 (@fr@TECHARROW.onmicrosoft.com)'.	Mailbox Provisioning Job
<input type="checkbox"/>	7/3/2015 11:15 AM	7/3/2015 11:15 AM	7/2/2015 9:40 AM	Adding new mailbox	Adding new mailbox '25 (@fr@TECHARROW.onmicrosoft.com)' to DB.	Mailbox Provisioning Job
<input type="checkbox"/>	7/3/2015 11:19 AM	7/3/2015 11:19 AM	7/2/2015 9:40 AM	Mailbox permission change	Mailbox permission changed for '24 (@support@TECHARROW.onmicrosoft.com)'.	Mailbox Provisioning Job
<input type="checkbox"/>	7/3/2015 11:19 AM	7/3/2015 11:19 AM	7/2/2015 9:40 AM	Adding new mailbox	Adding new mailbox '24 (@support@TECHARROW.onmicrosoft.com)' to DB.	Mailbox Provisioning Job
<input type="checkbox"/>	7/7/2015 11:16 AM	7/7/2015 11:18 AM	7/2/2015 9:40 AM	Mailbox permission change	Mailbox permission changed for '23 (@ale@tech-arrow.com)'.	Mailbox Provisioning Job
<input type="checkbox"/>	7/7/2015 11:16 AM	7/7/2015 11:18 AM	7/2/2015 9:40 AM	Adding new mailbox	Adding new mailbox '23 (@ale@tech-arrow.com)' to DB.	Mailbox Provisioning Job
<input type="checkbox"/>	7/7/2015 12:16 PM	7/7/2015 12:17 PM	7/2/2015 9:40 AM	Mailbox permission change	Mailbox permission changed for '22 (@peter.madina@tech-arrow.com)'.	Mailbox Provisioning Job
<input type="checkbox"/>	7/7/2015 12:16 PM	7/7/2015 12:17 PM	7/2/2015 9:40 AM	Adding new mailbox	Adding new mailbox '22 (@peter.madina@tech-arrow.com)' to DB.	Mailbox Provisioning Job

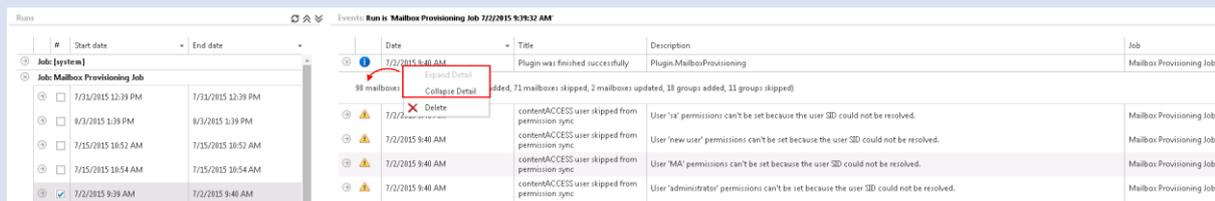
checkbox - This checkbox to view events from this time interval
 98 mailboxes processed (25 mailboxes added, 71 mailboxes skipped, 2 mailboxes updated, 4 groups added, 11 groups skipped)

click here to open further details

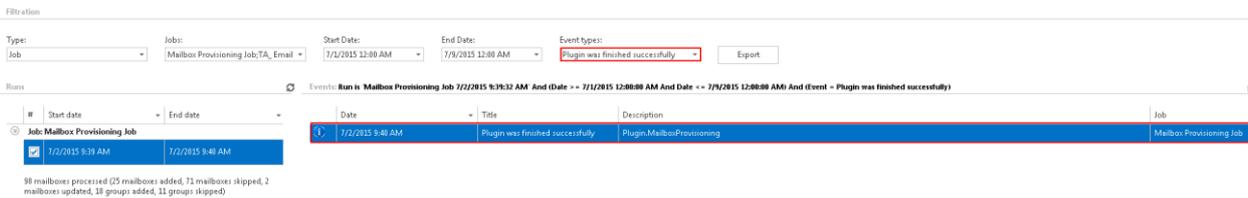
Note: The exact details of a job/system running can be opened/collapsed with a right click on the particular session and selecting **Expand Details/Collapse Details** from the context menu.



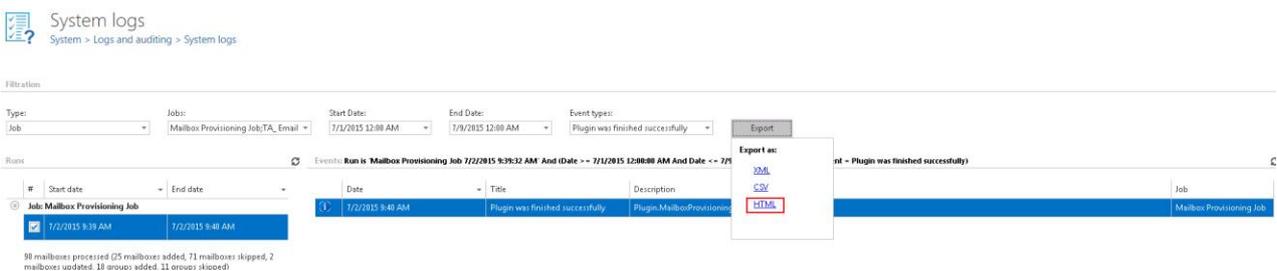
Note: The user can open/close additional details related the selected event with a right mouse click on a particular event and selecting **Expand Detail/Collapse Detail** from the context menu.



Now, if you want to visualize only information about **Plugin was finished successfully** type of event, then set this filter in the **Event types** checkbox. As result, only this type of event will be displayed in the table of **Events**.



With the **Export** function you can save this report in one of the file types, for example in HTML:



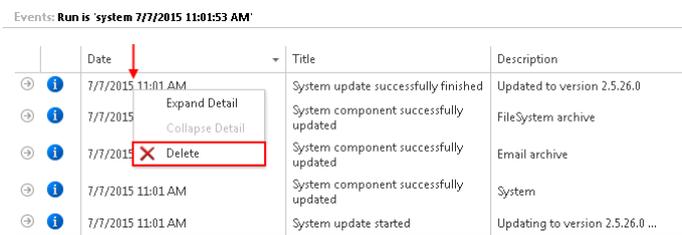
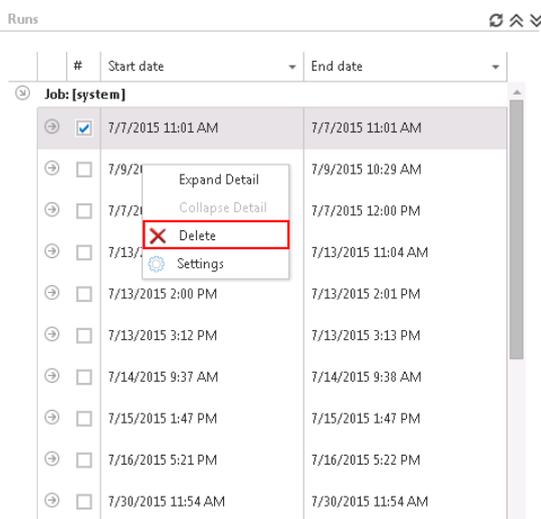


The report will contain all necessary information that might be very useful for a user to identify any failure, or just check the last event(s) of this job at the time period that was filtered out.

ID	Code	Type	Title	Date	Job ID	Message	Details
Filter: Run is 'Mailbox Provisioning Job 7/2/2015 9:39:32 AM' And (Date >= 7/1/2015 12:00:00 AM And Date <= 7/9/2015 12:00:00 AM) And (Event = Plugin was finished successfully)							
158	13103	Info	Plugin was finished successfully	7/2/2015 9:40:23 AM	56	Plugin.MailboxProvisioning	<d t="MonitoringStatDetails" <+ 88 mailboxes processed (25 mailboxes added, 71 mailboxes skipped, 2 mailboxes updated, 18 groups added, 11 groups skipped)</+></d>

How to manually remove system/job runs and system/job related events from System logs:

- **To delete system/job runs** right click on the particular system/job run in column **Runs** and select **Delete** from the context menu (Screenshot A).
- **To delete a particular event** right click on the particular event and select **Delete** from the context menu (Screenshot B)



Screenshot A: Deleting system/job runs

Screenshot B: Deleting system/job events

What to do if more space is needed on the System logs page? If there are too many events and the user would like to have more space on the System logs page, it's a good idea to hide the ribbon with clicking on the arrow sign at the upper right corner of the user interface, under the **About** menu.

Configuration auditing

The **Configuration auditing** captures the configuration changes in contentACCESS. With this feature, you will be able to discover which user changed "what" and "when".

To view and search the auditing data, navigate to **System -> Logs and auditing -> Configuration auditing**.



Scope	Object	Operation name	Date	Initiated by	Access IP	State
Job actions	SP archive	Update	23/01/2020 17:04:50	Administrator	192.168.190.96	Succeeded
Job actions	SP delete	Update	23/01/2020 17:00:54	Administrator	192.168.190.96	Succeeded
Job configuration	SP delete	Update	23/01/2020 17:00:09	Administrator	192.168.190.96	Succeeded
Job actions	SP delete	Update	23/01/2020 16:58:58	Administrator	192.168.190.96	Succeeded
Job configuration	SP delete	Update	23/01/2020 16:58:48	Administrator	192.168.190.96	Succeeded
Job actions	SP archive	Update	23/01/2020 16:51:12	Administrator	192.168.190.96	Succeeded
Job actions	SP delete	Update	23/01/2020 16:44:39	Administrator	192.168.190.96	Succeeded
Job configuration	SP delete	Update	23/01/2020 16:44:34	Administrator	192.168.190.96	Succeeded
Job actions	SP archive	Update	23/01/2020 16:40:54	Administrator	192.168.190.96	Succeeded
Job actions	SP delete	Update	23/01/2020 16:36:22	Administrator	192.168.190.96	Succeeded
Job configuration	SP delete	Update	23/01/2020 16:35:32	Administrator	192.168.190.96	Succeeded
Job actions	SP archive	Update	23/01/2020 16:30:53	Administrator	192.168.190.96	Succeeded

You can filter the auditing entries by:

- User that did the changes
- Object type - role, job, user, database configuration, storage configuration, etc.
- A specific object - job, database, storage, etc.
- Date and action – create, update, delete

If you expand a row, you can see the changes that were done. If the old values/settings are known, both previous and the new values/settings are displayed. In this case, we are able to view all settings.



Configuration auditing
System > Logs and auditing > Configuration auditing

Filteration

Users: (Anyone) Scope: (Any scopes) Objects: (Any operations) Operation name: (Any operations) Start Date: End Date:

Export

Events:

Scope	Object	Operation name	Date	Initiated by	Access IP	State
Job management	FSA retention change	Delete	30/01/2020 17:44:55	Administrator	192...	Succeeded
Job configuration	FSA retention change	Update	30/01/2020 17:44:04	Administrator	192...	Succeeded

Job configuration: Administrator updated FSA retention change

Retention Repo	Old value	New value
	<SerializableRepoReference> <ObjectId>0</ObjectId> </SerializableRepoReference>	<SerializableRepoReference> <Name>1 year</Name> <ObjectId>3</ObjectId> </SerializableRepoReference>
Scheduler		Manual

Show all settings

Scope	Object	Operation name	Date	Initiated by	Access IP	State
Job management	FSA retention change	Create	30/01/2020 17:37:56	Administrator	192...	Succeeded
Job actions	SP archive	Update	23/01/2020 17:04:50	Administrator	192...96	Succeeded

Page 1 of 1 (21 items)

[Online help](#)

Scope	Object	Operation name
Job management	FSA retention change	Create

Job management: Administrator created FSA retention change

Cluster Node Id	null
Custom Name	FSA retention change
Display Name	File system archive retention changer
Is Active	true
Load Plugin	true
Name	Plugin.FileArchive.RetentionChanger
Plugin Id	10152
Tenant Id	1
Tenant Name	TECH-ARROW

Screenshot: A job was created

Scope	Object	Operation name
Job configuration	FSA retention change	Update

Job configuration: Administrator updated FSA retention change

Retention Repo	Old value	New value
	<SerializableRepoReference> <ObjectId>0</ObjectId> </SerializableRepoReference>	<SerializableRepoReference> <Name>1 year</Name> <ObjectId>3</ObjectId> </SerializableRepoReference>
Scheduler		Manual

Show all settings

Screenshot: A job was updated

Scope	Object	Operation name
Job management	FSA retention change	Delete

Job management: Administrator deleted FSA retention change

Cluster Node Id	null
Custom Name	FSA retention change
Display Name	Plugin.FileArchive.RetentionChanger
Is Active	true
Load Plugin	true
Name	Plugin.FileArchive.RetentionChanger
Plugin Id	10152
Tenant Id	1
Tenant Name	TECH-ARROW

Screenshot: A job was deleted

The list of the auditing entries can be exported to HTML, CSV and XML format by clicking on the **Export** button and choosing the desired format.

Configuration auditing
System > Logs and auditing > Configuration auditing

Filteration

Users: (Anyone) | Scope: (Any scopes) | Objects: | Operation name: (Any operations) | Start Date: | End Date:

Export

Export as:
[XML](#)
[CSV](#)
[HTML](#)

Object	Operation name	Date
SP archive	Update	23/01/2020 17:04:50
SP delete	Update	23/01/2020 17:00:54
SP delete	Update	23/01/2020 17:00:09
SP delete	Update	23/01/2020 16:58:58

Archive auditing

The Archive auditing feature allows logging every file access, executed search queries, user log in/log out actions and actions about legal hold creation and deletion.

Configuration

The Archive auditing feature has to be configured and enabled in order to function properly. (**System → Logs and auditing → Archive auditing**)



contentACCESS Central Administration

System	File Archive	Email Archive	SharePoint Archive	BackMailz	GDPR	Custom plugins
Save Discard changes	Roles Users Invitations Login providers	System Licensing Notifications Cluster Statistics Legal hold Task runner Indexing SMTP Servers SMTP Mappings	System logs Configuration auditing	Archive auditing		
Edit	Security	Services	Logs and auditing			

Archive auditing
System > Logs and auditing > Archive auditing

⚠ Auditing is not activated. [Activate auditing](#)

contentACCESS Central Administration

System	File Archive	Email Archive	SharePoint Archive	BackMailz	GDPR	Custom plugins
Save Discard changes	Roles Users Invitations Login providers	System Licensing Notifications Cluster Statistics Legal hold Task runner Indexing SMTP Servers SMTP Mappings	System logs Configuration auditing	Archive auditing		
Edit	Security	Services	Logs and auditing			

Archive auditing
System > Logs and auditing > Archive auditing

Auditing settings

Enable auditing:

Database settings

Database connection:

Options

- **Enable auditing:** the Archive auditing functionality can be enabled or disabled anytime. If the Archive auditing is disabled, then no new entries will be added to the Archive auditing log.
- **Database connection:** the database where the log entries will be saved. The database shouldn't be changed. If the database is changed, then the previously created Archive auditing logs will not be accessible.

After the page is saved, the user is automatically redirected to the Archive auditing logs browse mode.



contentACCESS Central Administration

System	File Archive	Email Archive	SharePoint Archive	BackMailz	GDPR	Custom plugins
Save Discard changes	Roles Users Invitations Login providers	System Licensing Notifications Cluster Statistics Legal hold Task runner Indexing SMTP Servers SMTP Mappings	System logs Configuration auditing Archive auditing			
Edit	Security	Services	Logs and auditing			

Archive auditing
System > Logs and auditing > Archive auditing

Filteration

Users: (All users) Start Date: End Date: Event types:

Export Settings

Events: User = All users

Date	Title	Description
No data to display		

To modify the settings, click on the **Settings** button on the Archive auditing logs browse view.

Archive auditing log browsing

The view is similar to the [System logs](#). The user can filter the Archive auditing logs by user, date range or different event types. The grid that contains the Archive auditing logs can also be sorted by clicking on the column headers.

contentACCESS Central Administration

System	File Archive	Email Archive	BackMailz	SharePoint Archive	GDPR	Custom plugins
Save Discard changes	Roles Users Invitations Login providers	System Licensing Notifications Cluster Statistics Legal hold Task runner Indexing SMTP Servers SMTP Mappings	System logs Configuration auditing Archive auditing	Tenants All databases	contentWEB officeGATE contentACCESS Virtual drive configuration application	Applications settings
Edit	Security	Services	Logs and auditing	Tenants	Client Applications	

Archive auditing
System > Logs and auditing > Archive auditing

Filteration

Users: (All users) Start Date: End Date: Event types: (All events) Export Settings

Events: User = All users

Date	Title	Description	User
1/29/2020 3:08:32 PM	Item was viewed	The next generation of email archiving is here!	Administrator
1/29/2020 3:08:21 PM	User performed search	The user system has searched for the term:	Administrator
1/29/2020 3:08:05 PM	Item was viewed	The next generation of email archiving is here!	Administrator
1/29/2020 3:07:56 PM	User performed search	The user system has searched for the term:	Administrator
1/29/2020 3:06:14 PM	Item was viewed	The next generation of email archiving is here!	Administrator
1/29/2020 3:06:02 PM	User performed search	The user system has searched for the term:	Administrator
1/29/2020 3:05:20 PM	Item was viewed	TECH-ARROW at Cloud Expo Europe	Administrator
1/29/2020 3:05:15 PM	Item was viewed	The next generation of email archiving is here!	Administrator
1/29/2020 3:05:02 PM	User performed search	The user system has searched for the term:	Administrator
1/29/2020 3:04:36 PM	Item was viewed	The next generation of email archiving is here!	Administrator
1/29/2020 3:04:23 PM	User performed search	The user system has searched for the term:	Administrator
1/29/2020 3:03:45 PM	Item was downloaded	1491684_881391335220066_778840978841172619_v.jpg	Administrator

Page 1 of 106 (3163 items)



Column description

The columns contain the following information:

- **Date:** The exact date when the logged event happened
- **Title:** The title of the event
- **Description:** A short description of the event
- **User:** The user, who has done the action, which was logged into the Archive auditing. There are 2 special users - System and Anonymous. An Auditing event has the System user when a document is accessed by a job. The Anonymous user is used when the „Link security” option is disabled in the [System settings](#) and a document is downloaded from an external source (for example with an URL).

Auditing log details

By clicking on the arrow icon left of the auditing entry, a detailed view will appear where the user can see more data about the action that caused the event.

The screenshot shows the 'Archive auditing' interface. At the top, there's a navigation bar with various system management icons. Below it, a breadcrumb trail reads 'System > Logs and auditing > Archive auditing'. A filter section allows users to filter by 'Users' (set to 'All users'), 'Start Date', 'End Date', and 'Event types' (set to 'All events'). Below the filters is a table of events. One event is selected, and its details are shown in a sidebar on the left. The details include:

- Model type:** EmailArchive
- Model Id:** Merged1[EmailArchive]0
- Entity name:** dne@ta.internal
- Entity Id:** 9|a39ad7c2-3957-47b8-8cd6-d91f8a0b6b44
- Folder Id:** 3
- Download link:** [The next generation of email archiving is here!.msg](#)
- Open in contentWEB:** [The next generation of email archiving is here!.msg](#)
- IP address:** 192.168.190.96

If the item was viewed, there will be a **Download link** and an **Open in contentWEB** option. If the item was downloaded, there will be only the **Download link**.

	1/29/2020 3:08:05 PM	Item was viewed	The next generation of email archiving is here!
--	----------------------	-----------------	---

Model type:	EmailArchive
Model Id:	Merged1[EmailArchive]0
Entity name:	dne@ta.internal
Entity Id:	9 a39ad7c2-3957-47b8-8cd6-d91f8a0b6b44
Folder Id:	3
Download link:	The next generation of email archiving is here!.msg
Open in contentWEB:	The next generation of email archiving is here!.msg
IP address:	192.168.190.96

Distributed environment in contentACCESS — Clusters

Why is it efficient to use clusters? A server cluster is a group of independent servers (nodes) working together as a single system to provide high availability of services for clients. When a failure occurs on one computer in a cluster, resources are redirected and the workload is redistributed to another computer (node) in the cluster. It can happen that one processing job is currently running on a processing node, but a server failure occurs and the server will shut down. In this case a second, alternative node (either with “Job runner” or “Universal” role) can pick the task up to finish the archiving process. To achieve this, the running of this particular job should be allowed on any available node.

contentACCESS’s cluster technology guard against the following types of failure:

- ✓ **System and hardware failures**, which affect hardware components such as CPUs, drives, memory, network adapters, and power supplies.
- ✓ **contentACCESS’s application and service failures**, which affect the software, its applications and essential services.

Thanks to clustering in contentACCESS, the user can make the job processes scalable, and thus increase the performance. The user may decide how the nodes should be used, and how the work processes should be divided between them. The jobs can be run on a specific or any available node. It is also possible to install the full contentACCESS on one node and the contentACCESS server part on another nodes to ensure a better performance for job processing and for contentACCESS as a whole. It is also possible to use the nodes in a balanced mode; in this case the nodes are selected according to their Memory and CPU usage. The actually running jobs on the node will be considered as well.

There are 3 main node roles available in contentACCESS (can be adjusted from the context menu of the particular node).

- ✓ **Universal**: this type can be used for all operations performed in contentACCESS;
- ✓ **Model provider (retriever)** type can be used to publish models, i.e. this type is used to connect client applications with contentACCESS and to retrieve items through these client applications;
- ✓ **Job runner (processing)** type was developed to run jobs (plugin instances) in contentACCESS.



The user must decide, which role type he assigns to a particular node, how he divides work processes between the nodes, and how he makes the work processes more effective. A typical use case is when a customer installs the contentACCESS server, Central Administration and contentWEB on one node and contentACCESS server on a second node. Then he sets the first node to “Universal”, the second to “Job runner”, assigns File system archive jobs to the first node and the Email archive jobs to the second node.

Now, let’s assume that contentACCESS is already installed on the first “main” node (TANEWS), where the file system archive jobs are running. Our customer has decided to buy TECH-ARROWS’s Email archive and he would like to run email archive jobs on a second node. To achieve this, he needs to install the contentACCESS server on a second node (e.g. TECHNB0002).

Before the user starts to install any contentACCESS component on a second node, it is always recommended to set the node to disabled (to prevent the new node from picking up new tasks before it is fully configured). We set now the default role type to “Job processing”, as we will use it to run the email archive jobs. For more information about these default cluster settings please refer to section [System](#), section “Cluster settings”.

Cluster settings	
Node update interval (sec):	30
Node auto logoff time (sec):	120
Events retention time (sec):	1800
Events distribution interval (sec):	60
Task auto disable time (sec):	30
Stop task after ping failures (count):	2
Node selection strategy:	First wins
Default node role:	Job runner (processing)
Enabled by default:	<input type="checkbox"/>

To install any contentACCESS component on a second node, start to run the contentACCESS setup package on the selected server (TECHNB0002). First, you will be required to select the installation type. As we are now installing a contentACCESS component (a node) in an existing contentACCESS environment, we select the “Additional component” option:



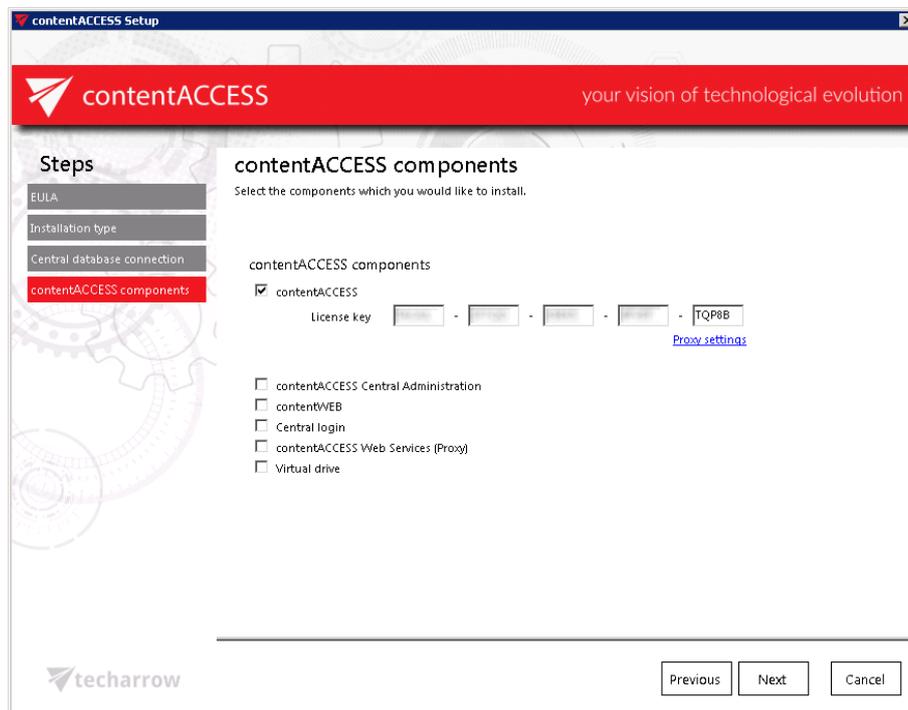
The screenshot shows the 'contentACCESS Setup' window. The title bar reads 'contentACCESS Setup'. Below the title bar is a red header with the 'contentACCESS' logo and the tagline 'your vision of technological evolution'. On the left, a 'Steps' sidebar lists 'EULA', 'Installation type', and 'Central database connection'. The 'Installation type' step is currently selected. The main area is titled 'Installation type' and contains the following text: 'Choose the contentACCESS installation type.' Below this are two radio button options: 'First server' (unselected) and 'Additional server or component' (selected). The 'Additional server or component' option has a sub-description: 'Choose this option if you are installing an additional server or component in an existing contentACCESS installation or cluster.' At the bottom right, there are three buttons: 'Previous', 'Next', and 'Cancel'. The 'techarrow' logo is in the bottom left corner.

In the next step you will be asked to specify the central database connection that is already used. Enter the server name, where the database is already installed (in our case it is installed on our 1st node called “TANEWS”), enter the name of the already existing system database (in this case it is “CONTENTACCESSDB”; can be checked on the SQL server), type here the database user credentials and the database schema.

The screenshot shows the 'contentACCESS Setup' window at the 'Central database connection' step. The title bar reads 'contentACCESS Setup'. Below the title bar is a red header with the 'contentACCESS' logo and the tagline 'your vision of technological evolution'. On the left, a 'Steps' sidebar lists 'EULA', 'Installation type', and 'Central database connection'. The 'Central database connection' step is currently selected. The main area is titled 'Central database connection' and contains the following text: 'Please specify the contentACCESS central database connection parameters. This is the database you've specified when installing the first server.' Below this are several input fields: 'Database server' (containing 'TANEWS\SQLEXPRESS'), 'Database name' (containing 'CONTENTACCESSDB'), 'User name' (containing 'sa'), 'Password' (masked with asterisks), and 'Schema' (containing 'dbo'). There is a checkbox for 'Use Windows integrated authentication (TA\administrator)' which is unchecked. A red 'Test' button is located at the bottom right of the input fields. At the bottom of the window, there are three buttons: 'Previous', 'Next', and 'Cancel'. The 'techarrow' logo is in the bottom left corner.

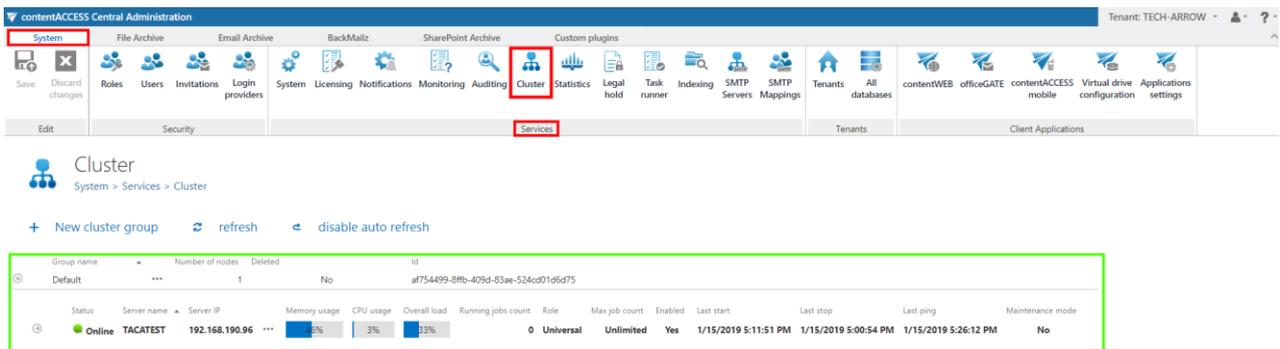
Important!!! In the Database connection settings either a domain user must be specified (if Windows authentication is used), or an SQL user's credentials must be added to connect to the database.

Further you need to select the components to be installed. As mentioned above, in this use case we select the contentACCESS server to install on this second node:



Finish the installation process of this second node. Now, let's check the available nodes in the Central Administration.

Status pane of nodes, grid of nodes, available operation from the nodes' context menu: Nodes, where contentACCESS components are installed, can be viewed with navigating to **System** tab → **Services** → **Cluster**, in the nodes' grid below the status bar (displayed with **green** color on the below displayed screenshot).



Screenshot: Nodes' grid

There are 3 control buttons available in the status pane of the available nodes:

- ✓ “+ New cluster group” button allows the administrator to create new cluster groups;
- ✓ “refresh” button serves to reload the last cluster status from the database;
- ✓ “disable auto refresh”/“enable auto refresh” buttons serve to disable/enable auto refresh (in every 5 seconds) of the last state from the database.

After clicking on the + **New cluster group**, a pop-up window will open. Here the administrator can specify the name of the group and also description (not necessary). Click **OK**.

Change cluster group ✕

Group name:

Description:



Nodes can be added to the cluster group using the **Manage nodes** option from the context menu.

+ New cluster group
refresh

Group name	Number of nodes	Delete
<div style="display: flex; align-items: center;"> ⌵ ✓ Default ⋮ </div>	1	
<div style="display: flex; align-items: center;"> ⌵ ● Online TACA <div style="border: 1px solid red; padding: 2px;">Manage nodes</div> </div>	0.96	⋮

Select nodes for cluster group ✕

Drag a column header here to group by that column

<input checked="" type="checkbox"/>	Name	IP address
<input type="checkbox"/>		
<input checked="" type="checkbox"/>	TACATEST	192.168.190.96

Reset job to 'Any available' if the job is assigned to one of the removed nodes

OK
Cancel



The cluster group can be then assigned to tenants, where the tenant's jobs will run only on the nodes assigned to the tenant's cluster group. This feature is useful for hosting solutions, where contentACCESS nodes are located in multiple data centers. In such cases, the tenant's data will be processed by the nodes, which are geographically the closest to the tenant's resources.

The node, where contentACCESS Central Administration is installed, is marked with a bold black color.

Status	Server name	Server IP	Memory usage	CPU usage	Overall load	Running jobs count	Role	Max job count	Enabled	Last start	Last stop	Last ping
Online	TANEWS	192.168.190.63	1%	1%	0.67%	0	Universal	Unlimited	Yes	9/17/2015 10:20:20 AM	Never	9/17/2015 1:45:14 PM
Online	TECHNB0002	192.168.30.1	0%	0%	20.33%	0	Job runner (processing)	Unlimited	No	9/17/2015 1:45:08 PM	9/17/2015 1:33:56 PM	9/17/2015 1:45:08 PM

How can a node be configured? Node configurations are available for the user from the node's context menu, by clicking on "Edit" in the dropdown list and configuring it in the "Change node" dialog.

The screenshot shows the 'Cluster' management page. At the top, there is a breadcrumb 'System > Services > Cluster' and a tree icon. Below this are buttons for '+ New cluster group', 'refresh', and 'disable auto refresh'. A table lists cluster groups, with 'Default' having 1 node. Below the cluster groups is a table of nodes. The 'TACATEST' node (IP: 192.168.190.96) is highlighted, and its context menu is open, showing options: 'Edit', 'Delete', 'Shutdown', 'Set to maintenance', and 'Reset maintenance'. The 'Edit' option is highlighted with a red box.

Change node ✕

Enabled:

Role: Universal

Max job count: -1 Unlimited

Description:

Capabilities:

Maintenance mode:

OK
Cancel

In this dialog it is possible to set up the following node configurations:

- ✓ Enable/disable a node with checking/unchecking the **Enable** checkbox;
- ✓ Change the role assignment of the selected node with selecting the role type from the **Role** dropdown list;
- ✓ Set the maximum count of jobs that can parallel run on the node (option **Max. job count**)
- ✓ Set the mode to **Maintenance** by checking the **Maintenance mode** checkbox.

The following information are available in the nodes' grid, when reading from left to right:

Status: This column marks if the selected node is online or offline, i.e. if it is ready to process tasks or not.

Status	Server name	Server IP	Memory usage	CPU usage	Overall load	Running jobs count	Role	Max job count	Enabled	Last start	Last stop	Last ping
Online	TANEWS	192.168.190.63	39%	1%	30%	0	Universal	Unlimited	Yes	9/17/2015 10:20:20 AM	Never	9/17/2015 3:36:55 PM
Online	TECHNB0002	192.168.30.1	62%	36%	433%	0	Job runner (processing)	Unlimited	No	9/17/2015 2:36:13 PM	9/17/2015 2:31:35 PM	9/17/2015 3:36:49 PM

The node can have one of these 3 statuses:

- ✓ The green (●) spot means, that the node is enabled, i.e. its service is running and the node is ready for processing;
- ✓ The yellow (●) spot means, that the node is disabled, i.e. its service is stopped and the user cannot run any plugin on it. However, the server is still running. The yellow spot appears also for **Maintenance mode**.



- ✓ The red spot (●) means that the contentACCESS server on the selected node is currently turned off. A node in offline status can be started again with starting up its service (“GATE.contentACCESS” windows service must be started).

Our TECHN0002 node was installed in disabled mode, which is indicated with a yellow spot in the status column:

Status	Server name	Server IP	Memory usage	CPU usage	Overall load	Running jobs count	Role	Max job count	Enabled	Last start	Last stop	Last ping
Online	TANEWS	192.168.190.63	31%	1%	7.33%	0	Universal	Unlimited	Yes	9/17/2015 10:20:20 AM	Never	9/17/2015 11:17:40 AM
Online	TECHNB0002	192.168.30.1	78%	12%	7.33%	0	Job runner (processing)	Unlimited	No	9/17/2015 10:20:37 AM	Never	9/17/2015 11:17:45 AM

A node can be enabled/disabled with opening the node’s context menu, clicking on “Edit” and checking/unchecking the “Enabled” checkbox in the “Change node” dialog:

Server name: The server name, where the contentACCESS node is installed, is displayed here. Our first node is installed on server “TANEWS”, and the second node installed on “TECHNB0002”.

Status	Server name	Server IP	Memory usage	CPU usage	Overall load	Running jobs count	Role	Max job count	Enabled	Last start	Last stop	Last ping
Online	TANEWS	192.168.190.63	39%	1%	30%	0	Universal	Unlimited	Yes	9/17/2015 10:20:20 AM	Never	9/17/2015 3:36:55 PM
Online	TECHNB0002	192.168.30.1	82%	36%	49.33%	0	Job runner (processing)	Unlimited	No	9/17/2015 2:36:13 PM	9/17/2015 2:31:35 PM	9/17/2015 3:36:49 PM

Server IP: The IP of the server, where the node is installed, is displayed here.

Status	Server name	Server IP	Memory usage	CPU usage	Overall load	Running jobs count	Role	Max job count	Enabled	Last start	Last stop	Last ping
Online	TANEWS	192.168.190.63	39%	1%	30%	0	Universal	Unlimited	Yes	9/17/2015 10:20:20 AM	Never	9/17/2015 3:36:55 PM
Online	TECHNB0002	192.168.30.1	82%	36%	49.33%	0	Job runner (processing)	Unlimited	No	9/17/2015 2:36:13 PM	9/17/2015 2:31:35 PM	9/17/2015 3:36:49 PM



Memory usage, CPU usage, Overall load: Displays actual information about the load balance of the selected node. If the cluster selection strategy is set to “Balanced”, then the nodes will be selected for the tasks and they should perform according to these values. If the node is in offline status, the value will be “0”. If the value is more than 70%, then the value will get a red background color.

Status	Server name	Server IP	Memory usage	CPU usage	Overall load	Running jobs count	Role	Max job count	Enabled	Last start	Last stop	Last ping
Online	TANEWS	192.168.190.63	38%	1%	30%	0	Universal	Unlimited	Yes	9/17/2015 10:20:20 AM	Never	9/17/2015 3:36:55 PM
Online	TECHNB0002	192.168.30.1	62%	36%	49.33%	0	Job runner (processing)	Unlimited	No	9/17/2015 2:36:13 PM	9/17/2015 2:31:35 PM	9/17/2015 3:36:49 PM

Running job count: Informs the user about the currently running job count on a specific node. On the screenshot below we can see that two file system archive jobs are running on node “TANEWS”. The user may open the details of these 2 job runs by clicking on the arrow sign at the left side of the row:

Status	Server name	Server IP	Memory usage	CPU usage	Overall load	Running jobs count	Role	Max job count	Enabled	Last start	Last stop	Last ping																					
Online	TANEWS	192.168.190.63	40%	2%	10.67%	2	Universal	Unlimited	Yes	9/17/2015 10:20:20 AM	Never	9/17/2015 12:42:43 PM																					
<table border="1"> <thead> <tr> <th>ID</th> <th>Tenant</th> <th>Display Name</th> <th>Status</th> <th>Last Duration</th> <th>Progress</th> <th>Summary</th> </tr> </thead> <tbody> <tr> <td>72</td> <td>TECH-ARROW</td> <td>File archive job</td> <td>Running</td> <td>7 seconds</td> <td>0%</td> <td>0 folders processed 28 documents processed (7 versions created, 21 newly archived)</td> </tr> <tr> <td>139</td> <td>TECH-ARROW</td> <td>File archive with DELETE method</td> <td>Running</td> <td>6 seconds</td> <td>0%</td> <td>0 folders processed 21 documents processed (21 newly archived)</td> </tr> </tbody> </table>													ID	Tenant	Display Name	Status	Last Duration	Progress	Summary	72	TECH-ARROW	File archive job	Running	7 seconds	0%	0 folders processed 28 documents processed (7 versions created, 21 newly archived)	139	TECH-ARROW	File archive with DELETE method	Running	6 seconds	0%	0 folders processed 21 documents processed (21 newly archived)
ID	Tenant	Display Name	Status	Last Duration	Progress	Summary																											
72	TECH-ARROW	File archive job	Running	7 seconds	0%	0 folders processed 28 documents processed (7 versions created, 21 newly archived)																											
139	TECH-ARROW	File archive with DELETE method	Running	6 seconds	0%	0 folders processed 21 documents processed (21 newly archived)																											
Online	TECHNB0002	192.168.30.1	50%	24%	4%	2	Job runner (processing)	Unlimited	No	9/17/2015 10:20:37 AM	Never	9/17/2015 12:42:59 PM																					

Role: A node can be either universal, job runner or model provider; the role type of the particular node can be viewed here. As we can see, our “TANEWS” node has “Universal” role assigned and “TECHNB000” has “Job runner” role assigned.

Status	Server name	Server IP	Memory usage	CPU usage	Overall load	Running jobs count	Role	Max job count	Enabled	Last start	Last stop	Last ping
Online	TANEWS	192.168.190.63	38%	1%	30%	0	Universal	Unlimited	Yes	9/17/2015 10:20:20 AM	Never	9/17/2015 3:36:55 PM
Online	TECHNB0002	192.168.30.1	62%	36%	49.33%	0	Job runner (processing)	Unlimited	No	9/17/2015 2:36:13 PM	9/17/2015 2:31:35 PM	9/17/2015 3:36:49 PM

The assigned roles can be edited by clicking on “Edit” in the node’s context menu and setting the desired node in the “Change node” dialog.

The screenshot shows a table with columns: Group name, Number of nodes, Deleted. A row for 'Default' group has 1 node and is not deleted. Below the table, a context menu is open for node 'TACATEST' (192.168.190.96) with 'Edit' highlighted. An arrow points from 'Edit' to a 'Change node' dialog box. In the dialog, 'Enabled' is checked, 'Role' is set to 'Job runner (processing)', 'Max job count' is 'Unlimited', 'Description' is 'Job runner (processing)', and 'Capabilities' is 'Universal'. 'Maintenance mode' is unchecked. 'OK' and 'Cancel' buttons are at the bottom.

If we are planning to use a node for multiple tasks in the future, we can modify its role to “Universal”.



Max. job count: The maximum count of jobs, that can run in parallel on a node, can be viewed right here. The number of jobs that can run on a node can be limited. In case of our nodes this job count is unlimited.

Status	Server name	Server IP	Memory usage	CPU usage	Overall load	Running jobs count	Role	Max job count	Enabled	Last start	Last stop	Last ping
Online	TANEWS	192.168.190.63	39%	1%	30%	0	Universal	Unlimited	Yes	9/17/2015 10:20:20 AM	Never	9/17/2015 3:36:55 PM
Online	TECHNB0002	192.168.30.1	52%	36%	49/33%	0	Job runner (processing)	Unlimited	No	9/17/2015 2:36:13 PM	9/17/2015 2:31:35 PM	9/17/2015 3:36:49 PM

This value can be adjusted by opening the “Change node” dialog from the node’s context menu. Click on “Edit” in the node’s context menu, and set the desired value in the dialog. Now we set this value to “10”:

Change node

Enabled:

Role: Universal

Max job count: 10 Unlimited

Description:

Capabilities:

Maintenance mode:

OK
Cancel

If 10 jobs are running in parallel on this node and we want to start up a new (11th) job on this node, the job will be in waiting status until the processing node is available again.

139	File archive with DELETE method	File system archive	Waiting	2 hours ago	12 seconds	-	Waiting for 1 second	-	Yes	TANEWS[192.168.190.63]
-----	---------------------------------	---------------------	---------	-------------	------------	---	----------------------	---	-----	------------------------

If our 11th job can run on any available node, then another node will pick it up for processing. The node, where the job should run, depends on the job settings. For more information check section [“Jobs’ page, jobs’ context menu”](#).

Enabled: A node can either be enabled (it is online, and its service is currently running) or disabled. A node is disabled when it is running, but it is unavailable for further processing tasks. By default, the nodes are in enabled state, but it is recommended to set them here as disabled in case of planned system updates, or if any failure occurred and the problem must be fixed.

Status	Server name	Server IP	Memory usage	CPU usage	Overall load	Running jobs count	Role	Max job count	Enabled	Last start	Last stop	Last ping
Online	TANEWS	192.168.190.63	39%	1%	30%	0	Universal	Unlimited	Yes	9/17/2015 10:20:20 AM	Never	9/17/2015 3:36:55 PM
Online	TECHNB0002	192.168.30.1	52%	36%	49/33%	0	Job runner (processing)	Unlimited	No	9/17/2015 2:36:13 PM	9/17/2015 2:31:35 PM	9/17/2015 3:36:49 PM

To enable/disable nodes - open the “Change node” dialog by clicking on “Edit” in the node’s context menu, and check/uncheck the “Enabled” checkbox in the dialog.

Change node ✕

Enabled:

Role: Universal

Max job count: 10 Unlimited

Description:

Capabilities:

Maintenance mode:

OK
Cancel

The times of **Last start/Last stop** and **Last ping** are available in the right part of the grid.

Group name	Number of nodes	Deleted	Id	
Default	***	1	No	af754499-8ffb-409d-83ae-524cd01d6d75

Status	Server name	Server IP	Memory usage	CPU usage	Overall load	Running jobs count	Role	Max job count	Enabled	Last start	Last stop	Last ping	Maintenance mode
Online	TACATEST	192.168.190.96	37%	3%	30%	0	Universal	Unlimited	Yes	1/25/2019 4:55:11 PM	1/15/2019 5:00:54 PM	1/25/2019 5:47:07 PM	No

Maintenance mode: This column shows if the selected node is in **Maintenance mode**. When a node is in **Maintenance mode**, no new jobs can be started on it, but the running jobs continue to run.

Once the running jobs are finished, the administrator can do a maintenance on the node:

- update
- patch
- restart
- or other necessary actions.

The node in maintenance can serve the clients further. Once the maintenance is finished, the **Maintenance mode** should be reset (i.e. back to normal).

The node can be put to/out of **Maintenance mode** by two ways:

1. Context menu -> Edit -> check the Maintenance mode checkbox
2. Context menu -> Set to maintenance/Reset maintenance



Group name	Number of nodes	Deleted	Id	
Default	***	1	No	af754499-8ffb-409d-83ae-524cd01d6d75

Status	Server name	Server IP	Memory usage	CPU usage	Overall load	Running jobs count	Role	Max job count	Enabled	Last start	Last stop	Last ping	Maintenance mode
Online	TACATEST	192.168.190.96	36%	3%	9.67%	0	Universal	Unlimited	Yes	1/25/2019 4:55:11 PM	1/15/2019 5:00:54 PM	1/25/2019 5:37:17 PM	No

How to assign a job to the selected node? Now we will assign an Email archive job to the “TECHNB0002” node. We navigate to the **Email Archive** tab → **Archive** → **Jobs** on the ribbon, and open the Jobs’ page. Here we click on **+ new** to create an email archive job, which will be assigned to this node.

contentACCESS Central Administration

System | File Archive | **Email Archive** | BackMailz | SharePoint Archive | Custom plugins

Save | Discard changes | Databases | System settings | Provisioning settings | Retentions | Shortcut configuration | Storages | Schedules | User experience | View address book | Jobs | Remote agents | PST import | Legacy data configuration

Jobs
Email Archive > Archive > Jobs

+ new | refresh | disable auto refresh | manage access | Show all jobs

The “Add new job instance” dialog will open. Here we set up the desired job, and select “TECHNB0002” from the “Run on node” dropdown list. Then we click on “Add”.

Add new job instance ✕

Available jobs:

Run on node:

Display name:

Description:

We need to configure the newly added job on its job configuration page. For more information about how to configure processing jobs, please refer to the respective sections.

Now we can enable the TECHNB0002 node.



Status	Server name	Server IP	Memory usage
Online	TANEWS	192.168.190.63	39%
Online	TECHNB0002	192.168.30.1	62%

Change node

Enabled:

Role: Universal

Max job count: -1 Unlimited

Description:

Capabilities:

Maintenance mode:

OK Cancel

The node will start to run the assigned job at the time, which is configured in the job's scheduler settings.

Important!!! When configuring a job that may run in a cluster, the system the administrator must specify a **storage and a database that is accessible by all the nodes** in the cluster. If a node, which picks up the job, can't access the configured storage or database, the job will fail and will not execute the task:

- In the **database repository settings** of the database (selected for the job) the administrator must **establish the connection with SQL user credentials**. If an explicit user is not specified, the contentACCESS service user will be used and the service must run under the same domain user. This ensures that the database can be accessed by the job, regardless of where it is running.
- The administrator must **specify the storage as a network share** (e.g. `\\ServerName\RootFolder\Subfolder`) in the **storage repository settings** of the storage (specified for the job), so it can be later accessible by the job from anywhere.

How to shut down a node? In certain cases it might happen that a node should be turned off. This operation can be done from the context menu of the selected node. Click on the ellipses (...) and select "Shutdown" option from the dropdown list. With this action the contentACCESS service on the selected node will be turned off, and the node will get a red color (offline). Node shutdown is a deferred action and it might take 1 minute.

Status	Server name	Server IP	Memory usage	CPU usage	Overall load	Running jobs count	Role	Max job count	Enabled	Last start	Last stop	Last ping	Maintenance mode
Online	TACATEST	192.168.190.96	39%	1%	30%	0	Universal	Unlimited	Yes	1/22/2019 1:44:06 PM	1/15/2019 5:00:54 PM	1/23/2019 5:27:27 PM	No

Edit

Delete

Shutdown

Set to maintenance

Reset maintenance

If you are quite sure that you want to shut down the node, answer "OK" for the following pop-up window:



tacatest:3333 says

Are you sure to shut down the node?



Note: If you are about to turn off the node where Central Administration is running, a next pop-up window will warn you about this again.

tacatest:3333 says

Are you sure to shut down the node to which the central admin is connected?

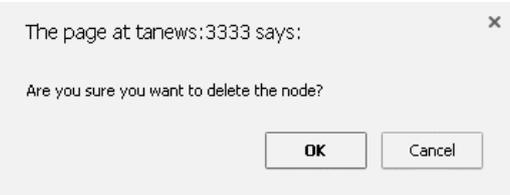


How can a node be deleted? With this action the user may delete a node from the node list. Only nodes with offline status can be deleted. When the contentACCESS service is started up again, the node will appear on the list. To delete it, click on it, open its context menu by clicking on the ellipses (...), then select “Delete”.

Status	Server name	Server IP	Memory usage	CPU usage	Overall load	Running jobs count	Role	Max job count	Enabled	Last start	Last stop	Last ping	Maintenance mode
Online	TACATEST	192.168.190.96	40%	3%	31%	0	Universal	Unlimited	Yes	1/22/2019 1:44:06 PM	1/15/2019 5:00:54 PM	1/23/2019 6:18:40 PM	No

- Edit
- Delete
- Shutdown
- Set to maintenance
- Reset maintenance

contentACCESS will ask the user again, if he is sure about deleting the node.



Statistics

The telemetry service of contentACCESS permanently collects data from the

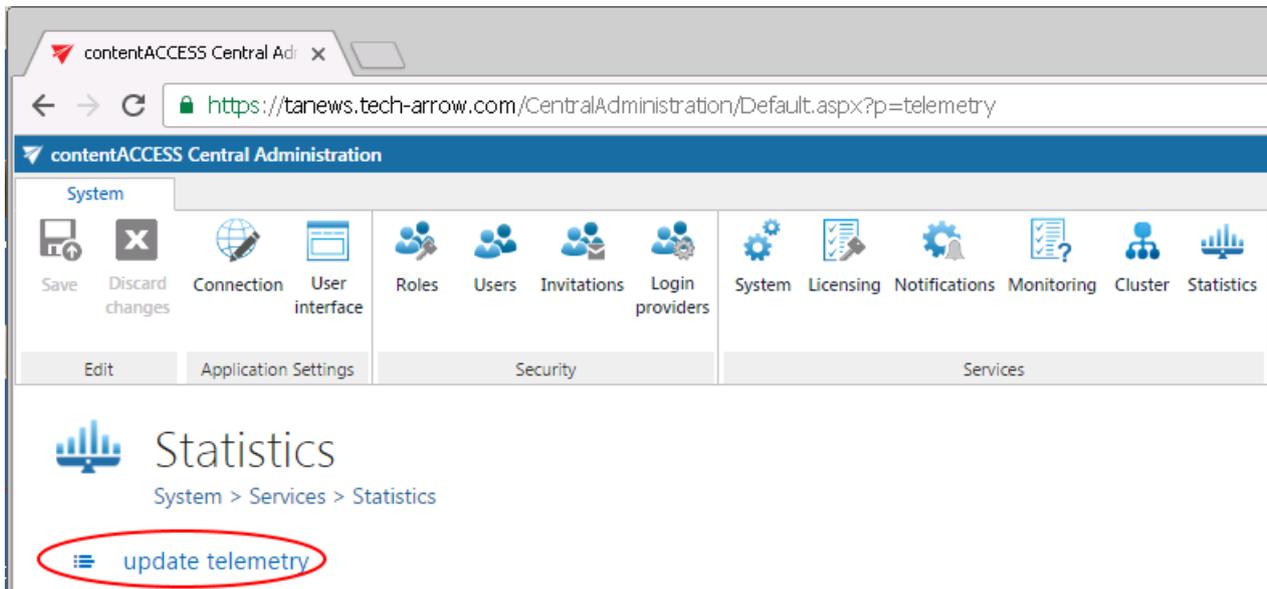
- a) contentACCESS system as a whole
- b) Email archive jobs
- c) File archive jobs



- d) GDPR for Applications job
- e) GDPR for Exchange job
- f) GDPR for File system job
- g) SharePoint archive jobs
- h) Teams archive jobs

and makes a record of the collected data. The data changes are summarized into telemetry graphs. These graphs give a simple and quick overview about the actual data usage during the last 10 days. The graphs can be viewed on the **Statistics** page, which is reachable by navigating to **System** → **Services** → **Statistics** on the ribbon. The values displayed on this page are permanently updated by the telemetry job, which runs and collects the necessary data every night between 1 AM to 2 AM. If you want to see the actual data usage immediately, you can run the **telemetry updater**, which will actualize it for you immediately.

The telemetry job's configuration page can be opened by clicking on the "update telemetry" option. Only a user with manage tenant permissions has access to the telemetry job. By clicking the option, the telemetry job is automatically triggered, too.



A new scheduler may be created and resource settings may be changed for the telemetry job on this page. The job can be started/stopped or activated/deactivated from the same page's status bar, too.



start immediately
 refresh
 disable auto refresh
 deactivate job
 logs
 edit
 ↑

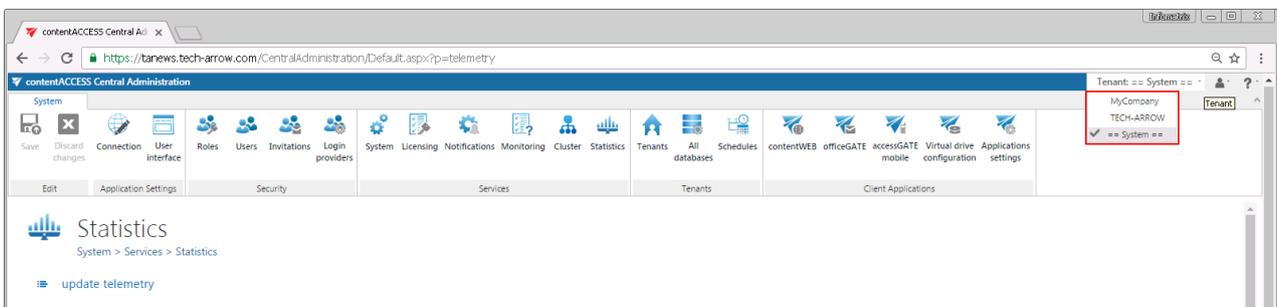
Status: **Idle**
 Progress: 9 Plugins updated (completed 34 seconds ago)

Scheduling settings
 Scheduled in:

Resource settings
 Worker thread count:

The telemetry information may be checked to the

- **system** as a whole– if the system tenant is selected
- **given tenant** – if the given tenant is selected in the upper right menu:

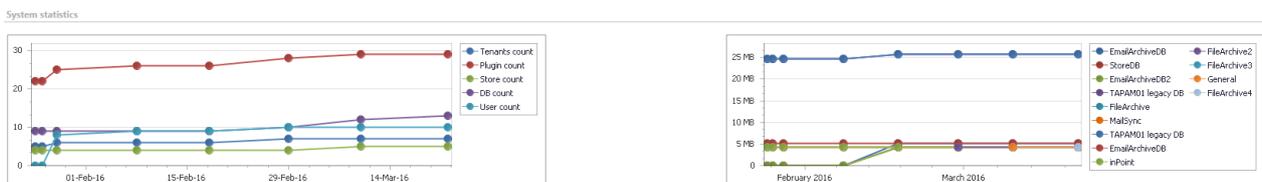


The given page is divided into 8 sections and contains 9 graphs. Any growth or reduction in the count of tenants, archived items, databases, root folders, mailboxes etc. can be checked here using the respective graphs.

System statistics

The **1st chart** displays the actual count of tenants (blue line), plugins (red line), stores (green line), databases (purple line) and users (light blue line) depending on the selected day. Move with your cursor over the grid to view the exact values in the given time period.

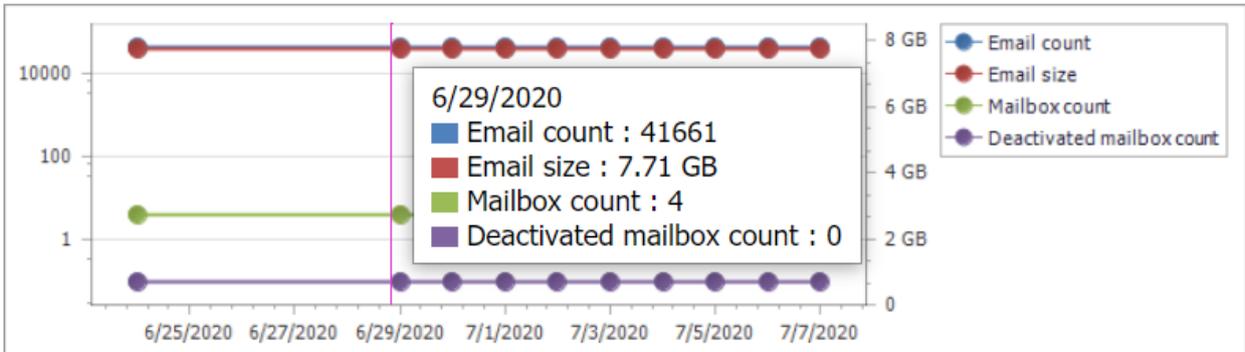
The **2nd chart** displays the size of the configured databases. Each database is marked with a different color.





The actual information is displayed when you move the cursor over a given date in the chart.

Email archive statistics

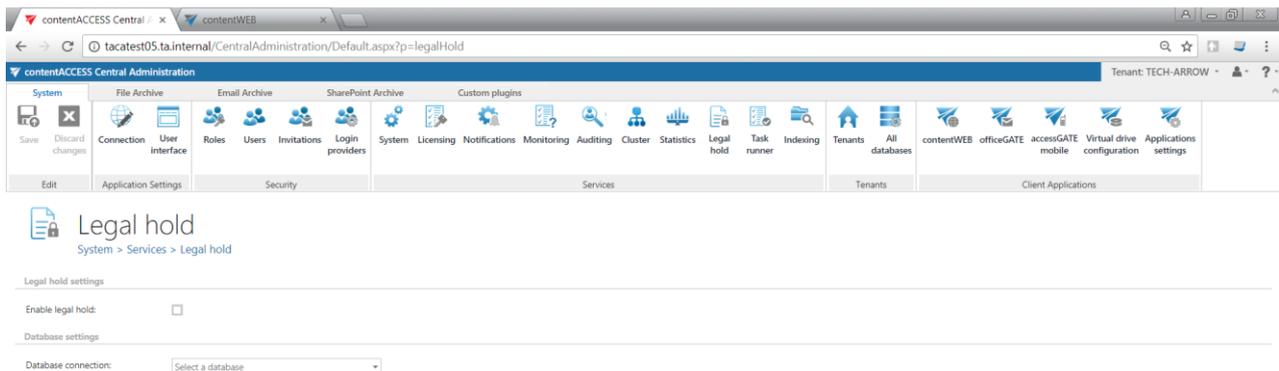


Legal hold

The legal hold feature allows to create a legal hold case, where the user can put documents afterwards. Documents which are under a legal hold case can't be deleted from the system until the legal hold case expires. Legal hold has the same functionality in File, Email and also SharePoint archive.

Configuration

From the configuration side, the Legal hold management is asynchronous, all the operations regarding the Legal hold are asynchronous and are managed by the Task runner (**System -> Task runner**). The Legal hold feature can be activated and configured per tenant.



The following settings are available:

✓ **Legal hold**

The Legal hold must be enabled here if the user wants to use it. If this option is checked, the **Task runner** will process also **create/update legal hold cases** tasks from contentWEB.

✓ Database

For database settings select an already configured connection from the dropdown list, where the Legal hold metadata will be stored. (For further information about how to set database connections please refer to section [Databases](#).)

Legal hold needs an additional storage, where all the exported files will be stored. It should be set in central administration under “System”. Here the UNC path can be provided, where all the exported files will be stored by Legal hold plugin.

System		File Archive		Email Archive		SharePoint Archive		Custom plugins				
												
Save	Discard changes	Connection	User interface	Roles	Users	Invitations	Login providers	System	Licensing	Notifications	Monitoring	Auditing
Edit	Application Settings		Security				Services					

Resource storage settings

Storage path:

Use explicit credentials:

User name:

Password:

Confirm password:

User experience

To see how Legal hold can be used, please read [this](#) section.

Task runner

The Task runner plugin is processing server tasks created from [contentWEB](#), for example:

- Export to Zip
- Export to PST
- Recovery
- Mark/unmark for/from delete
- [Legal hold](#)



During the installation of contentACCESS, Task runner plugin is automatically deployed for all tenants. It uses tenant database to store the tasks, so the tenant must have a tenant database configured.

Tenant name	Tenant database	Search server url
✓ David	DavidDB	
INDEX TEST2	EAdbMNE02	
MNETEST	MNEtestDB	
TECH-ARROW	EAdbMNE01	
Test tenant	MNEdatabase	

In System -> Services -> System, the user must set the Resource storage.

System
System > Services > System

General settings

Is system configured:

Plugins directory: C:\Program Files\TECH-ARROW\contentACCESS\coi

User search settings

Disable user searching:

Resource storage settings

Storage path: C:\LH_Storage

[Scheduler](#) for Task runner is set to 2 minutes as default, but it's possible to change it. The user can choose a previously configured schedule or create a new one.



contentACCESS Central Administration Tenant: TECH-ARROW

System | File Archive | Email Archive | SharePoint Archive | Custom plugins

Save | Discard changes | Connection | User interface | Roles | Users | Invitations | Login providers | System | Licensing | Notifications | Monitoring | Auditing | Cluster | Statistics | Legal hold | **Task runner** | Indexing | Tenants | All databases | contentWEB | officeGATE | accessGATE mobile | Virtual drive configuration | Applications settings

Edit | Application Settings | Security | Services | Tenants | Client Applications

Task runner

System > Services > Task runner

start immediately | refresh | disable auto refresh | deactivate job | logs | edit

Status: idle
Progress: 0 tasks under processing (completed 4 seconds ago)

Scheduling settings

Scheduled in:  

Notification settings: MANUAL

Send where: TaskRunnerScheduler

Recipient list: john.doe@example.com,peter.white@example.com

Resource settings

Worker thread count:

[Online help](#)



Indexing

The content indexing jobs

- assign the previously created index zones to files/emails of the selected entities
- use Elasticsearch as back end server (3rd party index server) to manage and store indexes and to perform search
- crawl the contentACCESS archive and send document text and metadata to Elasticsearch server

Note: Document text is extracted from various document formats through IFilter components. The appropriate IFilter pack should be installed on the server, where contentACCESS is also installed (filters are used to get plain text content from binary formats such as .doc, .pdf etc.).

On the configuration page of the given job the user is required to specify the following settings:

✓ Scheduling settings

In this step the running time(s) of the job must be selected. It is possible either to select a scheduler from the list or to create a new scheduler via **create new** ... option from the dropdown list. Using schedulers the administrator may automatize the running times of the given job. The mailboxes are periodically synchronized with the categories written into the queue in time intervals, which are set here. For more information how to set schedulers refer to section [Schedules](#) above.

✓ Resource settings

Set the values, which will determine how many items will be processed simultaneously by the job. The recommended value is "2".

✓ Filtering settings

Set here the file types that should and shouldn't be processed.

The file types can be added individually, but also grouping functionality is provided. The **composed filtering** allows the administrator/user to select a group of file extensions at once instead of selecting all required file types individually.



There are some extension groups predefined and ready to use:

- **Office Documents** – containing extensions docx, doc, pptx, ppt, sldx, xls, xlsx, pdf, one, accdb, pub, htm, html, csv, odt
- **All text documents** – containing extensions txt, log, config, rtf, zip, 7z, vcf, rar, msg, eml, ics, mhtml, mhtml

The composed filtering works both for the **White** and **Black listed file types**. Just click on the Select file types button on the Indexing page, and a pop-up window will appear with all groups and individual extensions. In this window, multiple file types and groups can be selected at once. The extensions can be selected in three ways:

- with the search bar, the user can search for the extensions individually or can search for the groups
- Note:** If the user tries to find – for example – “pdf” and the Office Documents group contains this extension, then Office Documents will come as a filtered result as well.
- the user can scroll down on the list
 - add manually to the Custom file types textbox

In the **right section of the Select file types window**, three text boxes are available:

- **Selected file types** – read-only textbox, the selected file types are listed here
- **Custom file types** – the user can add the extensions/file types manually here, which are not present on the list
 - the extensions can be added with commas and dots (for example .txt or txt,) or without commas and dots (for example txt)
 - the comma is required only if the user select multiple file types at the same time
- **Description** – those file types are listed here, which are part of the selected group



Scheduling settings

Scheduled in:

Resource settings

Worker thread count:

Filtering settings

White listed file types: Process ONLY the selected file types Select file types

Black listed file types: DO NOT process the selected file types Select file types

Entities to index

+ select

Process only selected file types

Select all for whitelist

Search here

- All text documents
- Office documents
- 3g2
- 3gp
- 3gp2
- 3gpp
- 7z
- AAC
- accda
- accdb
- accdc

Selected file types:

All text documents,

Custom file types:

pdf, docx

Description:

txt, log, config, rtf, zip, 7z, vcf, rar, msg, eml, ics, mhtml, mhtml

OK
Cancel

✓ **Entities to index**

Set here the entities that will be processed by the indexing job.

✓ **Index zone settings**

Set the index zone that will be assigned to items by the indexing job.

The screenshot shows the 'contentACCESS Central Administration' interface. The 'Indexing' icon in the top navigation bar is highlighted with a red box. Below it, the 'EA content indexing' configuration page is visible. The 'Indexing' icon in the top navigation bar is highlighted with a red box. The page shows various settings for the indexing job, including scheduling, resource, filtering, and entities to index. The 'Index zone settings' section is highlighted with a red box, showing the 'Index zone' set to 'Default index zone'. The 'Notification settings' section is also visible, showing 'Send when' set to 'Never' and 'Recipient list' set to 'john.doe@example.com,peter.white@example.com'.



Index zones

Index zones can be defined as a set of one or more Elasticsearch indexes, which are used for logical and physical separation of indexed documents. They were introduced to keep Elasticsearch indexes small, since smaller indexes are easier to move and distribute on multiple Elasticsearch servers.

Index zones can be assigned to entites directly or can be assigned and then overwritten by indexing jobs.

The **Maximum entities per group** column shows the amount of entities that will use the same indexes on Elasticsearch. The grouping is done automatically by the indexing job. By default, the maximum number of entities per group is 10. The recommended value for **File archive** is 2, for **Email archive** 10. If the limit is reached, then a new zone is opened and the rest of entities is included in it.

The screenshot shows the 'contentACCESS Central Administration' interface. The 'Indexing' section is active, displaying a table of indexing jobs. Below it, the 'Index zones' section is visible, showing a table with one entry: 'Default index zone' with a maximum of 10 entities per group and it is the default zone.

ID	Display Name	Type	Status	Last Start	Last Duration	Progress	Summary	Next Start	Is active	Cluster node	Running on
19	SPA indexing	Content indexing	Idle	1 year and 2 months ago (January 2018)	4 minutes	0 %	1 entities processed 12 items processed (4 failed)	Never	Yes	Any available	-
51	XYZ	Content indexing	Idle	1 year and 2 months ago (January 2018)	2 minutes	0 %	3 entities processed 28 items processed (1 failed)	Never	Yes	Any available	-
13	EA content indexing	Content indexing	Idle	10 months ago (June 2018)	1 minute	0 %	0 entities processed (1 failed) 0 items processed (1 failed)	Never	Yes	Any available	-
61	Indexing test	Content indexing	Idle	7 months ago (September 2018)	16 seconds	0 %	1 entities processed 10 items processed	Never	Yes	Any available	-
8	Content Indexing	Content indexing	Idle	9 months ago (July 2018)	18 seconds	0 %	3 entities processed 11 items processed	Never	Yes	Any available	-

Index zone name	Max entities per group	Is default
Default index zone	10	Yes

Index zone name and **Maximum entities per group** value can be changed by selecting **Edit** from the context menu of the index zone. Specify the desired name and value and then click on **Save**.

Index zone

Index zone name:

Maximum entities per group:



SMTP Servers

The SMTP (Simple Mail Transfer Protocol) server is a server used to process emails. The SMTP servers are tenant independent, all the SMTP servers are getting the same settings, therefore any of them can process incoming emails and archive them into contentACCESS.

The SMTP Servers page can be found under **System -> Services** section in Central Administration. The page consists of **4 sections**:

- SMTP servers
- SMTP domains
- Blacklisted domains
- SMTP mappings

SMTP servers

In this section a list of all the SMTP servers that have been registered in contentACCESS can be found. There are some basic info displayed about the servers. 2 different statuses are available - Online and Offline. In case an SMTP server didn't ping contentACCESS in the last 15 minutes, it is automatically treated as Offline. If the server is disabled, then it will not process any newly acquired emails, however, it will remain Online, because it is polling the contentACCESS to see whether the server has been re-enabled.

There are 2 different options available in the context menu - Edit (to edit some SMTP server related configuration) and Disable (to disable the selected SMTP server).

SMTP servers

Status	Display name	Server name	IP address	Is enabled	Server ID
Offline	✓ tacatest.ta.internal	*** tacatest.ta.internal	192.168.190.96	Yes	24C8CDA8-EA1C-4C8E-AF00-C2196CD706E8
		<div style="border: 1px solid #ccc; padding: 2px;"> Edit Disable </div>			

On this page it is possible to edit the parameters and settings that were read-only/disabled in the [SMTP server](#) configuration tool.



tacatest.ta.internal

System > Client Applications > SMTP Servers > tacatest.ta.internal

Delete settings

Deletion types: Delete files automatically after archive if they are older than days
 Delete files automatically if they are stored for more than days

Resource settings

Maximum number of parallel incoming connections:
Maximum number of archiving threads:

Delete settings

Delete files automatically after archive if they are older than X days: Enabling this option will allow the SMTP server to delete the locally saved emails after archiving, when the number of the given days has expired

Delete files automatically if they are stored for more than X days: Enabling this option will allow the SMTP server to delete the locally saved emails when they're not archived after the given number of days. This option is disabled by default.

Resource settings

Maximum number of parallel incoming connections: The SMTP server will listen for the incoming emails on that many threads as the number specified in this option.

Maximum number of archiving threads: This option is setting the number of the threads that are used to archive the incoming emails into contentACCESS.

When the page is saved the options are immediately sent to the SMTP server.

SMTP domains

In this section the user can see and define a list of domains, which can be used later to create [SMTP mappings](#). The listening email addresses for the incoming emails can only be configured in SMTP mappings



if they have been previously set here in this section. The SMTP domains can be edited and deleted as well from their context menu.

SMTP domains

[+ new smtp domain](#)

Domain name

tacatest.ta.internal

...

tech-arrow.com

...

microsoft.com

...

Page 1 of 1 (3 items)



To add another SMTP domain, simply click on the [+ new smtp domain](#), enter the name and click **Save**.

Add smtp domain

Domain name:

Blacklisted domains

In this section the user can define a list of domains, which will act as a forbid list - any of the incoming emails that has any of these domains in any of the recipient addresses will be rejected from the archiving process.

The blacklisted domains can be edited and deleted as well from their context menu.

Blacklisted domains

[+ new blacklisted domain](#)

Domain name

gmail.com

...

Page 1 of 1 (1 items)





To add another blacklisted domain, simply click on the **+ new blacklisted domain**, enter the name and click **Save**.

Add blacklisted domain ✕

Domain name:

SMTP mappings

In this section the user can see a read-only list of the created SMTP mappings for overview purposes.

SMTP mappings

Email address	Folder name	Model name	Entity name	Tenant name
mne.testing@tech-arrow.com	SMTP	Email archive	dne@ta.internal	MNE Tenant

Page 1 of 1 (1 items)





SMTP Mappings

The SMTP mappings page can be found under **System -> Services** section in Central Administration. On this page the user can define new SMTP mappings, edit the existing ones (the listening address cannot be changed) and/or delete them using their context menu. Upon adding a new mapping, editing or deleting an existing one, the new list of the mappings is synchronized to the SMTP servers immediately.

The columns in the grid are the following:

Email address: the address the SMTP server listening on for incoming emails

Folder name: the name of the folder in the target mailbox, to which the emails archived by the SMTP server will be saved

Model name: the name of the model, where the selected target entity lives (the Email archive model enabled for SMTP based archiving)

Entity name: name of the target entity - the email address of the target mailbox



+ new smtp mapping

Email address	Folder name	Model name	Entity name
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
mne.testing@tech-arrow.com	*** SMTP	Email archive	dne@ta.internal
john.smith@microsoft.com	*** SMTPmapping	Email archive	SNE@ta.internal
andrew.tech@tech-arrow.com	*** Mappings	Email archive	ANE@ta.internal

Page 1 of 1 (3 items) ◀ 1 ▶

To add a new SMTP mapping, click on the **+ new smtp mapping** and specify the following:

Email address: the address that the SMTP server is listening on for incoming emails. The domain part is a dropdown list and contains the domains specified in the **SMTP domains** section in the [SMTP Servers](#) page

Folder name: the name of the folder in the target mailbox, to which the emails archived by the SMTP server will be saved

Model name: the name of the model, where the selected target entity lives (the Email archive model enabled for SMTP based archiving)



Entity name: name of the target entity - the email address of the target mailbox. For a mailbox to show up here, it must have an archive database and an index zone assigned.

SMTP Mapping ✕

SMTP mapping

Email address:	<input type="text" value="jack.bolton"/>	@	<input type="text" value="tech-arrow.co"/>
Folder:	<input type="text" value="SMTP mails"/>		
Model:	<input type="text" value="Email archive"/>		
Entity:	<input type="text" value="dne@ta.internal"/>		

Note: If the email address is not specified in any of the mappings, it cannot be processed by the SMTP server.

Important: One **Email address** can be associated only with one **Entity**! However, one **Entity** can be associated with multiple **Email addresses**.

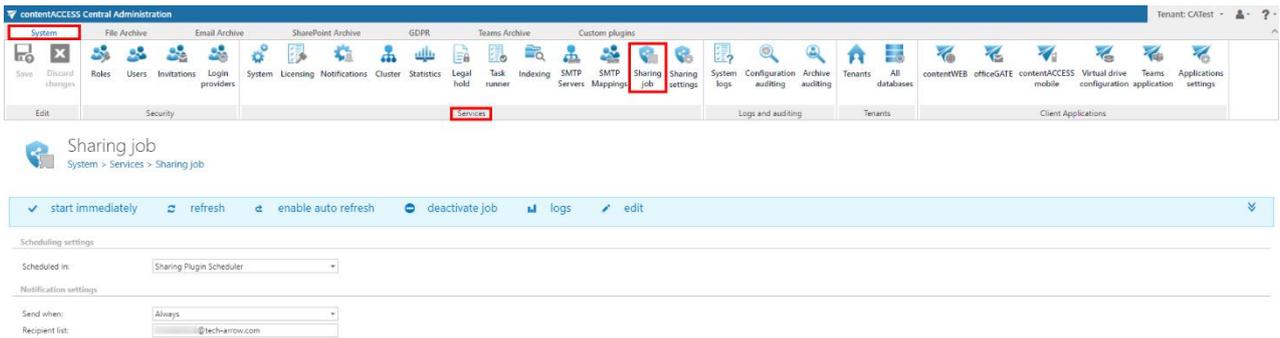
Sharing job

The sharing job is a system-wide job that handles asynchronous post-processing and management of the shared files and all sharing inside the system.

This job does the following tasks:

- updates and synchronizes channel and chat memberships for the files that were shared through **contentACCESS Teams app**
- deletes the expired files from the store

To configure the sharing job, navigate to **System -> Services -> Sharing job**.



On this page, you will be able to set the following:

✓ **Scheduling settings:**

In this step the running times of the sharing job must be selected. It is possible either to select a scheduler from the list or to create a new scheduler via create new option. For more information about how to set schedulers please refer to the section [Schedules](#) above.

Scheduling settings

Scheduled in:

✓ **Notification settings:**

The user may select here, in which cases he needs to get notifications from the sharing job. It is possible to set here that the notification emails will be sent only in case of errors or warnings, or they can be sent in all cases, too. Into the **Recipient list** textbox, insert the email addresses of the people, whom these emails should be sent to. Notifications emails may be used as tools of the troubleshooting process.

Notification settings

Send when:

Recipient list:

Sharing settings

The **sharing feature** allows the user to specify the restriction and retention to be applied for the shared items when sharing them. It also automates the **user invitation** process in case the items are shared with



an external recipient and sends an email with links pointing to the shared items. Full [Auditing](#) logs are provided about the sharing and file downloads, too.

More settings for the **Sharing** module can be configured here. Navigate to **System** -> **Services** -> **Sharing settings**.

The screenshot shows the 'Sharing settings' page in the contentACCESS Central Administration interface. The page is titled 'Sharing settings' and includes the following sections:

- Storage settings:** A dropdown menu for 'Storage name' is set to 'CAtest Storage'.
- Index zone settings:** A dropdown menu for 'Index zone' is set to 'Default index zone'.
- Sharing settings:**
 - 'Allow public sharing:' is checked.
 - 'Allow sharing with organization:' is checked.
 - 'Allowed organization domains:' is set to 'tech-arrow.com'.
 - 'Show organization shares in client applications:' is checked.
- Proxy settings:** A 'Configure...' button is present.

On this page, you will be able to set the following:

✓ **Storage settings:**

Choose an already configured storage from the dropdown list. The binaries for the files that were directly uploaded during the sharing will be stored here, items shared from the archive won't be duplicated into this storage. For more information on how to set storages check section [Storages](#) above.

Storage settings

Storage name: [Change](#)

✓ **Index zone settings:**

Pick the Index zone that will be assigned to the **shared items** from the dropdown list. If you want to configure a new one, navigate to **System** ⇒ **Services** ⇒ **Index zones**.

Index zone settings

Index zone:



✓ Sharing settings:

In this part, you can set the following:

- **Allow public sharing** – if checked, you will be able to share archived items from contentWEB with anyone, even the people the sharing link or email is forwarded to will be able to open it; in case of public sharing, no authentication is required, therefore the [Auditing](#) is not able log the identity of the user that downloaded the item
- **Allow sharing with organization** – by checking this checkbox, the next two options will get enabled; the organization sharing will enable you to easily allow access to a file for everyone inside the organization. This is very useful when sharing company-wide documents.
- **Allowed organization domains** – in this textbox you can specify organization domain(s), which will be then used when selecting the option to share with “My organization” in contentWEB - the system will be checking the user’s login name for the domains. In case the organization owns multiple domains, all domains must be specified here for the users to be able to download the files.
- **Show organization shares in client applications** – if the option mentioned above was used, the organization shares will be visible in client applications; The files shared with organization access will be displayed for all users inside the organization.

Sharing settings

Allow public sharing:	<input checked="" type="checkbox"/>
Allow sharing with organization:	<input checked="" type="checkbox"/>
Allowed organization domains:	<input type="text" value="tech-arrow.com X"/>
Show organization shares in client applications:	<input checked="" type="checkbox"/>

✓ Proxy settings:

It is possible to also share not only archived, but also **live SharePoint files** that are not in the archive. By using the **SharePoint proxy**, all extra features (date/download restrictions, common view about the shared files,...) provided by contentACCESS are applied, while the files stay in SharePoint. The file download and access is done by a superuser, but during the sharing process, the permissions of the user that is sharing the file(s) are verified, if the user really has access to the file(s).

Requirement: O365 SharePoint is needed, and the sharing user must have O365 login in contentACCESS.



To **Configure SharePoint proxy**, click on the **Configure...** button.

Sharing settings
System > Services > Sharing settings

Storage settings

Storage name: Change

Index zone settings

Index zone:

Sharing settings

Allow public sharing:

Allow sharing with organization:

Allowed organization domains:

Show organization shares in client applications:

Proxy settings

Configure SharePoint proxy:

SharePoint proxy allows to share SharePoint documents

First, you will need to activate the SharePoint proxy by clicking on the **Activate proxy** button. In our case, it is already activated, that is why only the **Deactivate proxy** button is enabled.

Note: by deactivating the SharePoint proxy, any previously shared file will be unavailable. By re-activating the proxy, the files will be available again.

SharePoint proxy
SharePoint Archive > Settings > SharePoint proxy

Activation status

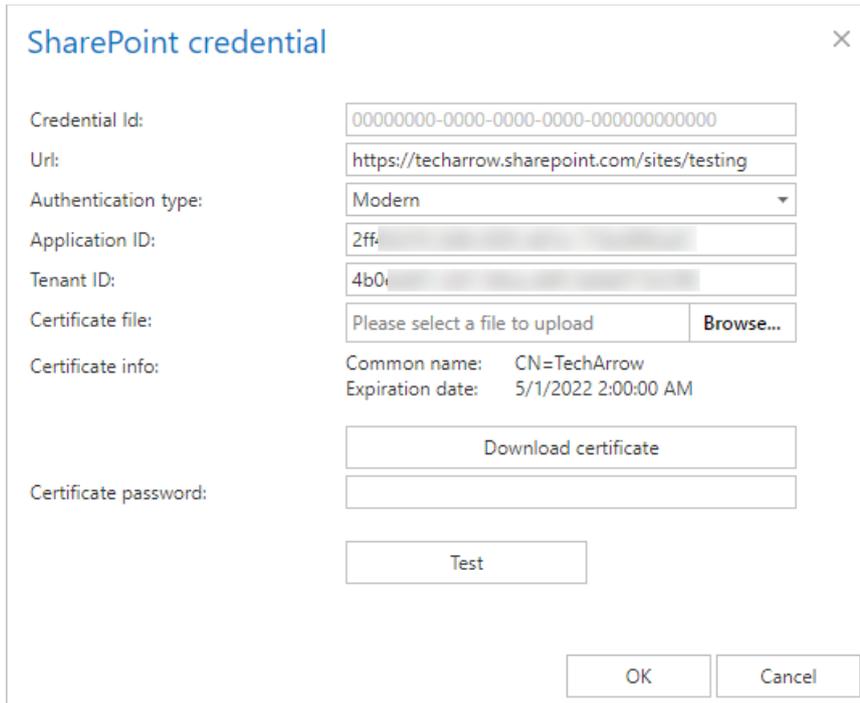
SharePoint proxy activation status: Activated

SharePoint credentials

[+ new](#)

Uri	Authentication	User
https://techarrow.sharepoint.com/sites/testing	▲ Modern	

Each site collection you would like to share files from needs to be specified separately. To specify a new site collection, click on **+new**. The **SharePoint credential** window opens. Enter the **URL** and choose the **Authentication type** from the dropdown list – **Integrated**, **Basic** or **Modern**. All the authentication types are explained in [this](#) section.



How to create/configure databases — All databases

Processing plugins of a tenant write the metadata into the selected SQL database, which was formerly created by the administrator. The system database is always created during the installation process of contentACCESS, but it is not associated with a tenant. Databases associated with specific tenants are set up by the system administrator on the **All databases** page.

Factors to be considered before creating databases:

- ✓ The number of users expected for your database – if the company (tenant) has more than 2,000 mailboxes, it is recommended to create more archive databases (e.g. for storage, email archive, provisioning, or to set separate databases for the Exchange groups) to ensure a better transparency of data.



- ✓ The amount of expected data in the database – always estimate how much space your data will require.
- ✓ It is also worth to consider the retrieving capacities of the database.

To open **All databases** page in contentACCESS, navigate to **System** tab → **Tenants** → **All databases** control on the Central Administration ribbon. On this page you may find all databases created for all tenants. The server, where the tenant databases are installed, the database name, schema, user details and the associated tenants are also displayed in the grid:

The screenshot shows the 'All databases' page in the contentACCESS Central Administration interface. The page title is 'All databases' and the breadcrumb is 'System > Tenants > All databases'. There are three main actions: '+ configure existing', '+ create new', and 'update all databases'. Below these actions is a table with the following data:

Connection name	Server	Type	Database	Schema	User	Tenant
Email Archive DB	*** TANNEWS	0	Email Archive DB	dbo	DBAdmin	TECH-ARROW
eimDB	*** taem01	0	eimDB	dbo	sa	TECH-ARROW
File Archive DB	*** TANNEWS	0	File Archive DB	dbo		TECH-ARROW
SharePoint_Archive_DB	*** TANNEWS	0	SharePoint_Archive_DB	dbo		MyCompany

+ create new

To be able to run processing jobs in contentACCESS, a new database must be created. This database must be then selected on the job's configuration page, or in case of archiving the Exchange, it can be also associated with a mailbox from the address book. Click on **+ create new** option and fill required data in the **Database repository** window.



Database repository
✕

Connection name:

Use system database server (TANEWS)

Type:

Server name:

Database:

Schema:

Database user

Use explicit user

New or existing user:

Password:

Confirm password:

Connect with user

Use explicit credentials

User:

Password:

Confirm password:

✔ Database connection is successful!

Tenant:

Connection name: Enter a display name for the newly created database. This will be the name of the database in contentACCESS Central Administration.

If you want to use system database server check the “Use system database server” checkbox as it is shown on the screenshot above. This will populate the server settings. Type the database name into the “Database” field. This will be the name of the database on the SQL server. If you want to use database server that differs from the system database server, then follow the next steps:

- a) **Type:** choose the type of database from the dropdown list (**MSSQL** is supported by default)
- b) **Server name:** enter the name of the database server (where MSSQL is installed) here
- c) **Database:** the database will be created on SQL server under this name
- d) **Schema:** type in the database schema (optional)

Under **Database user** configurations you may create a database user. There are multiply options how to create a database user: 1) You can use an already existing user to connect to the database, or 2) you can create a new database user. 3) It is also possible to use the service user credentials to connect to the database, or 4) you may create a database user with random credentials (the user name can be edited).



- 1) If you want to use an already existing user, check the **Use explicit user** checkbox and enter the user credentials into the **New or existing user/Password/Confirm password** textboxes.

Database user

Use explicit user

New or existing user:

Password:

Confirm password:

- 2) If you want to create a new database user with custom credentials, type them into the **New or existing user/Password/Confirm password** textboxes. Do NOT click on the **Generate user and password** button.

Database user

Use explicit user

New or existing user:

Password:

Confirm password:

- 3) To connect with the service account, leave the **Use explicit user** checkbox unchecked and leave all the fields empty.

Database user

Use explicit user

New or existing user:

Password:

Confirm password:

- 4) To create a new user with a random password check the **Use explicit user** checkbox, and click on the **Generate user and password** button. The user name can be edited directly here.

Database user

Use explicit user

New or existing user:

Password:

A newly created database user will have access permissions only to the currently created database.

Under **Connect with user** enter the credentials of the database user, who has the right to create a new database on the SQL server. If the **Use explicit credentials** checkbox is not checked, then contentACCESS



will automatically connect to the database (MSSQL) under the contentACCESS service account. If you want to connect with an explicit user, check this checkbox, then enter the login data.

Test database connection: with a click on this button, you can run a test connection to check if contentACCESS managed to connect to the selected database server (MSSQL).

Tenants: select a tenant from the dropdown list with which the database will be associated.

Click on **Save** and the **New database** will turn up in the list of databases.

Note: When we are archiving from the Exchange server, the database must be associated with the mailbox from the address book, or the first running email archive job will associate the configured database to the archived mailbox(es). In case of file system archive, a database must be selected during the configuration process of the job.

+ configure existing

If you need to establish a connection between an already existing SQL database and contentACCESS, click on **+ configure existing** and configure the required data in the **Database repository** window. In this case, you do not create a new database - an already existing database from the SQL server is used.

Connection name: Enter a display name for the database. This will be the name of the database in contentACCESS.



If you want to use system database server check the “Use system database server” checkbox as it is shown on the screenshot above. This will populate the server settings. Type the database name into the “Database” field. This will be the name of the database on the SQL server. If you want to use database server which differs from the system database server, follow the next steps:

- a) **Type:** choose the type of database from the dropdown list (**MSSQL** is supported by default)
- b) **Server name:** enter the name of the database server here (where MSSQL is installed)
- c) **Database:** type here the name of an already existing database on the SQL server
- d) **Schema:** type in the database schema (optional)

Use explicit credentials: if this checkbox is not checked, then contentACCESS will automatically connect to the database (MSSQL) under the contentACCESS service account. If you want to use an explicit database user, check the checkbox and enter the user credentials.

Test database connection: with a click on this button, you can run a test connection to check if contentACCESS managed to connect to the selected database server (MSSQL).

Tenants: select a tenant from the dropdown list – the database will belong to this tenant

Click on **Save** and the **New database** will turn up in the list of databases.

Note: The “create new” and “configure existing” options are unavailable for the logged on user, if the Add repository item permission on the tenant is not allowed in his role assignment. Read more in [Role details](#).

Update all databases

With a click on this option it is possible to update the structure of all databases. Click this button and the status bar of the updating plugin will appear. In this status bar, the following operations are accessible; start/stop running, manual refresh, enable/disable auto refresh and logs (this will redirect the user to the last run session of the database updating plugin):



All databases

System > Tenants > All databases

+ configure existing + create new ↻ update all databases

✓ start immediately ↻ refresh ↺ disable auto refresh ⏸ deactivate job ✎ edit ⬆

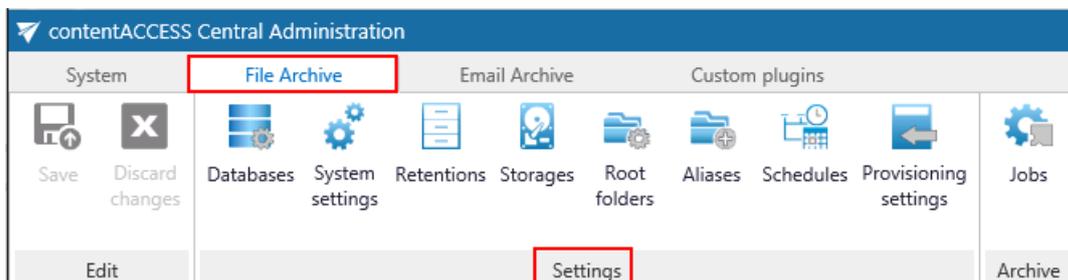
Status: **Idle**
Progress: 11 databases processed (11 skipped) (completed 3 minutes ago)

Common features

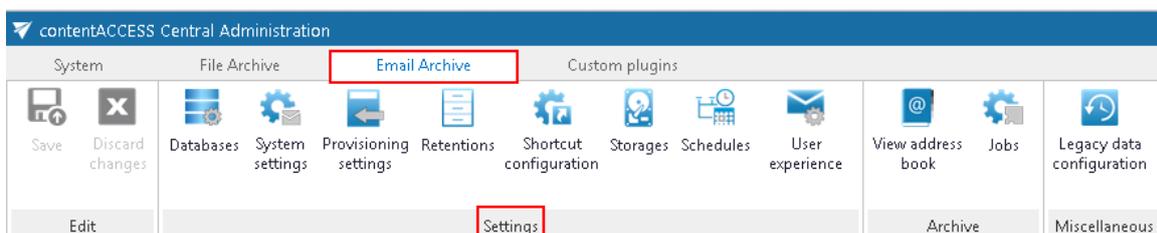
To crawl mailbox and folder contents, contentACCESS uses **plugins**. A plugin in contentACCESS is a component of the software that adds specific features to the application. Each type of plugin has its own specific use-case, but its features can be simply extended, depending on the process that it should implement.

Depending on the implemented process, the administrator creates certain instances from these plugins, which we call “jobs”. Even these jobs differ from each other concerning their settings, but there are certain features that are common to all of these jobs: all jobs use a database, where they write metadata, they have a storage where they store binaries, they have a scheduler, which specifies their running times, they have a retention which determines the period for how long the data (documents, emails, etc.) processed by a job must be accessible etc. These settings are configurable in the following groups:

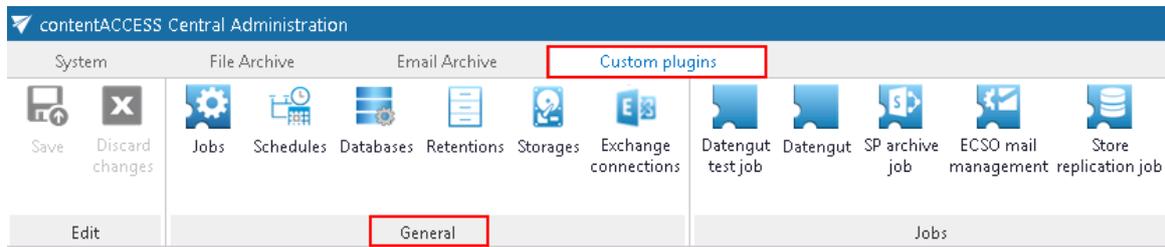
- **File Archive tab** → **Settings** group by the File Archive;



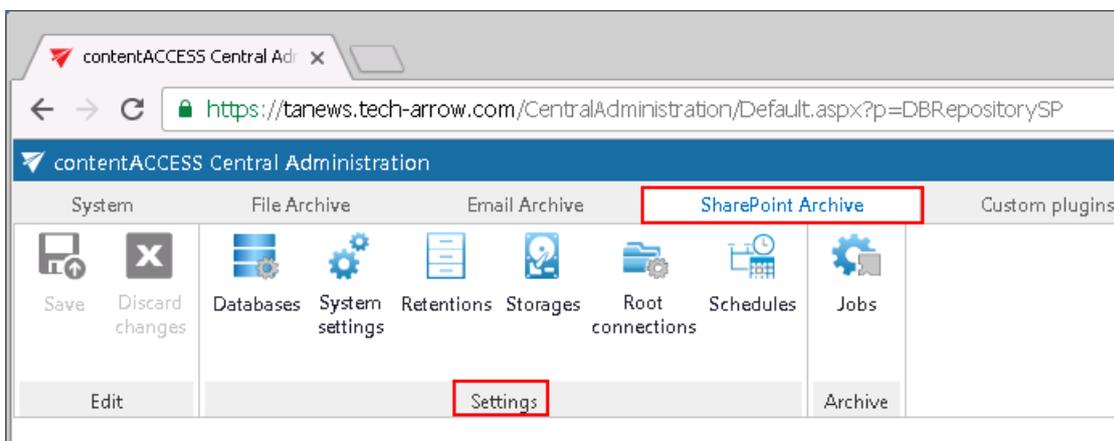
- **Email Archive tab** → **Settings** group by Email Archive;



- **Custom plugins tab** → **General** group by Custom plugins.



- **SharePoint Archive tab** → **Settings** group by the SharePoint Archive;



Only the features configured in these settings can be selected on the processing job's configuration page.

In this section we will explain how to adjust these framework features. These configurations can be done the same way for all plugin types - by navigating to the appropriate control button on the Central Administration ribbon. The configuration logic is from left to right. If you follow this logic, then all necessary configuration will be done for the next step.

Databases

(Email Archive → Settings → Databases button;

File Archive → Settings → Databases button;

SharePoint Archive → Settings → Databases button;

Custom plugins → General → Databases button)

Open the **Databases** page from the  **Databases** button. The databases configured for your selected tenant are displayed in the database grid on this page. The grid contains the following database information: the server name, where the database is installed, the type of database (MSSQL), the database name on SQL,



the schema and the database user name. The administrator can configure a connection on this page, where the processed metadata **of this particular tenant** will be stored. If such a database needs to be configured, click on the **+ configure new** button and fill the required fields in the **Database repository** window. If the system database server will be used, check the **Use system database server** checkbox. Type the already existing SQL database name (if such a database has not been created yet, refer to **+ create new** in section [“SMTP Mappings](#)

[The SMTP mappings page can be](#) found under **System -> Services** section in Central Administration. On this page the user can define new SMTP mappings, edit the existing ones (the listening address cannot be changed) and/or delete them using their context menu. Upon adding a new mapping, editing or deleting an existing one, the new list of the mappings is synchronized to the SMTP servers immediately.

The columns in the grid are the following:

Email address: the address the SMTP server listening on for incoming emails

Folder name: the name of the folder in the target mailbox, to which the emails archived by the SMTP server will be saved

Model name: the name of the model, where the selected target entity lives (the Email archive model enabled for SMTP based archiving)

Entity name: name of the target entity - the email address of the target mailbox



SMTP Mappings

System > Services > SMTP Mappings

[+ new smtp mapping](#)

Email address	Folder name	Model name	Entity name
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
mne.testing@tech-arrow.com	*** SMTP	Email archive	dne@ta.internal
john.smith@microsoft.com	*** SMTPmapping	Email archive	SNE@ta.internal
andrew.tech@tech-arrow.com	*** Mappings	Email archive	ANE@ta.internal

Page 1 of 1 (3 items)



To add a new SMTP mapping, click on the **+ new smtp mapping** and specify the following:

Email address: the address that the SMTP server is listening on for incoming emails. The domain part is a dropdown list and contains the domains specified in the **SMTP domains** section in the SMTP Servers page



Folder name: the name of the folder in the target mailbox, to which the emails archived by the SMTP server will be saved

Model name: the name of the model, where the selected target entity lives (the Email archive model enabled for SMTP based archiving)

Entity name: name of the target entity - the email address of the target mailbox. For a mailbox to show up here, it must have an archive database and an index zone assigned.

Note: If the email address is not specified in any of the mappings, it cannot be processed by the SMTP server.

Important: One **Email address** can be associated only with one **Entity**! However, one **Entity** can be associated with multiple **Email addresses**.

Sharing job

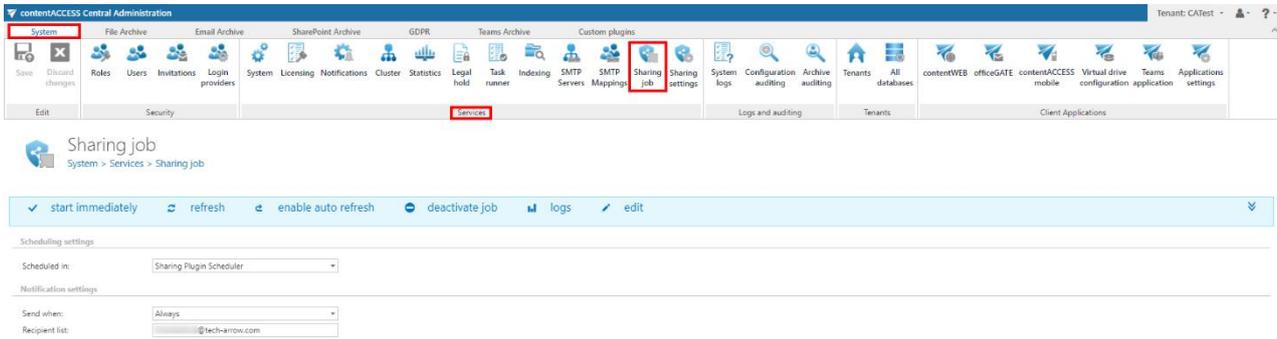
The sharing job is a system-wide job that handles asynchronous post-processing and management of the shared files and all sharing inside the system.

This job does the following tasks:

- updates and synchronizes channel and chat memberships for the files that were shared through **contentACCESS Teams app**
- deletes the expired files from the store



To configure the sharing job, navigate to **System -> Services -> Sharing job**.



On this page, you will be able to set the following:

✓ **Scheduling settings:**

In this step the running times of the sharing job must be selected. It is possible either to select a scheduler from the list or to create a new scheduler via create new option. For more information about how to set schedulers please refer to the section Schedules above.

Scheduling settings

Scheduled in:

✓ **Notification settings:**

The user may select here, in which cases he needs to get notifications from the sharing job. It is possible to set here that the notification emails will be sent only in case of errors or warnings, or they can be sent in all cases, too. Into the **Recipient list** textbox, insert the email addresses of the people, whom these emails should be sent to. Notifications emails may be used as tools of the troubleshooting process.

Notification settings

Send when:

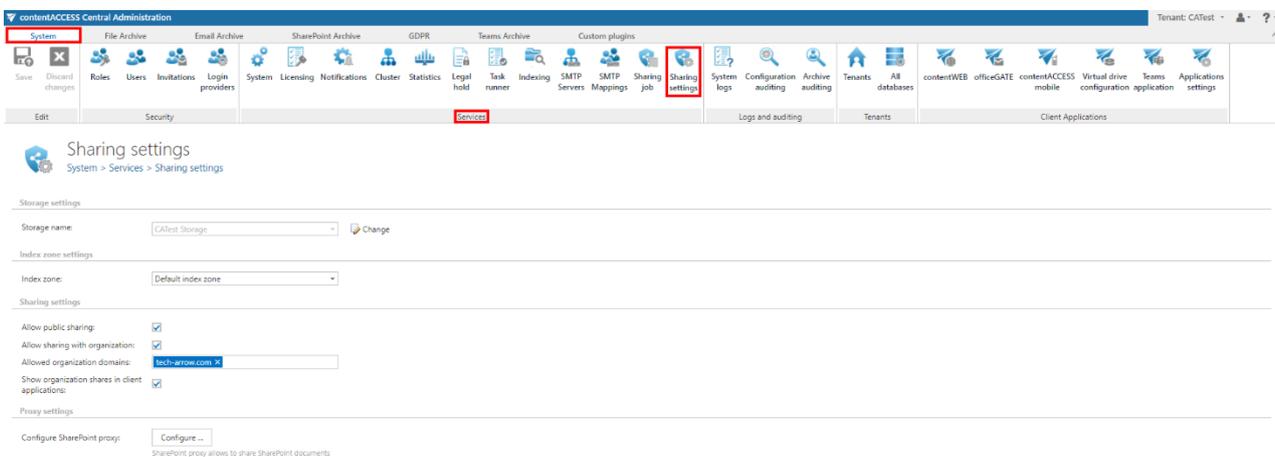
Recipient list:



Sharing settings

The sharing **feature allows** the user to specify the restriction and retention to be applied for the shared items when sharing them. It also automates the user **invitation process** in case the items are shared with an external recipient and sends an email with links pointing to the shared items. Full Auditing logs are provided about the sharing and file downloads, too.

More settings for the **Sharing** module can be configured here. Navigate to **System -> Services -> Sharing settings**.



On this page, you will be able to set the following:

✓ Storage settings:

Choose an already configured storage from the dropdown list. The binaries for the files that were directly uploaded during the sharing will be stored here, items shared from the archive won't be duplicated into this storage. For more information on how to set storages check section [Storages](#) above.

Storage settings

Storage name:

CAtest Storage



✓ Index zone settings:

Pick the Index zone that will be assigned to the **shared items** from the dropdown list. If you want to configure a new one, navigate to **System ⇒ Services ⇒ Index zones**.



Index zone settings

Index zone:

Default index zone ▼



✓ Sharing settings:

In this part, you can set the following:

- **Allow public sharing** – if checked, you will be able to share archived items from contentWEB with anyone, even the people the sharing link or email is forwarded to will be able to open it; in case of public sharing, no authentication is required, therefore the Auditing is not able log the identity of the user that downloaded the item
- **Allow sharing with organization** – by checking this checkbox, the next two options will get enabled; the organization sharing will enable you to easily allow access to a file for everyone inside the organization. This is very useful when sharing company-wide documents.
- **Allowed organization domains** – in this textbox you can specify organization domain(s), which will be then used when selecting the option to share with “My organization” in contentWEB - the system will be checking the user’s login name for the domains. In case the organization owns multiple domains, all domains must be specified here for the users to be able to download the files.
- **Show organization shares in client applications** – if the option mentioned above was used, the organization shares will be visible in client applications; The files shared with organization access will be displayed for all users inside the organization.

Sharing settings

Allow public sharing:	<input checked="" type="checkbox"/>
Allow sharing with organization:	<input checked="" type="checkbox"/>
Allowed organization domains:	<input type="text" value="tech-arrow.com X"/>
Show organization shares in client applications:	<input checked="" type="checkbox"/>

✓ Proxy settings:

It is possible to also share not only archived, but also **live SharePoint files** that are not in the archive. By using the **SharePoint proxy**, all extra features (date/download restrictions, common view about the shared files,...) provided by contentACCESS are applied, while the files stay in SharePoint. The file download and access is done by a superuser, but during the sharing process, the permissions of the user that is sharing the file(s) are verified, if the user really has access to the file(s).

Requirement: O365 SharePoint is needed, and the sharing user must have O365 login in contentACCESS.



To **Configure SharePoint proxy**, click on the **Configure...** button.

Sharing settings
System > Services > Sharing settings

Storage settings

Storage name: Change

Index zone settings

Index zone:

Sharing settings

Allow public sharing:

Allow sharing with organization:

Allowed organization domains:

Show organization shares in client applications:

Proxy settings

Configure SharePoint proxy:

SharePoint proxy allows to share SharePoint documents

First, you will need to activate the SharePoint proxy by clicking on the **Activate proxy** button. In our case, it is already activated, that is why only the **Deactivate proxy** button is enabled.

Note: by deactivating the SharePoint proxy, any previously shared file will be unavailable. By re-activating the proxy, the files will be available again.

SharePoint proxy
SharePoint Archive > Settings > SharePoint proxy

Activation status

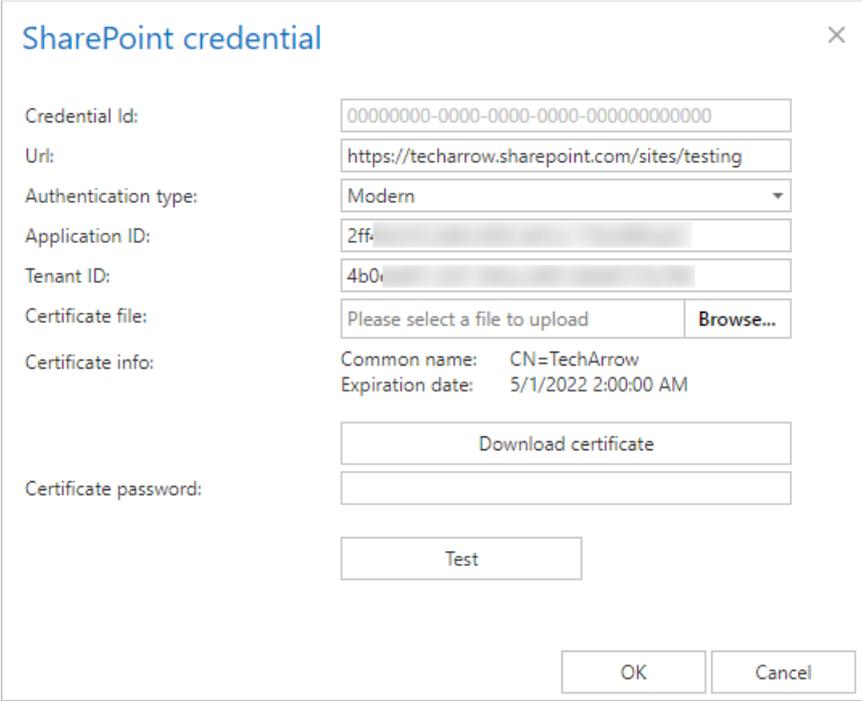
SharePoint proxy activation status: Activated

SharePoint credentials

[+ new](#)

Uri	Authentication	User
https://techarrow.sharepoint.com/sites/testing	▲ Modern	

Each site collection you would like to share files from needs to be specified separately. To specify a new site collection, click on **+new**. The **SharePoint credential** window opens. Enter the **URL** and choose the **Authentication type** from the dropdown list – **Integrated**, **Basic** or **Modern**. All the authentication types are explained in this section.



SharePoint credential

Credential Id: 00000000-0000-0000-0000-000000000000

Url: https://techarrow.sharepoint.com/sites/testing

Authentication type: Modern

Application ID: 2ff: [redacted]

Tenant ID: 4b0: [redacted]

Certificate file: Please select a file to upload **Browse...**

Certificate info: Common name: CN=TechArrow
Expiration date: 5/1/2022 2:00:00 AM

Download certificate

Certificate password: [redacted]

Test

OK **Cancel**

How to create/configure databases — All databases”) into the **Database** textbox

By default, contentACCESS is connected to the database with the credentials of the user, under whom contentACCESS is running. If you want to use other credentials, which differ from these credentials data, then check the checkbox **Use explicit credentials** and enter the **User** and **Password** that you want to use for connecting to the tenant database. You can also run a test connection with the **Test database connection** button in the left corner of the window.

Database repository ✕

Connection name:

Use system database server (TANEWS)

Type:

Server name:

Database:

Schema:

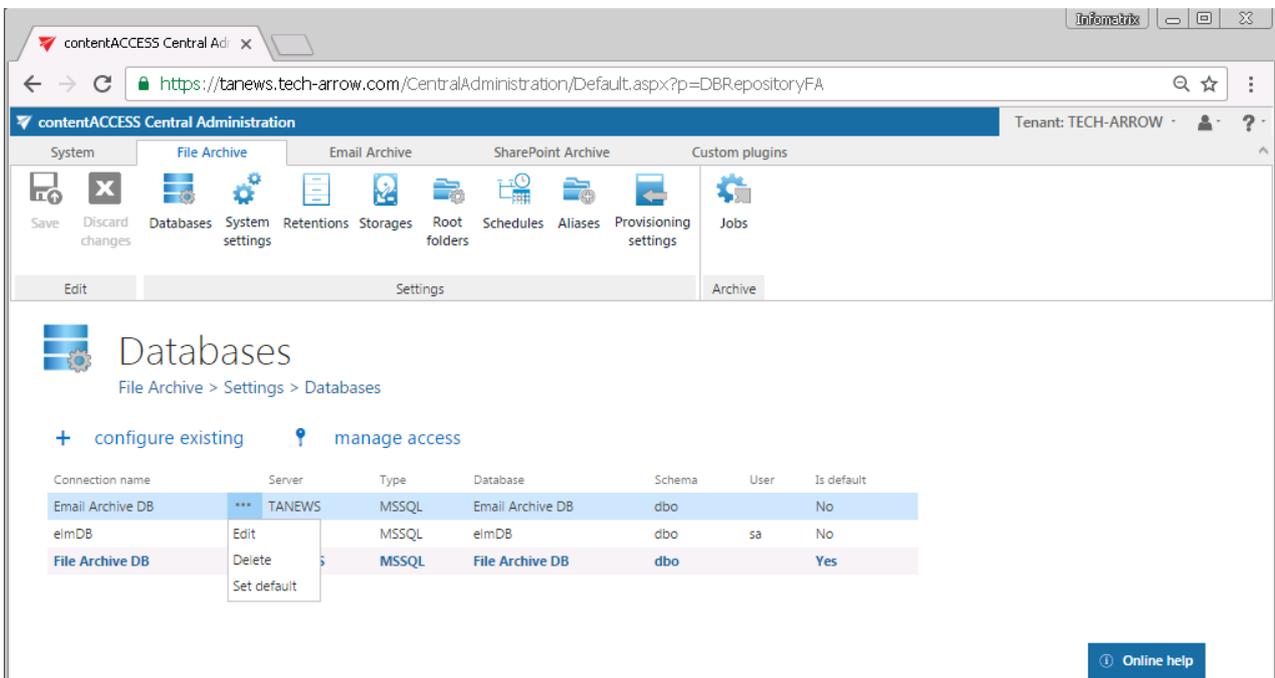
Use explicit credentials

User:

Password:

Confirm password:

It is possible to modify the settings, delete the database or set the database as default on the **Databases** page, from the database’s context menu, as it is shown on the screenshot below:



Note: The “configure existing” option (i.e. to configure an existing database connection) is unavailable for the logged on user, if the Add repository item permission on the tenant is not allowed in his role assignment. The “manage access” option allows to grant access permissions on the selected database connection for a second user. This “manage access” option is available for the logged on administrator, if his role assignment

contains the Edit repository item – All allowed permission on the tenant. Read more in [Managing access to contentACCESS objects](#).

Schedules

Email Archive → Settings → Schedules button;

File Archive → Settings → Schedules button;

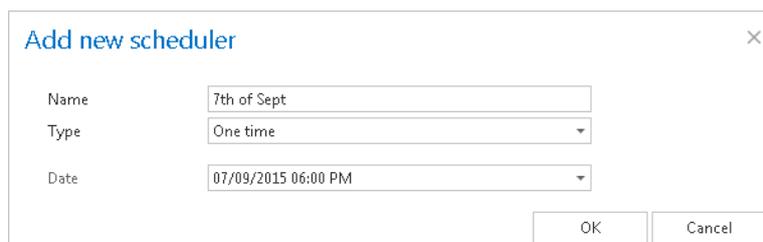
SharePoint Archive → Settings → Schedules button;

Custom plugins → General → Schedules button)

How to use schedulers in contentACCESS? Jobs in contentACCESS can be automatically triggered with the help of schedules. Schedules are used to define, when a processing task should start automatically and when the processing should end and restart again. In other words, administrator may schedule jobs which will automatically run at times, which are configured in the given job's scheduler settings. It is possible to set numberless schedulers and then select the appropriate one when configuring an exact job. Schedules help the users to work more efficiently, so they won't have to waste their time by logging into the software and starting the processing manually.

Navigate to the **Schedules** page from the  **Schedules** button on the ribbon. Here click on **+ new** option. In the **Add new scheduler** dialog window enter the scheduler **Name**, select the **Type** of scheduler from the dropdown list. In contentACCESS, there are 3 types of schedulers which can be set: **One time**, **Always run** and **Week schedule with repeat**.

One time will run only once; by this type of scheduler we specify the start date only; the job will end when it finished the processing. One time schedulers are often used by restore or recovery jobs, i.e. by jobs which are run occasionally. The schedule that we set up now will start to run on 7th of September at 6 PM, and will end once the job finished its task:





Always run will run always without interruption. The job that uses this scheduler type will be started immediately after being configured and saved. With the use of **Frequency in minutes** function the user may set the time intervals, when the scheduler should check if the job is running. In case of our “Non-stop” scheduler (check the screenshot below), the running frequency is set to 1 minute, so the scheduler will wake up each minute to check if the job is still running. If it is running, then it will check the running after 1 minute again; if it is not running, then the job will be started again. This scheduler type is typically used by archiving from journal mailboxes.

Week schedule with repeat will run at the same hours every week, repeatedly. In the scheduling tab click on the fields to set the days and hours, when the processing should start. One cell represents one hour. By using the **Running frequency in minutes** option the user may set the time intervals, when the scheduler should check if the job is running. If running frequency is set e.g. to 5 minutes, then the scheduler will check in every 5 minutes, if the job is still running. If it is running, then it will check the running after 5 minutes again: if it is not running, then the job will be started again. It is worth to use this option if the processing should run continuously, e.g. from morning to evening, and new tasks are continuously added that should be processed. If we check the **Run only once per interval** checkbox, then the running frequency will be automatically deactivated and the job will run only once during this time period. It is recommended to run a process once in an interval, if the processing should be performed e.g. at the end of each working day. With checking the **Stop job at interval end** checkbox the user may stop a job after the set time interval. You don't have to mind any unfinished processing, the job will be forcibly stopped and started again, according to the scheduler settings. The red color of the **Add new scheduler's** cells mark the time intervals, when the job is not running.

Our “Every night” scheduler (its setting can be viewed on the screenshot below) will run the job from 7 PM till midnight, will stop processing at midnight, even if the process is not finished. It will run only once during this interval. We can use a similar scheduler to archive the old company documents. It makes no sense to select running frequency in this case, because during the night nobody will add new files to archive into the file location.



Add new scheduler

Name:

Type:

Week schedule with repeat

	0	6	12	18
Monday	Light Blue	Light Blue	Light Blue	Dark Blue
Tuesday	Light Blue	Light Blue	Light Blue	Dark Blue
Wednesday	Light Blue	Light Blue	Light Blue	Dark Blue
Thursday	Light Blue	Light Blue	Light Blue	Dark Blue
Friday	Light Blue	Light Blue	Light Blue	Dark Blue
Saturday	Light Blue	Light Blue	Light Blue	Dark Blue
Sunday	Light Blue	Light Blue	Light Blue	Dark Blue

[Clear]

Run only once per interval:

Running frequency in minutes:

Stop job on interval end:

OK Cancel

Setting the **Running frequency in minutes** option might be useful when the user is archiving from an Exchange journal mailbox for example, or from any location, where the tasks to be performed are accumulating continuously during a time period. If the job has processed all the items, the schedule should be also periodically checking if there is anything new to archive. The “Every working day” scheduler (on the screenshot below) is set to process the email records from 7 AM till 6 PM. The first archive process will run from 7 AM until it has finished all current tasks, and the scheduler will check each 5 minutes if any new tasks (email records) were added to process. The archiving will end at 6 PM each day, even if there is something left unfinished. A scheduler similar to this may be set to archive journal mailboxes on the Exchange:

Add new scheduler

Name:

Type:

Week schedule with repeat

	0	6	12	18
Monday	Light Blue	Dark Blue	Dark Blue	Light Blue
Tuesday	Light Blue	Dark Blue	Dark Blue	Light Blue
Wednesday	Light Blue	Dark Blue	Dark Blue	Light Blue
Thursday	Light Blue	Dark Blue	Dark Blue	Light Blue
Friday	Light Blue	Dark Blue	Dark Blue	Light Blue
Saturday	Light Blue	Light Blue	Light Blue	Light Blue
Sunday	Light Blue	Light Blue	Light Blue	Light Blue

[Clear]

Run only once per interval:

Running frequency in minutes:

Stop job on interval end:

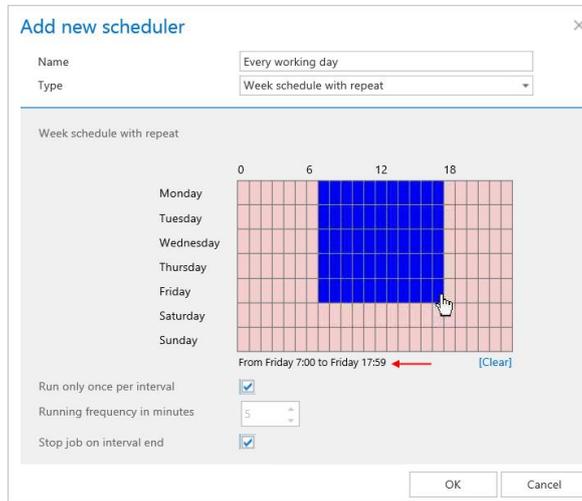
OK Cancel

This scheduler type is often used to run provisioning jobs, too.

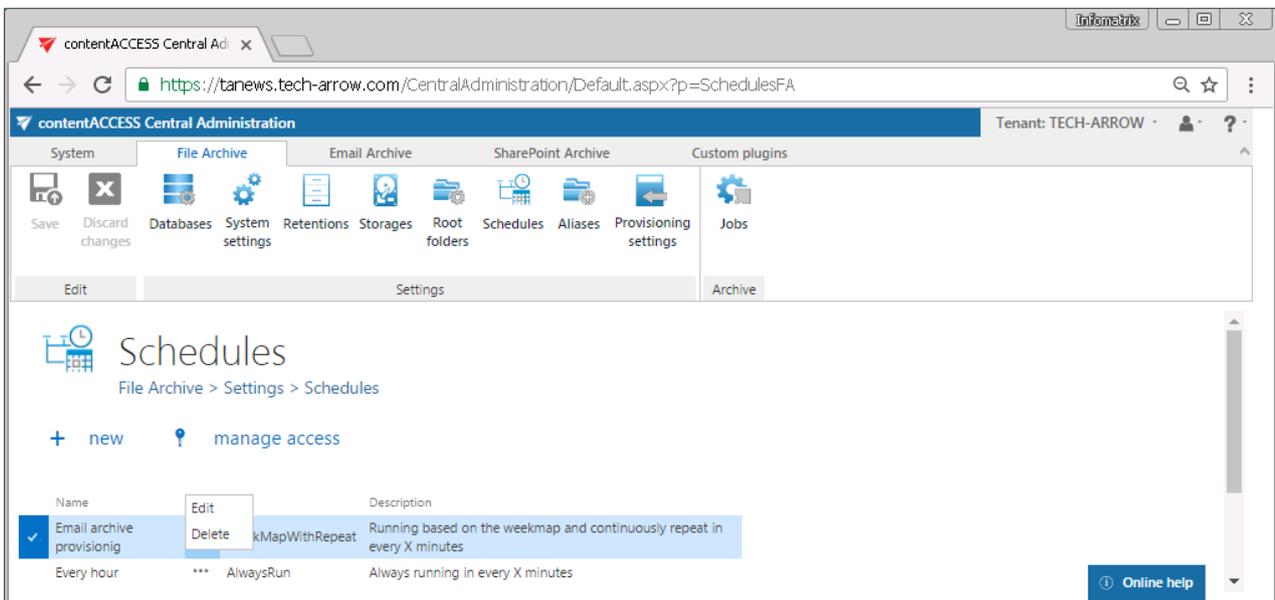
If the user would not like to end the processing at 7 PM, he should uncheck the “Stop job at interval end” option.



Tip: When the user is setting a desired time range or just moves the cursor over the selected time range, the Weekmap scheduler highlights this time range and displays the exact start and end times beneath the calendar:



It is possible to edit or delete a scheduler’s configuration using its context menu (left click on **...** next to its name) if any modifications must be implemented. The scheduler type and its description can be also viewed in the grid.



Note: The “+ new” option above the item list is unavailable for the logged on user if the “Add scheduler” permission is not allowed in his role assignment on the tenant.



The “manage access” option allows to grant access permissions on the selected scheduler for a second user. This “manage access” option is available for the logged on administrator if his role assignment contains the **Edit scheduler – All allowed** permission on the tenant. Read more in [Managing access to contentACCESS objects](#).

Retentions

(**Email Archive** → Settings → Retentions button;

File Archive → Settings → Retentions button;

SharePoint Archive → Settings → Retentions button;

Custom plugins → General → Retentions button)

What is retention time? It represents the period of time for which a document should be kept or "retained" electronically. Each country has different retention times required, so it is recommended to set a time, which is required by the competent organization in your country or by the internal regulations of the company.

The documents can't be deleted by the **Delete job** nor manually from the archive during this period of time. After the retention time expires, the documents can be deleted by the **Delete job**, but first they must be **marked for delete in contentWEB**.

Note: If the **Delete even if not marked for delete** checkbox is checked in **Delete job** configuration, the expired items will be deleted without needing to be marked for delete.



What is unprotected retention time? It represents the period of time when the document will not be deleted automatically by the **Delete job**, but can be deleted manually.

When the unprotected retention time expires, the item can be deleted by the **Delete job** without the need to be marked for delete in contentWEB.

What is reference date and where to set it?

Email archive

System settings: the reference date can be only Sent date

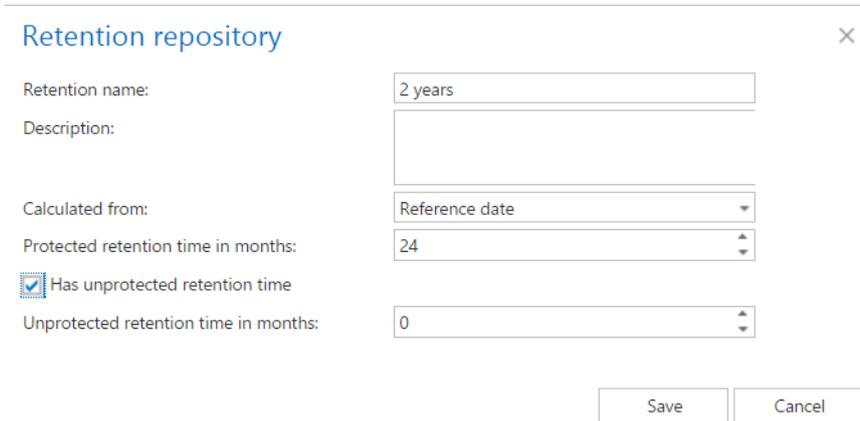
File archive

System settings: creation date, modification date, last date

SharePoint archive

System settings: creation date, modification date, last date

On the **Retentions** page the administrator may see all already configured retentions and set up new retention times, which will be used by a processing job. Only retentions configured on the **Retentions** page can be selected when configuring a processing job. To set up a new retention, click on **+ new** option. In the **Retention repository** dialog enter the **Retention name**, fill the **Description**, choose if the retention will be calculated from **Archivation date** or **Reference date** and set the **Retention time in months**. If you check the **Has unprotected retention time** checkbox, you will need to set the time in months. Click **Save**.



Retention repository ×

Retention name:

Description:

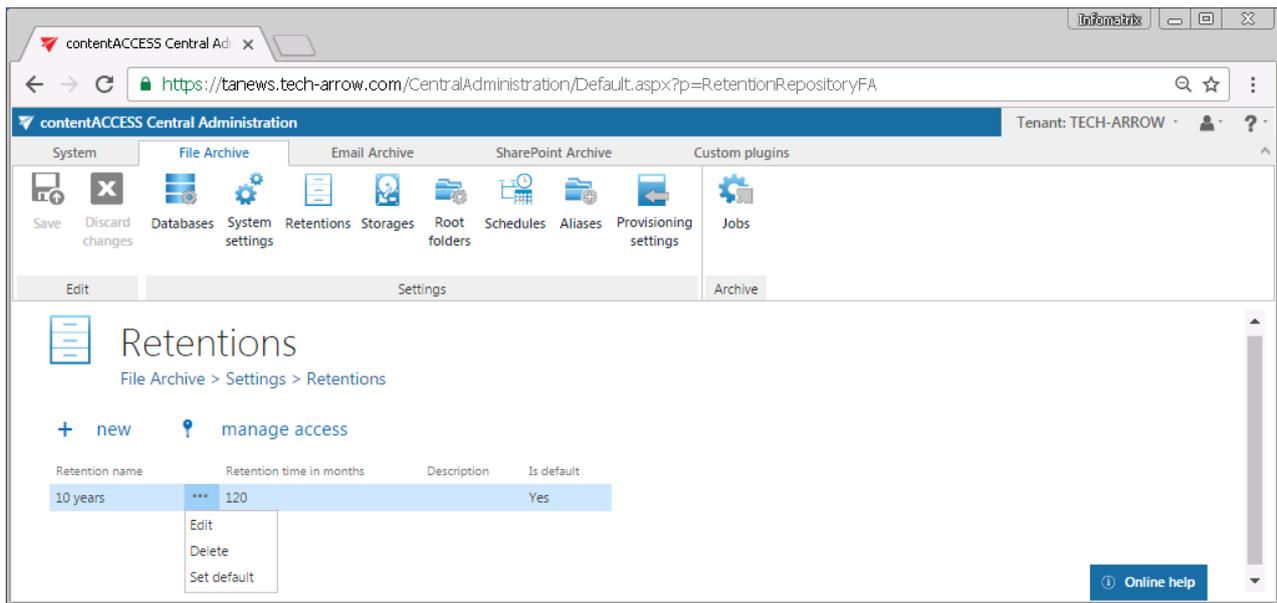
Calculated from:

Protected retention time in months:

Has unprotected retention time

Unprotected retention time in months:

It is possible to modify the settings, delete the item or set the retention as **default** from the retention's context menu (left click on **...** next to its name), as it is shown on the screenshot below:



Default retentions are used by manual archiving/manual restoring of emails directly from the mailbox.

Note: The “+ new” option above the item list is unavailable for the logged on user if the “Add scheduler” permission is not allowed in his role assignment on the tenant.

The “manage access” option allows to grant access permissions on the selected scheduler for a second user. This “manage access” option is available for the logged on administrator if his role assignment contains the **Edit scheduler – All allowed** permission on the tenant. Read more in [Managing access to contentACCESS objects](#).

Storages

(Email Archive → Settings → Storages button;

File Archive → Settings → Storages button;

SharePoint Archive → Settings → Storages button;

Custom plugins → General → Storages button)

For storage configurations, open the **Storages** page (navigate to  **Storages** button on your ribbon). The storages configured on this page can be selected as a destination for the processed binaries when configuring a certain contentACCESS job. contentACCESS supports **Disk** storage (most frequently used type), **H&S Hybrid Store**, **Perceptive**, **Datengut** storage etc. The table of storages is initially empty.



To configure a new storage, click on **+ new** on the **Storages** page. The **Storage repository** window will open. Type in the **Store name** and select a **Store type** from the list. The required storage settings depend on the storage type that you have selected.

Configurations of the most frequently used storage types will be detailed in the following sections of this chapter:

✓ **Disk** store type

This store type is used if the user would like to store the binaries on a single local or remote disk. This is the most frequently used store type from the types listed above. After this store type has been selected, fill in the **Path** (the target destination for the binaries) and enter credentials if required.

The user also has the possibility to decide if he wants to use the **Compression function**. With checking this checkbox, all files larger than 4 kilobytes will be compressed, except of already compressed file formats such as JPG, MP3 etc. This feature may slow down the store functionality, but on the other hand it will spare storage space.

It is also possible to enable SnapLock for disk store. To do this, check the **Enable SnapLock** checkbox – thanks to this the storage system can prevent deletion of the files until the specified retention is expired. This feature can be used for storage systems which support this function, for example NetApp.

If you wish to keep only one copy of the physical file in the store, check the **Use single instancing** checkbox.

To enhance the storage security, it is possible to store files in encrypted form in the disk storage by checking the **Use file encryption** checkbox. This way the files will be encrypted (using the AES encryption algorithm) and stored in one go. The encryption key must be stored in case of database failure, without it the stored files will be unreadable. Download it by clicking on the **Download** link in this section. If the user tries to save storage configuration without downloading the encryption key, system will warn about this.

tacatest:3333 says

Please download the encryption key and store on a safe place before finishing the configuration.

OK

Note: The file encryption option may be slowing down the storage functionality, both for archive and retrieve.



Under **Database settings** select a **Database connection**. This configuration will play an important role when using the [Storage replication plugin](#). **We recommend NOT to change the already configured database that the disk storage uses** (however, it can be changed using the “Change” button if it is needed).

We also advise to verify the connection using the **Test** button. **The test is checking if the right credentials have been specified, and if the connection with the database has been established.**

Storage repository ✕

Storage settings

Store name:

Store type:

Path:

Use explicit credentials:

Username:

Password:

Confirm password:

Compression:
(Compresses all files larger than 4KB except already compressed formats like JPG, AVI, MP3 etc. This feature might slow down the store functionality, but can spare storage space.)

Enable SnapLock:

Use single instancing:
Only one instance of the physical file will be present on the store.

Use file encryption:
 Files will be stored in encrypted form.
[Download](#) the encryption key and store on a safe place.

Database connection: ✔

When using Disk store type, please consider requirements for data deduplication. Data deduplication finds and removes duplication within data on a volume while ensuring that the data remains correct and complete. This makes it possible to store more file data in less space on the volume. Deduplication is not supported on:

- ✓ System or boot volumes;
- ✓ Remote mapped or remote mounted drives;



- ✓ Cluster shared volume file system (CSVFS) for non-VDI workloads or any workloads on Windows Server 2012;
- ✓ Files approaching or larger than 1 TB in size;
- ✓ Volumes approaching or larger than 64 TB in size.

What to consider before a previously configured disk storage is changed?

In some cases, it may happen that the administrator needs to move the already configured storage to a new location (e.g. if "C" disk got full and the storage should be moved to disk "D"). In this case, the following steps must be executed to ensure an access to the already archived data and to continue with archiving the new data:

1. Stop all running jobs!!!
2. Move your old storage location manually into the new storage location (e.g. the folder of "C" disk into a new location on "D" disk);
3. Open the **Storages** page on the contentACCESS Central Administration ribbon, locate your old storage in the list and double click on it to open the **Storage repository** window for that storage;
4. In the **Storage repository** window specify the new storage path (where you moved your old storage location);

Storage repository ✕

Storage settings

Store name:

Store type:

Path: !

Use explicit credentials:

Username:

Password:

Confirm password:

Compression:
(Compresses all files larger than 4KB except already compressed formats like JPG, AVI, MP3 etc. This feature might slow down the store functionality, but can spare storage space.)

Enable SnapLock:

Use single instancing:
Only one instance of the physical file will be present on the store.

Use file encryption:
 Files will be stored in encrypted form.
[Download](#) the encryption key and store on a safe place.

Database connection: ✔

These settings will ensure, that the archive and restore jobs will automatically use this new storage path. The administrator will not be required to change the storage settings on the jobs' configuration page, too. The new value will be automatically used by the jobs, where the "old" storage was already configured.

✓ HybridStore

contentACCESS supports the connection with the Hybrid Store. This connection allows contentACCESS to connect to any third-party storage that is supported by this store type. If you want to store the binaries in the Hybrid Store, select it from the **Store type** dropdown list and specify the required connection settings. The following storage settings are required:

Store name: optional name for the Hybrid Store that contentACCESS will use

Store type: HybridStore

Server name: the server, where the Hybrid Store is installed



Binding: **http** – universal protocol

net.tcp –can be used only in case that the Hybrid Store and contentACCESS are in the same domain

net.pipe – the fastest and **recommended protocol**; can be used only in case that the Hybrid Store and contentACCESS are installed on the same machine

Use secure connection: Check this option to allow a secure connection with the Hybrid Store. The communication will be secured by a Windows authentication (the contentACCESS service user will be used).

Hybrid store tenant: Click on “Load” to load the list of available tenants based on your Hybrid Store configurations and select the one that should be applied. There are some requirements to load the tenants:

- NET.TCP or NET.PIPE connection must be used (on HTTP the loading is not supported)
- the contentACCESS service user must be a local system administrator on the HybridStore machine

If the tenants are not loaded, then the user needs to enter the HybridStore tenant ID (GUID) manually.

Scheme: Click on “Load” to load the available Hybrid Store schemes and select the one that should be applied. If Hybrid Store uses secure connection and the option is not checked in the dialog, the schemes will not be loaded.

Database settings: Select here an already created database that contentACCESS will use to store the necessary data. It is **NOT recommended to change** the already configured database that the Hybrid store uses. However, it can be changed using the “Change” button if it is really necessary.

It is recommended to verify the database connection using the “Test” button at the bottom of the dialog.

Storage repository
✕

Storage settings

Store name:

Store type:

Server name:

Binding: http
 net.tcp
 net.pipe

Use secure connection:

Hybrid store tenant:

Scheme:

Database connection:

✓ Datengut

This storage type is currently used when synchronizing emails in multiple mailboxes. For more information please refer to [Email synchronizer plugin](#).

After this store type has been selected in **Storage settings**, name your storage. contentACCESS will use this name to display the storage on the **Storages** page. Further configure the following sections in the dialog:

Connection configuration: necessary settings to establish a connection with the Datengut storage

- **Endpoint URL:** Datengut service URL
- **Api key:** optional setting, any value can be entered here
- **Email archive default folder id:** during the archiving process Datengut storage saves the data into a specific storage folder; the ID of this folder must be set here

User credentials: set the Username and Password that can be used to connect to the storage

Plugin configuration: The email synchronizer job(s) that are already created in **Custom plugins** → **General** → **Jobs** will be listed in the dropdown list. Select from the dropdown list the **Email synchronizer job** that will collect the metadata of the archived emails in a queue. This job is used to synchronize the email message categories in multiple mailboxes based on the metadata that are saved into its queue.

Note: For more information refer to chapter [Email synchronizer plugin](#).

Database settings: select an already created database that Datengut storage will use to store the necessary data

Storage repository
✕

Storage settings

Store name:

Store type:

Connection configuration

Endpoint URL:

Api key:

Email archive default folder id:

User credentials

Username:

Password:

Plugin configuration

Plugin job:

Database settings

Database connection: ✔

✓ Perceptive

After this store type has been selected, name your storage. contentACCESS will use this name for the given storage on the **Storages** page. The user is further required to specify the following connection parameters:

- **Server name:** the server name where the storage is installed
- **CC library path:** path on which the Classic Connector jar files can be reached, e.g. *C:\Program Files\SAPERION\Application\scr\scr-classicconnector\lib*
- **JAVA_HOME:** JAVA home directory must be set depending on the application bitness, x64 or x86, e.g.: *c:\Program Files\Java\jre1.8.0_66*



- **Tenant:** in case of non-multitenant system this field is blank, otherwise the Perceptive tenant should be specified
- **Login type:** “INDEX”, “ADMIN” or “ELM” can be used, the recommended type is “INDEX”
- **Authentication:** choose the applicable authentication from the dropdown list; the recommended is “UserName”
- **User, Password:** specify the applicable user and credentials to be applied for the connection with the storage
- **DDC:** the DDC name where the files will be packed

✓ Kendox storage

Kendox storage can be used for various operations like email and file archiving, SharePoint archiving and publishing data into SharePoint libraries and custom lists as well. In the **Storage repository** window, select the **Kendox** store type, name your storage and configure the connection as follows:

Connection configuration section:

Endpoint URL: Kendox service URL



Culture: The names of folders, properties will be shown in the language specified here. The language can be a country-code (e.g. de) or both the language and country-code (e.g. de-CH).

Authentication configuration:

Username and password: Specify the Username and Password that can be applied to connect to the storage.

Use empty password: Use empty password. If this is checked, in a password empty string is saved. Otherwise - if the username was not changed - the old password is saved.

Default folder path: During the archiving or publishing process the data will be saved/published from the folder, which is specified in the path.

Mobile Web Client URL: This configuration option needs to be set only in case that the storage is used in a [SharePoint Publishing job](#), and the job is configured to create custom lists with links pointing to the source documents. The URL must be the Kendox Mobile Web Client's URL, where the published documents can be accessed. The URL is used to generate the retrieve URL of the published document.

Import template configuration:

In the archiving process, import template is used to map the metadata between the source document and the newly created document in the Kendox store. Click the "Get available import templates" button to get the available import templates. This import template is only used if the target folder doesn't have any default import template, otherwise it is ignored.

Storage repository

Storage settings

Store name:

Store type:

Connection configuration

Endpoint URL:

Culture:

Authentication configuration

Username:

Use empty password:

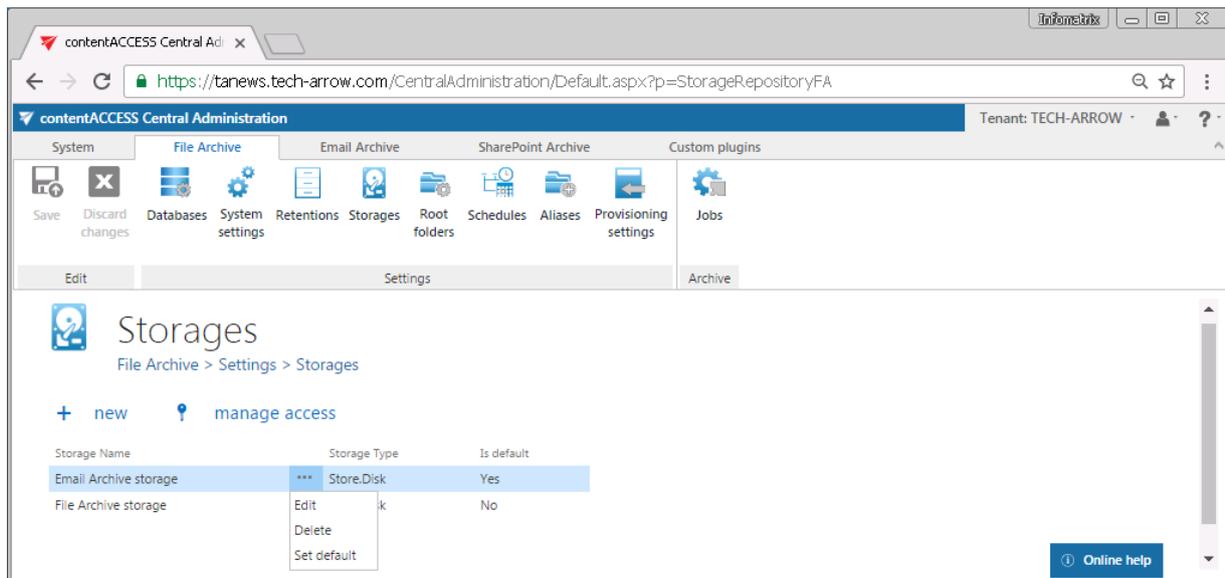
Password:

Default folder path:

Mobile Web Client URL:

Import template configuration

From the given storage's context menu, on the **Storages** page, you can modify (Edit/Delete/Set default) the storage settings by clicking on ellipsis (...). The configurations set in the **Storage repository** window can be viewed in the grid.



Note: The “+ new” option above the item list is unavailable for the logged on user, if the “Add repository items” permission on the tenant is not allowed in his role assignment.

The “manage access” option allows to grant access permissions on the selected storage for a second user. This “manage access” option is available for the logged on administrator, if his role assignment contains the Edit repository items – All allowed permission on the tenant. Read more in [Managing access to contentACCESS objects](#).

✓ Azure storage

Azure Storage is a cloud storage solution. It also provides the storage foundation for Azure Virtual Machines and is accessible from anywhere in the world, from any type of application and any type of device. Azure storage is using blob store to store its metadata.

In case of the user having/using a [German cloud](#) (dedicated and isolated Microsoft Azure version for Germany), the Azure storage account name must contain the **.core.cloudapi.de** suffix. This is displayed in Azure configuration, when the user creates the storage.

Storage repository



Storage settings

Store name:

Store type:

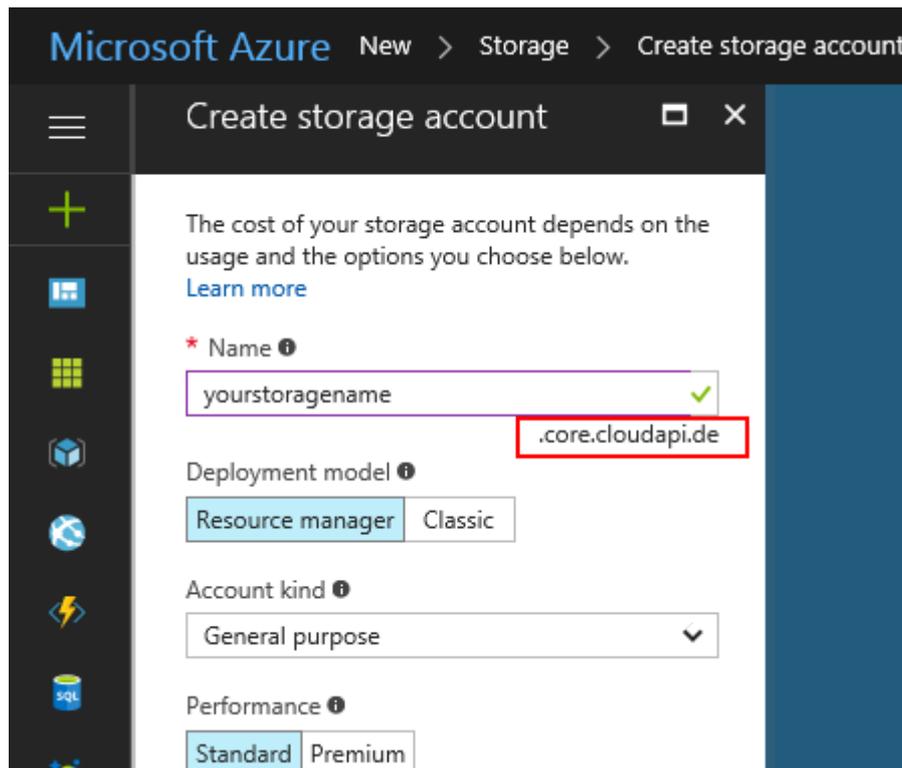
Account:

Key:

Compression:
(Compresses all files larger than 4KB except already compressed formats like JPG, AVI, MP3 etc. This feature might slow down the store functionality, but can spare storage space.)

Use single instancing:
Only one instance of the physical file will be present on the store.

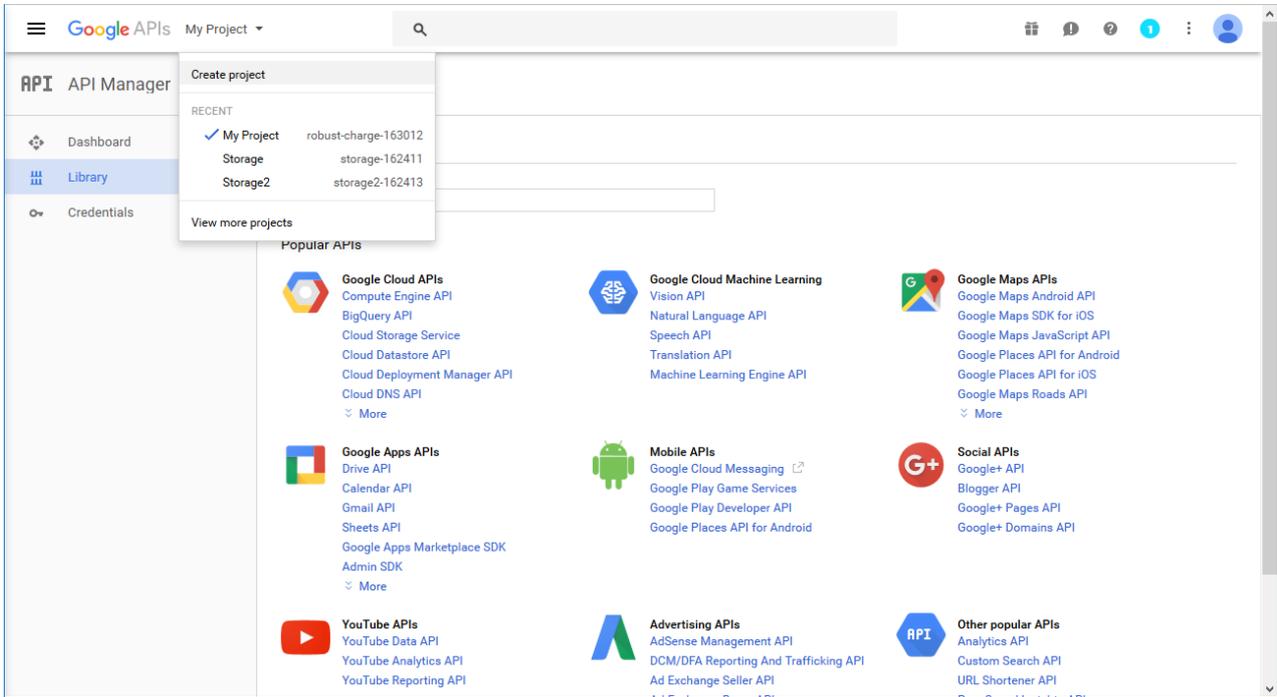
Database connection:



Google drive storage

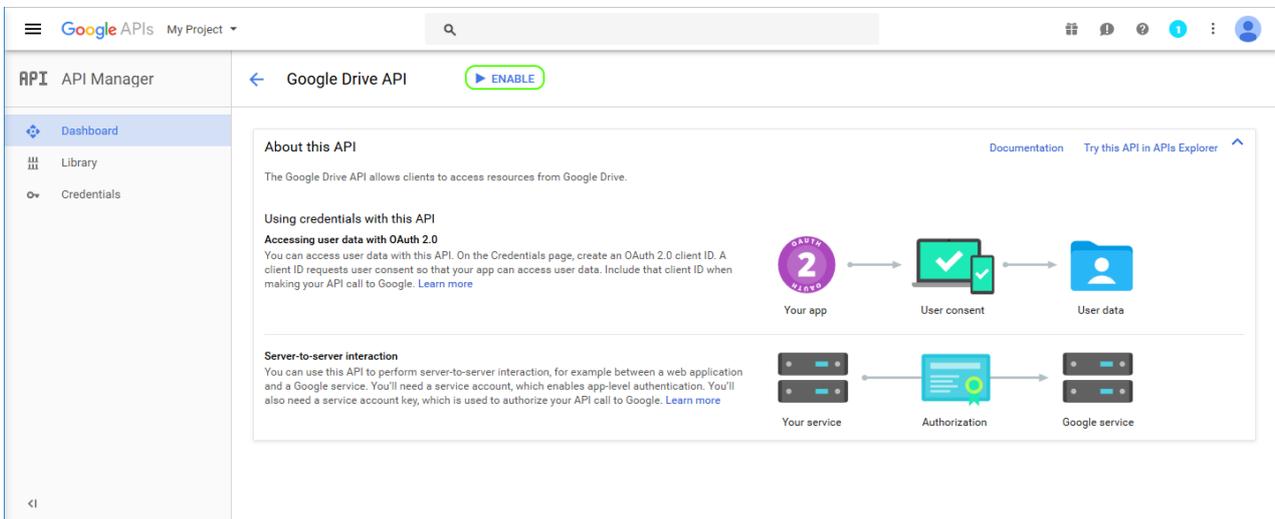
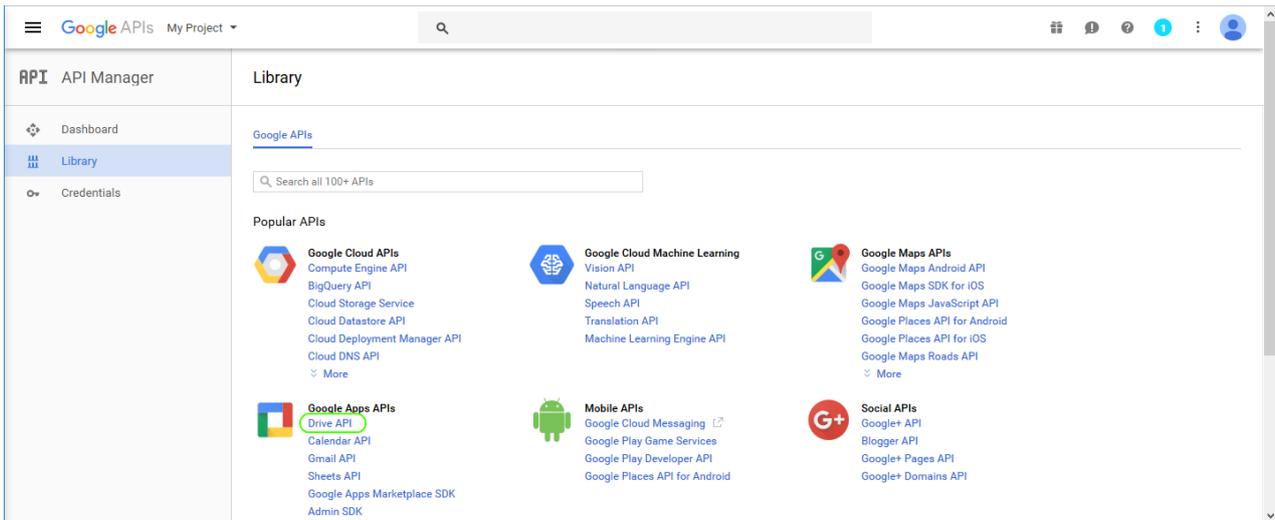
1. Create a Google account.
2. Log on to <https://console.developers.google.com> with your Google account.

3. Create new project with an arbitrary name:



4. Enable the required (Drive) API for this service:







5. Create service account and credentials:

1 Find out what kind of credentials you need

We'll help you set up the correct credentials
If you wish you can skip this step and create an [API key](#), [client ID](#), or [service account](#)

Which API are you using?
Determines what kind of credentials you need.
Google Drive API

Where will you be calling the API from?
Determines which settings you'll need to configure.
Other non-UI (e.g. cron job, daemon)

What data will you be accessing?

- User data
Access data belonging to a Google user, with their permission
- Application data**
Access data belonging to your own application

Are you using Google App Engine or Google Compute Engine?

- Yes, I'm using one or both
- No, I'm not using them**

[What credentials do I need?](#)

2 Get your credentials

[Cancel](#)

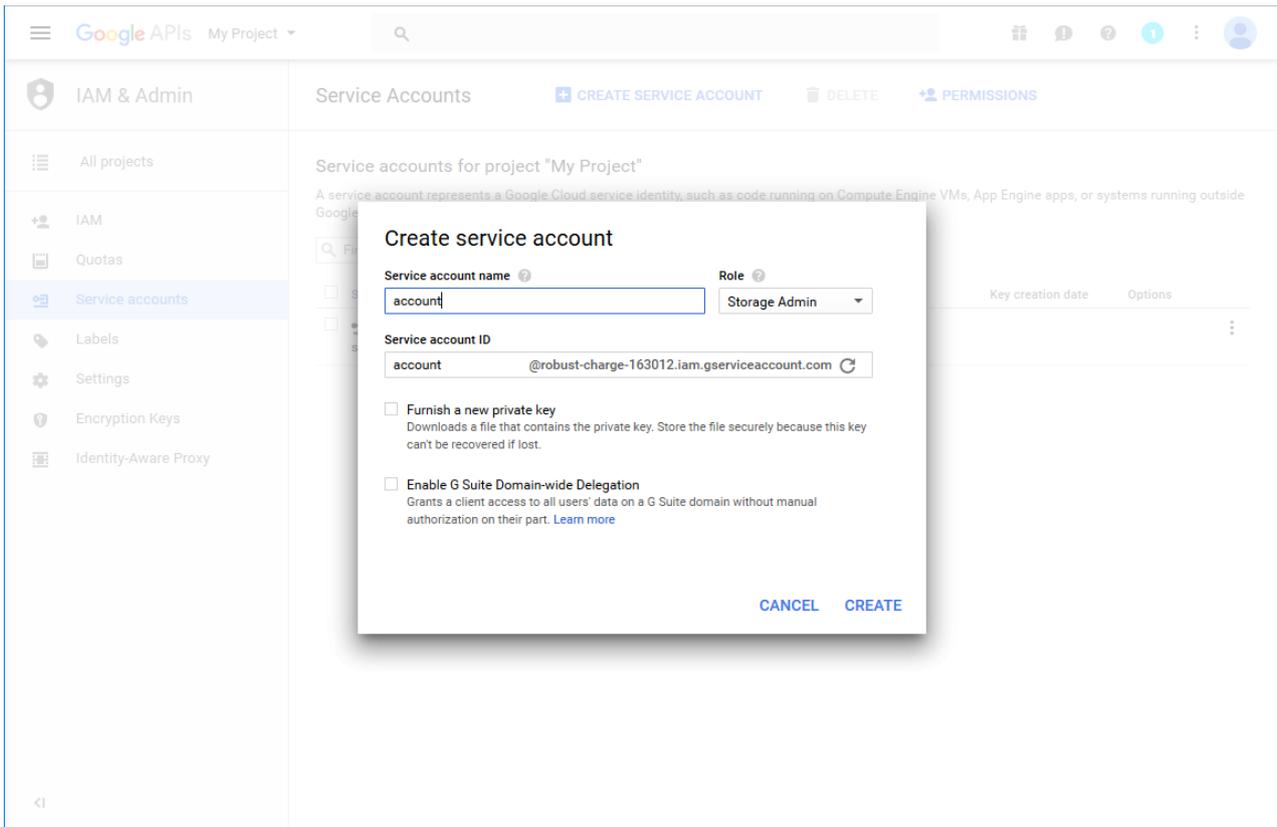
Service Accounts [+ CREATE SERVICE ACCOUNT](#) [DELETE](#) [PERMISSIONS](#)

Service accounts for project "My Project"

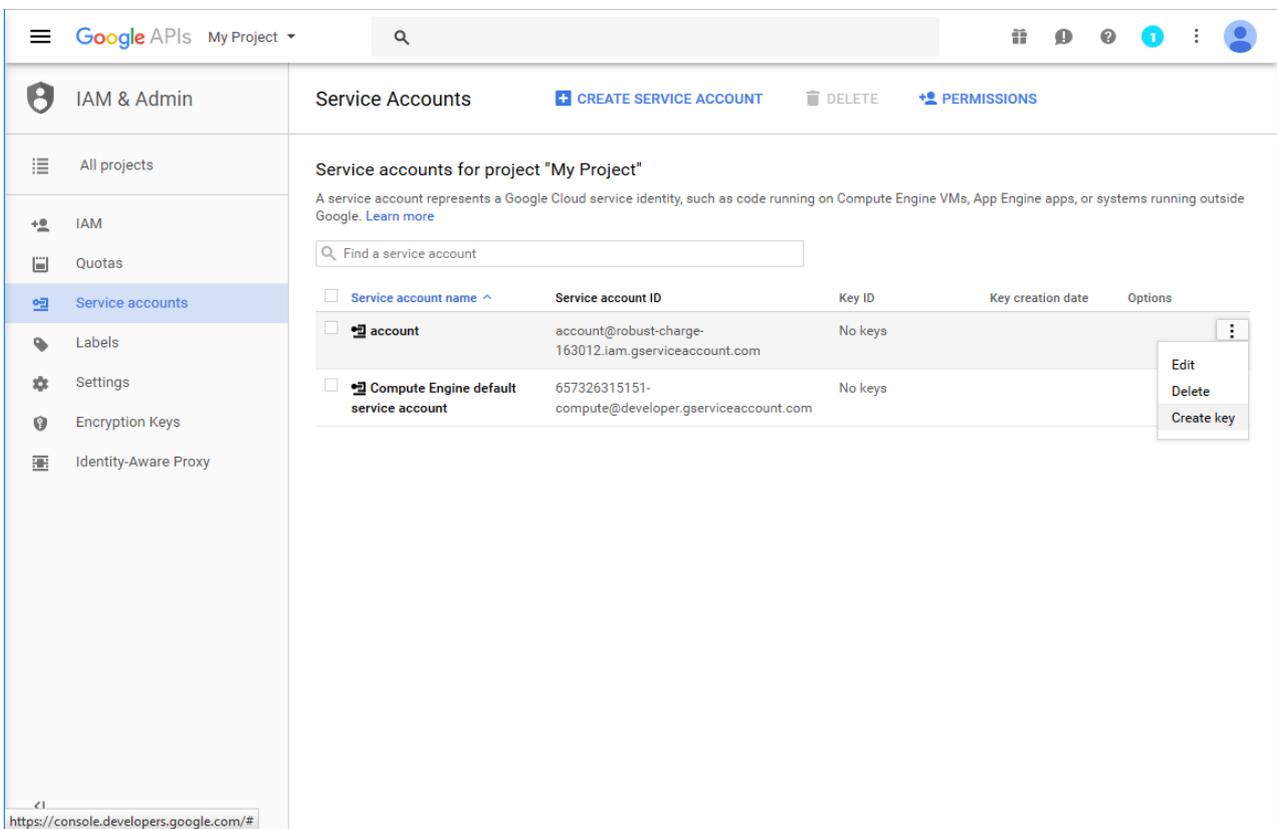
A service account represents a Google Cloud service identity, such as code running on Compute Engine VMs, App Engine apps, or systems running outside Google. [Learn more](#)

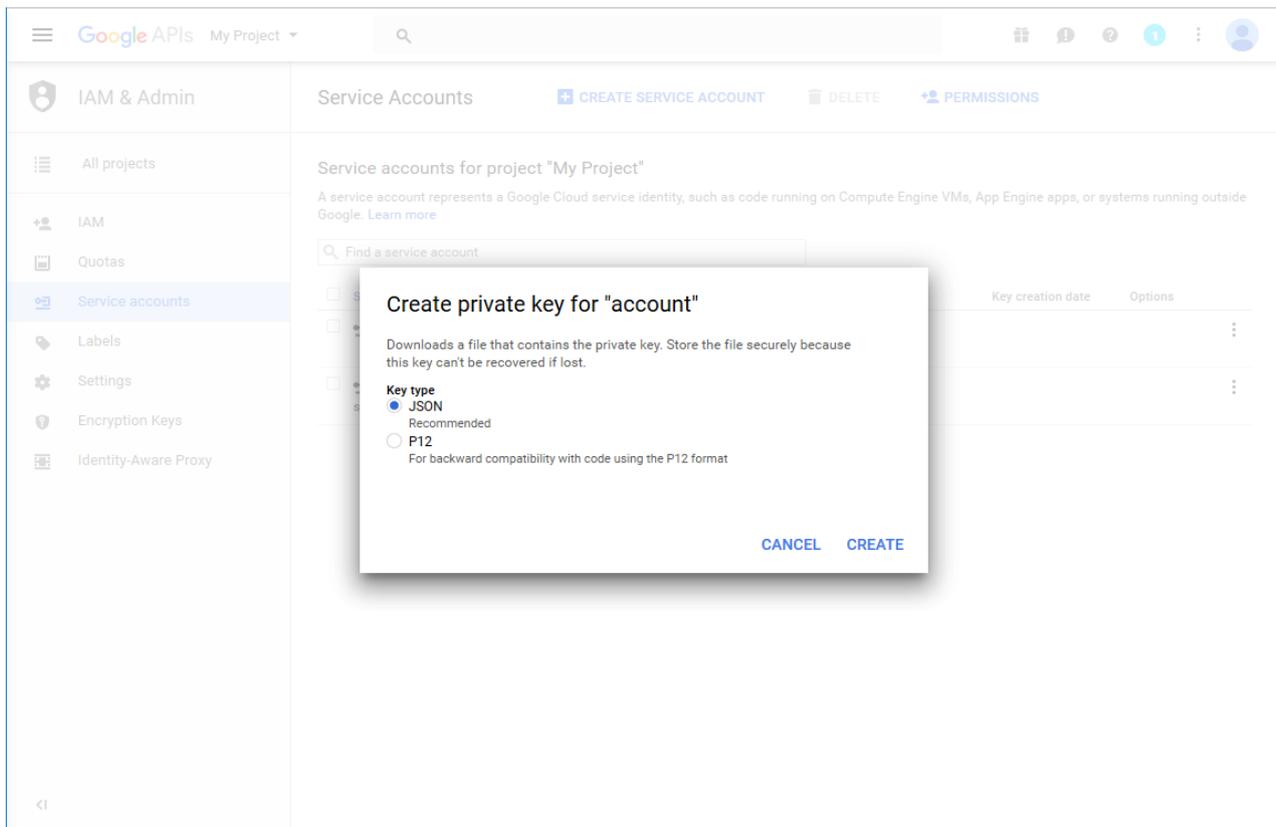
Find a service account

<input type="checkbox"/> Service account name ^	Service account ID	Key ID	Key creation date	Options
<input type="checkbox"/> Compute Engine default service account	657326315151-compute@developer.gserviceaccount.com	No keys		



Create key for your service account:

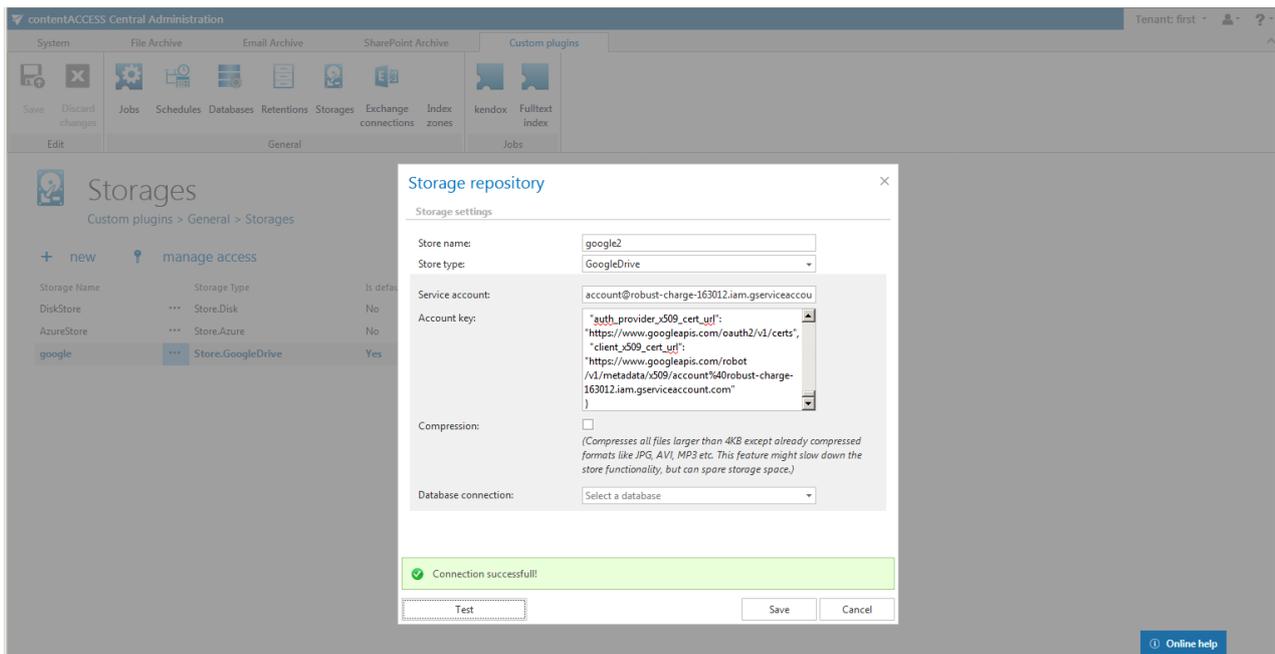




Download the key and store it securely. It will be required for calling Google API from the storage provider.

6. Create and configure a Google Drive storage in contentACCESS

Create new storage of type “GoogleDrive”. Take the name of the created service account (in this case account@robust-charge-163012.iam.gserviceaccount.com, you can take it also from the downloaded JSON key file) and paste it to “Service account” box. Paste the whole JSON key file into “Account key” box. If the connection test succeeds, the storage is configured and ready for use.



Important: You will not be able to see the archived files in your Google Drive web UI as they were stored under different account. If there is be such a requirement, we should set an explicit sharing rights on stored files.

A quote from [here](#):

“A few important things to note about a service account is that it is not you. Just because you created the service account does not mean that it has access to the files you have stored in your Google drive. You can take the service account email address and give it access to a directory on your Google drive. It will then be allowed to upload to that directory, but you won’t have access to the files. You will need to complete a second step and give yourself personally permission to access those files by updating or patching the file permissions.”

Amazon S3

The Amazon S3 store supports any type of cloud storage if it’s using the Amazon S3 interface.

The store connects to the endpoint that you select for a specific service. In contentACCESS, the service endpoints for Amazon Simple Storage Service and Alibaba Cloud Object Storage, which also uses Amazon S3 interface, are preconfigured. If you want to use a different cloud service, which supports Amazon S3



interface, it is possible to select **Custom service URL** for the service and then enter a custom URL for that service endpoint.

The service authentication identifier is fixed for Amazon S3 and Alibaba, it's not possible to change it. However if you are using custom endpoint URL, you can enter the identifier here. This identifier is used in the authentication request.

The version specifies which communication version to use for the service endpoint (the service version is specified by the endpoint service). If you are using Amazon S3, you can use Service Version 2 or 4, but Alibaba supports only Version 2 at this moment. The **Access Key** and **Secret Access Key** are used to authenticate the caller by the cloud service. These keys are provided by the cloud storage service.

This store type also supports compression and single instancing, which can save you a lot of space.

Storage repository ✕

Storage settings

Store name:

Store type:

Service:

Endpoint:

Service authentication identifier:

Service version:

Access key:

Secret access key:

Compression:
(Compresses all files larger than 4KB except already compressed formats like JPG, AVI, MP3 etc. This feature might slow down the store functionality, but can spare storage space.)

Use single instancing:
Only one instance of the physical file will be present on the store.

Database connection: ✔

Screenshot 01 – configuring Amazon S3 storage with Amazon S3 service URL (preconfigured by contentACCESS)

Storage repository ✕

Storage settings

Store name:

Store type:

Service:

Custom endpoint url:

Service authentication identifier:

Service version:

Access key:

Secret access key:

Compression:
(Compresses all files larger than 4KB except already compressed formats like JPG, AVI, MP3 etc. This feature might slow down the store functionality, but can spare storage space.)

Use single instancing:
Only one instance of the physical file will be present on the store.

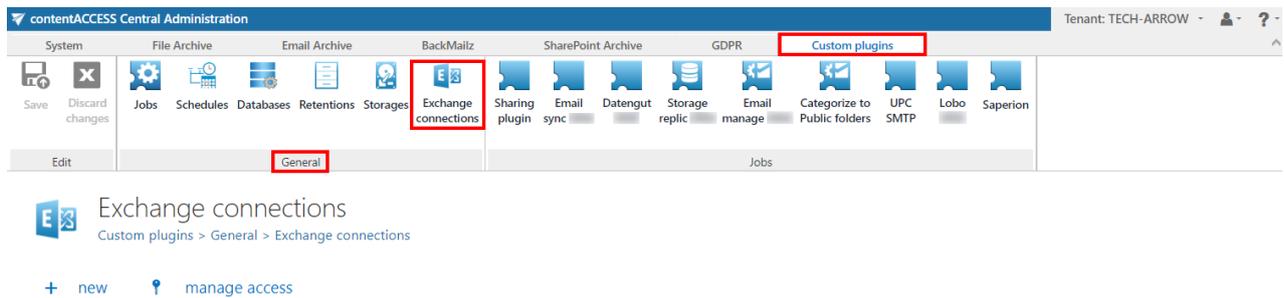
Database connection: ✔

Screenshot 02 – configuring Amazon S3 storage with custom service URL

Exchange connections

During the configuration of Exchange-based jobs it is obligatory to set the Exchange server connections, where the mailbox to be crawled is located. The Exchange connections can be configured on the following pages of the Central Administration:

- In case of Custom jobs on the **Exchange connections** page (Custom plugins → General group →  Exchange connections button).



Here select option **+ new** and specify the necessary data in the **Exchange connection repository** window.

Note: The “+ new” option above the item list is unavailable for the logged on user if the “Add repository items” permission on the tenant is not allowed in his role assignment.

The “manage access” option allows to grant access permissions on the selected Exchange connection for a second user. This “manage access” option is available for the logged on administrator, if his role assignment contains the Edit repository items – All allowed permission on the tenant. Read more in [Managing access to contentACCESS objects](#).

By the custom plugins it is possible to configure multiple Exchange connections.

- In case of Email Archive jobs on the **System settings** page (**Email Archive** → **Settings** → **System settings**, under **EWS settings** section).

Note: In case the user who has MFA enabled is also Admin for email archiving, the user must use the app password instead of the regular password in the **Email archive** -> **System settings** -> **EWS settings**.

In case of Email Archive, either an Exchange Online O365 or On-premise Exchange server connection can be configured within one tenant. If there are multiple Exchange server versions used in a company (e.g. both Exchange server 2013 and Exchange server 2010), always define the highest Exchange server version in the **System settings**. Read more in chapter **Mixed Exchange environments**.

contentACCESS Central Administration

System File Archive **Email Archive** BackMailz

Save Discard changes Databases **System settings** Provisioning settings Retentions Shortcut configuration Storages Sche

Edit **Settings**

Database settings

Database connection: MNEtestDB

Exchange connection settings

Exchange server type: Exchange Online (O365)

Region: Global

Exchange server interface version: Exchange 2016 or higher

EWS Url: https://outlook.office365.com/EWS/Exchange.asmx

Use impersonation:

EWS authentication mode: Basic

PowerShell Url: https://ps.outlook.com/PowerShell

PowerShell auth: Basic

Max connection count: 2

Ignore SSL errors:

Keep connection alive:

Use explicit credentials:

User name: administrator@ta.internal
administrator@domain.com or domain\administrator

Password:

If you are configuring EWS connection to custom plugins, a **Connection name** must be also entered into the **Exchange connection repository** dialog. Under **Exchange server type** and **Exchange server version** select the type and version of the server, which is used by your email provider. Then enter the **EWS URL**.

Region: In case of the user having/using a [German cloud](#) (dedicated and isolated Microsoft Azure version for Germany), **Germany** must be selected in the **Region** dropdown list.



In case that the predefined settings for **O365** and **PowerShell** don't match your expectation and/or needs, it is possible to select the **Custom** option from the **Region** dropdown list and specify your own values.

Exchange Connection repository ×

EWS settings

Connection name:	<input type="text" value="Exchange CR"/>	
Exchange server type:	<input type="text" value="Exchange Online (O365)"/>	
Region:	<input type="text" value="Custom"/>	
Exchange server version:	<input type="text" value="Exchange 2016 or higher"/>	←
EWS Url:	<input type="text" value="https://outlook.office365.com/EWS/Exchange.asmx"/>	←
Use impersonation:	<input type="checkbox"/>	
EWS authentication mode:	<input type="text" value="Basic"/>	
PowerShell Url: <input type="text" value="https://ps.outlook.com/PowerShell"/> ←		

Use impersonation: By default, this checkbox is turned off. If it is turned on, **Impersonation** will be used instead of **delegation** (more information in [this](#) section). Impersonation allows the superuser account to impersonate any other user's account and access their mailboxes.

Note: Only accounts with the **ApplicationImpersonation** role can use impersonation. For more information about how to configure impersonation for your account, please check [this](#) page.

If the O365 user has “desktopless” license, his account **can't be used** for impersonation. The problem is that EWS access is disabled for such user (he is unable to connect to EWS).

EWS authentication mode: Select one **EWS authentication mode** from the dropdown list. There are 2 options: **Basic** and **Modern**. **Basic** authentication method was used by default in previous versions and it wasn't possible to select another authentication type. **Modern** authentication is more secure and complex and requires the app to be registered on **Azure portal**. How to register it and gain the necessary **IDs** and **client secret** is described in [this](#) section.



EWS authentication mode:	Modern
OAuth application ID:	72c73
OAuth tenant ID:	4b0e
OAuth client secret:

Specify the **PowerShell URL** and select the **PowerShell authentication** type. **PowerShell** can use **Basic** and **Modern** authentication type, too.

The **EWS** and **PowerShell** data must be requested from the email provider you are using (the configuration properties are the same for On-premise and Hosted Exchange).

Under **Max. connection count** option the user may define the number of parallel connections that will be maintained by the system when connecting to PowerShell. It is also possible to disregard any SSL errors with checking the **Ignore SSL errors** checkbox.

Keep connection alive: If it is turned on, then the connection between contentACCESS and the Exchange server is cached, which increases the performance. If the Exchange is load balanced, some requests can land on another Exchange and therefore cause errors in contentACCESS. In these cases, unchecking the keep alive option will destroy the connection after each request and will rebuild it on the next request. The recommended settings of “keep alive” option are as follows:

- If you are communicating with **one Exchange server: turn it on** to increase the performance
- If you have a **load balanced Exchange environment** and there are **communication problems** with the Exchange: it is recommended to **turn it off**

If you want to use an explicit user for Exchange connection, check **Use explicit credentials** and enter the **User name** and **Password**. It is also possible to log in under service-credentials. In this case the **Use explicit credentials** option must be unchecked. Run a test connection via **Test** button. Do not forget to save the changes.



Exchange Connection repository ✕

EWS settings

Connection name:	<input type="text" value="Exchange CR"/>
Exchange server type:	<input type="text" value="Exchange Online (O365)"/>
Region:	<input type="text" value="Global"/>
Exchange server version:	<input type="text" value="Exchange 2016 or higher"/>
EWS Url:	<input type="text" value="https://outlook.office365.com/EWS/Exchange.asmx"/>
Use impersonation:	<input type="checkbox"/>
EWS authentication mode:	<input type="text" value="Modern"/>
OAuth application ID:	<input type="text" value="72c73"/>
OAuth tenant ID:	<input type="text" value="4b0ed"/>
OAuth client secret:	<input type="text" value="....."/>
PowerShell Url:	<input type="text" value="https://ps.outlook.com/PowerShell"/>
PowerShell auth:	<input type="text" value="Basic"/>
Max connection count:	<input type="text" value="2"/>
Ignore SSL errors:	<input type="checkbox"/>
Keep connection alive:	<input checked="" type="checkbox"/>
Use explicit credentials:	<input checked="" type="checkbox"/>
User name:	<input type="text" value="companyadmin@tech-arrow.com"/>
Password:	<input type="text" value="....."/>
Confirm password:	<input type="text"/>

Screenshot: Exchange connection configurations for custom jobs



Exchange connection settings

Exchange server type:	Exchange Online (O365) ▼
Region:	Global ▼
Exchange server interface version:	Exchange 2016 or higher ▼
EWS Url:	<input type="text" value="https://outlook.office365.com/EWS/Exchange.asmx"/>
Use impersonation:	<input checked="" type="checkbox"/>
EWS authentication mode:	Basic ▼
PowerShell Url:	<input type="text" value="https://ps.outlook.com/PowerShell"/>
PowerShell auth:	Basic ▼
Max connection count:	2 ▲▼
Ignore SSL errors:	<input checked="" type="checkbox"/>
Keep connection alive:	<input checked="" type="checkbox"/>
Use explicit credentials:	<input checked="" type="checkbox"/>
User name:	<input type="text" value="administrator@ta.internal"/> administrator@domain.com or domain\administrator
Password:	<input type="password" value="....."/>
<input type="button" value="Test connection"/>	

Exchange connection configuration in Email Archive system

Important!!! The user set under *Exchange connections* must have a full access to the mailbox(es) that he/she would like to archive (in case of not using **Impersonation**). Provisioning job requires to have “View-Only Organization Management” right on the Exchange. Roles **Org Custom Apps**, **Org Marketplace Apps** and **User Options** must be assigned for the EWS user on the [Email archive System settings](#) page, in section **EWS settings**, if [Mail app](#) will be also used. These roles enable an administrator to install and manage custom apps for the organization (read more about the roles [here](#)).

Note: To speed up the email archiving processes, TECH-ARROW has implemented MAPI protocol for communication with the Exchange server. MAPI can be used only in case that the customer has an on premise Exchange server (Exchange 2013 or earlier), and uses contentACCESS with Email archive licence (for custom plugins MAPI cannot be selected). MAPI can be selected only on the email archive/restore/recovery job’s configuration page. By default, contentACCESS uses EWS settings to connect to the Exchange. **Some functionalities still require EWS settings. For this reason, it is a must to configure EWS settings as well.**



Exchange performance settings – turning off the Exchange throttling policies

Throttling is a mechanism of Exchange Server to distribute the Exchange resources evenly between the users. It gives every user the chance to access their emails. The users are limited for example to send max 5 emails in a minute. If this limit is reached, the user is throttled, forcing the user to wait a minute until a new mail can be sent.

The archiving user requires more resources: it needs to access multiple mailboxes, process multiple messages. The standard throttling policy is not suitable for the archiving user (superuser).

If you are experiencing problems that may be caused by these policies, you can turn them off. The commands below are turning off any limitations for the archiving user, allowing to use as many Exchange resources as needed.

Exchange 2013

```
New-ThrottlingPolicy -Name CAPolicy -ThrottlingPolicyScope Organization

Set-ThrottlingPolicy CAPolicy -RCAMaxConcurrency Unlimited -EWSMaxConcurrency
Unlimited -EWSMaxSubscriptions Unlimited -CPAMaxConcurrency Unlimited -
EwsCutoffBalance Unlimited -EwsMaxBurst Unlimited -EwsRechargeRate Unlimited

Set-Mailbox "Administrator" -ThrottlingPolicy CAPolicy
```

Exchange 2010

```
New-ThrottlingPolicy -Name CAPolicy

Set-ThrottlingPolicy CAPolicy -RCAMaxConcurrency $null -RCAPercentTimeInAD
$null -RCAPercentTimeInCAS $null -RCAPercentTimeInMailboxRPC $null -
EWSMaxConcurrency $null -EWSPercentTimeInAD $null -EWSPercentTimeInCAS $null -
EWSPercentTimeInMailboxRPC $null -EWSMaxSubscriptions $null -
EWSFastSearchTimeoutInSeconds $null -EWSFindCountLimit $null -
CPAMaxConcurrency $null -CPAPercentTimeInCAS $null -CPAPercentTimeInMailboxRPC
$null -CPUStartPercent $null

Set-Mailbox "Administrator" -ThrottlingPolicy CAPolicy
```

There are 3 commands which must be run in PowerShell to apply the throttling for the superuser:



#1 New-ThrottlingPolicy

Creates a new policy, gives a name to the policy. It is created with default values.

#2 Set-ThrottlingPolicy

This changes the parameters of the policy – turning off any throttling for the contentACCESS user.

This list should be discussed with the customer, they might not allow all these options. This is a matter of support.

#3 Set-Mailbox

Assign the policy to the user.

The whole association can be verified by running this command: **Get-Mailbox "Administrator" | fl ThrottlingPolicy**

Mixed Exchange environments in the Email Archive system

contentACCESS is supporting a wide range of Exchange Servers, starting from Exchange 2007 SP1 up to Exchange 2016. A company can simultaneously use multiple versions of Exchange servers. In such cases contentACCESS needs to process/archive the mailboxes hosted by all these Exchange servers (versions).

There are some rules for how to configure the archiving in a mixed Exchange environment. This chapter will provide you with a quick overview about these configurations.

In this use case, we have the following Exchange versions in our domain:

- **Exchange server 2013**
- **Exchange server 2010**

We would like to archive some mailboxes – the part of them are hosted by Exchange 2013, but some of them are still on Exchange 2010. This is a common scenario when the company is already migrating mailboxes from a lower to a higher Exchange version. As first step, it is recommended to sort the mailboxes



to be migrated into Exchange groups – these groups will be later provisioned by the Email Archive Provisioning job into the contentACCESS Address book.

Further we continue with the **EWS (Exchange Web Services) settings**. In Central Administration, open the **System settings** page (**Email Archive** tab → **Settings** group → **System settings**). Go to section **EWS settings**. Select your server type (On-premise) and select the highest Exchange server version that is used – in this use case **Exchange 2013**. Set the necessary parameters described earlier, test the connection and save your settings.

The screenshot shows the 'contentACCESS Central Administration' interface. The 'Email Archive' tab is selected, and the 'System settings' page is open. The 'Database settings' section shows 'Database connection' set to 'MNEstestDB'. The 'EWS settings' section is highlighted with a red box and contains the following configuration:

- Exchange server type: On-premise
- Exchange server interface version: Exchange 2013 (indicated by a red arrow)
- EWS Url: https://tadc01.ta.internal/EWS/Exchange.asmx
- PowerShell Url: https://tadc01.ta.internal/PowerShell
- PowerShell auth: Basic
- Max connection count: 2
- Ignore SSL errors:
- Keep connection alive:
- Use impersonation:
- Use explicit credentials
- User name: administrator@ta.internal
administrator@domain.com or domain/administrator
- Password: [Empty field]
- Confirm password: [Empty field]

A 'Test connection' button is located at the bottom of the EWS settings section. An 'Online help' button is visible in the bottom right corner of the page.

Now we need to set the **Exchange groups to be archived in the Email Archive Provisioning settings**. Open the **Provisioning settings** page (**Email Archive** → **Settings** → **Provisioning settings**).

Select the **specific Exchange groups** (or Exchange servers including all groups) that should be archived and start the provisioning job to synchronize them to the contentACCESS Address book.



The screenshot shows the 'Provisioning Settings' page in contentACCESS Central Administration. The breadcrumb trail is 'Email Archive > Settings > Provisioning settings'. The 'Scheduled in' dropdown is set to 'Every night'. Under 'Notification settings', 'Send when' is 'Never' and the 'Recipient list' contains 'john.doe@example.com,peter.white@example.com'. The 'Exchange servers' section has a 'select' button. Below it, a table shows 'Name' and 'Server DN' columns with 'No data to display'. The 'Exchange groups' section, indicated by a red arrow, has a 'select' button and an '+ add' button. Below it, another table shows 'Name' and 'Group DN' columns with 'No data to display'. An 'Online help' button is in the bottom right corner.

After the provisioning job has finished the task, both Exchange versions (2010 & 2013) and the provisioned Exchange groups will be in the Address book (exchange 2013 not shown on the screenshot):

The screenshot shows the 'View address book' page. The breadcrumb trail is 'Email Archive > Archive > View address book'. The 'Servers' tab is highlighted in red. Below the tabs, there are links for 'import servers manually' and '+ add server manually'. A table lists server information:

Name	EWS version	Create contentWEB access	Associate with role	Server DN
TADC01	*** Exchange2010_SP2	No		/o=First Organization/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Configuration/cn=Servers/cn=TADC

Page 1 of 1 (1 items) is shown at the bottom.



View address book

Email Archive > Archive > View address book

Mailboxes Public folders **Groups** Servers

import groups manually + add group manually

Name	Create contentWEB access	Associate with role	Active	Group DN	
	***	Yes	Inherited	Yes	CN=...,CN=Users,DC=ta,DC=internal
	***	Yes	Inherited	Yes	CN=...,CN=Users,DC=ta,DC=internal
	***	Yes	Inherited	Yes	CN=...,CN=Users,DC=ta,DC=internal
TECH-ARROW	***	No		Yes	

Page 1 of 1 (4 items) 1

The context menu of the Exchange servers allows to change the server settings:



View address book

Email Archive > Archive > View address book

Mailboxes Public folders Groups **Servers**

import servers manually + add server manually

Name	EWS version	Create contentWEB access	Associate with role	Server DN
TADC01	Exchange2010_SP2	No		/o=First Organization/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Configuration/cn=Servers/cn=TADC

Page 1 of 1 (1 items) 1

- Automatically create contentWEB user
- Do not create contentWEB user
- Change server settings**

By clicking this option, the “Server configuration” window opens, which allows to change the EWS version for the server and to define a custom EWS URL for the server. “For the server” means that all mailboxes belonging to the server will use those values. This is useful in mixed environments (example: 2010 and 2013 in one domain – you can define different URL for both servers!).

Server configuration

EWS version:

Custom EWS Url:

The combo box allows you to select the option “Not specified”. This is a way to reset your custom settings – and use the global one (see the **System settings** page – **EWS server interface version**).



Server configuration ✕

EWS version:

Custom EWS Url:

- Exchange 2007 SP1
- Exchange 2010
- Exchange 2010 SP1**
- Exchange 2010 SP2
- Exchange 2013 or higher

Cancel

Importing contentACCESS configurations from files

contentACCESS allows to import data from files in the following available file formats: CSV, XML, Tab delimited files and Space delimited files. This simplifies adding of huge amount of data to different configuration sections in contentACCESS instead of entering each entry manually. There's an option to set if we want to overwrite the existing items, update or skip them. The user may also download a sample file to check if the file that he wishes to import contains all necessary information (columns) for the given configuration section. Column names are displayed in the sample file if the **"First row is header"** option is turned on in the respective importer dialog.

Important!!! When importing **Email archive** and **Email restore** configuration sections, it is highly recommended to define the mailbox folders to be imported with wildcards (e.g. %INBOX%). Wildcards ensure, that the given mailbox folder (e.g. the "INBOX" folder) will be processed regardless of the language settings of the mailbox. This is important mainly for companies who archive mailboxes using different languages.

Since the backslash "\ " is used as path separator, it can't be used in folder name. If you want to include or exclude a folder which contains backslash in its name, enter it with "_|_" instead of "\ ".

After browsing the file to be uploaded and configuring the importer, the file can be uploaded. After the initial upload, the file's columns can be mapped to the importable entry's fields by dragging the column headers. When the mapping is finished, the newly imported entries will be added to the configuration section.

contentACCESS allows to **import the folders to be archived/restored/recovered/excluded**:

1. to **File archive**, **File restore**, **File recovery** jobs

The import option is available on the respective job configuration page, under sections "Folders to process" and "Exclude folders":

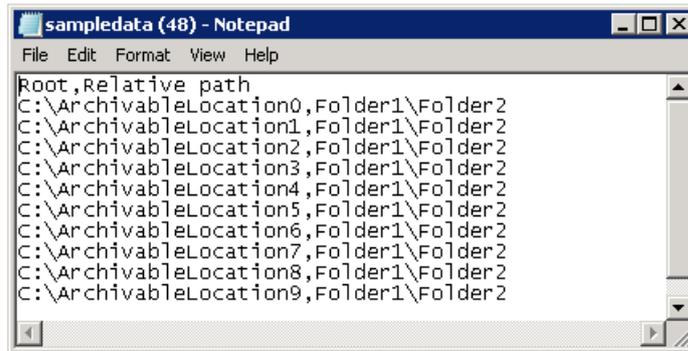


An importable file with **Folders to process** contains the following rows:

- **Root – mandatory**

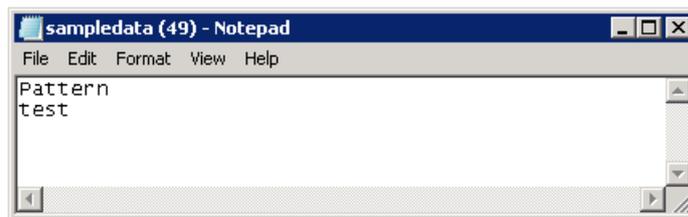
- **Relative path – nullable**

Example in case of a CSV file:



An importable file with **Folders to exclude** contains the

- **Exclude pattern**, e.g. if folder called “test” needs to be excluded, the CSV will look like this:



2. to **Email archive, Email restore, Email recovery jobs**

The import option is available on the respective job configuration page, under section “Exclude folders” and “Exclude addresses”:



An importable file with **Excludable folders** contains the

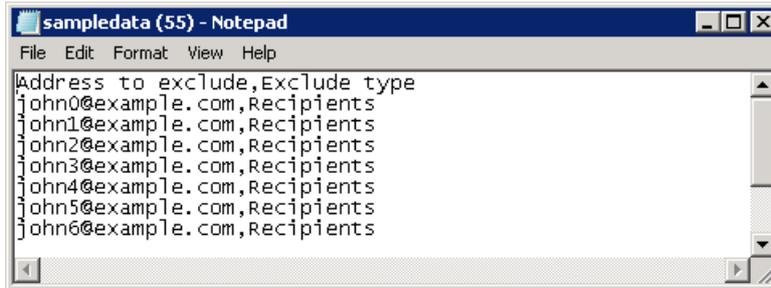
- **Exclude pattern**, e.g. if mailbox folder called “test” needs to be excluded, the CSV will look like this:



An importable file with **Exclude addresses** contains the:

- **Address(es) to include**
- **Exclude type(s)** – Sender/Recipients/All

Example in case of a CSV file:



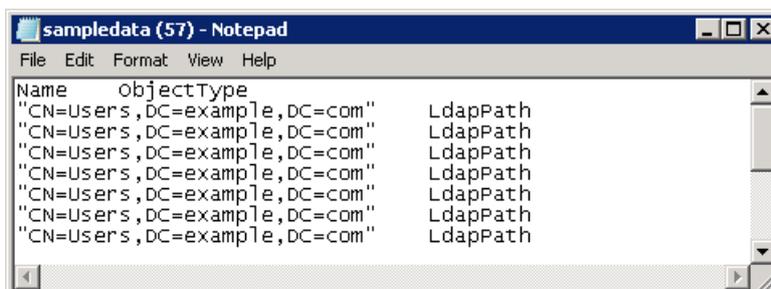
3. File Archive provisioning job (used to synchronize the users in the Active Directory with contentACCESS) also uses this feature to import the objects to be provisioned:



The importable file must include the:

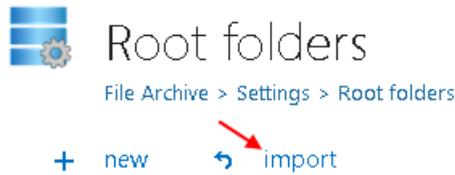
- **Name**
- **Object type**

Example in case of a Tab delimited file:



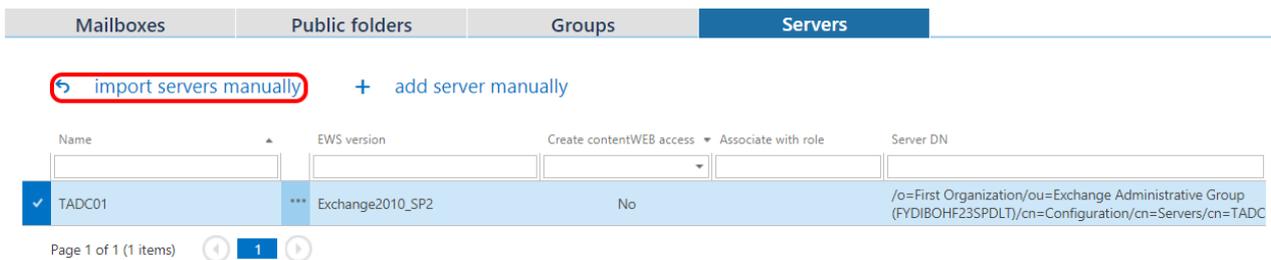


4. The **root folders** used in File Archive may be also imported into contentACCESS from files (read more [here](#)):



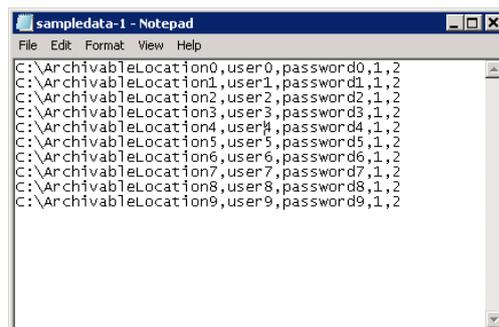
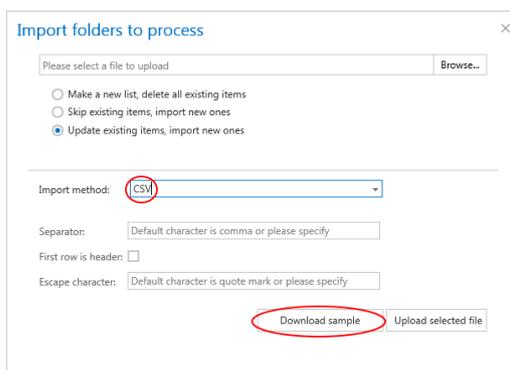
5. Servers/groups/mailboxes can be imported from files to the contentACCESS Address book using options **“Import servers manually”**/ **“Import groups manually”**/ **“Import mailboxes manually”** on the respective tabs as well (read more [here](#)):

View address book
Email Archive > Archive > View address book

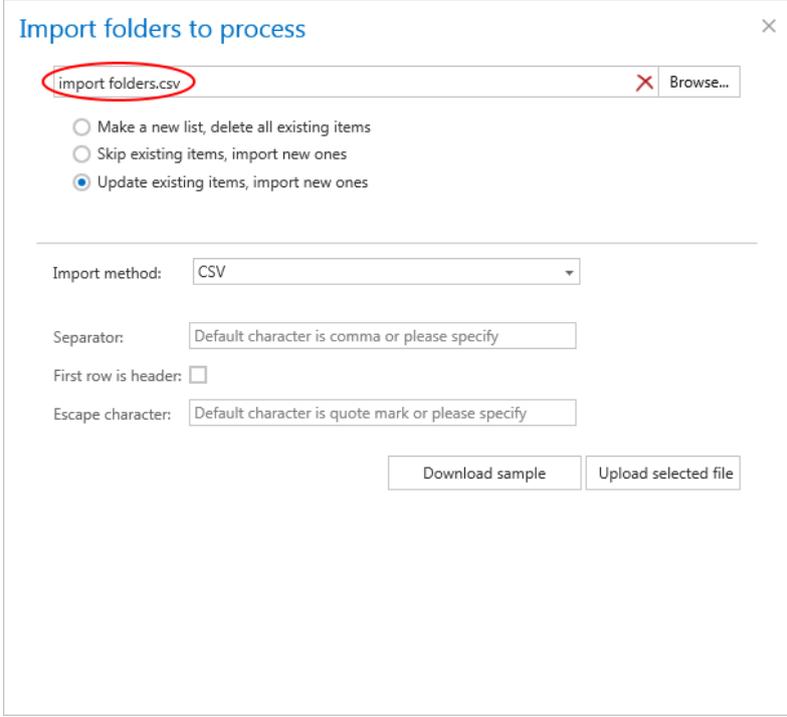


To import a file follow these steps:

- Click the **import** button on the respective configuration page. The importer dialog opens.
- From the **Import method** dropdown list select an import method to be applied (in our case CSV) and download a sample file using the **Download sample** option. Based on the sample file, prepare the file to import and verify if your prepared file contains all necessary information for the respective configuration section.



- Further click “**Browse**” and locate the file to be imported. (On the picture below we have selected a CSV file.)



Import folders to process ×

import folders.csv × Browse...

Make a new list, delete all existing items
 Skip existing items, import new ones
 Update existing items, import new ones

Import method:

Separator:

First row is header:

Escape character:

- **Further specify how the selected file should be imported.** Choose one from the 3 available options (the available options are configuration specific, not all are available by all configurations):

Make a new list, delete all existing items – select this option to create a completely new list of items; any already set items will be deleted

Skip existing items, import new ones – select this option to add the new items from the list; the already configured items will be skipped

Update existing items, import new ones – this option is available for importing root folders from files; it can be applied if the password has been changed and should be updated

- **Depending on the selected import method, the user is further required to specify the following settings:**

In case of CSV:

Specify the CSV separator (in our case it is a comma). If the first row in the CSV file is a header, mark the respective checkbox. Further specify the escape character, if such exists in your CSV file (in our case quotation marks)



Import method:*

Separator:

First row is header:

Escape character:

In case of Tab delimited file

If the first row of the file is a header, mark the respective checkbox. Further specify the escape character, if such exists in the file.

Import method:*

Settings

First row is header:

Escape character:

In case of Space delimited file

If the first row of the file is a header, mark the respective checkbox. Further specify the escape character, if such exists in the file.

Import method:*

Settings

First row is header:

Escape character:*

In case that the file to be imported is an XML, no further settings are required.

Import method:*

- Click **Upload selected file** to upload the file with the desired items.

Import folders to process ✕

Import method:

Path	User	Password	Store Id	Database Id
C:\TestPath1	user1	password1	1	2
C:\TestPath2	user2	password2	1	2
C:\TestPath3	user3	password3	1	2
C:\TestPath4	user4	password4	1	2
C:\TestPath5	user5	password5	1	2
C:\TestPath6	user6	password6	1	2
C:\TestPath7	user7	password7	1	2
C:\TestPath8	user8	password8	1	2
C:\TestPath9	user9	password9	1	2
C:\TestPath10	user10	password10	1	2

- Click **“OK”**. The list of imported items will be added to the respective section.

In a file containing multiple columns the user may specify, which column should be imported. Simply drag and drop the column header (on the picture below the **Database ID** header) over the respective column that should be imported.



Import folders to process

Import method: CSV

Path	User	Password	Store Id	Database Id		
C:\TestPath1	user1	password1	1	2	3	4
C:\TestPath2	user2	password2	1	2	3	4
C:\TestPath3	user3	password3	1	2	3	4
C:\TestPath4	user4	password4	1	2	3	4
C:\TestPath5	user5	password5	1	2	3	4
C:\TestPath6	user6	password6	1	2	3	4
C:\TestPath7	user7	password7	1	2	3	4
C:\TestPath8	user8	password8	1	2	3	4
C:\TestPath9	user9	password9	1	2	3	4
C:\TestPath10	user10	password10	1	2	3	4

OK
Cancel

Manual import of Exchange servers/groups/mailboxes to the contentACCESS Address book

As already mentioned, contentACCESS allows to import servers, groups and mailboxes manually into the address book from CSV or XML files as well. The importing options are available on the **View address book** page of the Central administration (**Email Archive** tab → **Archive** group → **View address book** button) on the respective tabs.



View address book

Email Archive > Archive > View address book

Mailboxes
Public folders
Groups
Servers

↶ import servers manually
+ add server manually

Name	EWS version	Create contentWEB access	Associate with role	Server DN
TADC01	*** Exchange2010_SP2	No		/o=First Organization/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Configuration/cn=Servers/cn=TADC

Page 1 of 1 (1 items) ⏪ 1 ⏩

How can you import?

In all cases you need to create a CSV file as in the sample file – select the import method in the dialog and click **Show sample**:

Import servers manually ✕

Please select a file to upload Browse...

Skip existing items, import new ones

Import method: CSV ▾

Settings

Separator: Default character is comma or please specify

First row is header:

Escape character: Default character is quotation mark or please specif

Show sample Import...

Nullable fields are not mandatory and can be left empty.

A row in the **CSV file with SERVERS** contains:

- **Name**
- **Server DN - nullable**
- **Settings – nullable**

Example: **Office365,Office365,settings**

If you do not have some of the nullable data, no problem. Simple add an empty character instead of them,

e.g.: server: **Office365,,,**

```

sampledata (17) - Notepad
File Edit Format View Help
Name,Server DN,Settings
name0,/o=TECH-ARROW/ou=Exchange Administrative Group (AAAAAAAAAAAAA)/cn=Configuration/cn=Servers/cn=EX2k10,"Version 14.3 (Build 123.4);Mailbox, ClientAccess, HubTransport"
name1,/o=TECH-ARROW/ou=Exchange Administrative Group (AAAAAAAAAAAAA)/cn=Configuration/cn=Servers/cn=EX2k10,"Version 14.3 (Build 123.4);Mailbox, ClientAccess, HubTransport"
name2,/o=TECH-ARROW/ou=Exchange Administrative Group (AAAAAAAAAAAAA)/cn=Configuration/cn=Servers/cn=EX2k10,"Version 14.3 (Build 123.4);Mailbox, ClientAccess, HubTransport"
name3,/o=TECH-ARROW/ou=Exchange Administrative Group (AAAAAAAAAAAAA)/cn=Configuration/cn=Servers/cn=EX2k10,"Version 14.3 (Build 123.4);Mailbox, ClientAccess, HubTransport"
name4,/o=TECH-ARROW/ou=Exchange Administrative Group (AAAAAAAAAAAAA)/cn=Configuration/cn=Servers/cn=EX2k10,"Version 14.3 (Build 123.4);Mailbox, ClientAccess, HubTransport"
name5,/o=TECH-ARROW/ou=Exchange Administrative Group (AAAAAAAAAAAAA)/cn=Configuration/cn=Servers/cn=EX2k10,"Version 14.3 (Build 123.4);Mailbox, ClientAccess, HubTransport"
name6,/o=TECH-ARROW/ou=Exchange Administrative Group (AAAAAAAAAAAAA)/cn=Configuration/cn=Servers/cn=EX2k10,"Version 14.3 (Build 123.4);Mailbox, ClientAccess, HubTransport"
name7,/o=TECH-ARROW/ou=Exchange Administrative Group (AAAAAAAAAAAAA)/cn=Configuration/cn=Servers/cn=EX2k10,"Version 14.3 (Build 123.4);Mailbox, ClientAccess, HubTransport"
name8,/o=TECH-ARROW/ou=Exchange Administrative Group (AAAAAAAAAAAAA)/cn=Configuration/cn=Servers/cn=EX2k10,"Version 14.3 (Build 123.4);Mailbox, ClientAccess, HubTransport"
name9,/o=TECH-ARROW/ou=Exchange Administrative Group (AAAAAAAAAAAAA)/cn=Configuration/cn=Servers/cn=EX2k10,"Version 14.3 (Build 123.4);Mailbox, ClientAccess, HubTransport"
    
```

A row in the **csv file with GROUPS** contains:

- **Name**
- **Display name – nullable**
- **Sid**
- **Distinguished name - nullable**
- **When changed**
- **When created**



```

sampledata (10) - Notepad
File Edit Format View Help
Name,display name,sid,distinguished name,when changed,when created
name0,display name0,S-1-1-11-1111111111-11111111-11111111-1111,"CN=TestUsers,OU=Resource Groups,OU=TECH,DC=tech,DC=Internal",1900-01-01 00:00:00.000,2016-03-11 09:36:34.000
name1,display name1,S-1-1-11-1111111111-11111111-11111111-1111,"CN=TestUsers,OU=Resource Groups,OU=TECH,DC=tech,DC=Internal",1900-01-01 00:00:00.000,2016-03-11 09:36:34.000
name2,display name2,S-1-1-11-1111111111-11111111-11111111-1111,"CN=TestUsers,OU=Resource Groups,OU=TECH,DC=tech,DC=Internal",1900-01-01 00:00:00.000,2016-03-11 09:36:34.000
name3,display name3,S-1-1-11-1111111111-11111111-11111111-1111,"CN=TestUsers,OU=Resource Groups,OU=TECH,DC=tech,DC=Internal",1900-01-01 00:00:00.000,2016-03-11 09:36:34.000
name4,display name4,S-1-1-11-1111111111-11111111-11111111-1111,"CN=TestUsers,OU=Resource Groups,OU=TECH,DC=tech,DC=Internal",1900-01-01 00:00:00.000,2016-03-11 09:36:34.000
name5,display name5,S-1-1-11-1111111111-11111111-11111111-1111,"CN=TestUsers,OU=Resource Groups,OU=TECH,DC=tech,DC=Internal",1900-01-01 00:00:00.000,2016-03-11 09:36:34.000
name6,display name6,S-1-1-11-1111111111-11111111-11111111-1111,"CN=TestUsers,OU=Resource Groups,OU=TECH,DC=tech,DC=Internal",1900-01-01 00:00:00.000,2016-03-11 09:36:34.000
name7,display name7,S-1-1-11-1111111111-11111111-11111111-1111,"CN=TestUsers,OU=Resource Groups,OU=TECH,DC=tech,DC=Internal",1900-01-01 00:00:00.000,2016-03-11 09:36:34.000
name8,display name8,S-1-1-11-1111111111-11111111-11111111-1111,"CN=TestUsers,OU=Resource Groups,OU=TECH,DC=tech,DC=Internal",1900-01-01 00:00:00.000,2016-03-11 09:36:34.000
name9,display name9,S-1-1-11-1111111111-11111111-11111111-1111,"CN=TestUsers,OU=Resource Groups,OU=TECH,DC=tech,DC=Internal",1900-01-01 00:00:00.000,2016-03-11 09:36:34.000
    
```

A row in the csv file with MAILBOXES contains:

- Name
- Display name- nullable
- MailboxGuid
- User principal name
- Sam account name
- Primary smtp address
- Linked master account- nullable
- Is linked
- Is mailbox enabled
- Is resource
- Is shared
- Quota
- Use database quota defaults
- Archive GUID- nullable
- Email addresses - nullable
- Mailbox DN- nullable
- Recipient type- nullable
- Distinguished name
- When changed
- When created
- Associated user sid

```

sampledata (21) - Notepad
File Edit Format View Help
Name,display name,MailboxGuid,User principal name,Sam account name,Primary smtp address,Linked master account,Is linked,Is mailbox enabled,Is resource,Is shared,Quota,Use database
quota defaults,Archive GUID,Email addresses,Mailbox DN,Recipient type,Distinguished name,When changed,When created,Associated user sid
name 0,display name 0,F0F600A2-30F9-4efc-97cd-F9ec5d69c975,testuser0@testdomain.com,testuser0,tu0@testdomain.com,NT AUTHORITY
\SELF,False,False,False,False,0,True,SMTPT:testuser0@testdomain.com,/o=Tech-Arrow/ou=Exchange Administrative Group
(AAAAAAAAAAAAAAAAAA)/cn=Recipients/cn=aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa,UserMailbox,"CN=Test0,CN=Users,DC=testdomain,DC=com",1900-01-01 00:00:00.000,2016-03-11 09:36:34.000,S-1-
2-21-1218810553-3938697923-1081931466-1090234
name 1,display name 1,F0F600A2-30F9-4efc-97cd-F9ec5d69c975,testuser1@testdomain.com,testuser1,tu1@testdomain.com,NT AUTHORITY
\SELF,False,False,False,False,0,True,SMTPT:testuser1@testdomain.com,/o=Tech-Arrow/ou=Exchange Administrative Group
(AAAAAAAAAAAAAAAAAA)/cn=Recipients/cn=aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa,UserMailbox,"CN=Test1,CN=Users,DC=testdomain,DC=com",1900-01-01 00:00:00.000,2016-03-11 09:36:34.000,S-1-
2-21-1218810553-3938697923-1081931466-1090234
name 2,display name 2,F0F600A2-30F9-4efc-97cd-F9ec5d69c975,testuser2@testdomain.com,testuser2,tu2@testdomain.com,NT AUTHORITY
\SELF,False,False,False,False,0,True,SMTPT:testuser2@testdomain.com,/o=Tech-Arrow/ou=Exchange Administrative Group
(AAAAAAAAAAAAAAAAAA)/cn=Recipients/cn=aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa,UserMailbox,"CN=Test2,CN=Users,DC=testdomain,DC=com",1900-01-01 00:00:00.000,2016-03-11 09:36:34.000,S-1-
2-21-1218810553-3938697923-1081931466-1090234
name 3,display name 3,F0F600A2-30F9-4efc-97cd-F9ec5d69c975,testuser3@testdomain.com,testuser3,tu3@testdomain.com,NT AUTHORITY
\SELF,False,False,False,False,0,True,SMTPT:testuser3@testdomain.com,/o=Tech-Arrow/ou=Exchange Administrative Group
(AAAAAAAAAAAAAAAAAA)/cn=Recipients/cn=aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa,UserMailbox,"CN=Test3,CN=Users,DC=testdomain,DC=com",1900-01-01 00:00:00.000,2016-03-11 09:36:34.000,S-1-
2-21-1218810553-3938697923-1081931466-1090234
name 4,display name 4,F0F600A2-30F9-4efc-97cd-F9ec5d69c975,testuser4@testdomain.com,testuser4,tu4@testdomain.com,NT AUTHORITY
\SELF,False,False,False,False,0,True,SMTPT:testuser4@testdomain.com,/o=Tech-Arrow/ou=Exchange Administrative Group
(AAAAAAAAAAAAAAAAAA)/cn=Recipients/cn=aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa,UserMailbox,"CN=Test4,CN=Users,DC=testdomain,DC=com",1900-01-01 00:00:00.000,2016-03-11 09:36:34.000,S-1-
2-21-1218810553-3938697923-1081931466-1090234
name 5,display name 5,F0F600A2-30F9-4efc-97cd-F9ec5d69c975,testuser5@testdomain.com,testuser5,tu5@testdomain.com,NT AUTHORITY
\SELF,False,False,False,False,0,True,SMTPT:testuser5@testdomain.com,/o=Tech-Arrow/ou=Exchange Administrative Group
(AAAAAAAAAAAAAAAAAA)/cn=Recipients/cn=aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa,UserMailbox,"CN=Test5,CN=Users,DC=testdomain,DC=com",1900-01-01 00:00:00.000,2016-03-11 09:36:34.000,S-1-
2-21-1218810553-3938697923-1081931466-1090234
    
```

When importing mailbox(es), you need to set some common properties from the outside – there is an extra configuration available for the mailboxes import in the **Mailbox options** section of the importer dialog. Only values marked with "*" are mandatory. The mailbox options configurations allow to associate the importable mailboxes to an already provisioned/imported Exchange group, to an archive database and storage.



Import mailboxes manually ✕

Please select a file to upload Browse...

Skip existing items, import new ones

Mailbox options

Server *:	<input type="text"/>
Add mailboxes to group:	<input type="checkbox"/>
Group:	<input type="text"/> <small>Note: Please start to type the group name</small>
Associate with storage:	<input type="text"/>
Associate with email archive database:	<input type="text"/>
Exchange mailbox database *:	<input type="text"/>
Exchange archive database:	<input type="text"/>
Import method:	<input type="text"/> Please select an import method

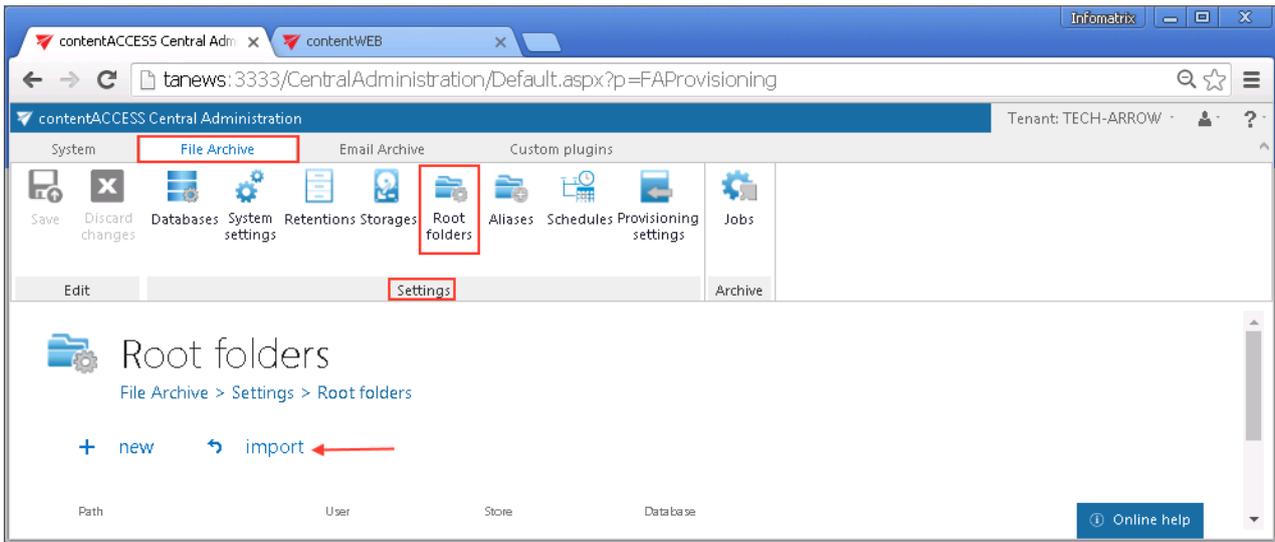
These properties will be set for all the imported mailboxes:

- **Server**
- **Group – nullable if checkbox is not checked**
- **Database – nullable**
- **Storage - nullable**
- **Exchange database**
- **Archive database- nullable**

The importer control uses the [skip existing items](#) method for importing.

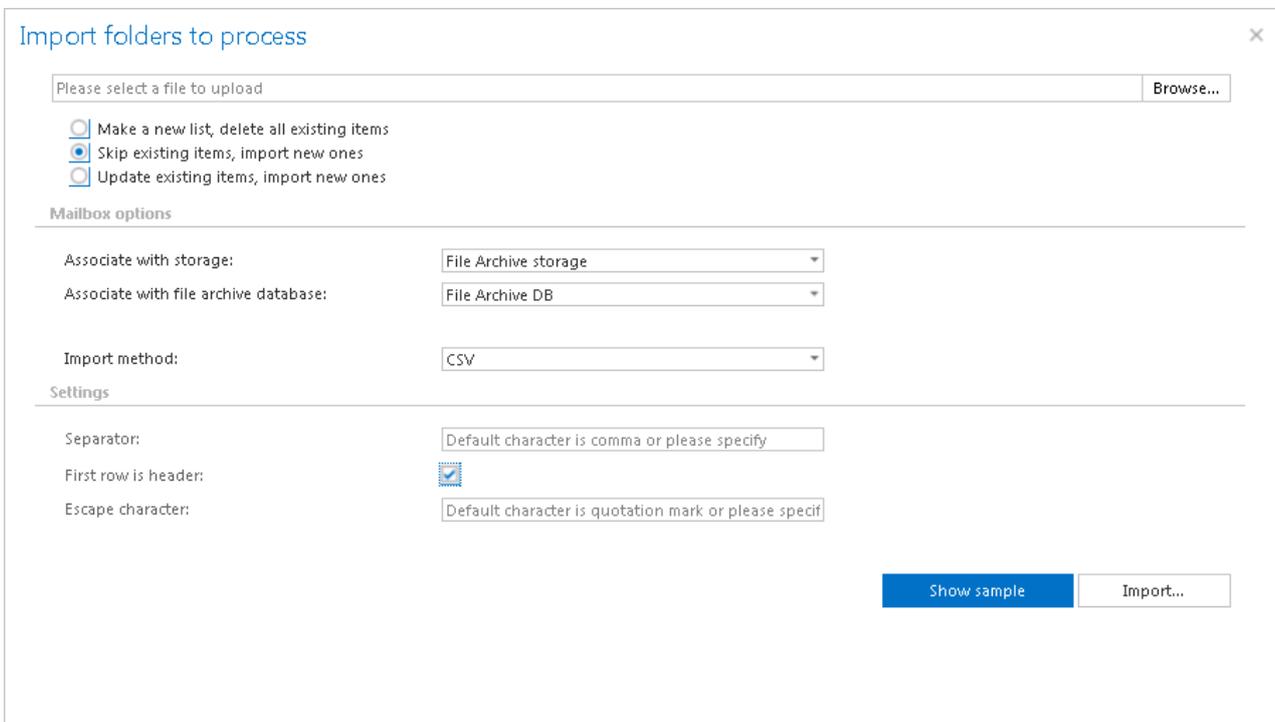
Importing File Archive root folders to be archived

As mentioned already, contentACCESS allows to import root folders to be archived from files. The importing option is available on the **Root folders** page of the Central administration (**File Archive** tab → **Settings** group → **Root folders** button).



How can you import?

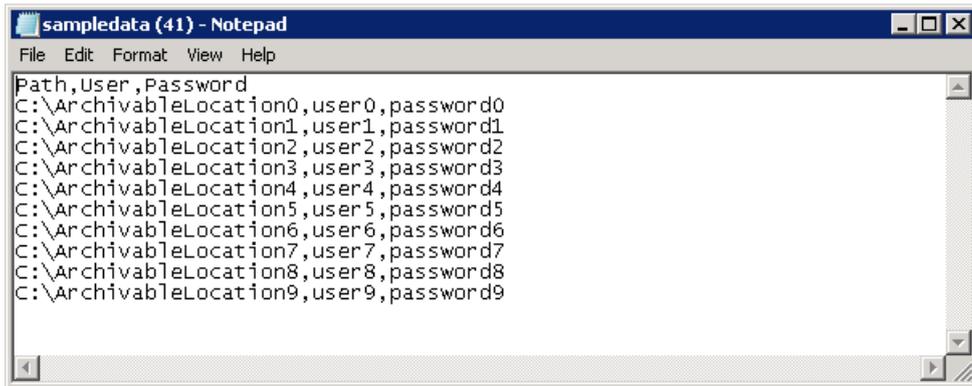
In all cases you need to create a CSV file as in the sample file – a) select the import method in the dialog, b) associate your importable root folder(s) with an archive storage and archive database and c) click **Show sample**:



A row in the CSV file contains:

- **Root folder(s) to be archived**

- **User name**
- **Password**



```
Path,User,Password
C:\ArchivableLocation0,user0,password0
C:\ArchivableLocation1,user1,password1
C:\ArchivableLocation2,user2,password2
C:\ArchivableLocation3,user3,password3
C:\ArchivableLocation4,user4,password4
C:\ArchivableLocation5,user5,password5
C:\ArchivableLocation6,user6,password6
C:\ArchivableLocation7,user7,password7
C:\ArchivableLocation8,user8,password8
C:\ArchivableLocation9,user9,password9
```

Finally browse for your file and import it to the root folders grid.

Note: One importable file can have only one archive database and archive storage associated. If you have multiple roots to be archived and you want to archive them to different archive databases and storages, you need to prepare multiple import files with different database and storage settings and import them into contentACCESS one-by-one.



Creating new jobs in contentACCESS

contentACCESS is a modular product and its functionality is extended with plugins, which are intended to manage certain data management processes. The licensed plugins can be also customized and fitted to ones needs. To achieve this, it is necessary to create **new jobs** from an available plugin.

A new job is created from a type of a built-in plugin, which is characteristic with its own configuration settings (scheduling, retention, database, storage settings etc.). These configurations assign certain data processing tasks to the job. It is possible to create countless jobs from the same type of a plugin. Each of them will have different configurations regarding the database where the processed metadata will be located, the storage where the processed binaries will be stored, the frequency of their running etc.

In contentACCESS, plugins can be categorized into 4 main groups:

- **Email Archive** plugins,
- **File Archive** plugins,
- **SharePoint Archive** plugins,
- and **Custom plugins** (all licensed plugins except of Email Archive and File Archive plugins are accessible here).

To create a new job from any of these plugins, the administrator should open the **Jobs** page and here click on **+ new**.

Note: The “+ new” option (i.e. to create new job) is unavailable for the logged on user if the “Add jobs” permission on the tenant is not allowed in his role assignment.

The “manage access” option allows to grant access permissions on the selected job for a second user. This “manage access” option is available for the logged on administrator if his role assignment contains the Edit jobs – All allowed permission on the tenant. Read more in [Managing access to contentACCESS objects](#).

The **Jobs** page can be opened with navigating to the following button on the Central Administration ribbon:

- **File Archive** → **Archive** → **Jobs** (for the File Archive plugin type);



contentACCESS Central Administration Tenant: Default

System | **File Archive** | Email Archive | SharePoint Archive | Custom plugins

Save | Discard changes | Databases | System settings | Retentions | Storages | Root folders | Schedules | Aliases | Provisioning settings | **Jobs** | Remote agents

Edit | Settings | **Archive**

Jobs

File Archive > Archive > Jobs

+ new refresh disable auto refresh manage access Show all jobs

ID	Display Name	Type	Status	Last Start	Last Duration	Progress	Summary	Next Start	Is active	Cluster node	Running on
6	File archive original	File system archive	Idle	6 days ago	5 seconds	100 %	4 folders processed 26 documents processed (4 newly archived)	Never	Yes	Any available	-
7	File archive shortcut	File system archive	Idle	6 days ago	11 seconds	100 %	3 folders processed 22 documents processed	Never	Yes	Any available	-
8	File archive	File system	Idle	6 days ago	0 seconds	100 %	3 folders processed 22 documents	Never	Yes	Any available	-

[Online help](#)

- **Email Archive → Archive → Jobs** (for the Email Archive plugin type);

contentACCESS Central Administration Tenant: Default

System | File Archive | **Email Archive** | SharePoint Archive | Custom plugins

Save | Discard changes | Databases | System settings | Provisioning settings | Retentions | Shortcut configuration | Storages | Schedules | User experience | View address book | **Jobs** | Legacy data configuration

Edit | Settings | **Archive** | Miscellaneous

Jobs

Email Archive > Archive > Jobs

+ new refresh disable auto refresh manage access Show all jobs

ID	Display Name	Type	Status	Last Start	Last Duration	Progress	Summary	Next Start	Is active	Cluster node	Running on
13	Shortcut synch	Shortcut synchronization	Idle	-	-	-	-	-	Yes	Any available	-
15	TestArchive	Email archive	Idle	-	-	0 %	-	Never	Yes	Any available	-

[Online help](#)



- **SharePoint Archive → Archive → Jobs** (for the SharePoint Archive plugin type)

contentACCESS Central Administration Tenant: Default

System File Archive Email Archive **SharePoint Archive** Custom plugins

Save Discard changes Databases System settings Retentions Storages Root connections Schedules Provisioning settings **Jobs**

Jobs
SharePoint Archive > Archive > Jobs

+ new refresh disable auto refresh manage access Show all jobs

ID	Display Name	Type	Status	Last Start	Last Duration	Progress	Summary	Next Start	Is active	Cluster node	Running on
16	SPArchive	SharePoint archive	Idle	-	-	0 %		Never	Yes	Any available	-

[Online help](#)

- **Custom plugins → General → Jobs** (for the Custom plugin type).

contentACCESS Central Administration Tenant: Default

System File Archive Email Archive SharePoint Archive **Custom plugins**

Save Discard changes **Jobs** Schedules Databases Retentions Storages Exchange connections UPC plugin

Jobs
Custom plugins > General > Jobs

+ new refresh disable auto refresh manage access Show all jobs

ID	Display Name	Type	Status	Last Start	Last Duration	Progress	Summary	Next Start	Is active	Cluster node	Running on
17	UPC plugin	UPC plugin	Idle	-	-	-		-	Yes	Any available	-

[Online help](#)

On the same page, the user may refresh the status information of all jobs. This can be done either manually with the **refresh** button or by enabling/disabling automatic refresh with the **enable/disable auto refresh** button.

How to create new jobs: Open the **Add new job instance** dialog with a click on **+ new** on the **Jobs** page. Select an available plugin from the dropdown list (the list contains only the licensed plugins). Open the **Run**



on **node** dropdown list and select a node from the cluster, where the job should run. If you would not like to specify a node, select **Any available** from the list. Enter a **Display name** for your job. In the same window below you can read a very short description about the selected plugin type. Click on **Add**.

A pop-up window will ask you if you would like to configure the newly created job immediately.

By clicking on **OK**, the Job's configuration page will be automatically loaded. If you would like to configure the job later on, click on **Cancel** in this window. In this case the job will be only added to the list of jobs on the **Jobs** page (but will not run as it is not configured yet).

ID	Display Name	Type	Status	Last Start
13	Shortcut synch	Shortcut synchronization	Idle	-
15	TestArchive	Email archive	Idle	-
18	MNE mailbox	Email archive	Idle	-

Further information about configuring jobs in contentACCESS can be read in the respective subchapters.

Jobs' page, jobs' context menu

The **Jobs** page is accessible with a click on the **Jobs** button of the respective tab in the contentACCESS Central Administration ribbon (**Email Archive** → **Archive** → **Jobs**; **File Archive** → **Archive** → **Jobs**; **Custom plugins** → **General** → **Jobs**). Here you can view the list of all jobs created from a particular plugin type.



Jobs

File Archive > Archive > Jobs

[+ new](#)
[refresh](#)
[disable auto refresh](#)
[manage access](#)

ID	Display Name	Type	Status	Last Start	Last Duration	Progress	Summary	Next Start	Is active	Cluster node	Running on
6	File archive original	File system archive	Idle	6 days ago	5 seconds	100 %	4 folders processed 26 documents processed (4 newly archived)	Never	Yes	Any available	-
7	File archive shortcut	File system archive	Idle	6 days ago	11 seconds	100 %	3 folders processed 22 documents processed	Never	Yes	Any available	-
8	File restore	File system restore	Idle	6 days ago	9 seconds	100 %	3 folders processed 22 documents processed (22 restored)	Never	Yes	Any available	-
9	File recovery	File system recovery	Idle	6 days ago	9 seconds	100 %	1 entities processed 3 folders processed 22 documents processed (9 skipped, 13 recovered)	Never	Yes	Any available	-

The grid contains the following columns. Each instance has an **ID** number, a **Display name** a **Type** and a **Status**. If the job is in *Idle* status, this means that it has completed the task and it is not running.

Next columns hold certain information about the **Last start**, **Last duration** and **Next start** of the job. The **Progress** column informs about the volume of the already processed items, while **Summary** gives a general overview about the processed/skipped/failed items. In **Is active** column it is possible to see if a job is active or if it has been deactivated. Active jobs will run based on the schedule; the data that they are processing are accessible. Inactive (deactivated) jobs are not running (nor can be manually started); the data that they have processed are still accessible. In the **Cluster node** column we can check the node, where the selected job can run. The **Running on** column informs the user about the node, where the job is currently running. On the screenshot above we can see that **EBA's mailbox archive_shortcutting** job can be run on any available node, and is currently running on TANEWS.

ID	Display Name	Type	Status	Last Start	Last Duration	Progress	Summary	Next Start	Is active	Cluster node	Running on
114	EBA's invoice restore	Email restore	Idle	5 weeks ago	3 seconds	100 %	1 mailboxes processed 0 emails processed (1 failed)	-	Yes	TANEWS [192.168.190.63]	-
135	EBA's mailbox archive_shortcutting	Email archive	Running	1 second ago	-	0 %	-	-	Yes	TANEWS [192.168.190.63]	TANEWS [192.168.190.63]
142	ECSO's mailbox recovery	Email recovery	Idle	5 weeks ago	2 minutes	100 %	1 entities processed 47 items processed (42 skipped)	Never	Yes	TANEWS [192.168.190.63]	-
143	Mailbox move for edit.balazy@tech-arrow.com	Mailbox move	Idle	-	-	0 %	-	-	Yes	TANEWS [192.168.190.63]	-

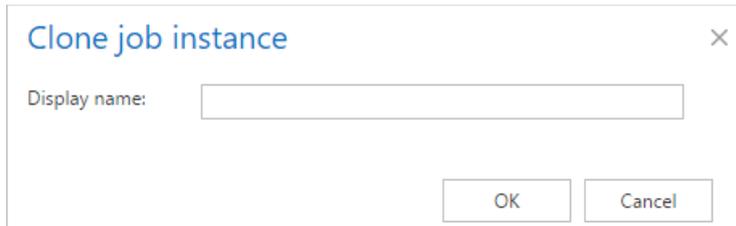
Any changes to a job can be done from the job context menu by selecting the corresponding job from the list and left clicking on the ellipses (...). Now we select **EBA's mailbox archive_shortcutting** job from the list. With the help of this job we will demonstrate how to handle jobs from the context menu.

ID	Display Name	Type	Status	Last Start	Last Duration	Progress	Summary	Next Start	Is active	Cluster node	Running on
114	EBA's invoice restore	Email restore	Idle	2 weeks ago	2 minutes	100 %	1 mailboxes processed 93 emails processed (1 failed)	Never	Yes	TECHNB002 [192.168.190.20]	-
135	EBA's mailbox archive_shortcutting	Email archive	Idle	20 minutes ago	14 seconds	100 %	1 mailboxes processed 2 emails processed	in 5 hours	Yes	Any available	-
138	Mailbox move for edit.balazy@tech-arrow.com	Mailbox move	Idle	-	-	-	-	-	Yes	TECHNB002 [192.168.190.20]	-
142	ECSO's mailbox recovery	Email recovery	Idle	-	-	-	-	-	Yes	Any available	-



The context menu of a job contains the following options:

- **Clone:** use this option to create a clone of an already configured job. A cloned job has the same configurations as the original job that it was created from. With clicking the “Clone” option the “Clone job instance” window opens, which requires to name the job:



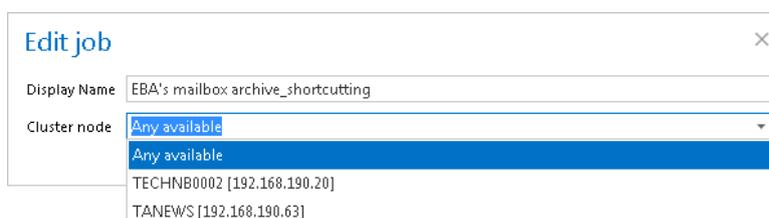
If a job with the same name already exists, an error message warns the user about this.

- **Start:** with a click on “Start” the administrator can start the job run manually;
- **Stop:** with a click on “Stop” the administrator stops the run of the selected job;
- **Configure:** required values can be configured for the job on its configuration page, which can be opened using this option.
- **Show last logs:** by selecting this option the user will be redirected to the **System logs** page, where the last run of the selected job will be preselected and the corresponding events will be displayed in the table of events;

#	Start date	End date	Date	Title	Description	Job
Job: EBA's mailbox archive_shortcutting						
1	9/28/2015 11:05 AM	9/28/2015 11:05 AM	9/28/2015 11:05 AM	Plugin was finished successfully	Plugin.EmailArchive	EBA's mailbox archive_shortcutting
1 mailbox processed 2 emails processed						
2	9/28/2015 10:52 AM	9/28/2015 10:54 AM	9/28/2015 11:05 AM	Mailbox processing information	Processing was finished	EBA's mailbox archive_shortcutting
3	9/28/2015 10:41 AM	9/28/2015 10:41 AM	9/28/2015 11:05 AM	Mailbox processing information	Mailbox processing finished. Mailbox: 'edit.balazy'. Total mails: 2 Mails processed: 2 Failed mails: 0 Skipped mails: 0	EBA's mailbox archive_shortcutting
4	9/28/2015 10:40 AM	9/28/2015 10:40 AM	9/28/2015 11:05 AM	Mailbox processing information	Abort signal received	EBA's mailbox archive_shortcutting
5	9/21/2015 10:53 AM	9/21/2015 1:46 PM	9/28/2015 11:05 AM	Mailbox processing information	Processing was started. Number of mailboxes: 1	EBA's mailbox archive_shortcutting
6	9/21/2015 10:51 AM	9/21/2015 10:51 AM	9/28/2015 11:05 AM	Processing was started	Plugin.EmailArchive	EBA's mailbox archive_shortcutting

- **Edit:** with a click on this option the **Edit job** dialog opens, where the user can:

- ✓ rename the job;
- ✓ change the node, where the job can be run.

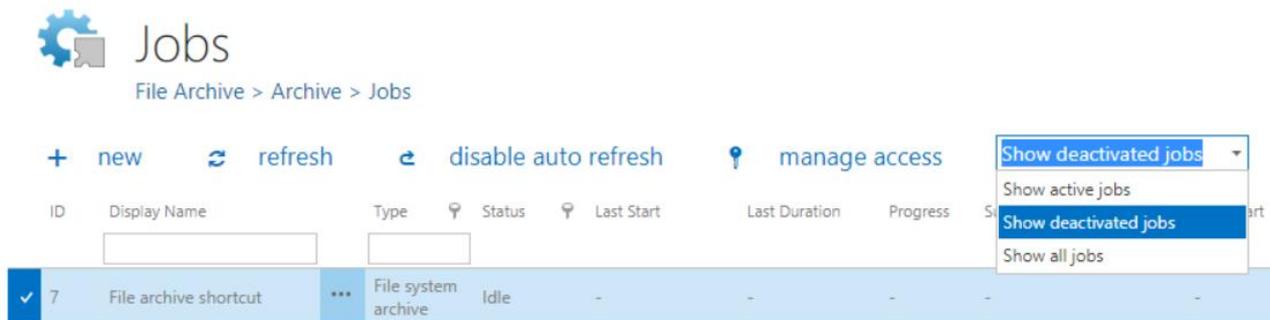




- **Deactivate:** it is recommended to deactivate jobs which are not in use for a longer time, but very probably will be used in the future (e.g. restore or recovery jobs). By selecting this option, the administrator does not permanently delete the job from the list. The deactivated job will be only hidden and it will not run according to the schedule (nor can be manually started). Running and waiting jobs cannot be deactivated.
- **Delete:** with this option the administrator can permanently delete selected jobs from the list; the processed data by some plugin types will not be accessible through the standard interfaces (data processed by file archive jobs will not be accessible if all file archive jobs wrote the data into the same database and all of them were deleted; if only one job, which wrote data into this particular database remained, then all data processed by all file archive jobs will be accessible. In case of email archive jobs the data will be still accessible, even if the jobs have been deleted). Running and waiting jobs cannot be deleted.

Filtration between active/inactive jobs

A job can be either active (an active job will be started according to the configured schedule, or can be started manually), or its status may be set to deactivated (if the administrator sets a job to deactivated, it cannot be started neither by the scheduler, nor manually). On the page of **Jobs** the user can filter among **Active/Deactivated jobs**, or he can also choose to display all jobs in the list (**Show all jobs**).



If a job has been deactivated, it can be restored to the list of active jobs again. Select the job, open its context menu and choose **Activate** from the list:



Jobs
File Archive > Archive > Jobs

+ new refresh disable auto refresh manage access Show deactivated jobs

ID	Display Name	Type	Status	Last Start	Last Duration	Progress	Summary	Next Start	Is active	Cluster node	Running on
7	File archive shortcut	File system archive	Idle	-	-	-	-	-	No	Any available	-

- Clone
- Configure
- Show last logs
- Edit
- Activate
- Delete

Searching in name and type

It is possible to search in the name and type of jobs. Type the phrase you are looking for to the corresponding field.

Jobs
File Archive > Archive > Jobs

+ new refresh disable auto refresh

ID	Display Name	Type	Status
6	File archive original	File system archive	Idle
7	File archive shortcut	File system archive	Idle
8	File restore	File system restore	Idle
9	File recovery	File system recovery	Idle
10	Delete from archive	Delete from archive	Idle

Sorting between jobs

The jobs can be also sorted based on the type, status or cluster nodes where they are running. Click on the funnel () icon located next to the particular column in the grid:

 Jobs

File Archive > Archive > Jobs

[+ new](#)
[refresh](#)
[disable auto refresh](#)
[manage access](#)

ID	Display Name	Type	Status	Last Start	Last Duration	Progress	Summary	Next Start	Is active	Cluster node	Running on
6	File archive original	File system archive	Idle	6 days ago	5 seconds	100 %	4 folders processed 26 documents processed (4 newly archived)	Never	Yes	Any available	-
7	File archive shortcut	File system archive	Idle	-	-	-	-	-	No	Any available	-
8	File restore	File system restore	Idle	6 days ago	9 seconds	100 %	3 folders processed 22 documents processed (22 restored)	Never	Yes	Any available	-
9	File recovery	File system recovery	Idle	6 days ago	9 seconds	100 %	1 entities processed 3 folders processed 22 documents processed (9 skipped, 13 recovered)	Never	Yes	Any available	-

Available operations from the status bar of the job

With a double click on the selected job in the list of jobs you open the configuration page to the job. You will see the status bar of the job on a blue background.



[start immediately](#)
[refresh](#)
[disable auto refresh](#)
[deactivate job](#)
[logs](#)
[edit](#)
status bar button
collapse/expand the progress

Status: **Idle**
 Progress: 4 folders processed 23 documents processed (23 newly archived) (completed 2 hours ago)

With the arrows mark () at the right side of the status bar the user may collapse or expand the progress information about the job's run. The status bar's last state is always stored and the last state will be opened by navigating to the page again. The status bar of a job contains the following status bar buttons:

- **start immediately/stop:** with a click on this option the administrator can start/stop the job running manually;
- **refresh:** click on this option and the status bar information about the progress of the job will be refreshed;
- **disable/enable auto refresh:** turn on/off the auto refresh of progress bar information (if enabled, the information will be refreshed every 5 seconds)
- **deactivate/activate job:** use "deactivate" button if you want to temporarily cancel the job; use "activate" button if you want to restore the job among the active jobs;
- **logs:** by selecting this option the user will be redirected to the **System logs** page, where the last run of the selected job will be preselected and the corresponding events will be displayed in the table of events. Use this option for troubleshooting if any failure occurred during the run of the job;
- **edit control button** is used to change the name of the job and to specify the node on which the job should run.



The progress bar shows the current state of the job (if it is running or done). The email archive job reports the summary in the following format:

{0} mailboxes processed ({1} failed)

{0} = number of mailboxes which were started and finished processing

{1} = only displayed if there was a failure in at least one mailbox; number of failed mailboxes

When is a mailbox failed?

- The mailbox can't be opened
- The email address is invalid
- Missing permissions
- Some folders can't be opened

{2} emails processed or {2} ({3}) emails processed

{2} = number of archived emails; this is a sum of items which were archived: shortcut, keep original, journal shortcut

{3} = archived: blacklisted emails. If a mail should be shortcut but the message class does not allow it, the mail is blacklisted. This is only displayed if at least one blacklisted message was processed.

Note: If the job is using **keep original** method, but the message is **blacklisted**, it will be counted to **{3}**!

In the following chapters we will learn how to configure and use the contentACCESS File Archive, Email Archive, SharePoint archive, Email management, Store replication, Sharing and Email synchronization jobs.

Filtering in jobs

This configuration enables the user to filter among items by several conditions:

File archive job conditions:

- All text = file name and content of the file
- Creation date – the creation date of the file
- Extension - important to specify also with the dot, like: **.jpg, .png, .pdf**
- File name
- Modification date – the modification date of the file



- Path – folder path of the parent folder, where the item is located
- Size – the size of the item

Email archive job conditions (also Shortcut repair and PST import):

- All text = Body, Recipients, Sender, Subject, Attachment filenames and Attachment content
- Bcc
- Body
- Category
- Cc
- Folder path – folder path of the parent folder, where the item is located
- Has attachment
- Importance
- Is from In-Place Archive (this option is present only if there is at least one In-Place Archive in the Address book)
- Message class
- Received date
- Recipients
- Sender
- Sensitivity
- Sent date
- Size – the size of the item
- Subject
- To

Important: If the **Is from In-Place Archive** filter is not displayed on the list, **service restart** is required (Services -> GATE.contentAccess.Service).

SharePoint archive job conditions:

- All text = file content and also metadata
- Creation date – the creation date of the file
- Extension - important to specify also with the dot, like: **.jpg, .png, .pdf**
- File name
- Modification date – the modification date of the file



- Size – the size of the item
- Url

GDPR File system job conditions:

- All text
- Creation date – the creation date of the file
- Extension - important to specify also with the dot, like: **.jpg, .png, .pdf**
- File name
- Modification date – the modification date of the file
- Path – folder path of the parent folder, where the item is located
- Size – the size of the item

GDPR Exchange job conditions:

- All text = Body, Recipients, Sender, Subject, Attachment filenames and Attachment content
- Bcc
- Body
- Category
- Cc
- Folder path – folder path of the parent folder, where the item is located
- Has attachment
- Importance
- Message class
- Received date
- Recipients
- Sender
- Sensitivity
- Sent date
- Size – the size of the item
- Subject
- To

Note: If **Equals** is selected as the operator for **File name** filtering condition, **the whole name also with the extension** must be specified.

To specify a filter:

- click on the **Change filter** button, or

Filtering settings

Filter:

not set

- click on the **Change** button

Shortcutting

Shortcut types:

 Apply to NOT ARCHIVED items
Use shortcut for items where filter is not set[\[Change\]](#)
 Apply to ALREADY ARCHIVED items with keep original shortcutting method
Use shortcut for items where filter is not set[\[Change\]](#)

The **Filter settings** window will open. You can set filtering options in a user-friendly way (**visual** tab) or in a more technical way (**text** tab). It doesn't matter which tab you work with – if you change something on one, it will be changed on the other, too. In this section we will explain how to set filtering by working with the **visual** tab.

To add a new filtering condition, click on **+add condition**. Pick a **type from the first** dropdown list (one of the conditions mentioned above), then an **operator from the second** and specify the **value to the third** box.

Filter settings ✕

visual text

**A
N
D** ▼ Extension ▼ Equals ▼ .jpg ✕

[+add group](#) [+add condition](#)

[+add new group](#)

OK Cancel

Filtering conditions can be merged to **groups**. To add a new group, click on **+add group**. There are **3 different operators** that can be set for a group by clicking on the arrow in the blue part of the window:

- AND – by using this operator, items meeting all the set conditions will be processed

Filter settings ×

visual text

AND	File name	Contains	testing	×
	Extension	Equals	.doc	×
	Size	<	2	MB

+add group +add condition

+add new group

OK Cancel

- OR – by using this operator, items that meet one OR another condition (or one OR another group of conditions) will be processed

Filter settings ×

visual text

O R ▼	Size ▼	<= ▼	500	KB ▼	×
	Size ▼	>= ▼	1	MB ▼	×

+add group +add condition

+add new group

OK Cancel

- NOT – by using this operator, items meeting the conditions will be excluded from processing. If you want to add more than one NOT condition, they have to be added as shown on screenshot below.

Filter settings ✕

visual text

AND

NOT Size \geq 2 MB ✕
+add group +add condition

NOT Extension Equals .jpg ✕
+add group +add condition

+add group +add condition

+add new group

OK Cancel

Filtering conditions and groups can be removed by clicking on the **X**.

For some job types, it is also possible to add another filtering condition that isn't preconfigured. Click on the **+add custom property** button in the upper left corner of the **Filter settings** window.

Filter settings ×

+ add custom property 

visual text

**A
N
D** 

Sent date  <  10 days  

+add group +add condition

+add new group

OK Cancel

The **Add custom property** window will open. Here you have to specify **Display name**, **Name** and **Type** (String, Numeric, Date, Boolean, Lookup, Customizable lookup) for your new criteria. Click **OK**.



Add custom property ✕

Display name	<input type="text" value="Card number"/>
Name	<input type="text" value="Card number"/>
Type	<input style="border-bottom: 1px solid #ccc;" type="text" value="String"/>

When you are done, click on **OK**. The filter(s) will be added to the **Filtering settings** or **Shortcutting settings** section of the job configuration.

File Archive

With the help of File system archive jobs, it is possible to archive data located either in local file systems or on network shares (UNC paths). The time period, for which the documents are available in the archive, is set via retention categories. The File Archive database and storage are always assigned to a root folder (chapter [File Archive settings](#)). This prevents the user from archiving the same root to multiple databases/storages and having troubles with retrieving the file.

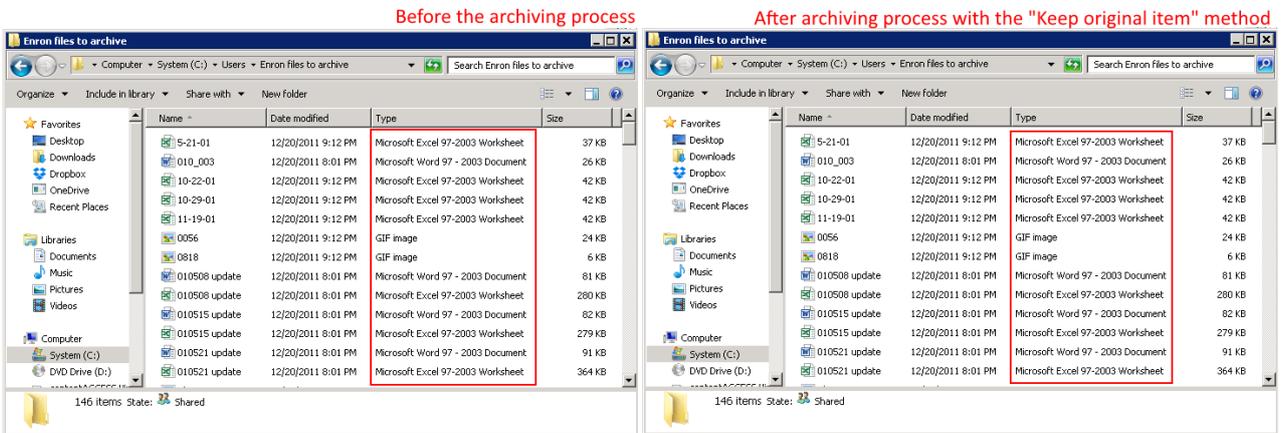
The archived files can be viewed either in contentWEB (more information [here](#)), or in the shared folders on virtual (more information [here](#)). It is also possible to restore the archived files from shortcuts, or to recover them if the original was deleted from the file system.

Introduction to File system archive

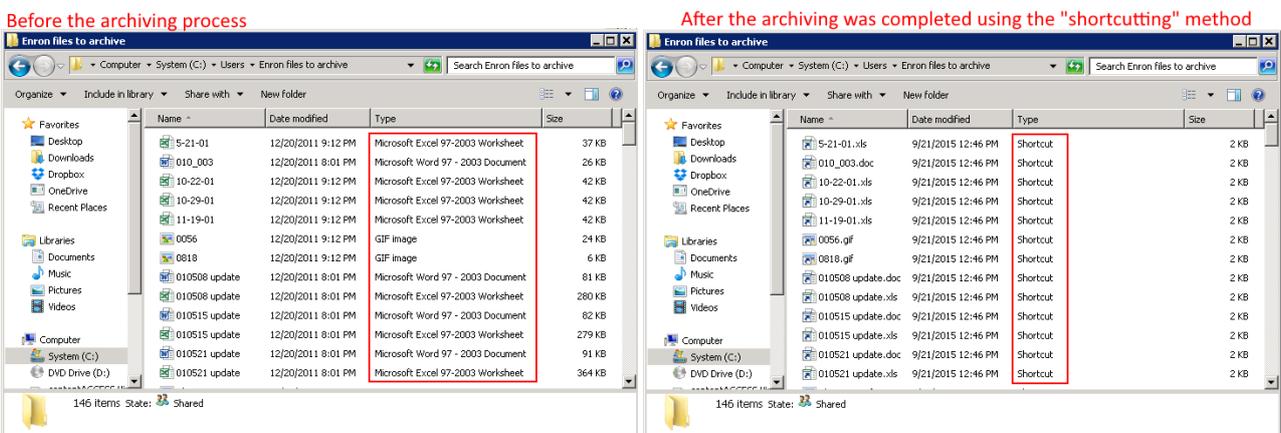
There are **4 file system job types** available in contentACCESS:

1) File system archive job is used to archive documents from the selected location into a selected storage. Archiving can be done in multiple ways. The administrator selects the archiving strategy and decides if the archived file is kept in the file location, replaced by shortcuts or deleted from there. The pictures below show the contents of the original file location before and after the archiving process:

a) With the “Keep original item” method the original file is kept in its original location (recommended archive method for files younger than 1 year):

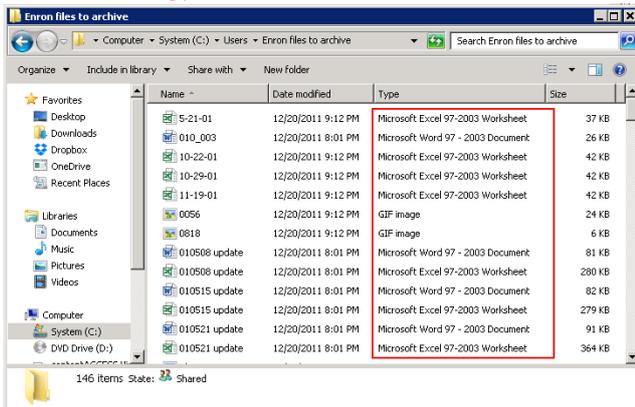


b) The archived items can be also replaced by a shortcut, thus not taking up so much space on the file-server archive, yet files are available for use as usual. In this case the “Create shortcut from original item” method should be used. This is the recommended archive method for files older than 1 year and younger than 2 years:

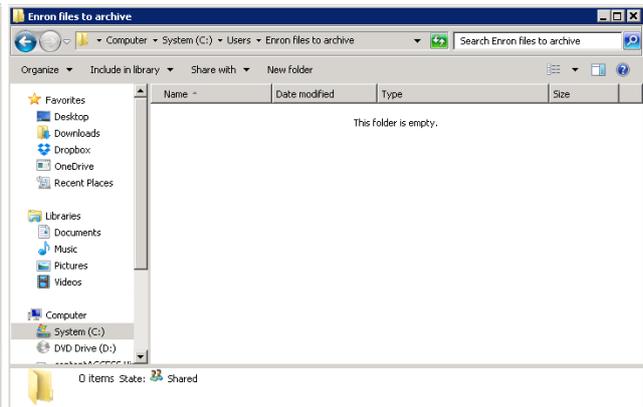


c) The archived item can be also deleted from its current location, in this case the “Delete original” method should be used (recommended archive method for files older than 2 years):

Before the archiving process



After the archiving process using the "Delete original" method is finished



It depends on a typical use case which method is the most advisable to use. Customers use the “Keep” original file method with versioning, when they are working on long-term projects and their files are modified too often. E.g. if an architect is working on a project and would like to have a version of it each day, then he may archive the project each day and create versions of it. This protects him from losing his work that he worked on for a longer time (e.g. if a hardware problem occurs). Shortcutting is used by older files that still may be used, so the user would not like to delete them from the file location yet (e.g. files older younger than 2 years). Those items, which are not in use any more - but must be retrievable from the archive during the retention time required by the law – should be deleted from its location when archived. In this case, it is advisable to use the “Delete original item” method.

2) File system restore job is used to restore the already archived items from shortcuts; from the storage (archive) back into the original location.

3) File system recovery may be used to recover deleted items/folders/recursive folder structure if they have been deleted from its original location. It might be very useful if any archived item or folder has been deleted by accident, or if deletion was caused by a technical failure etc. The user may recover either the original file or the shortcut.

4) Remote shortcutting job is a special job type, which can be used with the file archive jobs together. Use this job if you have several remote locations synchronized with your central data center. contentACCESS is installed on the data center, and continuously archives the files already synchronized with the data center. By the synchronization process the files are copied to the data center. So the archiving itself is done by a standard File system archive job; the Remote shortcutting job is used to create shortcuts on the remote locations.



Use this method, if you would like to run the archiving process in a central data center, and replace the remote files with shortcuts if they are not in use. If you have multiple remote shares to archive and you need to speed up the archiving process and save bandwidth, this is the right solution for you.

Editing of already archived files, file versions in File system archive

You can edit an already archived file by opening the original file (if was archived with the *Keep original method*) or the shortcut to it (LNK, if it was archived with the *Shortcutting method*) in the original file location or through the Virtual drive.

- if the file **was not shortcutted** (i.e. the already archived file is kept in the original file location), then you can open the file in a standard way, edit it and save it. The next archive job will create a version to this file in the archive.
- if the file is **shortcutted** (i.e. was archived using shortcuts) and you open the file through the shortcut, you can make changes to the file(s) if you have write access on the file(s) – by simply opening, editing and saving with the associated application. The **Virtual drive** will detect the change and create a new version from the file(s) after a short delay (about 30 seconds).

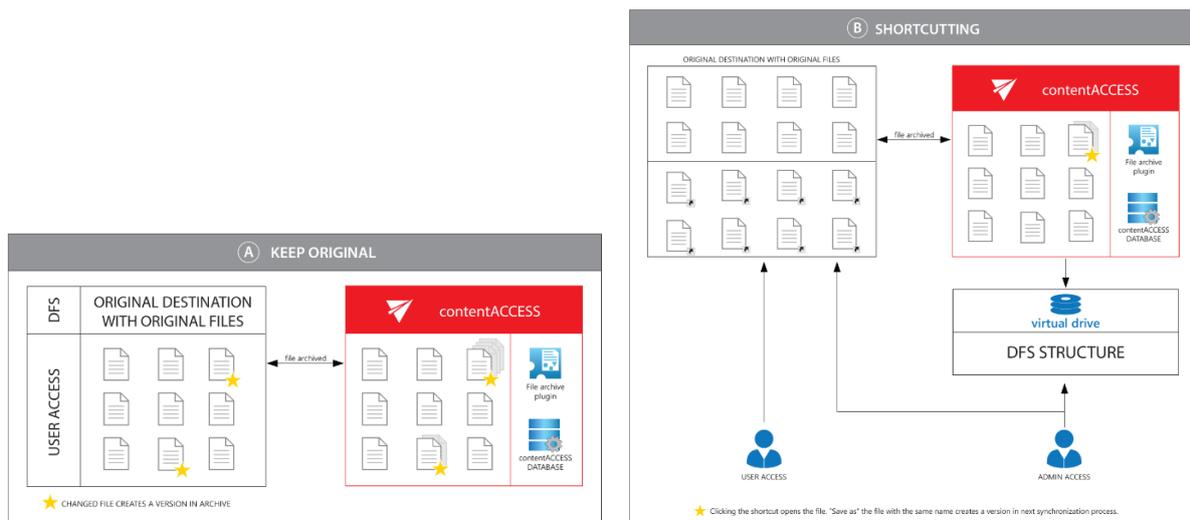
The screenshot shows the contentWEB interface for a file system archive. The main area displays a table of file versions for 'ENTEXRECAP.doc'. A red arrow points to the '- version 1' entry, which is highlighted in blue. A red text annotation reads 'new file version created by the archive job'.

Title	Created	Modified	Size	Versions
ENTEXRECAP.doc	7/21/2016 10:12 AM	7/22/2016 12:10 PM	35.8 KB	1
- version 1	7/21/2016 10:12 AM	12/20/2011 7:23 PM	31.7 KB	

The detailed view on the right shows the following information for the selected file version:

- Title:** ENTEXRECAP.doc
- Size:** 35.8 KB
- Created:** 7/21/2016 10:12:37 AM
- Created by:** Job #8 (Tenant #2)
- Modified:** 7/22/2016 12:10:39 PM
- Modified by:** Job #8 (Tenant #2)
- Path:** C:\FATesting\Testfolder2\beck-s\ENTEXRECAP.doc
- File name:** ENTEXRECAP.doc

The versioning feature might be very useful for users, who are working on long-term projects and would like to protect themselves from losing their data. In such cases, it is recommended to run an archive job for the project each day, and save the current state (version) of the file/project into the archive.



Screenshot A: Versions created when keeping the original item Screenshot B: Versions created when using shortcuts

Synchronization of rights to a folder/file

The synchronization of **user rights to a folder/file in contentWEB File Archive** is managed by the **File Archive job**. File Archive job writes the file system permissions to the database, and then synchronizes these user permissions in contentWEB, too. The File archive job synchronizes:

- the rights **to a folder** permanently at each job run;
- the rights **to a file** only in case that a new version of the respective file has been created.

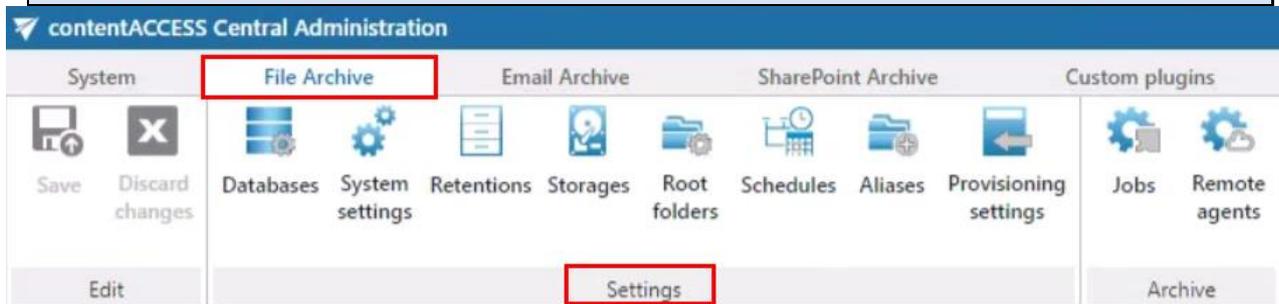
File Archive settings

To be able to use the contentACCESS File Archive, the following settings are mandatory in the Central Administration:

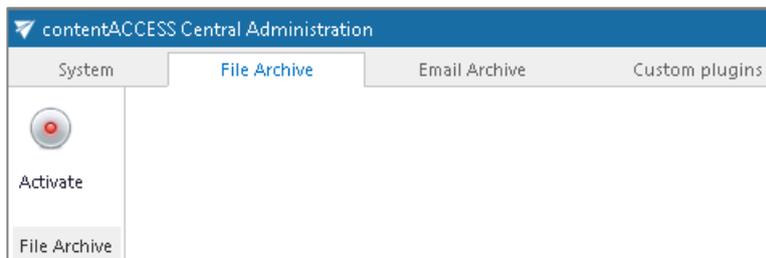
- 1) The virtual drive must be installed and configured (configurable here: **System** tab → **Client applications** → **Virtual drive configurations**). For more information please refer to [Virtual drive](#).
- 2) The LDAP settings must be configured (configurable here: **System** → **Services** → **System**, section **Active directory integration settings**). These will be used by contentWEB to evaluate user access permissions to folders/files. For more information please refer to [System](#).
- 3) Settings available in **File Archive** → **Settings** need to be configured. The configuration logic is from left to right. By following this logic everything will be configured for the next step. These settings will be described below in this chapter.



Note: Aliases are used by the *Remote shortcutting job* only. If you do not use a *Remote shortcutting job*, you can skip [Configuring aliases](#).



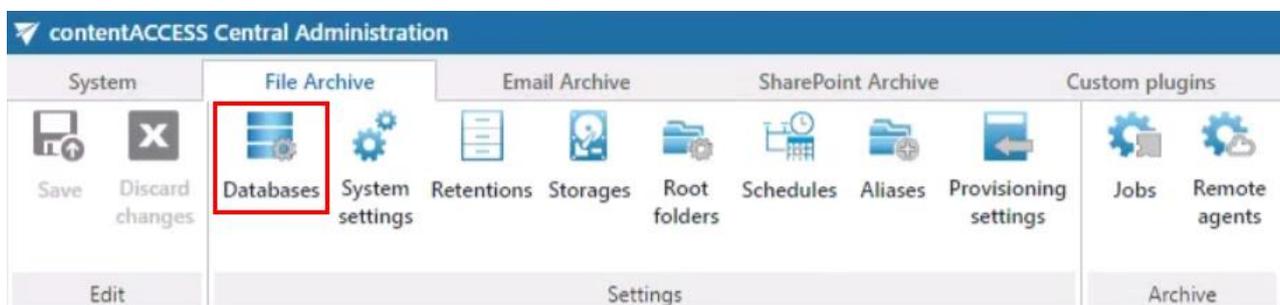
When starting to configure File Archive for the first time, the user is required to activate the File Archive provisioning job. Open the File Archive tab on the ribbon and click on the “Activate” button:



After successful activation the **Settings** of the File Archive are displayed. The tab (already mentioned in step 3) above) features the following configuration options:

File archive Databases

The administrator must set here the database, where File Archive will store the metadata; to create such database, please refer to the chapter [Databases](#) of this guide.





File archive System settings

The main system database for the File Archive is selected on this page. All the root folders (and its settings) that will be applied in the archive jobs are kept in this database. Select the database connection to be applied from the dropdown list ("MNEtestDB" in our use case).

Note: A database connection already configured on the **Databases** page (File Archive → Settings → Databases) can be selected as a file archive database.

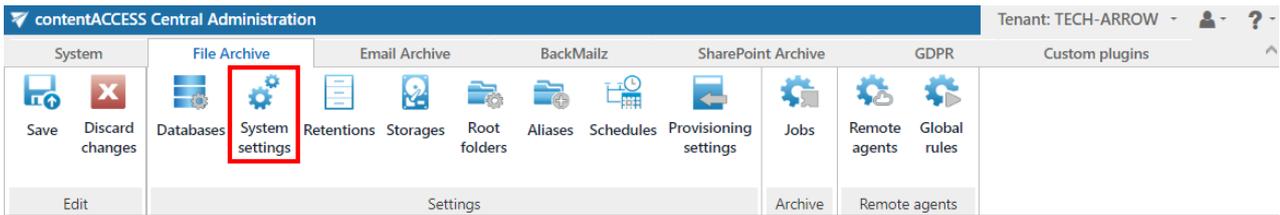
The date, from which the retention of the documents will be calculated, can be selected here. Choose the setting to be applied from the dropdown list.

By default, the file archive supports **versioning**. When a file is archived by the file archive for the first time, the **first (original) version** is created. If the File archive is creating shortcuts, the shortcuts are opened using the **Virtual drive**. When the user opens a shortcut, the file is opened in read/write mode and it is possible to edit it. Virtual drive detects the changes and after the file is closed, a new version is created in the File archive. The users are **always getting the latest version** when accessing a file/shortcut.

If the requirement is to not allow changing archived files, it is possible to disable versioning in File archive. This can be done by checking the **Turn off versioning** checkbox in **File Archive -> Settings -> System settings**, section **File archive settings**. If the versioning is turned off, the File archive won't allow to create versions (neither through the file archive job, nor through the shortcuts/Virtual Drive). If (for example) the user changes the file on the file system, the File archive job **will not create** a new version, but will generate a warning (see [monitoring](#)) instead. The File archive **will not create** a new version from the modified file.

Note: After the versioning settings are changed and saved, the **Virtual drive** needs to be restarted.

Save your settings.



System settings

File Archive > Settings > System settings

→ Database settings

Database connection: Change ✓

→ Retention settings

The retention of documents is either calculated from the time of archiving or from the file date. If file date is specified, here you can define which file date should be used for the retention calculation (reference date).

Retention reference date:

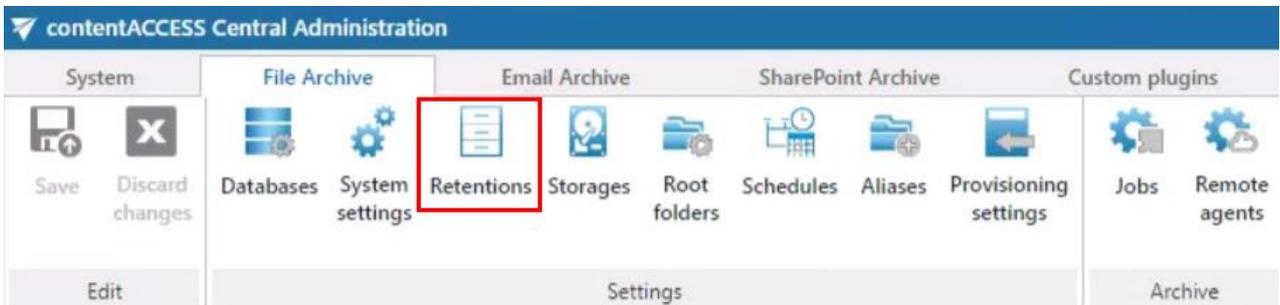
→ File archive settings

File archive global settings are valid for all file archive jobs on the tenant.

Versioning: Turn off versioning

File archive Retentions

The period of time, during which the archived data will be stored, is specified on this page; for more information on how to create retentions to be applied, please refer to chapter [Retentions](#) of this guide.



File archive Storages

The administrator must set here the File archive storage for the binaries; for detailed information on how to create a new storage connection, please refer to chapter [Storages](#) of this guide.





Root folders

The root folder paths to be applied in a file archive job are specified in this section. **The root folder defines the start point (start point = e.g. "C:") of the archive process.** A root folder set here is selected for an archive job on the given job's configuration page. The relative path (e.g. folder "Test files" if directory "C:\Test files" will be archived) can be set in the given job's configuration section further on.

The root folders and their settings are written to the file system database defined in section [File archive System settings](#) above (**File Archive** → **Settings** → **System settings**). A connection, that already exists in the system database, cannot be specified twice. E.g. if "[\\tanews\TECH-ARROW files to archive](#)" is already set, then "[\\tanews\TECH-ARROW files to archive\contracts](#)" cannot be added to the root folder's list. This feature prevents the users from archiving the same folder into two different databases/storages. If the user wants to add a root which already exists in the system database, he will be prompted about this.

Hint: When the root folders are defined, be careful to **NOT** add the **SAME PHYSICAL PATH TWICE**.

Example: D:\Share which is shared as [\\server\Share](#) can be added twice, like this:

- D:\Share

or as a shared path:

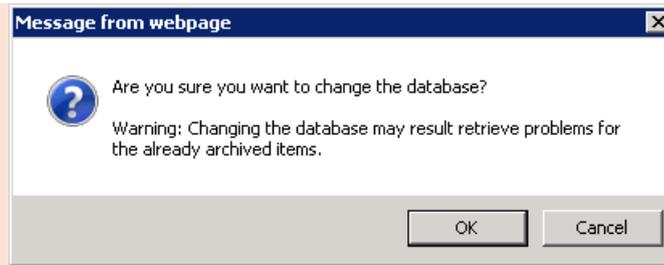
- [\\server\Share](#)

These paths are pointing to the same physical directory. contentACCESS can't detect such collision.

This configuration might result in an unpredictable behavior: if both root folders are assigned to a different database or they are processed by different jobs, it is not possible to predict in which archive the files will be stored.

A root folder must always have a database and a storage assigned. The job, which archives (restores/recovers) this root, will use this database and storage.

Hint: It is not recommended to change the database and storage connections already associated with a root folder. Changing the database will lead to problems when trying to retrieve the already archived items, because some of your data will be saved in the originally set database, and another part of data in the newly set database. The same retrieve problem might occur when changing the storage, too. The application warns the user about it:

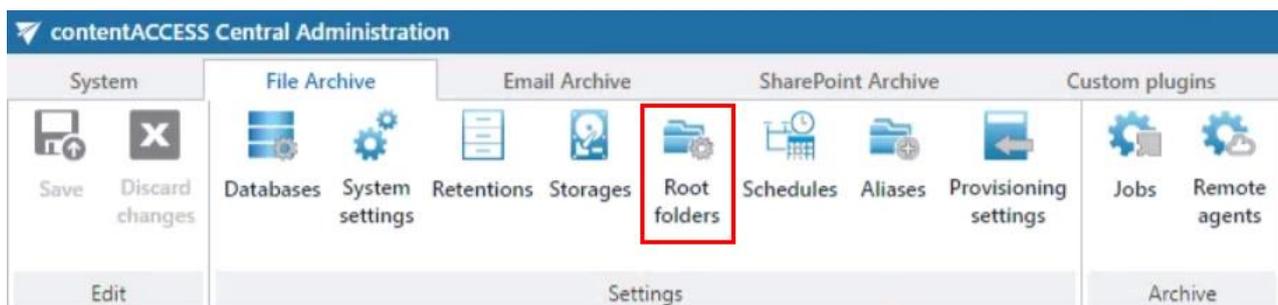


However, the database and storage assigned to a root can be changed using the “Edit” menu item in the root context menu. Do not use this option unless it is very necessary.

The root folders may be either

- imported using the “import” button (refer to chapter [Importing contentACCESS configurations from files](#)) or
- added to the list using the “new” button.

Click on “+ new” to manually add a root folder that should be processed by a job.



 Root folders
File Archive > Settings > Root folders

The **File Path** dialog opens. Enter the file path that should be applied and the applicable user credentials. The **Type of connection** shows if the files to be archived are located on the server (on-premise) or on network shares (remote). Version can be either way Business or Private. **The File Archive database, storage and index zone must be associated with this specific root folder directly in this dialog.** It is NOT recommended to change the database and storage that is already used, because it will lead to file retrieve problems (as mentioned in the hint above). Use the “Change” option only in case if such change is really necessary (e.g. if you haven’t archived the root yet).

File Path
✕

Path:

Use explicit credentials:
 Use explicit credentials

User name:

Password:

Confirm Password:

Type of connection:

Version:

Server:

✔
Connection successful!

Test

Database connection:

✔

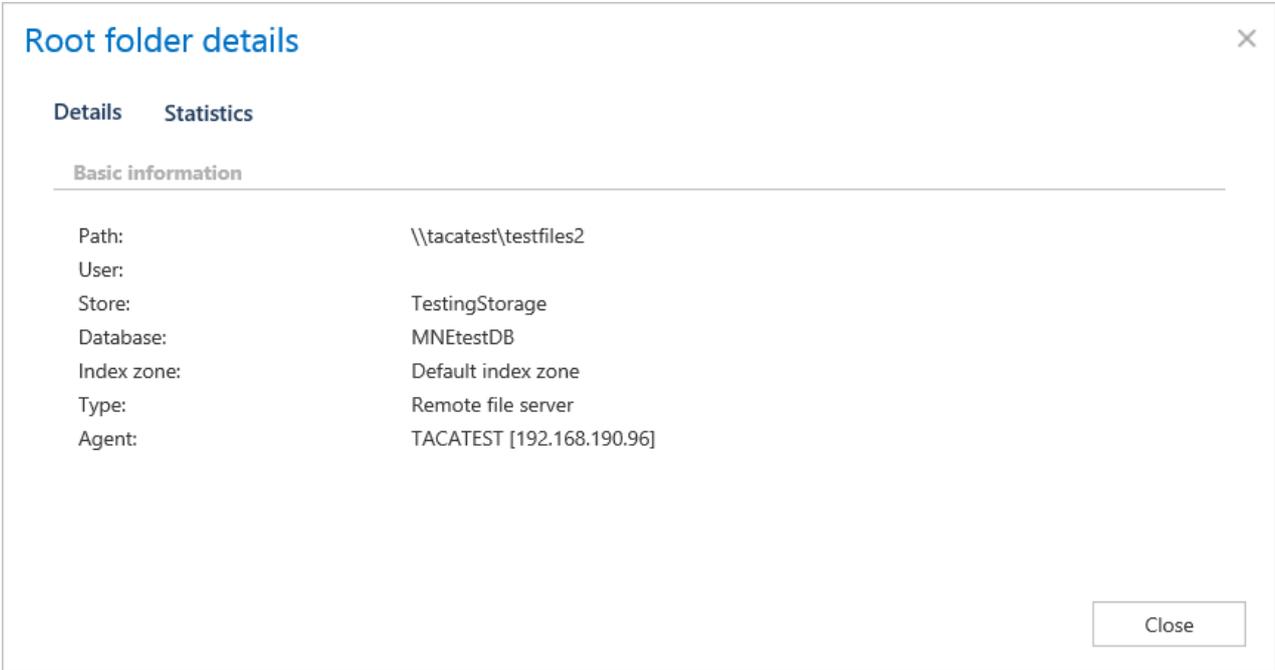
Storage name:

Index zone:

Note: We recommend to specify the parent folder (the start point of the archive process) in the File Path dialog. The relative folder path can be specified further on when configuring the respective job.

Root folder details

Details and archive statistics of the already configured root folders can be viewed by clicking on **Details** in the root's context menu.

Details:

Basic information	
Path:	\\tacatest\testfiles2
User:	
Store:	TestingStorage
Database:	MNEtestDB
Index zone:	Default index zone
Type:	Remote file server
Agent:	TACATEST [192.168.190.96]

Path – where the folder is located

User – if the username was specified, it will appear here

Store – storage assigned to the folder

Database – database assigned to the folder

Index zone – index zone assigned to the folder

Type – type of the server the folder was archived by

- on-premise
- remote (as on screenshot above)

Agent – if the folder was remotely archived, it will display the agent who archived it

Statistics:

Statistics show archived folders count, document count and total size of the files that were archived.

Root folder details ×

Details
Statistics

Archive statistics

Number of folders:	2
Number of files:	9
Size:	2 MB

Deleting a root:

Already configured root folders can be deleted from the list using the root's context menu. A deleted root is only hidden, but it still exists in the database. If the user wants to add an already deleted root again, he will be prompted that it already exists in the database, and he will be able to restore it, but only with the old settings (with the originally assigned database and storage).

Aliases

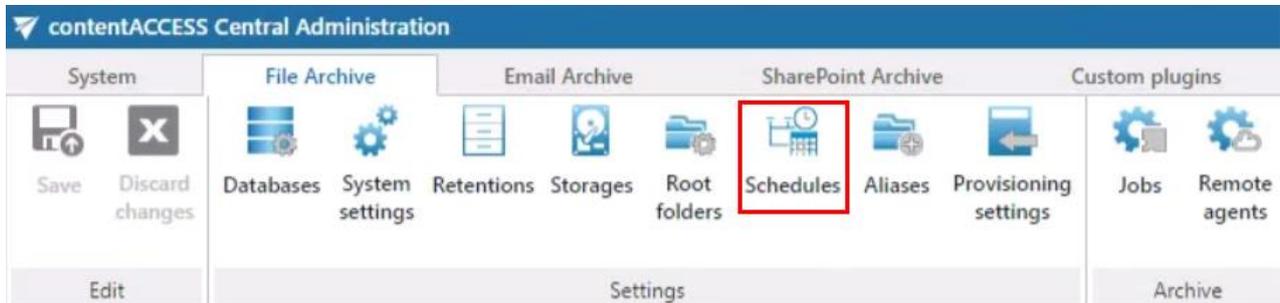
Use this feature to specify different folder names pointing to the same file location. Read chapter [Configuring aliases](#) for more information.

contentACCESS Central Administration

System	File Archive	Email Archive	SharePoint Archive	Custom plugins
 Save  Discard changes	 Databases  System settings	 Retentions  Storages	 Root folders  Schedules <div style="border: 2px solid red; padding: 2px; display: inline-block;">  Aliases </div>  Provisioning settings	 Jobs  Remote agents
Edit	Settings			Archive

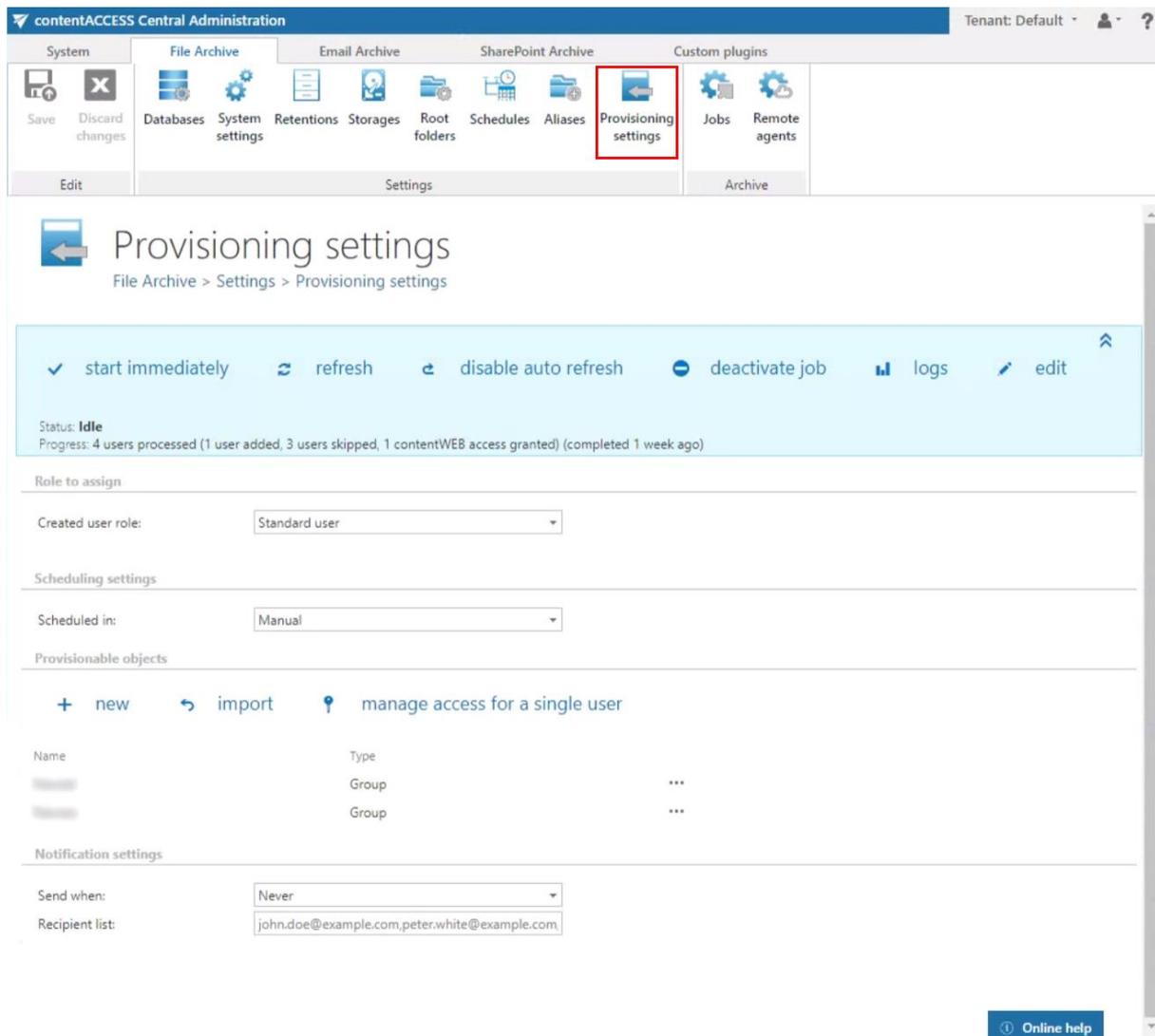
File archive Schedules

The schedulers automatizing the file archive process are configured on this page; for more information on how to create schedulers, please refer to this chapter: [Schedules](#).



Provisioning settings and managing access to contentWEB

The File Archive provisioning settings are accessible on the **File Archive** → **Settings** → **Provisioning settings** page.



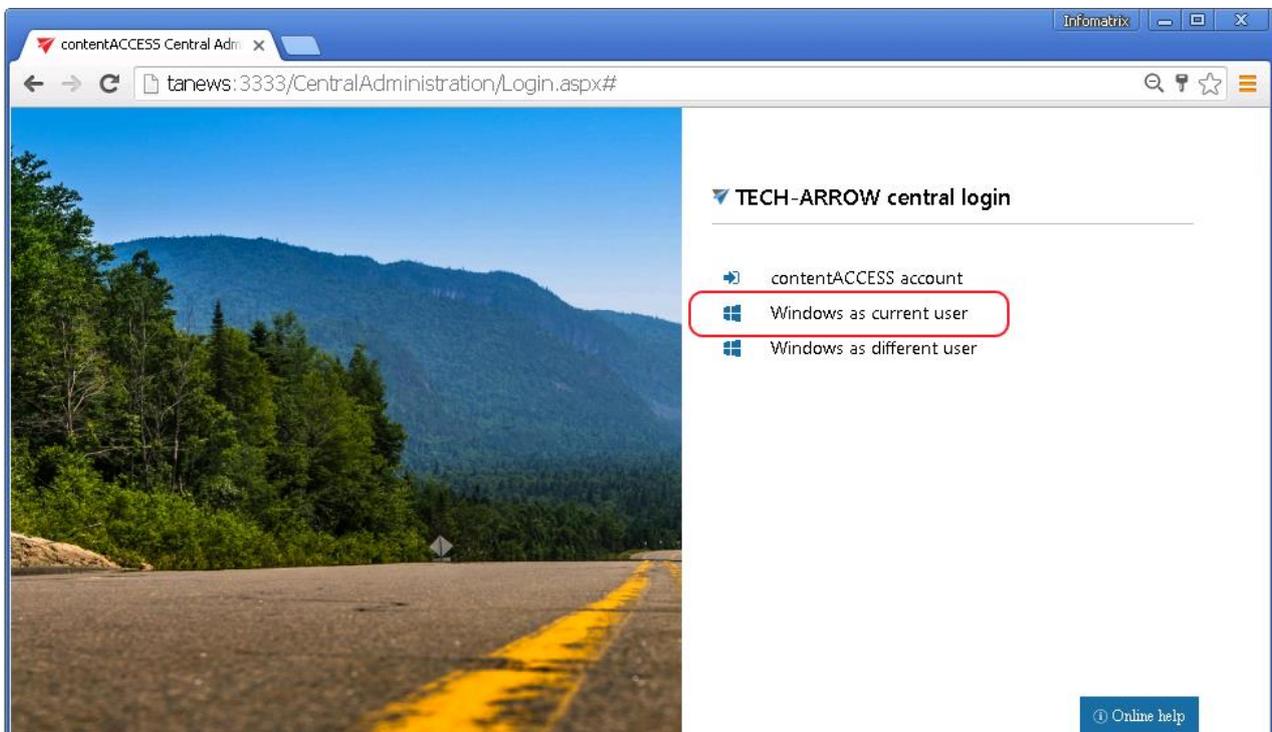
The provisioning job that synchronizes the Active directory with contentACCESS can be set directly on this page.

Note: The system's LDAP settings specified on page *System* → *Services* → *System* in section "Active directory integration settings" are used to connect to the Active Directory.

When the provisioning job is started, it automatically **adds the new Active Directory users into contentACCESS** based on provisioning settings. The provisioned objects will automatically get log on **rights to the contentWEB File Archive**.

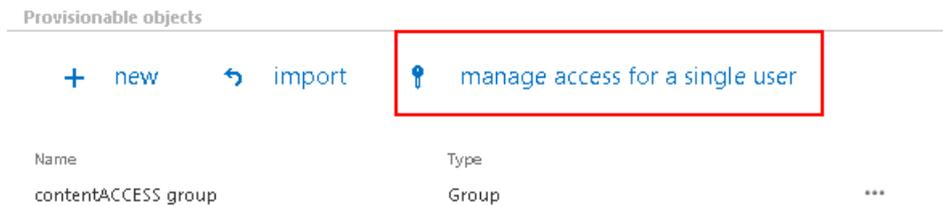
Hint: Access permissions on the file archive folders/items are **NOT** granted by the provisioning job. Provisioning job grants only log on rights to the contentWEB File Archive. The access rights to files/folders are evaluated and updated by the file system archive job. Read more in [Synchronization of rights to a folder/file](#).

The contentWEB users can log in to contentWEB using Windows authentication.





The existing contentWEB users can be viewed by clicking on the “manage access for single user” option on the **Provisioning settings** page:



The users that are already provisioned have an automatic flag, while manually added users have a manual flag:

Manage Access to File archive

System > Tenants > Tenants > Manage access

[+ new](#)

User name	Role name	Flags
tesztelek	Standard user	Manual
CONTENTACCESSUSER1	Standard user	Automatic (770)
CONTENTACCESSUSER2	Standard user	Automatic (770)
CONTENTACCESSUSER3	Standard user	Automatic (770)
CONTENTACCESSUSER4	Standard user	Automatic (770)

[Go back](#)

New contentWEB users (with default Standard role or manually created explicit role) can be manually added to the contentACCESS File Archive using the **+ new** option on the same (Manage access to File archive) page. File archive access rights can be given to an already existing or a new contentACCESS user.

Create new role association

Tenant information

Role:

Invitation type:

Search for existing user*:

Andras Katona

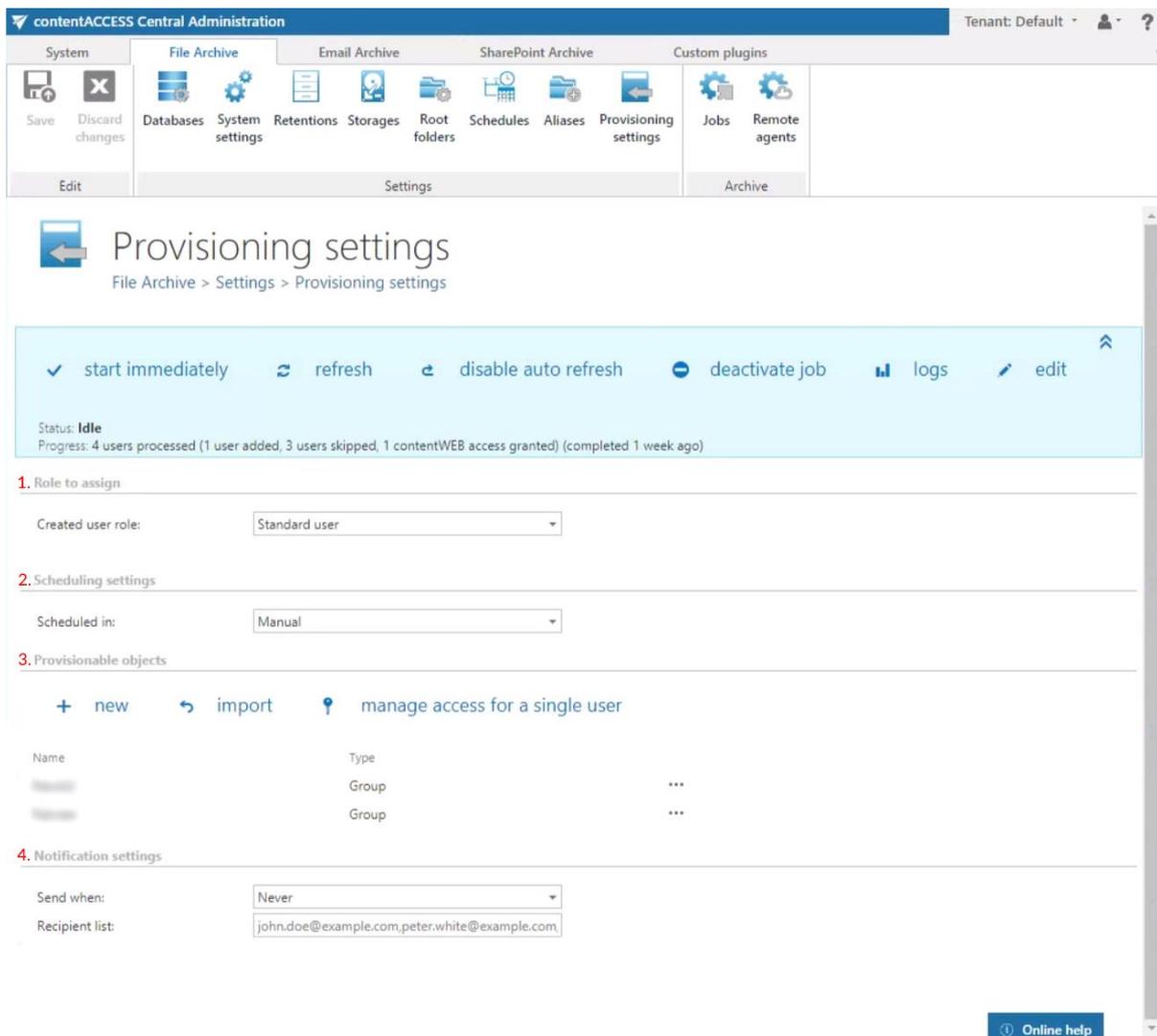
Andras Palffy

Note: This manage access option is available for the logged on administrator if his role assignment contains Manage tenant permission on the assigned tenant and also View archive folder rights. Read more in [Managing access to contentACCESS objects](#).

Configuration of File archive provisioning:

To configure the File archive provisioning, the administrator is required to set

1. The role, that will define the file archive user's permissions in contentWEB. Standard user role is available in the list by default, other roles with other permissions must be first configured on the **Roles** page.
2. The time periods, when the provisioning will run – this must be configured in section “Scheduling settings”.
3. The objects to be provisioned – must be set in section “Provisionable objects”
4. Notification settings (optional)



The screenshot displays the 'contentACCESS Central Administration' interface. The top navigation bar includes 'System', 'File Archive', 'Email Archive', 'SharePoint Archive', and 'Custom plugins'. The 'File Archive' section is active, showing sub-sections like 'Databases', 'System settings', 'Retentions', 'Storages', 'Root folders', 'Schedules', 'Aliases', 'Provisioning settings', 'Jobs', and 'Remote agents'. The 'Provisioning settings' page is open, showing a status bar with 'start immediately', 'refresh', 'disable auto refresh', 'deactivate job', 'logs', and 'edit' buttons. The status is 'Idle' with a progress report: '4 users processed (1 user added, 3 users skipped, 1 contentWEB access granted) (completed 1 week ago)'. The settings are organized into four sections:

- 1. Role to assign:** 'Created user role:' dropdown set to 'Standard user'.
- 2. Scheduling settings:** 'Scheduled in:' dropdown set to 'Manual'.
- 3. Provisionable objects:** Includes '+ new', 'import', and 'manage access for a single user' buttons. A table lists objects with columns for Name, Type, and Group.

Name	Type	
...	Group	...
...	Group	...
- 4. Notification settings:** 'Send when:' dropdown set to 'Never'. 'Recipient list:' text input containing 'john.doe@example.com,peter.white@example.com'.

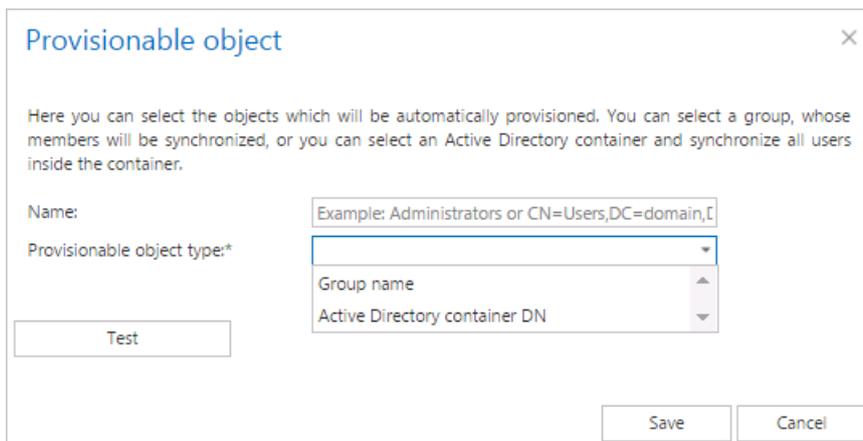
An 'Online help' button is located at the bottom right of the page.

Provisionable objects may be added:

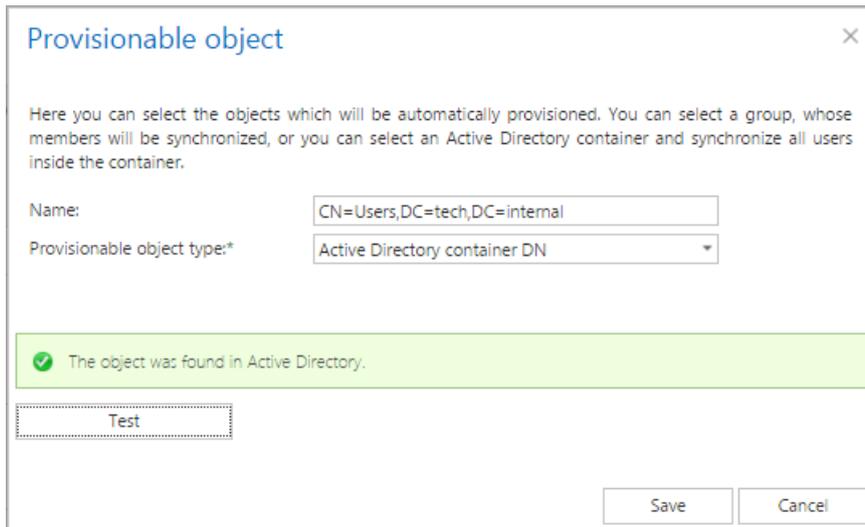
- a) from importable files, using the “import” function (described in more details in chapter [Importing contentACCESS configurations from files](#))
- b) manually, via the “new” button

To add object manually, click on “+ new” and specify the object(s) in the respective dialog. You can select a **group** that contains the objects to be provisioned, or you can select an **Active Directory container** and synchronize all users inside this container. Choose the object type and enter the data in the following format:

- in case of a **Group**: enter the name of the group
- in case of a **Container**: enter the distinguished name (DN) like in the sample.



It is recommended to use the “Test” button to verify if the Active Directory container DN/Group name has been correctly entered in the first text box.



Provisionable object [X]

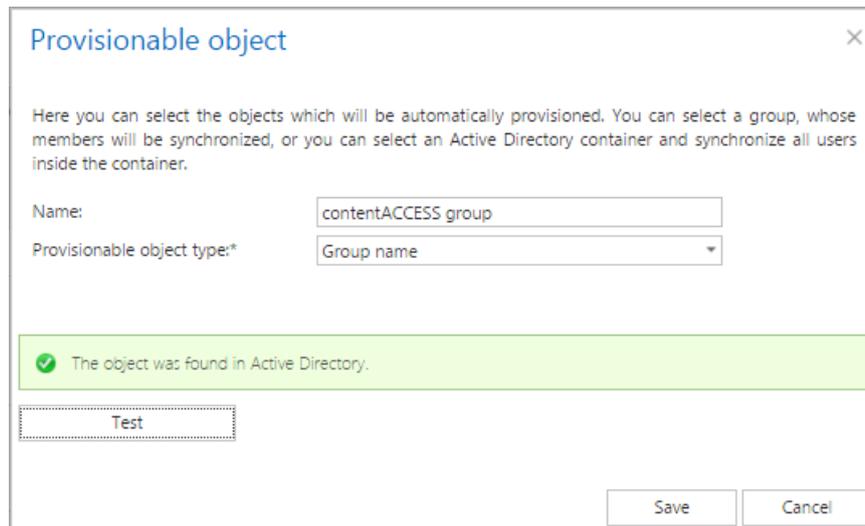
Here you can select the objects which will be automatically provisioned. You can select a group, whose members will be synchronized, or you can select an Active Directory container and synchronize all users inside the container.

Name:

Provisionable object type*:

The object was found in Active Directory.

Screenshot A: Selecting an AD container to be provisioned



Provisionable object [X]

Here you can select the objects which will be automatically provisioned. You can select a group, whose members will be synchronized, or you can select an Active Directory container and synchronize all users inside the container.

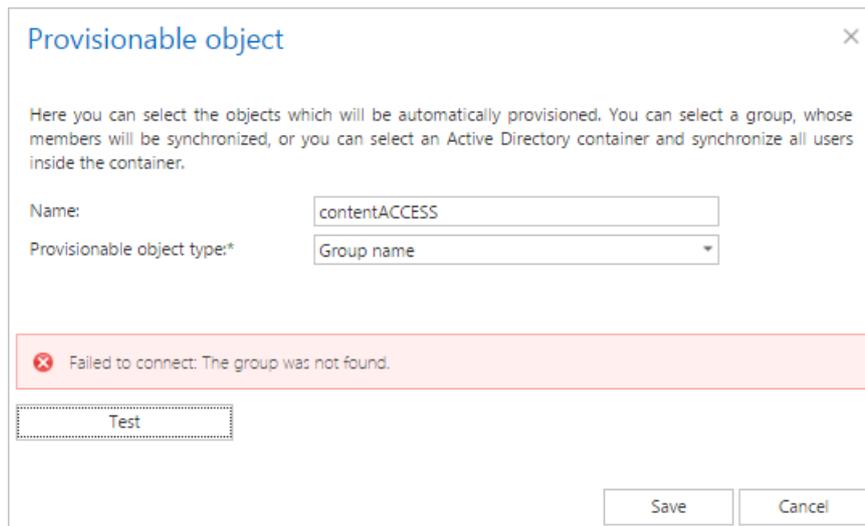
Name:

Provisionable object type*:

The object was found in Active Directory.

Screenshot B: Selecting an AD group to be provisioned

If incorrect data is entered, then the provisionable object is not found and the user is warned about this:



The provisioning job

- adds all the users involved in the Container/Group into contentACCESS
- grants contentWEB File Archive permissions (based on the selected role) for the users involved in the LDAP path/Group.

How to find the distinguished name (DN) of an Active Directory object

Objects are located within Active Directory domains according to a hierarchical path, which includes the labels of the Active Directory domain name and each level of container objects. The full path to the object is defined by the distinguished name (also known as a "DN").

If the object to be provisioned (to be synchronized) into contentACCESS is an Active Directory container, then it can be located in the Active directory using its DN. The distinguished name of an Active Directory object can be found using the "dsquery" command line application. For more information about the "dsquery" read [this](#) guide.

General use case for identifying the "Users" container in the Active directory

- Open a Windows command prompt.
- Type the command **dsquery group -name Users** (example: `dsquery group -name [known object name]`)
- The result will look like "CN=Users, CN=Builtin, DC=MyDomain, DC=com":

```

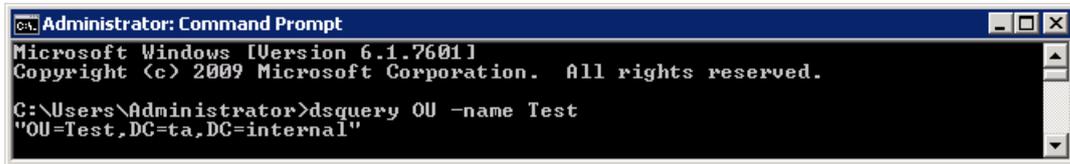
Administrator: Command Prompt
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>dsquery group -name Users
"CN=Users, CN=Builtin, DC=ta, DC=internal"

```

General use case for identifying the “Test” Organizational unit in the Active directory

- Open a Windows command prompt.
- Type the command ***dsquery OU -name Test*** (example: *dsquery OU -name [known object name]*)
- The result will look like “OU=Test, DC=MyDomain, DC=com”:



```

Administrator: Command Prompt
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>dsquery OU -name Test
"OU=Test, DC=ta, DC=internal"
  
```

File archive provisioning’s notification settings are used to send automatic email notifications to specific addresses if any warnings/errors occur. Set the notification emails if necessary and save your settings.

File system provisioning job description

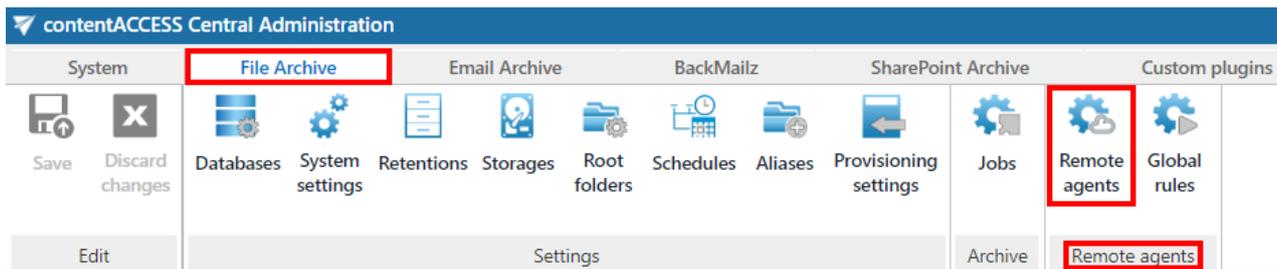
All the numbers and descriptions in the job’s progress have a particular meaning. In this section, we are going to explain the numbers and descriptions of a **File system provisioning job**.

Description	Explanation
x users processed	x users have been processed
x users added	x users have been added to the system
x users skipped	x users have been skipped
x users updated	x users have been updated in the system
x objects failed	x groups’ processing failed
x contentWEB accesses granted	contentWEB access has been granted for x users
x contentWEB accesses revoked	contentWEB access has been revoked from x users

Remote agents (file archive)

Go to **File Archive -> Remote agents -> Remote agents**.

The list of remotely installed agents, which are archiving files located on network shares or uploading PST files, can be found on this tab.



It is possible to download the [Remote File Archiving](#) agent (application) and contentACCESS web services (Proxy) setup or agent configuration (.XML file) here.



Remote agents

File Archive > Remote agents > Remote agents

[refresh](#)
[download agent](#)
[download proxy](#)
[download agent configuration](#)

Refresh

Refresh the list of remote agents.

Remote File Archiving agent

The Remote File Archiving agent is used to archive files that are not accessible to contentACCESS server, and thus no regular archiving job can be defined to archive them; or to upload PST files to be later used for PST import. After it was installed and configured on a computer (for more info please read the [Remote File Archiving](#) manual), the agent will appear in the agent's list and can be configured either from the Remote File Archiving client application locally or by using the contentACCESS Central Administration.

contentACCESS Proxy

The contentACCESS proxy is a web service which ensures communication between front-end applications and the contentACCESS server through secure channel (using https protocol, if configured that way). It forwards application requests to contentACCESS server and isolates the server from the outer world.

Agent configuration

Since you can download the agent configuration file from central administration, it is very easy to install remote agents with GPO.

You have to select the user and the models. The RFA will be logged in under the selected user and will support the features based on the selected models. It is possible to disable the logout option by checking



the **Disable logout** checkbox. It is also possible to pick a **Database**, **Storage** and **Index zone** from the respective dropdown lists.

Agent configuration ✕

Service url:

User:

Model: File system archive
 Email archive

Disable logout:

Database: ✔

Store:

Index zone:

Remote File Archiving configuration

Note: First, the agent must be installed and registered, otherwise the list will be empty.

After clicking on the context menu of the selected agent, list of the rules, which are assigned to that agent, will appear. The RFA rule is identical to the [File archive job](#) configuration. The context menu of the agent also allows to Assign database, storage and index zone; enable/disable it; create a new rule or open the active directory settings.



Remote agents

File Archive > Remote agents > Remote agents

Status	Server name	Server IP	Enabled	Last ping	Database	Store	Index zone
Offline	TACATEST	192.168.190.96	*** Yes	1/10/2019 8:49:46 PM	MNEstestDB	TestingStorage	Default index zone
<div style="border: 1px solid #ccc; padding: 5px;"> Assign database, store and index zone Enable Disable Create rule Active directory </div>							
Rule ID	Name	Type	Scope	Enabled	File status	Statistics	
12	Rule 01	*** RFA	Local	Yes	Finished successfully	Newly archived files: 11. Processed folders: 1.	
13	PST to cA importing	*** PST	Local	Yes	Finished successfully	Processed folders: 1. New PST files found: 3.	
14	PST to cA test	*** PST	Local	Yes	11/8/2018 3:27:16 PM	11/8/2018 3:27:17 PM	Finished successfully
15	Schedule test	*** RFA	Local	Yes	1/10/2019 8:49:48 PM	1/10/2019 8:49:53 PM	Finished with errors
8	PST import	*** PST	Global	Yes	10/26/2018 4:30:40 PM	10/26/2018 4:30:47 PM	Finished successfully
9	TECH-ARROW files	*** RFA	Global	Yes	11/30/2018 2:33:35 PM	11/30/2018 2:33:42 PM	Finished successfully
Offline	VMDJODEV	192.168.190.104	*** Yes	5/25/2018 12:34:47 PM	-	-	-
Offline	TACATEST05	192.168.190.106	*** Yes	6/14/2018 3:32:51 PM	-	-	-

The context menu of the rule allows to edit it, configure its settings or delete it (PST rule can be only configured).

Rule ID	Name	Type	Is readonly	Enabled
1	Rule04	RFA	No	Yes
2	Archive local	Edit	No	Yes
3	Archive share	Configure	No	Yes
6	DaniTest	Delete	No	Yes
7	PST import to cA	*** PST	No	Yes
10	PST 2	*** PST	No	Yes

Note: For more information about Remote agents and Remote File archiving, please check out [this](#) manual.

Global rules (remote file archive)

Go to **File archive -> Remote agents -> Global rules**.

On this page it is possible to define and manage global remote file archive rules for [Remote agents](#). These rules can be then assigned only to selected agent(s) or to all available agents and will appear in the list of rules on the [Archive tab](#).

To create a new rule, click on **+ new rule**. Fill in the display name and check the **Is enabled** checkbox if you want the rule to be available to be assigned to remote agents.

Global rule details ✕

Display name:

Is enabled:

When the rule's configuration page opens, you will see a warning that you are configuring a global rule.

 You are configuring a global rule. The changes will be applied on all of the agents, where the rule is assigned. ✕

On the configuration page go through the following sections; most of them are mandatory, filtering settings are optional:



✓ Scheduling settings

In this step the running times of the rule must be selected. It is possible either to select a scheduler from the list or to create a new scheduler via create new option. For more information about how to set schedulers please refer to the section [Schedules](#) above.

Scheduling settings

Scheduled in:

Manual

✓ Retention settings

Under retention settings, the administrator may select a previously configured time period. During this time it will be not possible to delete the archived items from the storage. It is recommended to set here a time interval based on data recording regulations required either by the law of the country, or by internal company policies. For more information how to set retentions check section [Retentions](#) above.

Retention settings

Retention:

1 year

✓ Remote locations

In this section the user is required to select the remote share(s) where the data to be archived are located. To add a new folder, click on **+new** to open the **File Path** dialog. Specify the remote folder location. If necessary, check the **Use explicit credentials** checkbox and enter the applicable user credentials (we highly recommend to do this for remote folders). Click **OK**.

File Path ✕

File location settings

Path:

Use explicit credentials: Use explicit credentials

User name:

Password:

Confirm Password:

Important!!! It is recommended to specify a file path that can be accessed from anywhere. This is quite important also in case that the user has contentACCESS installed in a distributed environment (using multiple cluster nodes).

✓ Item filtering

This configuration enables the user to filter among items by 3 types of criteria: by age, size or file type. It is also possible to use more filters simultaneously. For filtering files according to any of these criteria, activate the filter button by checking the checkbox next to it, then click on the activated button.

Item filtering

Filtering type:

Filters:

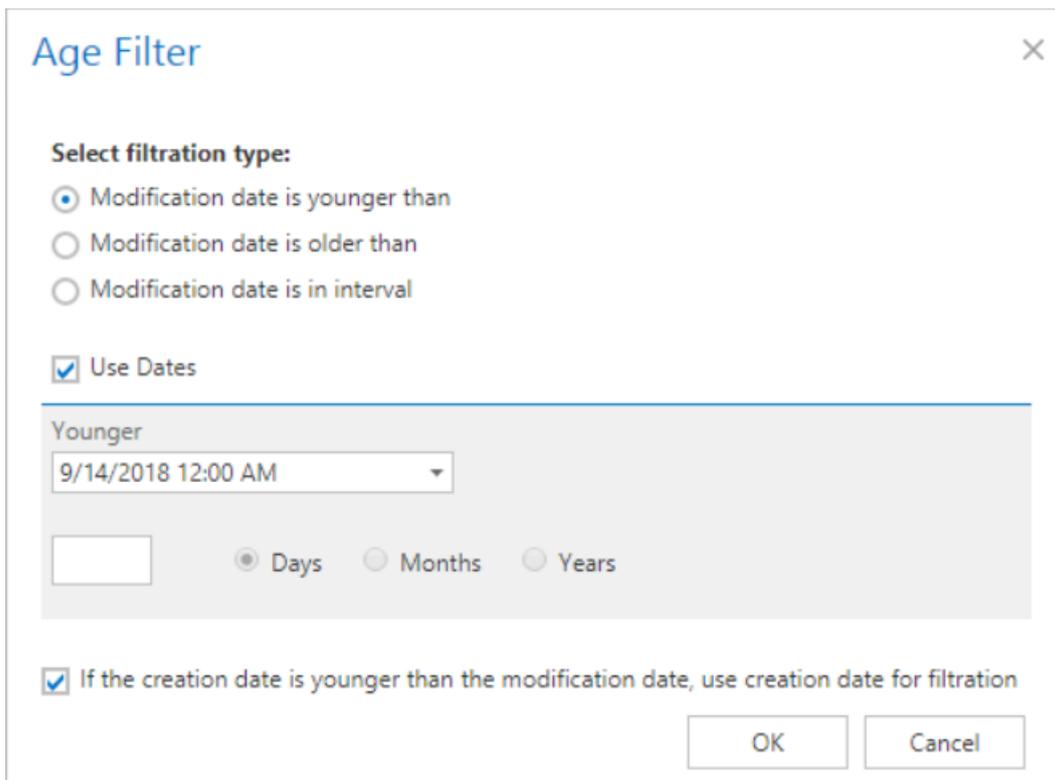
- Age filter
- Size filter
- File Type filter

▪ Age filter

With this filter the user may select files of specific age to be processed. The user has multiple choices here; he can select the filtration type from the list, and a) use either the **Use dates** option and pick up a date from the calendar, or b) he can enter a value into days/months/years textbox and search for the files that are younger than/older than or fall into time interval set here.

Using the creation date or modification date for filtering: By default, the modification date is the determinative date, but this can be changed by checking the **“If creation date is younger than the**

modification date, use creation date for filtration” checkbox. In certain cases, the creation date of a file is set to younger date than the modification date of a file. This happens when a file is copied to another external disk (for example from disk G to disk I). In this case, the creation date will be set to the date of the copy action. If the user would like to use this file in the future and would not like to archive it, this feature can solve the problem - it is possible to exclude the file with the newer creation date from the process. To create a proper archiving policy take into consideration these rules: <https://support.microsoft.com/en-us/kb/299648>.

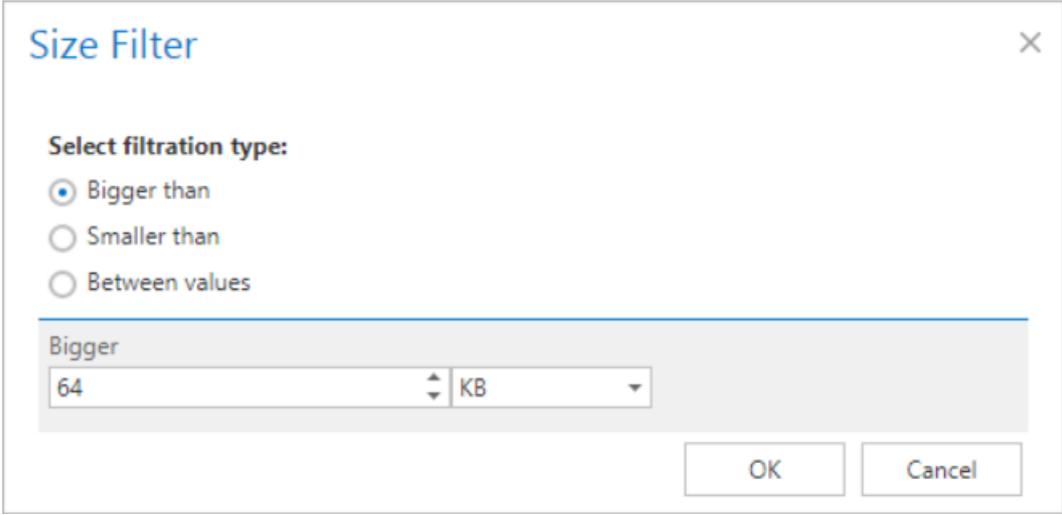


If the Age filter has been set, click **OK**.

▪ Size filter

This filter can be very useful because it enables to find the biggest files to archive and save space. For filtering files according to this criteria, activate **Size filter** button by checking the checkbox next to it, then click on the active button.

In the **Size filter** dialog choose from the filtering types (**Bigger than**, **Smaller than**, or **Between values**), enter the size in kilobytes, megabytes or gigabytes and click **OK**.



Important!!! When the user changes the file content of an already archived item, e.g. deletes a picture from the file and saves it to the original location, (and thus the file size will be reduced e.g. from 110 to 85 kB) and file size filter is set on >100 kB, then the rule will not archive the newly created item by the next processing. The newly created item will be saved in the original location, and the old shortcut will be present in the original location, which will still link to the old file without any changes.

For this reason, it is recommended to always check the size filter settings if a file has not been archived by the next run of the rule.

▪ File type filter

This filter was improved to select certain file types for processing. For filtering between documents according to this criteria, activate **File Type filter** button by checking the checkbox next to it, then click on the active button.

In the **File Type filter** dialog the user may select the file types that need to be processed (option **Process ONLY selected file types**), or he may specify file types that should be excluded from the processing (**DO NOT process selected file types**).

The file types selected in the whitelist/blacklist are displayed below the grid in a read-only text box. Any file types (also file types that are not included in the whitelist and/or blacklist) can be specified in the **Custom file types** text box.

File Type Filter ✕

Filter items based on file types:

Process ONLY selected file types

<input checked="" type="checkbox"/>	Select all for whitelist
<input type="checkbox"/>	7z
<input checked="" type="checkbox"/>	AAC
<input type="checkbox"/>	accda
<input type="checkbox"/>	accdb
<input checked="" type="checkbox"/>	accdc
<input type="checkbox"/>	accde
<input type="checkbox"/>	accdr

Selected file types:
3g2,3gp,AAC,accdc

Custom file types:
dwg

DO NOT process selected file types

<input checked="" type="checkbox"/>	Select all for blacklist
<input type="checkbox"/>	3g2
<input type="checkbox"/>	3gp
<input type="checkbox"/>	3gp2
<input type="checkbox"/>	3gpp
<input type="checkbox"/>	7z
<input type="checkbox"/>	AAC
<input type="checkbox"/>	accda

Selected file types:
jpg

Custom file types:

✓ Resource settings

Set the value, which will determine how many items will be processed simultaneously by the file archive job. The recommended value is 2, as in our case.

Resource settings

Worker thread count:

After everything is configured, **save your settings**.

On the configuration page, the user has also these options:



TECH-ARROW files

File Archive > Remote agents > Rules > TECH-ARROW files

[Assign to agents](#) [Disable rule](#) [Rule statistics](#)

- **Assign to agents** - assign the rule to selected agent(s) or to all available agents

Agent selection ✕

Automatically assign to all workstations

Assign rule to the following workstations:

Workstation name ▲

<input checked="" type="checkbox"/>	TACATEST
<input type="checkbox"/>	TACATEST05
<input type="checkbox"/>	VMDJODEV

[refresh agents list](#)

- **Enable/Disable rule** – if the rule is Disabled, it can be Enabled here (also vice versa)
- **Rule statistics** – check the statistics of the last run of the rule

On the **Global rules** page, it is possible to perform the following actions from the context menu of a rule:



Global rules

File Archive > Remote agents > Global rules

+ new rule

Name	Enabled	Tenant
RFA test rule	Yes	TECH-ARROW
TECH-ARROW files	Yes	TECH-ARROW

- Assign to agents
- Configure
- Disable
- Edit
- Show statistics
- Delete

- **Assign to agents** - assign the rule to selected agent(s) or to all available agents
- **Configure** – this opens the configuration page of the rule
- **Enable/Disable** – enable or disable the rule
- **Edit** – here the administrator can change the name and availability of the rule
- **Show statistics** – this shows an overview of the last run(s) of the rule on the assigned workstations
- **Delete** – this option will delete the selected rule

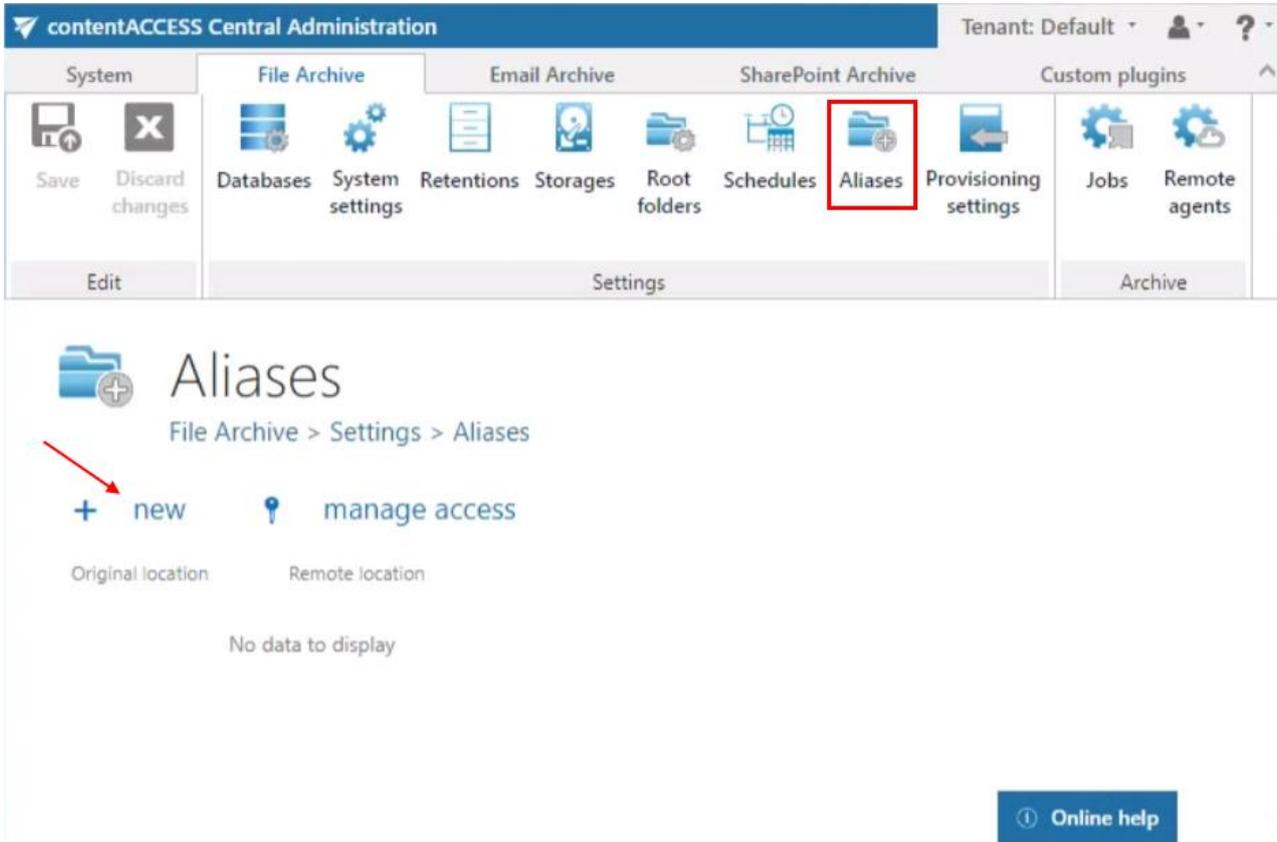
Configuring aliases

What are aliases? Aliases are multiple folder paths with different names, which point to the same folder/set of files.

Currently, contentACCESS uses aliases when mapping remote location paths to local paths, which is a must-to configuration for the Remote shortcutting job. (For more information refer to section [Configuration of Remote shortcutting job.](#))

Configuring an alias for the Remote shortcutting job. If you are shortcutting remote shares, but contentACCESS has archived the matching files on a local share, the shortcutting job must “pair” the remote share with the local share to be able to replace the matching files with shortcuts on the remote share and to open them. This “pairing” by the job can be done only in case, if remote and local shares are “paired” in contentACCESS, too (i.e. Aliases are specified).

Navigate to **File Archive** → **Settings** → **Aliases** tab on the Central Administration’s ribbon. On the **Aliases** page click on **+ new**:



The screenshot shows the 'contentACCESS Central Administration' interface. The top navigation bar includes 'System', 'File Archive', 'Email Archive', 'SharePoint Archive', and 'Custom plugins'. The 'File Archive' section is active, showing options like 'Databases', 'System settings', 'Retentions', 'Storages', 'Root folders', 'Schedules', 'Aliases' (highlighted with a red box), and 'Provisioning settings'. Below this, the 'Aliases' page is displayed, showing a breadcrumb 'File Archive > Settings > Aliases' and two main actions: '+ new' (with a red arrow pointing to it) and 'manage access'. Below these actions are labels for 'Original location' and 'Remote location', and a message 'No data to display'. An 'Online help' button is visible in the bottom right corner.

Note: The “+ new” option is unavailable for the logged on user if the “Add repository items” permission on the tenant is not allowed in his role assignment.

The “manage access” option allows to grant access permissions on the selected alias for a second user. This “manage access” option is available for the logged on administrator if his role assignment contains the Edit repository item – All allowed permission on the tenant. Read more in [Managing access to contentACCESS objects](#).

The **Alias repository** will open. The repository requires to specify the:

- **Original location:** select the file archive root folder from the dropdown list; this is the file path used by the archive job
- **Remote location:** add the matching remote file path that needs to be replaced with shortcuts

Further click on **Save**. The **Remote location** that you configured here can be selected on the **Remote shortcutting** job’s configuration page later on.



Alias repository ✕

Original location:

Remote location:

Note: A path extension can be added when setting the remote file location on the Remote shortcutting job's configuration page.

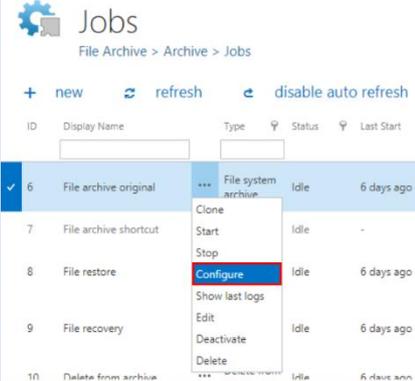
Configuration of jobs available in contentACCESS File Archive

Once all the necessary settings are done, select the tenant and navigate to the **File Archive** tab. Under **File Archive** → **Archive** group click on the **Jobs** control button, then click on **+ new** option.

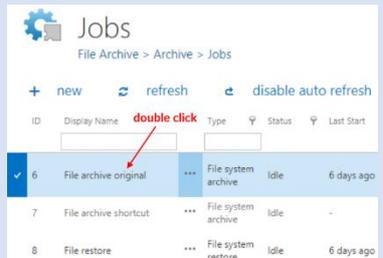
Note: You can configure a file system job either immediately, or later on by navigating to the file system jobs' page, using the "Configure" option in the given job's context menu. The job configuration page can be also opened with a double click on the selected job in the jobs' grid.



Screenshot A: Configure the job immediately when it is created



Screenshot B: Opening the job's configuration page from its context menu



Screenshot C: Opening the job's configuration page with a double click in the grid

Configuration of File archive retention changer job

This job changes the retention time of selected files if it's allowed to change the retention on storage level. Storages that support this change are: Disk, Azure, Amazon S3.

Go to Jobs -> click on **+new** -> select **File archive retention changer**.

Add new job instance ✕

Available jobs:

Run on node:

Display name:

Description: Changes the retention of the selected documents

On the job's configuration page go through the following sections:

✓ Running mode settings (mandatory)

The job can be run in 3 modes:

- 1) **Immediate processing** -> collects the documents and changes their retention.

Running mode settings

Run in mode:

- 2) **Create report** -> collects the documents and provides a csv file with a list of documents. The administrator can review and edit the list of affected documents.

Running mode settings

Run in mode:

Generated report file:

File name:	GeneratedRC_12_16_2019 7_42_18 PM.csv
Size:	2.6 KB
Date:	12/16/2019 7:42:18 PM

- 3) **Apply report** -> a csv file with a list of documents to be processed must be uploaded. The administrator can delete documents from the list before running the job (only documents which are in the list will be processed). The job reads the list and changes the retention of the documents that are on the list.



Running mode settings

Run in mode:	<input type="text" value="Apply report"/>
Reviewed report file:	<input type="text" value="Please upload a csv file"/> ...
File name:	GeneratedRC_12_16_2019 7_42_18 PM.csv
Size:	2.6 KB
Date:	12/16/2019
<input type="button" value="Get uploaded file"/>	

✓ Scheduling settings (mandatory)

In this section the running times of the **retention changer job** must be selected. It is possible either to select a scheduler from the list or to create a new scheduler via the **“Create new ...”** option.

Scheduling settings

Scheduled in:	<input type="text" value="Manual"/>
	<ul style="list-style-type: none"> Create new ... <li style="background-color: #0070c0; color: white;">Manual TaskRunnerScheduler

✓ Retention settings (mandatory)

Select the new retention to be applied for the documents.

Retention settings

Target retention:	<input type="text" value="5Y"/>
-------------------	---------------------------------

✓ Folders to process (mandatory)

In this section, the user is required to select the folder(s) where the archived data are located. There are two available options how the list of folders may be specified:

- a) The folder(s) may be added **via +new option**. In this case the folder(s) must be added manually one-by-one. Click on **+new** to open the **File Path** dialog.

Click on **“new”** to specify the folder that contains the files with retention to be changed. In the **“Folder to process”** dialog unroll the list of already created roots and select the one that should be applied. This

dropdown lists the roots that are already configured (in File Archive settings: *File Archive* → *Settings* → *Root folders*). Enter the **Relative path** if necessary, test the path via the “Test” button and click “OK”.

Folders to process

+ new ↶ import

Folder to process
×

Root

Relative path

✓
Connection successfull!

- b) The **folder list may be also imported from a file**. The file to be imported must contain the list of folders that should be processed. Click the **import** button and the **Import file location dialog** opens. Specify here the required settings according to chapter [Importing contentACCESS configurations from files](#) of this guide.

Folders to process

+ new ↶ import

Import folders to process
×

Make a new list, delete all existing items

Skip existing items, import new ones

Import method:



✓ Filtering settings (optional)

Click on the **Change filter** button and set the filtering according to your needs and/or regulations. To learn more about how to work with filtering settings, please, check [this](#) section of our documentation.

Filter settings

✕

visual text

AND	Creation date	Older than	1Y	📅	✕
	Creation date	Younger than	2Y	📅	✕

[+add group](#) [+add condition](#)

[+add new group](#)

OK Cancel

Note: In certain cases, the creation date of a file is set to younger date than the modification date of a file. This happens when a file is copied to another external disk (for example from disk G to disk I). In this case, the creation date will be set to the date of the copy action. Because of this, we recommend to always check **Filtering settings** if something does not get processed.



✓ Notification settings (mandatory)

Select here, when you will need to get notification emails from the **Retention changer job**. It is possible to set here if you need a notification email always/never, or you need it only if an error/warning occurred during the process – for example, if the retention change of one or more items failed, then you may get a notification email about this error. Into the **Recipient list** textbox insert the email addresses of the people whom you would like to send these emails to – if there are multiple recipients, the addresses must be separated by “,” or “;”.

Notification settings

Send when:

Recipient list:

✓ Resource settings (mandatory)

Set the value, which will determine how many items will be processed simultaneously by the **Retention changer job**. The recommended value is 2, as in our case.

Resource settings

Worker thread count:

At the end never forget to save your job configurations: click on **Save** in the left upper corner of UI.

Configuration of File system archive job

In this section we will configure a file system archive job, which will run every day from 6 PM, archive our 1-2 year old files and replace the archived files with shortcuts. Our database, storage, root folder, retention and scheduler are already configured. Navigate to **File Archive** → **Archive** → **Jobs** button, click on **+new**. In the **Add new job instance** dialog select **File system archive** job from the **Available jobs**: dropdown list. Select the node, where the job should run, from the **Run on node** list. Now we would not like to specify a node, so we select “Any available”. Enter a **Display name**, and click on **Add**.



Add new job instance ✕

Available jobs:

Run on node:

Display name:

Description: Plugin for File system archiving.

On the job's configuration page go through the following sections; most of them are mandatory, filtering settings are optional:

✓ **Report mode settings:**

If the **Use report mode** checkbox is checked, the job will run in report mode. After the job finishes its run in this mode, the user will be able to download a .csv report file here in this section. The file will contain a list of files that belong to the folder(s) that is (are) selected in section **Folders to process** of the job and some information to them, including whether they will be processed or not.

Report mode settings

Use report mode:	<input checked="" type="checkbox"/>	
Generated report file:	File name:	JobReport_7779b902-c4eb-49f0-b7de-6eed8313a926.csv
	Size:	1.3 KB
	Date:	4/4/2019 3:01:51 PM
<input type="button" value="Download report"/>		



	A	B	C	D	E
1	FileName	ModificationDate	Path	Status	Filter
2	10-crucial-	5/19/2017 13:26	C:\TestReport\	will be processed	no filter
3	256x256_p	1/18/2017 14:50	C:\TestReport\	will be processed	no filter
4	9h6c0qj.jp	1/12/2017 10:36	C:\TestReport\	will be processed	no filter
5	ai-email.jp	2/22/2017 14:26	C:\TestReport\	will be processed	no filter
6	bdb3d704:	2/1/2017 11:13	C:\TestReport\	will be processed	no filter
7	cloud.mail	2/7/2017 13:40	C:\TestReport\	will be processed	no filter
8	office-101	3/17/2017 13:10	C:\TestReport\	will be processed	no filter
9	Outlook-E	5/29/2018 11:18	C:\TestReport\	will be processed	no filter
10	pros-and-c	5/29/2018 11:18	C:\TestReport\	will be processed	no filter
11	TestingRFA	5/31/2018 12:23	C:\TestReport\	will be processed	no filter
12	windows-1	5/29/2018 11:18	C:\TestReport\	will be processed	no filter

Screenshot: Report file preview

✓ Scheduling settings:

In this step the running times of the archive job must be selected. It is possible either to select a scheduler from the list or to create a new scheduler via create new option. For archiving job, it is recommended to set up a scheduler that will run always, or in certain times during the week. Our job will run every day from 6 PM till midnight, after business hours. (For more information about how to set schedulers please refer to the section [Schedules](#) above.)

Scheduling settings

Scheduled in:

✓ Retention settings:

Under retention settings, the administrator may select a previously configured time period. During this time it will be not possible to delete the archived items from the storage. It is recommended to set here a time interval based on data recording regulations required either by the law of the country, or by internal company policies. In our country the required retention time is 10 years, so we set this here. (For more information how to set retentions check section [Retentions](#) above.)

Retention settings

Retention:

✓ Shortcut settings in File archive:

The user may decide, if the files will be archived using shortcuts or will be simply archived, creating a backup file to the original. It is also possible to set automatic deletion of the original document from the file system location. There are 3 shortcut types available in file system archive (the state before and after the archiving process is illustrated on the respective screenshots):

- a) **Keep original** method (backup files with versioning) is often used on a daily basis. The main advantage of this processing type is that the documents are ready at hand at any time and the versions can be accessed from the archive at any time, too. This method keeps the original item in the original file location:
- b) **Create shortcut from original item**: Files older than 1 year are usually archived with this shortcutting method. The main advantage of this method is the spared space on the computer. In case of need, the documents can be easily retrieved from the archive by clicking on the respective shortcut.

If the user modifies the file and saves it to the original location again, the next archive job will create a new version from it into the archive and will synchronize the shortcut with this new version.

- c) **Delete original**: with this method the user deletes the file from the original location when archiving it. This processing type is often used when the document is not in use any more, but it must be restorable until a definite date required by the general records retentions of the country.

The most suitable method to use depends on the situation. You can use all methods simultaneously to have your daily backup — create versions when files are changed or archive with shortcutting or delete original method in case of old(er) files.

Shortcut settings

Shortcut processing type: Create shortcut from original item ▼

Virtual drive server name: Keep original item Use default (tanews)

Create shortcut from original item

Delete original item

In this use case we will archive by using shortcuts. If you decide to use shortcutting, it is also necessary to specify the Virtual drive server name. This is the name of the server, where the virtual drive is installed. In our case it is *tanews*. It is strongly recommended to use a name of the server under which it will be always accessible (DNS alias at best). This server name is then included in the generated shortcuts. By using the **Use default** checkbox, you may automatically select the Virtual Drive, which is already configured in the **System → Client Applications → Virtual Drive configuration** section. It is very useful to use this option,



because if the Virtual Drive server name is changed, you have to change these settings only on the **Virtual Drive configuration** page. (For more information refer to section “



Virtual drive”).) On the jobs’ configuration page the default Virtual Drive will be prepopulated.

To check whether the connection to the Virtual drive server was established or not, please click on the **Test** button.

Shortcut settings

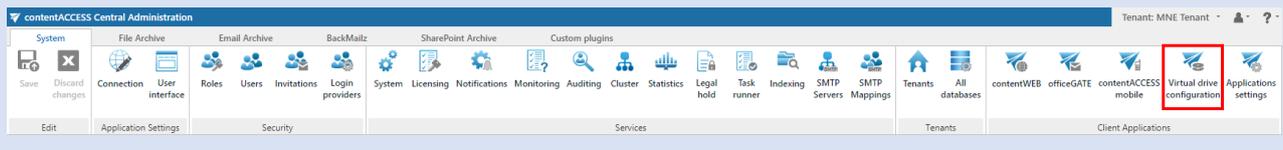
Shortcut processing type: Create shortcut from original item

Virtual drive server name: tanews Use default (tanews)

✓ Connection successfull

Test

Note: Virtual drive is included in the content ACCESS setup package. It needs to be configured on the *Virtual drive configuration* page (*System* tab → *Client applications* → *Virtual drive configuration* button on the ribbon). After these necessary steps, it will be shown among another drives (by default the Virtual drive will be the Z drive).



Note: The shortcuts used in file archive system are compatible with Macintosh operating system, too. It is a must to install TECH-ARROW’s WinShortcutter application on every client machine. It can be downloaded either from the Tools of the contentACCESS setup, or from our website, [here](#).

Note: It is important to bear in mind **that archiving an HTML** file with the shortcutting method in contentACCESS File Archive has certain technical limitations. If an HTML file to be archived contains pictures, then after the archiving process these pictures will not be visible when trying to open the HTML over the shortcut in the original location. However, these pictures will be still accessible when opening the HTML from the Virtual Drive.

✓ Folders to process:

In this section the user is required to select the local folder(s) or remote share(s) where the system data are located and will be archived. There are two available options how the list of folders may be specified:

- The folder(s) may be added **via +new option**. In this case the folder(s) must be added manually one-by-one. Click on **+new** to open the **File Path** dialog.

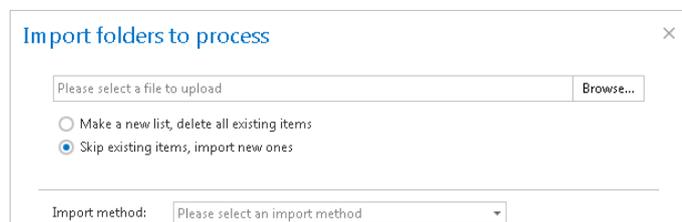
Click on **“new”** to specify the folder to be archived manually. In the **“Folder to process”** dialog unroll the list of already created roots and select the one that should be applied. This dropdown lists the roots that are already configured (in File Archive settings: *File Archive* → *Settings* → *Root folders*). Enter the **Relative path** if necessary, test the path via the **“Test”** button and click **“OK”**.

Folders to process




- The **folder list may be also imported from a file**. The file to be imported must contain the list of folders that should be processed. Click the **import** button and the **Import file location dialog** will open. Specify here the required settings according to chapter [Importing contentACCESS configurations from files](#) of this guide.

Folders to process

Important!!! It is recommended to specify a file path that can be accessed from anywhere. This is quite important also in case that the user has contentACCESS installed in a distributed environment (using multiple cluster nodes).



✓ **Exclude folders**

With this function, you may set which folders/subfolders should not be archived. If you would not like to exclude any folder from the archive process, you can skip these settings.

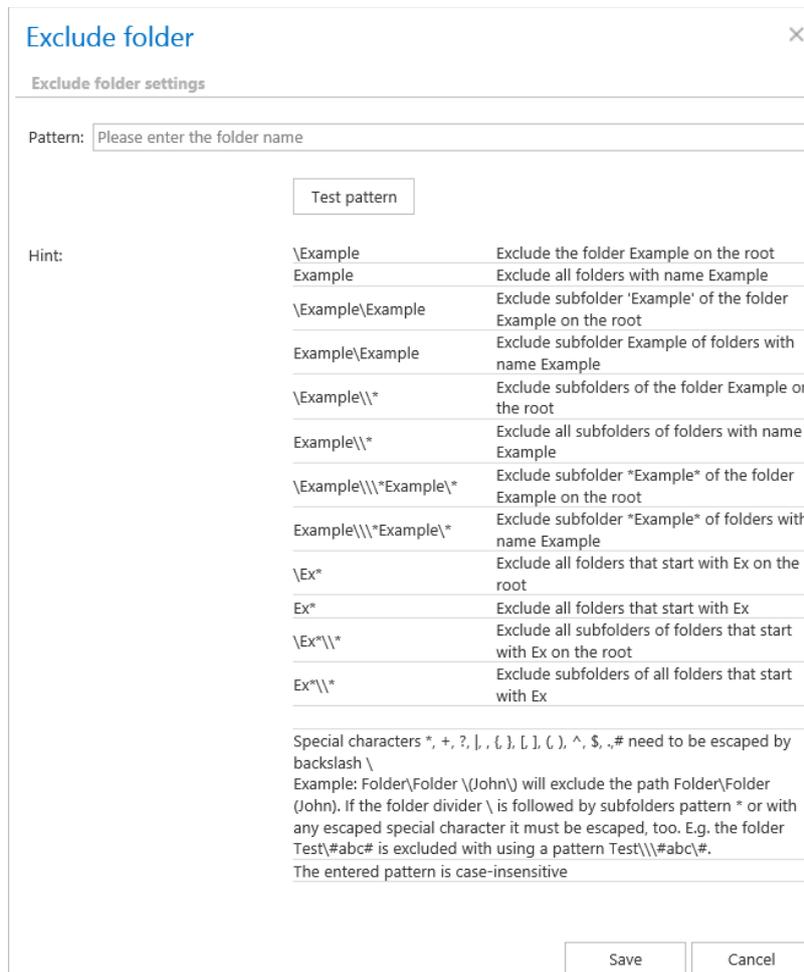
The folders may be excluded using one of the available methods: a) The folders to be excluded may be **added manually** via the **+ new** option or; b) may be **imported** in one of the available file formats via the **import** option.

Exclude folders

a) **+** new b) **↶** import

a) Add the folders to exclude manually:

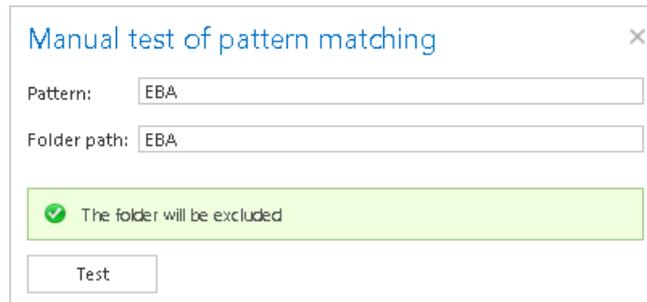
Click on **+ new** option. In the **Exclude folder** dialog's textbox specify the folder(s). Use the hints that are listed in the same dialog.



Test pattern button

This button is used to check if the entered pattern will be suitable for the path that the user would like to exclude from the archiving process. Click the **Test pattern** button to open the **Manual test of pattern matching** window. Enter the folder path into the **Folder path** field and click on **Test** button.

The test will be successful if the **Pattern** was correctly entered into the **Exclude folder** window.



b) **Import** the list of exclude folders:

Folders to be excluded may be imported as files in one of the available formats: CSV, XML, Tab delimited files or Space delimited file. The file to be imported must contain the list of folders to be excluded. To import such a file with the list of folders refer to chapter [Importing contentACCESS configurations from files](#) of this guide.

Excluding folders with special characters

Also the folders including special characters like brackets, hyphens, question marks etc. can be excluded from the archiving process. To exclude such folders from the archiving process, the special characters included in the folder(s) must be excluded **using the backslash “\” escape character**. The **escape character must be added before the special character** to be excluded in the **Exclude settings** of the archive job’s configuration page.

E.g. you have a “(folder)” in your file system, and the “(folder)” must be excluded (the special characters are the brackets), then you must specify the folder to be excluded like this: “\ (folder).”

This information is available at the bottom of the **Exclude folder** window:



Exclude folder ✕

Exclude folder settings

Pattern:

Hint:

\Example	Exclude the folder Example on the root
Example	Exclude all folders with name Example
\Example\Example	Exclude subfolder 'Example' of the folder Example on the root
Example\Example	Exclude subfolder Example of folders with name Example
\Example*	Exclude subfolders of the folder Example on the root
Example*	Exclude all subfolders of folders with name Example
\Example**Example*	Exclude subfolder *Example* of the folder Example on the root
Example**Example*	Exclude subfolder *Example* of folders with name Example
\Ex*	Exclude all folders that start with Ex on the root
Ex*	Exclude all folders that start with Ex
\Ex**	Exclude all subfolders of folders that start with Ex on the root
Ex**	Exclude subfolders of all folders that start with Ex

Special characters *, +, ?, [, , { }, [], (), ^, \$, ., # need to be escaped by backslash \

Example: Folder\Folder \John\ will exclude the path Folder\Folder (John). If the folder divider \ is followed by subfolders pattern * or with any escaped special character it must be escaped, too. E.g. the folder Test\#abc# is excluded with using a pattern Test\\#abc#.

The entered pattern is case-insensitive

✓ **Filtering settings:**

Click on the **Change filter** button and set the filtering according to your needs and/or regulations. To learn more about how to work with filtering settings, please, check [this](#) section of our documentation.

Filter settings
✕

visual

text

AND	Creation date ▼	>	2Y	📅 ✕
AND	Creation date ▼	<	1Y	📅 ✕

[+add group](#) [+add condition](#) Please pick a date or enter it as a relative date: 3D for 3 days, 3M for 3 months and 3Y for 3 years

[+add new group](#)

OK

Cancel

Note: In certain cases, the creation date of a file is set to younger date than the modification date of a file. This happens when a file is copied to another external disk (for example from disk G to disk I). In this case, the creation date will be set to the date of the copy action. Because of this, we recommend to always check **Filtering settings** if something does not get archived.

Important!!!: When the user changes the file content of an already archived item, e.g. deletes a picture from the file and saves it to the original location, (and thus the file size will be reduced e.g. from 110 to 85 kB) and file size filter is set on >100 kB, then File archive job will not archive the newly created item by the



next processing. The newly created item will be saved in the original location, and the old shortcut will be present in the original location, which will still link to the old file without any changes.

For this reason, it is recommended to always check the size filter settings if a file has not been archived by the next archiving process.

✓ **Notification settings.** Select here the cases, when you will need to get notification emails from the File Archive job. It is possible to set here if you need a notification email always/never, or you need it only if an error/warning occurred during the archiving process – for example, if the archive of one or more items failed, then you may get a notification email about this error. Into the **Recipient list** textbox insert the email addresses of the people, whom you would like to send these emails to. It may happen that the files are modified too often and too many version are created. With the **Notify if version count reaches** option it is possible to define a maximum number of versions, over which the notifications will be sent. It is recommended to set here a higher value. This feature might also be used for troubleshooting purposes. E.g. if the number of versions gets higher than the value specified here, then an error might have occurred during the processing. In this use case, the notifications will be sent to Walter White, if any errors or warning occur and/or version count reaches 50.

Notification settings

Send when:

Recipient list:

Notify if version count reaches:

✓ **Resource settings.** Set the value, which will determine how many items will be processed simultaneously by the file archive job. The recommended value is 2, as in our case.

Resource settings

Worker thread count:

Never forget to save your job configurations at the end: click on **Save** in the left upper corner of UI.



Now you need to wait till 6 PM, when the scheduler starts the job. Its running can be checked in the file archive jobs' grid.

Jobs
File Archive > Archive > Jobs

+ new refresh disable auto refresh

Filter: Active jobs

ID	Display Name	Type	Status
72	1 to 2 year old files	File system archive	Running

Where an end user may find his file system archive?

An end user has multiple choices where to view his archived files. He may either browse for them on the Virtual drive, or he can view them in contentWEB (contentWEB is the archive interface of contentACCESS). Virtual drive is a special contentACCESS extension developed by TECH-ARROW. Even if the archived item will not be present here on this drive (it will be present in contentACCESS), the user can browse for it here. A file opened through the Virtual drive is opened in read-only mode. This drive can be shared with any other users, so they can have a very easy access to the archived files. The shortcuts, that replace the originals, can be opened from the original file location. These shortcuts link to the virtual drive.

File system archive job description

All the numbers and descriptions in the job's progress have a particular meaning. In this section, we are going to explain the numbers and descriptions of a **File system archive job**.

Description	Explanation
x folders processed	x folders and their files have been processed, no further work on the folders required
x folders failed	x folders' processing failed, no items have been processed from these folders
x documents processed	x documents have been processed (archived, versioned or duplicated)

x skipped	x documents have been skipped, they were probably already archived or based on the filtering weren't even supposed to be processed
x failed	x documents' processing failed, see log for further information about the error
x version created	x documents' changed since the last archiving, therefore a new version has been created from them
x duplicates created	x documents have been found in another database and a new entry has been created for them in the current database
x newly archived	x documents have been newly archived
x folders skipped	x folders have been skipped because of filtering

Configuration of a File system restore job

File system restore jobs are used to restore already archived items from shortcuts back into the original file location. To create a restore job, navigate to **File Archive** → **Archive** → **Jobs** button (File archive jobs page), and click on **+new**. In the **Add new job instance** dialog, select **File system restore** job from the dropdown list, select a node where the job should run from the **Run on node** dropdown list (if you would not like to specify a node here and the job should run on any available node, then select “Any available”), enter a **Display name** and click on **Add**.



On the File system restore job's configuration page the user is required to set the following sections:



✓ Scheduling settings:

In this step the running times of the restore job must be selected. It is possible either to select a scheduler from the list or to create a new scheduler via create new option. Restore jobs are run only in specific cases. In most of the cases a **One time** scheduler is used for the restore job (e.g. with start date 7th of September as in our case). (For more information about how to set schedulers refer to the section [Schedules](#) above.)

Scheduling settings

Scheduled in:

✓ Folders to process

In this section you have to select the local folder(s) or remote share(s) where the shortcuts — which replaced the original files — are located. The job will restore the original files from these shortcuts. There are 2 methods how these folders may be specified:

- a) Via “**new**” button:

Click on **+ new** and fill in the path to restore into the **Folder to process** dialog.

Folders to process

+ new **↶ import**

Folder to process ×

Root: Relative path:

✔ Connection successful!

- b) Via the “**import**” button:

Folders to process

+ new **↶ import**

Import the folder path(s) to be restored from a file. Click “**import**”, browse for the import file, select the import method and specify the required settings, then upload the file with the desired file path(s). Learn more about importing files in chapter [Importing contentACCESS configurations from files](#) of this guide.

Important!!! It is highly recommended to specify file path(s) that can be accessed from anywhere. This is quite important also if the user has contentACCESS installed in a distributed environment (using multiple cluster nodes).



✓ **Exclude folders**

With this function, you may set which folders/subfolders should not be restored. The same rules as in the file archive job apply for these settings. If you would not like to exclude any folder from the restore process, you can skip these settings.

The folders may be excluded using one of the available methods: a) They may be **added manually** via the **+ new** option; b) or may be **imported** in one of the available file formats via the **import** option.

Exclude folders

a) **+** **new** b) **↶** **import**

a) Add exclude folders manually:

Click on **+ new** option. In the **Exclude folder** dialog's textbox specify the folder(s) to be excluded. Use the hints that are listed in the same dialog.

Exclude folder
✕

Exclude folder settings

Pattern:

Hint:		
	\Example	Exclude the folder Example on the root
	Example	Exclude all folders with name Example
	\Example\Example	Exclude subfolder 'Example' of the folder Example on the root
	Example\Example	Exclude subfolder Example of folders with name Example
	\Example*	Exclude subfolders of the folder Example on the root
	Example*	Exclude all subfolders of folders with name Example
	\Example**Example*	Exclude subfolder *Example* of the folder Example on the root
	Example**Example*	Exclude subfolder *Example* of folders with name Example
	\Ex*	Exclude all folders that start with Ex on the root
	Ex*	Exclude all folders that start with Ex
	\Ex**	Exclude all subfolders of folders that start with Ex on the root
	Ex**	Exclude subfolders of all folders that start with Ex

Special characters *, +, ?, |, {, }, [,], (,), ^, \$, ., # need to be escaped by backslash \
 Example: Folder\Folder \John\ will exclude the path Folder\Folder (John). If the folder divider \ is followed by subfolders pattern * or with any escaped special character it must be escaped, too. E.g. the folder Test\#abc# is excluded with using a pattern Test\\#abc\#.

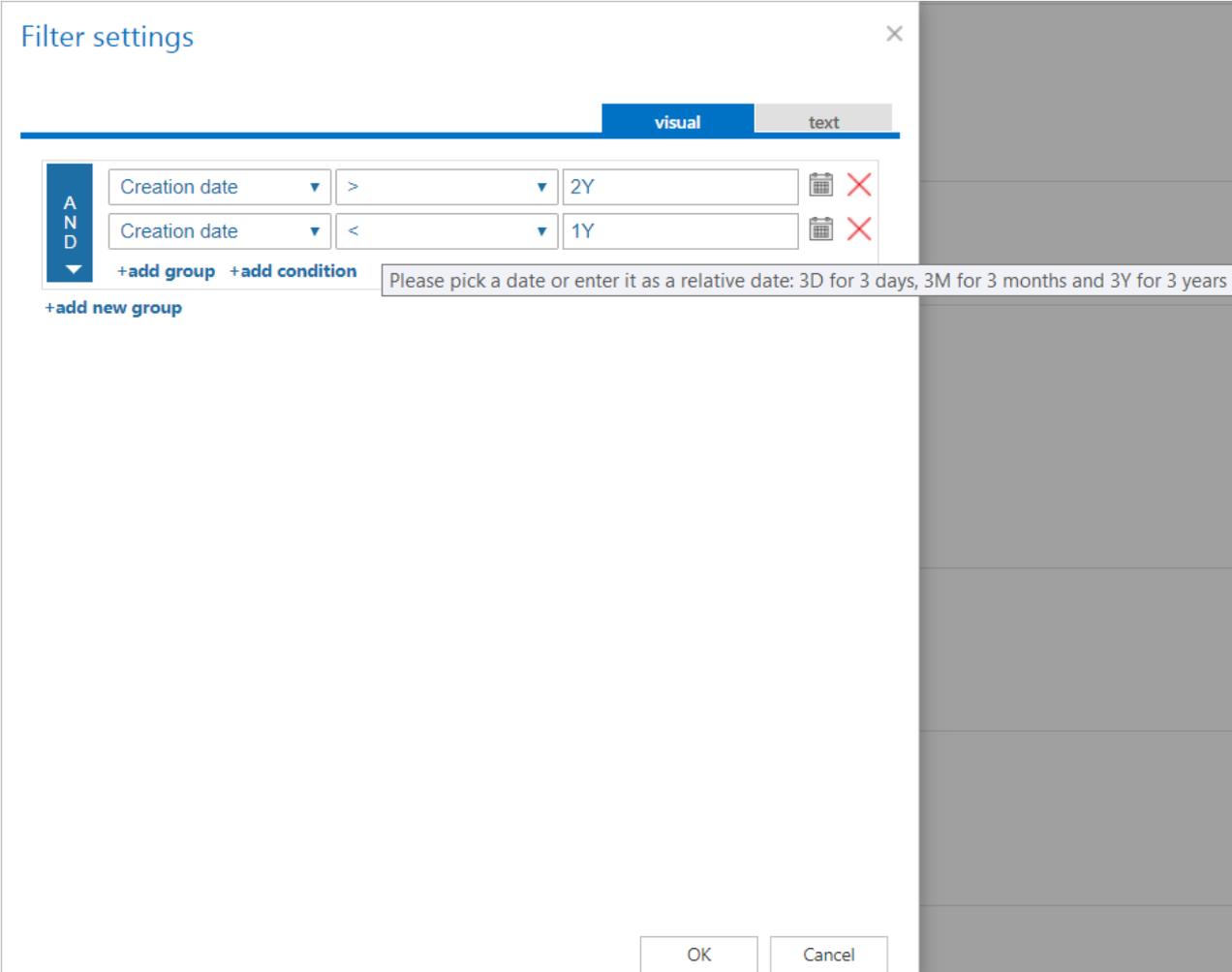
The entered pattern is case-insensitive

b) Import the list of folders:

Folders to be excluded may be imported as files in one of the available formats: CSV, XML, Tab delimited files or Space delimited file. The file to be imported must contain the list of folders to be excluded. To import such a file with the list of folders refer to chapter [Importing contentACCESS configurations from files](#) of this guide.

✓ Filtering settings:

Click on the **Change filter** button and set the filtering according to your needs and/or regulations. To learn more about how to work with filtering settings, please, check [this](#) section of our documentation.



Filter settings

visual text

AND

Creation date > 2Y

Creation date < 1Y

+add group +add condition

Please pick a date or enter it as a relative date: 3D for 3 days, 3M for 3 months and 3Y for 3 years

+add new group

OK Cancel



Note: In certain cases, the creation date of a file is set to younger date than the modification date of a file. This happens when a file is copied to another external disk (for example from disk G to disk I). In this case, the creation date will be set to the date of the copy action. Because of this, we recommend to always check **Filtering settings** if something does not get processed.

Important!!!: When the user changes the file content of an already archived item, e.g. deletes a picture from the file and saves it to the original location, (and thus the file size will be reduced e.g. from 110 to 85 kB) and file size filter is set on >100 kB, then File restore job will not restore the item by the next processing. For this reason, it is recommended to always check the size filter settings if a file has not been restored by the next restoring process.

✓ **Modification date**

This section allows to command to a restore job to restore the archived item a) either with the original modification date [**original modification date (default)**], or b) with the date of restore (**restore date**).

Modification date

Set the modification date of restored items to:

original modification date (default) ▼

original modification date (default)

restore date

It is rather recommended to restore the item with the original modification date, which is also set as default. However, “restore date” option might be useful in case that an archive job on the selected folder path is already running and the age filter is set to younger older than the restore date. With this setting, we can prevent the re-archivation of the restored document. For this reason we also set in this use case the “restore date” option.

- ✓ **Notification settings.** Select here the cases, when you will need to get notifications from the File Archive restore job. It is possible to set here if you need a notification email always/never, or you need it only if an error/warning occurred during the restoring process – for example, if the restore of one or more documents failed, then you will get a notification email about this error. Into the **Recipient list** textbox insert the email addresses of the people, whom you would like to send these emails to. Notifications emails may be used as means of troubleshooting of possible failures/errors. (In this use case we do not require such notifications, so we set it to “Never”)



Notification settings

Send when:

Recipient list:

- ✓ **Resource settings.** Set the value, which will determine how many items will be processed simultaneously by the file restore job. The recommended value is “2”.

Resource settings

Worker thread count:

Never forget to save your job configurations at the end: click on **Save** in the left upper corner of UI.

The restore job has finished its task. The restored items can be viewed with the restore dates in the original file location.

File system restore job description

All the numbers and descriptions in the job’s progress have a particular meaning. In this section, we are going to explain the numbers and descriptions of a **File system restore job**.

Description	Explanation
x folders processed	x folders and their files have been processed, no further work on the folders required
x folders failed	x folders’ processing failed, no items have been processed from these folders
x documents processed	x documents have been restored successfully
x documents skipped	x documents have been skipped, those items already exist in the file system in the original form
x documents failed	x documents' restoration failed, see logs for further details
x documents restored	x documents have been restored, equals to x documents processed



Configuration of File system recovery job

File system recovery jobs are used to re-generate a file system from the archive back into the original file location. This processing type can be used in the following cases:

- The entire folder structure has been deleted;
- One or more folders have been deleted;
- One or more documents from the folder(s) have been deleted and the user needs to get back these already archived documents from the archive.

The file system recovery can reconstruct the entire folder structure from the archive: the items that have been already archived will be put back into their source location. It will also create the folder if it was deleted from the folder structure. It is possible to recover any part of the structure:

- One or multiple folders;
- Recursive folder structure;
- One or more folder contents.

The file system recovery job is checking for the duplicates, so the same recovery job can be run safely multiple times, duplicates will not be created:

- If there is a shortcut for the recovered file in the folder – the file won't be recovered;
- If the file is already present in the folder – the file won't be recovered;
- If the same file is archived multiple times into the same folder – only the youngest file will be recovered.

The user has multiple options what to recover; it is possible to recover either the original file or the shortcut. The recovery job can be also used if the user archived the files with the "delete" method and these files should be put back into the file system.

To create a recovery job, navigate to **File Archive** → **Archive** → **Jobs** control button and click on **+new**. In the **Add new job instance** dialog, select **File system recovery** job from the dropdown list, select a node where the job should run from the **Run on node** dropdown list (if you would not like to specify a node here and the job should run on any available node, then select "Any available"), enter a **Display name** and click on **Add**.



Add new job instance ✕

Available jobs:

Run on node:

Display name:

Description:

On the File system recovery job's configuration page the user is required to set the following sections:

✓ Report mode settings:

If the **Use report mode** checkbox is checked, the job will run in report mode. After the job finishes its run in this mode, the user will be able to download a .csv report file here in this section. The file will contain a list of files that belong to the folder(s) that is (are) selected in section **Folders to process** of the job and some information to them, including whether they will be processed or not.

Report mode settings

Use report mode:

✓ Scheduling settings:

In this step the running times of the recovery job must be selected. It is possible either to select a scheduler from the list or to create a new scheduler via create new option. Recovery jobs are run only in specific cases. In most of the cases it is recommended to set a **One time** scheduler for the recovery job (e.g. with start date 7th of September at 6 PM), or to start the job manually from the status bar. (For more information about how to set schedulers refer to the section [Schedules](#) above.)

Scheduling settings

Scheduled in:

✓ Processing settings:

In this section, the user configures what will be recovered and how it will be recovered:



Recover - what will be recovered

- **Files and structure:** the recovery job will create the archived folder structure and recover the files from the archive
- **Structure only:** the recovery job will create the archived folder structure, but no files will be recovered

Overwrite existing file - when to overwrite the file if it already exists in the target location

- **Never:** do not overwrite existing files with the archived version
- **Always:** always overwrite existing files with the archived version
- **If older than the archived version:** overwrite only if the modification date of the existing file is older than the modification date of the archived file
- **If newer than the archived version:** overwrite only if the modification date of the existing file is newer than the modification date of the archived file

Set the modification date of recovered items to

- **Original:** the modification date of the archived item will be set on the recovered file
- **Recovery date:** the date, when the recovery job is running will be set on the recovered file

What to recover

- **Last known version:** the job will recover the latest version of the item from archive
- **Specific date:** the job will recover the version that was valid at the specified time. It means the version having modification date older or equal to the specified date.

Shortcut processing type

- **Recover original:** the job will recover the original file
- **Recover shortcut:** the job will recover the shortcut. If the user selects the shortcutting option, it is also required to specify the **Virtual drive server name**. By using the **Use default** option, the Virtual Drive that was already configured on the Virtual Drive configuration page will be automatically preselected. It is **recommended to use this option**, because if the settings are changed on the Virtual Drive configuration page, the value will be automatically used by the job, too, without a need to change the job's settings.



Processing settings

Recover:	Structure only	<input type="checkbox"/>
Overwrite existing file:	Never	<input type="checkbox"/>
Set the modification date of recovered items to:	Original	<input type="checkbox"/>
What to recover:	Last known version	<input type="checkbox"/>
Shortcut processing type:	Recover shortcut	<input type="checkbox"/>
Virtual drive server name:	<input type="text"/>	<input checked="" type="checkbox"/> Use default (test-cd-03.tech-arrow.com)
	<input type="button" value="Test"/>	

✓ Folders to process:

In this section the user is required to specify one or multiple archive folder(s), or recursive folder structure(s) that were deleted and need to be recovered from the archive. There are multiple options how to add new source location(s) with content needed to be recovered:

Folders to process

a) **+** new b) **↶** import

a) Via the **+ new** option:

Click **+new**. The **Folder to process** dialog will open. First, we select the **Root** (source) file path from the dropdown list and enter the subfolder to the **Relative path** text box if necessary. Next, select where the files from the folder will be recovered to:

To original location - items will be recovered to the place where they were archived from

Click on the **To original** button. You can test the accessibility by clicking on the **Test** button. Click **OK**.

Folder to process ✕

Root <input type="text" value="D:\TestTenant_FA_Root folder"/>	Relative path <input type="text"/>
Where to recover: <input checked="" type="button" value="To original location"/> <input type="button" value="To specific location"/>	
<input type="button" value="Test"/>	
<input type="button" value="OK"/> <input type="button" value="Cancel"/>	



To specific location - items will be recovered to a different folder

Click on the **To specific location** button. A new dropdown list will appear. Here you select the **destination folder** for the recovery (it must also be previously configured as a **Root folder**). You can also enter the subfolder to the **Relative path** text box if necessary. You can test the accessibility by clicking on the **Test** button – in this case, it checks the accessibility of both locations (the upper “source” and the below “target” location). Click **OK**.

b) It is also possible to import the files to recover from a file, where the file path(s) are specified. To import this file, click the “**import**” button and follow the steps specified in chapter [Importing contentACCESS configurations from files](#) of this guide.

Important!!! It is highly recommended to specify the file location as a path that can be accessed from anywhere. This is quite important also if the user has contentACCESS installed in a distributed environment (using multiple cluster nodes).

✓ **Exclude folders**

With this function you may set, which folders/subfolders should not be recovered. The same rules apply for these settings is in the file archive job. If you would not like to exclude any folder from the recovery process, you can skip these settings.

The folders may be excluded using one of the available methods: a) They may be **added manually** via the **+** **new** option; b) or may be **imported** in one of the available file formats via the **import** option.



Exclude folders

- a) + new
- b) ↶ import

a) Add exclude folders manually:

Click on + **new** option. In the **Exclude folder** dialog's textbox specify the folder(s) to be excluded. Use the hints that are featured in the same dialog.

Exclude folder
✕

Exclude folder settings

Pattern:

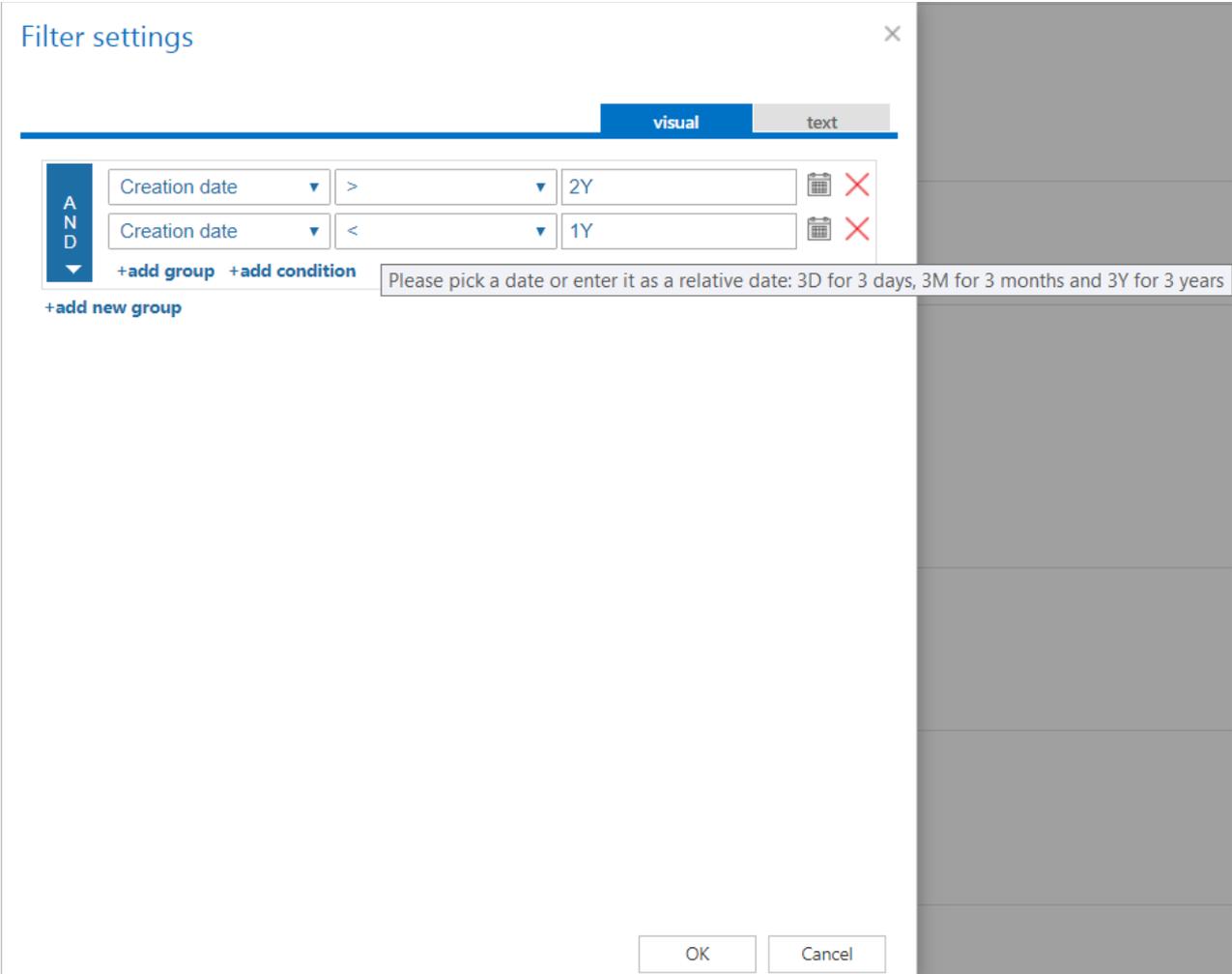
Hint:	<table style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 30%; padding-right: 10px;">\Example</td> <td>Exclude the folder Example on the root</td> </tr> <tr> <td>Example</td> <td>Exclude all folders with name Example</td> </tr> <tr> <td style="border-bottom: 1px solid #ccc; padding-bottom: 5px;">\Example\Example</td> <td style="border-bottom: 1px solid #ccc; padding-bottom: 5px;">Exclude subfolder 'Example' of the folder Example on the root</td> </tr> <tr> <td>Example\Example</td> <td>Exclude subfolder Example of folders with name Example</td> </tr> <tr> <td style="border-bottom: 1px solid #ccc; padding-bottom: 5px;">\Example*</td> <td style="border-bottom: 1px solid #ccc; padding-bottom: 5px;">Exclude subfolders of the folder Example on the root</td> </tr> <tr> <td>Example*</td> <td>Exclude all subfolders of folders with name Example</td> </tr> <tr> <td style="border-bottom: 1px solid #ccc; padding-bottom: 5px;">\Example**Example*</td> <td style="border-bottom: 1px solid #ccc; padding-bottom: 5px;">Exclude subfolder *Example* of the folder Example on the root</td> </tr> <tr> <td>Example**Example*</td> <td>Exclude subfolder *Example* of folders with name Example</td> </tr> <tr> <td style="border-bottom: 1px solid #ccc; padding-bottom: 5px;">\Ex*</td> <td style="border-bottom: 1px solid #ccc; padding-bottom: 5px;">Exclude all folders that start with Ex on the root</td> </tr> <tr> <td>Ex*</td> <td>Exclude all folders that start with Ex</td> </tr> <tr> <td style="border-bottom: 1px solid #ccc; padding-bottom: 5px;">\Ex**</td> <td style="border-bottom: 1px solid #ccc; padding-bottom: 5px;">Exclude all subfolders of folders that start with Ex on the root</td> </tr> <tr> <td>Ex**</td> <td>Exclude subfolders of all folders that start with Ex</td> </tr> </table>	\Example	Exclude the folder Example on the root	Example	Exclude all folders with name Example	\Example\Example	Exclude subfolder 'Example' of the folder Example on the root	Example\Example	Exclude subfolder Example of folders with name Example	\Example*	Exclude subfolders of the folder Example on the root	Example*	Exclude all subfolders of folders with name Example	\Example**Example*	Exclude subfolder *Example* of the folder Example on the root	Example**Example*	Exclude subfolder *Example* of folders with name Example	\Ex*	Exclude all folders that start with Ex on the root	Ex*	Exclude all folders that start with Ex	\Ex**	Exclude all subfolders of folders that start with Ex on the root	Ex**	Exclude subfolders of all folders that start with Ex
\Example	Exclude the folder Example on the root																								
Example	Exclude all folders with name Example																								
\Example\Example	Exclude subfolder 'Example' of the folder Example on the root																								
Example\Example	Exclude subfolder Example of folders with name Example																								
\Example*	Exclude subfolders of the folder Example on the root																								
Example*	Exclude all subfolders of folders with name Example																								
\Example**Example*	Exclude subfolder *Example* of the folder Example on the root																								
Example**Example*	Exclude subfolder *Example* of folders with name Example																								
\Ex*	Exclude all folders that start with Ex on the root																								
Ex*	Exclude all folders that start with Ex																								
\Ex**	Exclude all subfolders of folders that start with Ex on the root																								
Ex**	Exclude subfolders of all folders that start with Ex																								
<p>Special characters *, +, ?, , , { }, [], (), ^, \$, ., # need to be escaped by backslash \</p> <p>Example: Folder\Folder \(\John\) will exclude the path Folder\Folder (John). If the folder divider \ is followed by subfolders pattern * or with any escaped special character it must be escaped, too. E.g. the folder Test\#abc# is excluded with using a pattern Test\\#abc\#.</p> <p>The entered pattern is case-insensitive</p>																									

b) Import the list of exclude folders:

Exclude folders may be imported as files in one of the available formats: CSV, XML, Tab delimited files or Space delimited file. The file to be imported must contain the list of folders. To import such a file with the list of folders refer to chapter [Importing contentACCESS configurations from files](#) of this guide.

✓ Filtering settings:

Click on the **Change filter** button and set the filtering according to your needs and/or regulations. To learn more about how to work with filtering settings, please, check [this](#) section of our documentation.



Note: In certain cases, the creation date of a file is set to younger date than the modification date of a file. This happens when a file is copied to another external disk (for example from disk G to disk I). In this case,



the creation date will be set to the date of the copy action. Because of this, we recommend to always check **Filtering settings** if something does not get processed.

Important!!!: When the user changes the file content of an already archived item, e.g. deletes a picture from the file and saves it to the original location, (and thus the file size will be reduced e.g. from 110 to 85 kB) and file size filter is set on >100 kB, then job will not process the item during the next run.

For this reason, it is recommended to always check also the size filter settings if an item has not been processed.

✓ **Modification date**

The files can be recovered either with the original modification date or with the recovery date. It is recommended to set the recovery date if the folder is already processed by an archive job and the user wants to prevent the folder from re-archiving.

Modification Date

Set the modification date of recovered items to:

original modification date (default)
original modification date (default)
recovery date

✓ **Notification settings:**

The user may select here, in which cases he needs to get notifications from the recovery job. It is possible to set here that the notification emails will be sent only in case of errors or warnings, or they can be sent in all cases, too. Into the **Recipient list** textbox the user should insert the email addresses of the people, whom these emails should be sent to. Notifications emails may be used as tools of the troubleshooting process.

Notification settings

Send when:	Errors or warnings occur
Recipient list:	first name_last name@example.com

✓ **Resource settings:**

The user may set a value here, which will determine how many items will be processed simultaneously by the recovery job.



Resource settings

Worker thread count:

2

File system recovery job description

All the numbers and descriptions in the job's progress have a particular meaning. In this section, we are going to explain the numbers and descriptions of a **File system recovery job**.

Description	Explanation
x entities processed	x defined root folders have been processed
x entities failed	x defined root folders' processing failed, see logs for further details
x folders processed	x folders under the root have been processed
x folders failed	x number of subfolders' processing failed, see logs for further details
x documents processed	x documents have been processed by the recovery job
x documents failed	x number of documents' recovery failed
x documents skipped	x documents have been skipped because of filtering
x recovered	x documents have been successfully recovered

Configuration of Delete job in File archive

This job type deletes data, which have been archived, from the archive.

Note: First, you need to mark files/emails for delete in contentWEB (read more in [this](#) section).

Go to Jobs -> Add new -> Delete from archive.

Add new job instance ✕

Available jobs:

Run on node:

Display name:

Description: Removes the documents from the archive, with expired retention time.

On the job's configuration page go through the following sections; most of them are mandatory, filtering settings are optional:

✓ Running mode settings

The job can be run in 3 modes:

- 1) Immediate deletion** -> collects the expired documents and deletes them.

Running mode settings

Run in mode:

- 2) Create report** -> collects the expired documents and provides a csv file with a list of documents. The administrator can delete documents from the list.

Running mode settings

Run in mode:

Generated report file:

File name:	Generated_8_3_2017 7_27_25 PM.csv
Size:	120 B
Date:	8/3/2017 7:27:25 PM

- 3) Apply report** -> a csv file with a list of documents to be deleted must be uploaded. The administrator can delete documents from the list before running the job (only documents which are in the list will be processed). The job reads the list and if the documents are expired, deletes them.

Running mode settings

Run in mode:	<input type="text" value="Apply report"/>
Reviewed report file:	<input type="text" value="Please upload a csv file"/> ...
File name:	Generated_8_3_2017 7_27_25 PM.csv
Size:	120 B
Date:	8/3/2017
<input type="button" value="Get uploaded file"/>	

✓ Scheduling settings

In this step the running times of the delete job must be selected. It is possible either to select a scheduler from the list or to create a new scheduler via the “**Create new ...**” option.

Scheduling settings

Scheduled in:	<input type="text" value="Manual"/> <ul style="list-style-type: none"> Create new ... <li style="background-color: #007bff; color: white;">Manual TaskRunnerScheduler
---------------	--

✓ Folders to process

In this section the user is required to select the folder(s) where the archived data are located. There are two available options how the list of folders may be specified:

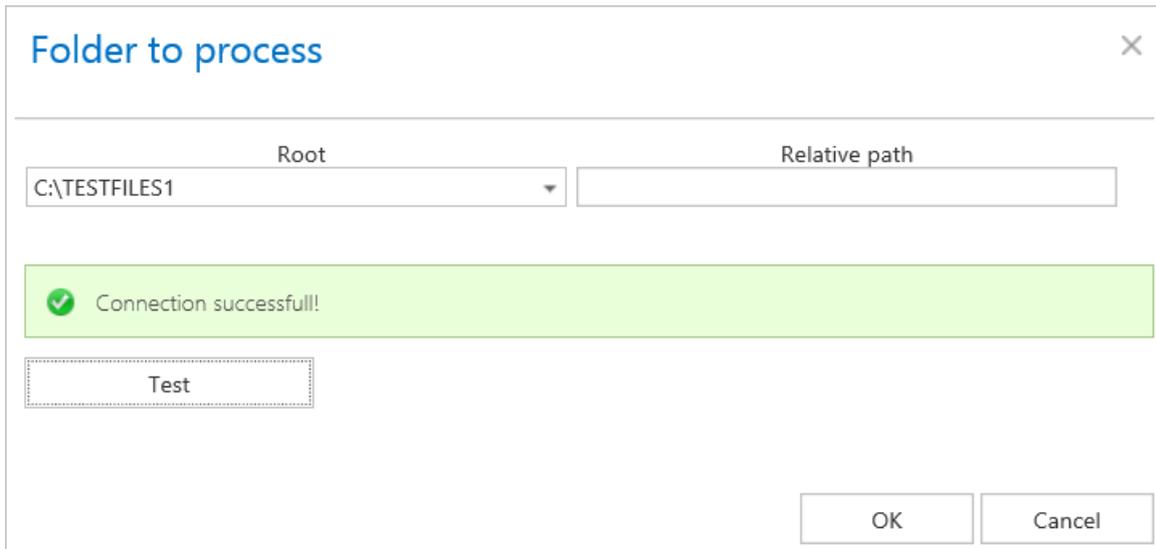
- c) The folder(s) may be added **via +new option**. In this case the folder(s) must be added manually one-by-one. Click on **+new** to open the **File Path** dialog.

Click on “**new**” to specify the folder from where the files should be deleted. In the “Folder to process” dialog unroll the list of already created roots and select the one that should be applied. This dropdown lists the roots that are already configured (in File Archive settings: *File Archive* → *Settings* → *Root folders*). Enter the **Relative path** if necessary, test the path via the “Test” button and click “OK”.

Folders to process

+ new

↶ import



Folder to process

Root: C:\TESTFILES1

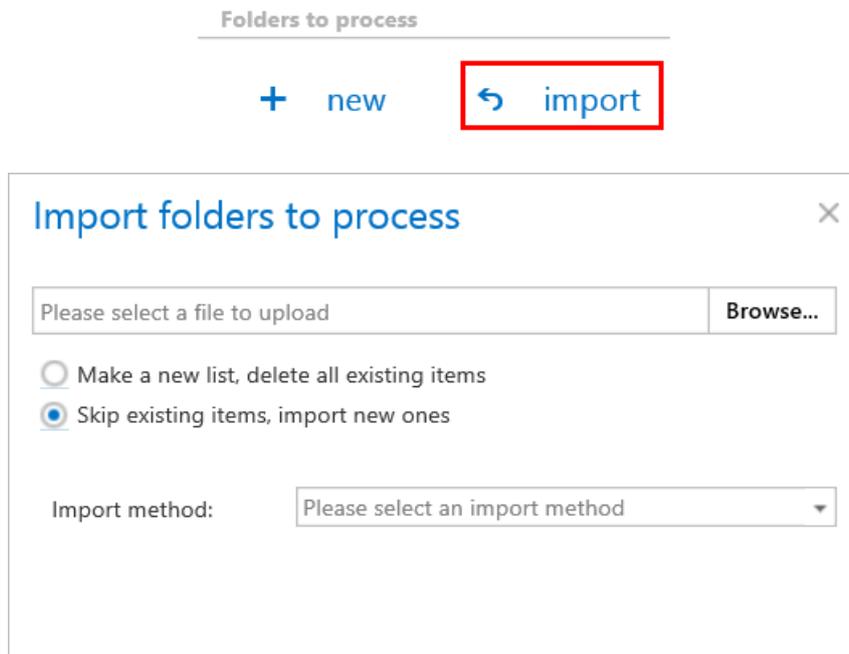
Relative path:

✓ Connection successful!

Test

OK Cancel

- d) The **folder list may be also imported from a file**. The file to be imported must contain the list of folders that should be processed. Click the **import** button and the **Import file location dialog** opens. Specify here the required settings according to chapter [Importing contentACCESS configurations from files](#) of this guide.



Folders to process

+ new **import**

Import folders to process

Please select a file to upload Browse...

Make a new list, delete all existing items

Skip existing items, import new ones

Import method: Please select an import method

✓ Processing settings

In this section, you may check the **Delete even if not marked for delete** checkbox. If you do so, the **Delete job** will delete the expired item without them needing to be marked for delete.

Processing settings

Delete even if not marked for delete:

✓ Filtering settings:

Click on the **Change filter** button and set the filtering according to your needs and/or regulations. To learn more about how to work with filtering settings, please, check [this](#) section of our documentation.

Filter settings
✕

visual

text

A
N
D

Creation date

>

2Y

✕

Creation date

<

1Y

✕

[+add group](#)
[+add condition](#)

Please pick a date or enter it as a relative date: 3D for 3 days, 3M for 3 months and 3Y for 3 years

[+add new group](#)

OK

Cancel

Note: In certain cases, the creation date of a file is set to younger date than the modification date of a file. This happens when a file is copied to another external disk (for example from disk G to disk I). In this case, the creation date will be set to the date of the copy action. Because of this, we recommend to always check **Filtering settings** if something does not get processed.



✓ Notification settings

Select here, when you will need to get notification emails from the Delete job. It is possible to set here if you need a notification email always/never, or you need it only if an error/warning occurred during the process – for example, if the deletion of one or more items failed, then you may get a notification email about this error. Into the **Recipient list** textbox insert the email addresses of the people whom you would like to send these emails to – if there are multiple recipients, the addresses must be separated by “,” or “;”.

Notification settings

Send when:

Recipient list:

✓ Resource settings

Set the value, which will determine how many items will be processed simultaneously by the delete job. The recommended value is 2, as in our case.

Resource settings

Worker thread count:

At the end never forget to save your job configurations: click on **Save** in the left upper corner of UI.

When does the document expire?

Retention repository ✕

Retention name:

Description:

Calculated from:

Protected retention time in months:

Has unprotected retention time

Unprotected retention time in months:



- 1) **If the protected retention has expired** (archive date / reference date + protected retention is in the past) and the document is not under legalhold and the document is marked for deletion
- 2) **If the unprotected retention is defined and has expired** (archive date / reference date + unprotected retention is in the past)

File system delete job description

All the numbers and descriptions in the job's progress have a particular meaning. In this section, we are going to explain the numbers and descriptions of a **File system delete job**.

Description	Explanation
x connections scanned	x root folders have been scanned for deletable documents in the archive
x failed	x root folders' processing failed, see logs for further details
x documents purged	x documents have been purged, or if the job ran in report mode x documents have been added to the report
x skipped	x documents' deletion, or in case of report mode x documents have not been added to the report because of the filtering settings
x failed	x documents' deletion failed

Configuration of File system shortcut synchronization job

This job is able to process and update shortcuts, which are pointing to files in the archive.

Go to Jobs -> Add new -> File system shortcut synchronization.



Add new job instance ✕

Available jobs:

Run on node:

Display name:

Description: Plugin for synchronizing file system shortcut changes to file archive.

On the job's configuration page go through the following sections:

✓ Scheduling settings

In this step the running times of the job must be selected. It is possible either to select a scheduler from the list or to create a new scheduler via the **“Create new ...”** option.

Scheduling settings

Scheduled in:

Create new ...

Manual

TaskRunnerScheduler

✓ Retention settings

Here it is possible to choose an already configured retention time from the dropdown list. The archived files will be stored during this time in the storage and it will be impossible to delete them from there. It is highly recommended to select a retention time that is required by the law of your country. (For more information on how to set retentions check section [Retentions](#)).

Retention settings

Retention:

✓ Processing settings

The processing settings specify the functions, which should be executed inside the job.

- The “Allow to update folder and file permissions” checkbox enables the permission updating functionality for the folders and files.
- The “Allow to update folder path based on the shortcut location” checkbox turns on/off the folder path synchronization.
- The “Allow to clean up orphaned shortcuts” checkbox turns on/off the function that deletes shortcuts, which are pointing to files that were deleted (purged) by the [Delete job](#).

Processing settings

- Allow to update folder and file permissions
- Allow to update folder path based on the shortcut location
- Allow to clean up orphaned shortcuts

✓ Folders to process

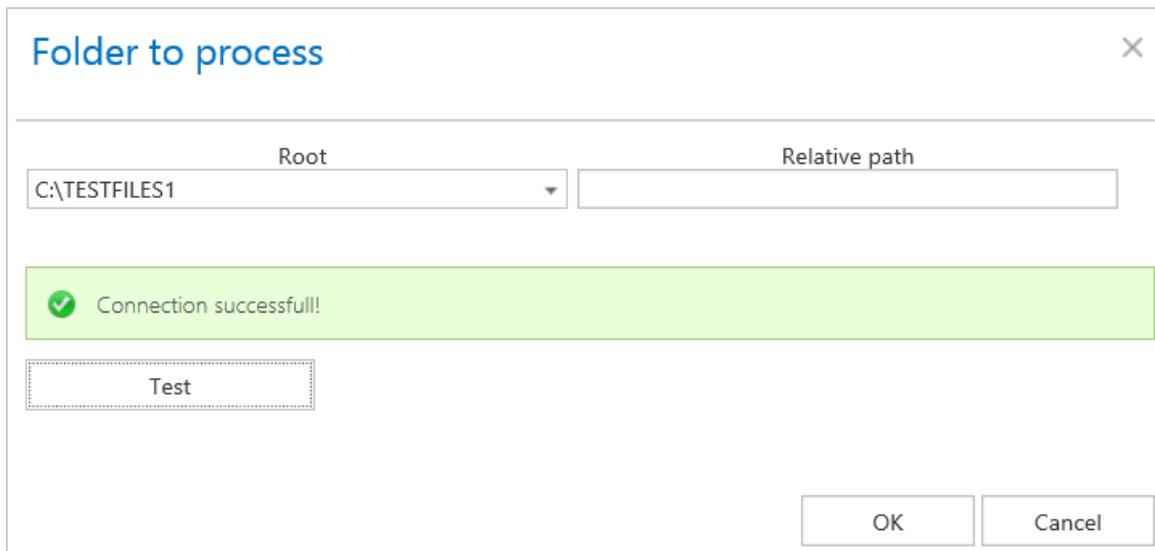
In this section the user is required to select the folder(s) that will be involved in the job. There are two available options how the list of folders may be specified:

- The folder(s) may be added **via +new option**. In this case the folder(s) must be added manually one-by-one. Click on **+new** to open the **File Path** dialog.

Click on “**new**” to specify the folder(s) to be processed. In the “Folder to process” dialog unroll the list of already created roots and select the one that should be applied. This dropdown lists the roots that are already configured (in File Archive settings: *File Archive* → *Settings* → *Root folders*). Enter the **Relative path** if necessary, test the path via the “Test” button and click “OK”.

Folders to process





Folder to process

Root: C:\TESTFILES1

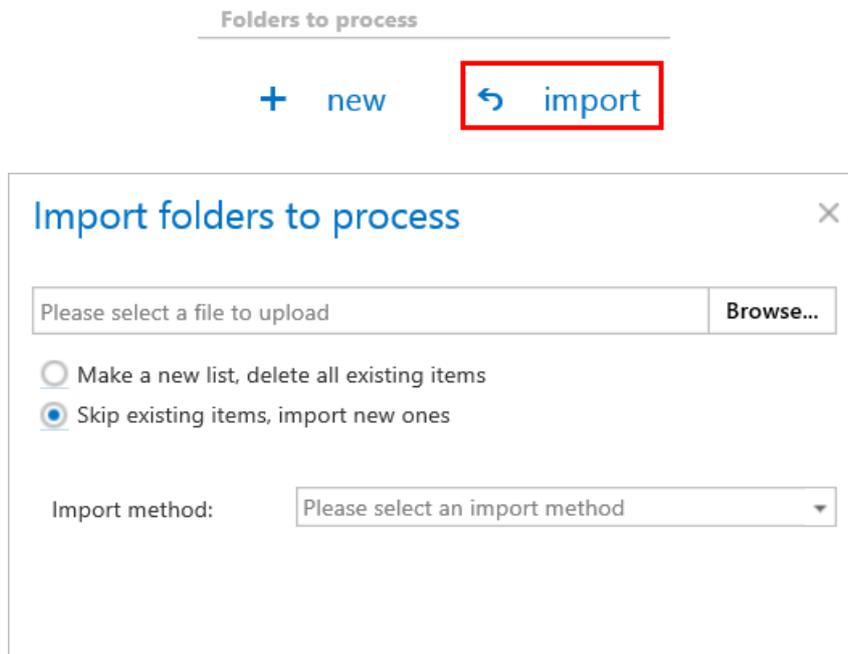
Relative path:

Connection successful!

Test

OK Cancel

- b) The **folder list may be also imported from a file**. The file to be imported must contain the list of folders that should be processed. Click the **import** button and the **Import file location dialog** opens. Specify here the required settings according to chapter [Importing contentACCESS configurations from files](#) of this guide.



Folders to process

+ new import

Import folders to process

Please select a file to upload Browse...

Make a new list, delete all existing items

Skip existing items, import new ones

Import method: Please select an import method

✓ Resource settings

Set the value, which will determine how many items will be processed simultaneously by the job. The recommended value is 2, as in our case.



Resource settings

Worker thread count:

At the end never forget to save your job configurations: click on **Save** in the upper left corner of UI.

File system shortcut synchronization job description

All the numbers and descriptions in the job's progress have a particular meaning. In this section, we are going to explain the numbers and descriptions of a **File system shortcut synchronization job**.

Description	Explanation
x folders processed	x folders and their files have been processed, no further work on the folders required
x folders failed	x folders' processing failed, no items have been processed from these folders
x documents processed	x documents have been successfully synchronized
x failed	x documents' shortcut sync failed, see logs for further details
x links deleted	x items have been deleted from the file system because previously they have been deleted from the archive
x duplicates created	x items have been found on a different path that is in the archive, from these a duplicated item has been created, so we can have them both in the archive
x versions created	x documents have been changed since they've been added to the archive, for these items a new version has been created

Configuration of Remote shortcutting job

Remote shortcutting job is a special job type, which is used together with the file archive job. This type of job is used if you have several remote locations synchronized with your central data center, you are

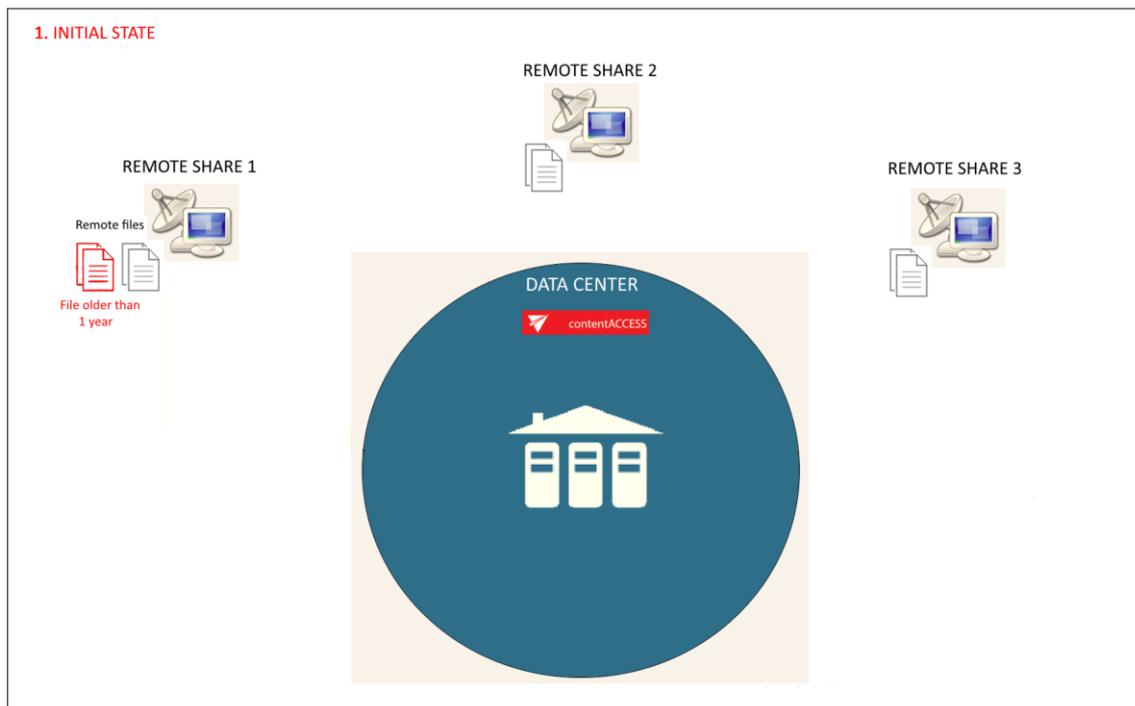


archiving files in the data center with a File system archive job and the remote files should be replaced by shortcuts (by the Remote shortcutting job) to spare storage space on the remote shares. contentACCESS is installed on the data center and continuously archives the files already copied to the data center. So the archiving itself is done by a standard File system archive job; the Remote shortcutting job is used to create shortcuts on the remote shares. Archiving from the data center can be done with the shortcutting, journal or with the keep original method, so all types can be used.

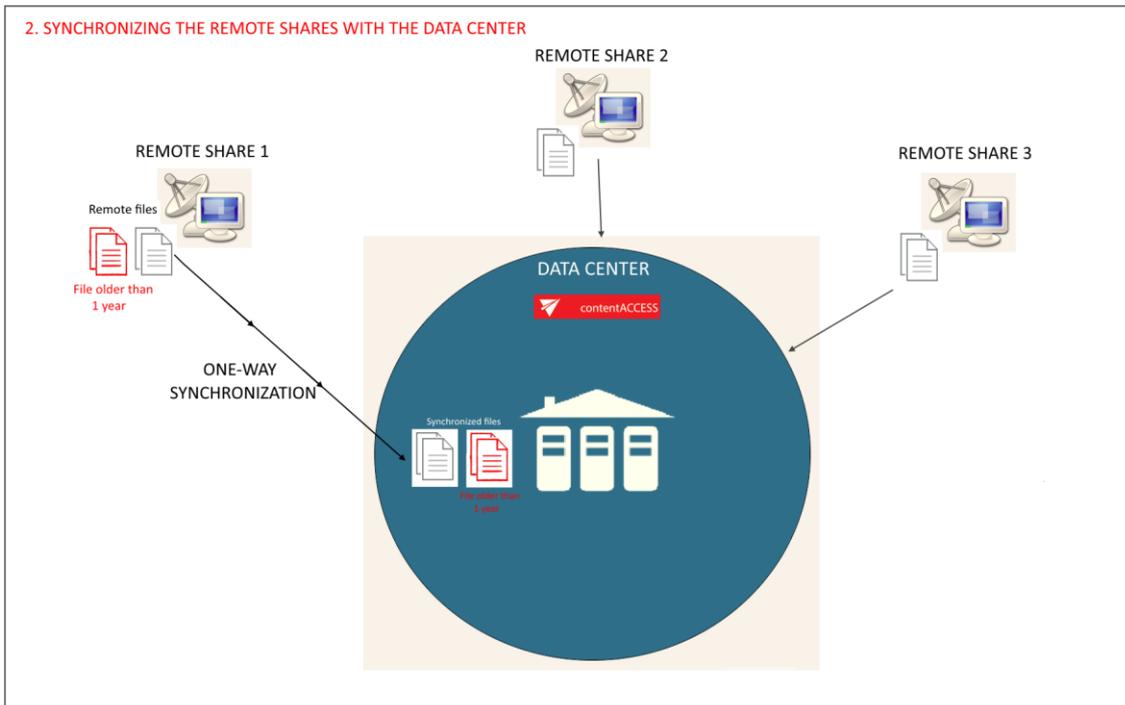
Note: Remote shortcutting job **can replace remote files with shortcuts** only in case if the matching file in the data center (where contentACCESS is installed and file archive job is running) has been **already archived**. The **modification date** of the remote file and data center-file **must be the same**, too, otherwise the shortcutting job will skip the file and will write this information into the .log file.

On the chart below you can see the phases of this shortcutting process; contentACCESS server is installed on the data center only:

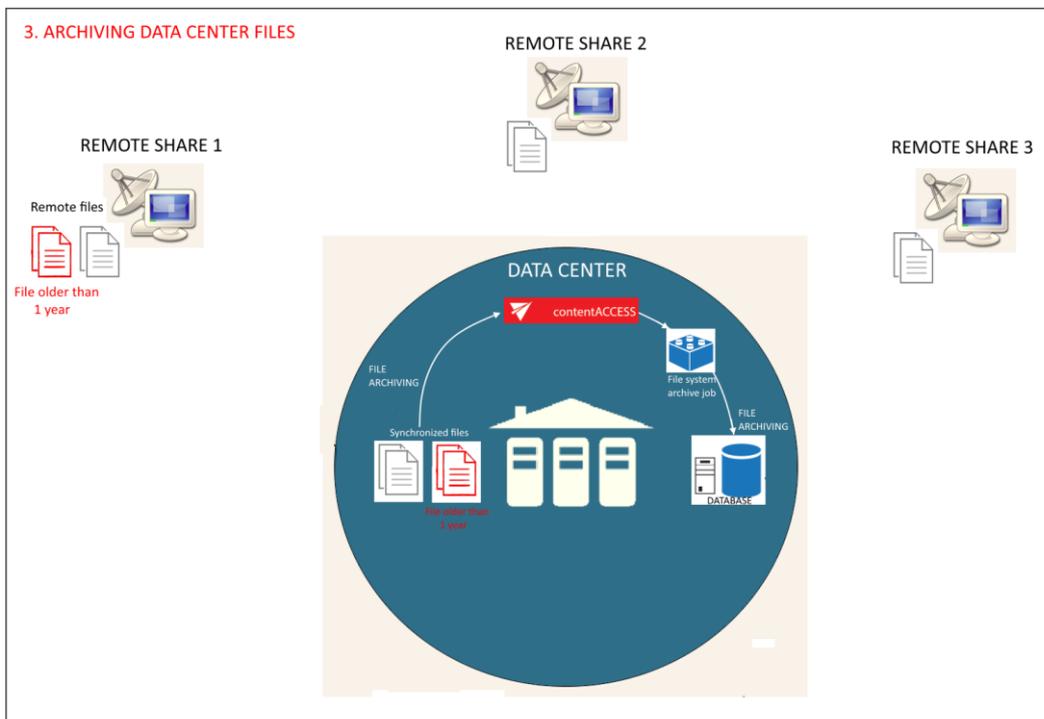
1. The first chart illustrates the initial state of the remote shares and the central data center, where the remote files will be synchronized;



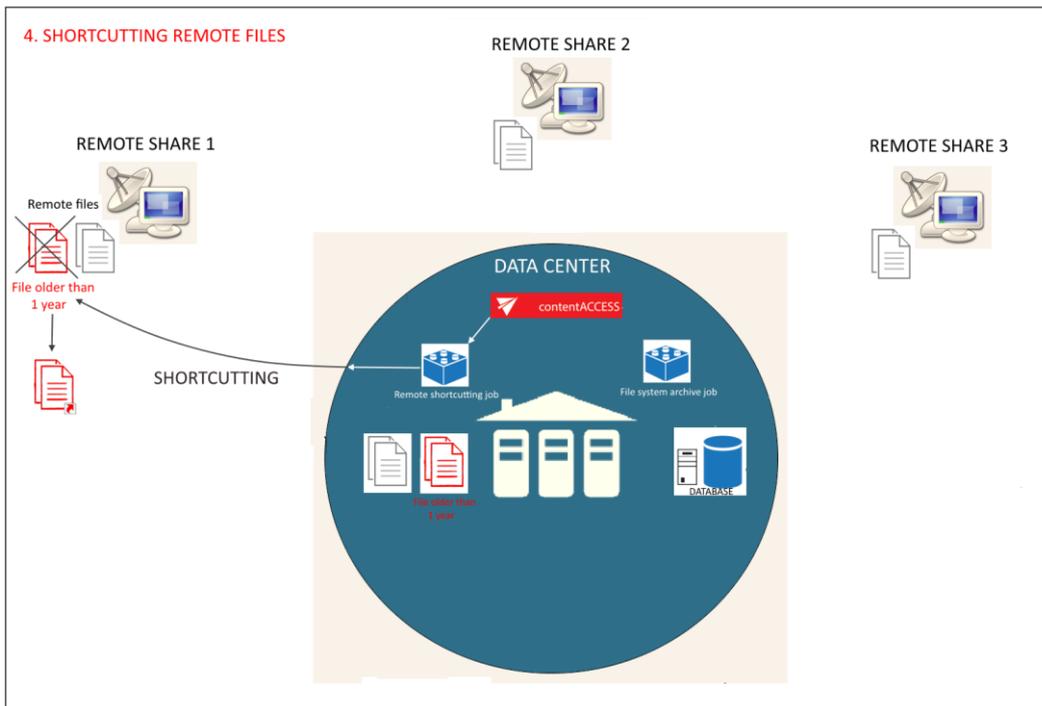
2. On the second chart you may see how the remote shares are synchronized by the data center (i.e. files from the remote share(s) are copied to the data center);



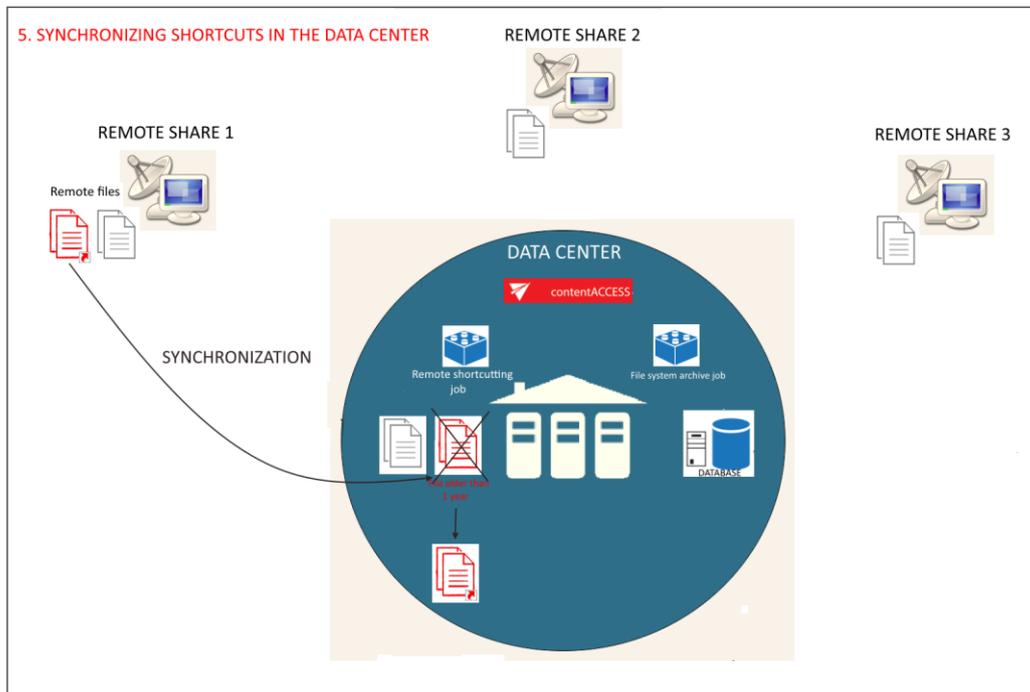
3. The third chart shows how the File system archive job archives the files in the data center into the contentACCESS database;



4. On the fourth chart the already archived, <1 year old files (the age is specified in the Remote shortcutting job) are replaced with shortcuts on the remote share; this process is executed by the Remote shortcutting job;



5. The last picture illustrates how the shortcuts on the remote share are synchronized with the data center files (i.e. the data center files are also replaced with shortcuts).



In this section we will configure a **Remote shortcutting** job, which will run every day from 6 PM and will replace our remote files with shortcuts, that weren't touched for a year (modification date is > 1 year). The



remote files are located in “\\tawin10\.....\Test documents for Remote shortcutter job”. Let’s assume that the remote files have been synchronized with the files in a data center and have been already archived, so our archive database is already configured in contentACCESS. (For more information refer to section [Databases](#)) We also assume that the remote share’s file path and the data center’s file path have been configured on the Aliases page. (For more information refer to section [Configuring aliases.](#))

Navigate to **File Archive** → **Archive** → **Jobs** button, click on **+new**. In the **Add new job instance** dialog select **Remote shortcutting** job from the **Available jobs:** dropdown list. Select the node, where the job should run, from the **Run on node** list. Now we would not like to specify a node, so we select “Any available”. Name it and click on **Add**.

On the job’s configuration page go through the following sections; most of them are mandatory, filtering settings are optional:

✓ **Scheduling settings:**

In this step the running times of the shortcutting job must be selected. It is possible either to select a scheduler from the list or to create a new scheduler via “create new ...” option. It is recommended to set up a scheduler that will run always, or in certain times during the week. Our job will run every day from 6 PM till midnight, after business hours. (For more information about how to set schedulers refer to the section [Schedules](#) above.)

✓ Processing settings

Enter the server name, where the virtual drive has been installed (DNS alias at best). Virtual drive will be used to open the shortcuts linking to the archived files.

By using the “**Use default**” option, the Virtual Drive that was already configured on the Virtual Drive configuration page will be automatically preselected. It is recommended to use this option, because if the settings have been changed on the Virtual Drive configuration page, the value will be automatically used by the job, too, without a need to change the job’s settings.

Processing settings

Virtual drive server name: Use default (tanews)

✓ Connection successfull!

✓ Remote file system locations

In this section the user needs to specify the remote share(s) containing the files to be replaced with a shortcut. It is also possible to specify multiple remote shares. Only the remote file path(s) specified on the **Aliases** page will be listed in the dialog. (For more information about configuring aliases refer to [Configuring aliases.](#))

Click on **+new** and the **Remote file path** dialog will open. Unroll the **Alias** dropdown list and select the alias that the job should use. The relative folder path must be set in the **Path extension** text box.

Remote file system locations

+ new

Remote file path

Remote file location settings

Alias: Path extension:

✓ Item filtering:

This configuration enables for the user to filter among items to be shortcutted by 3 types of criteria: by age, size or file type. It is also enabled to use more filters simultaneously. For filtering documents according to

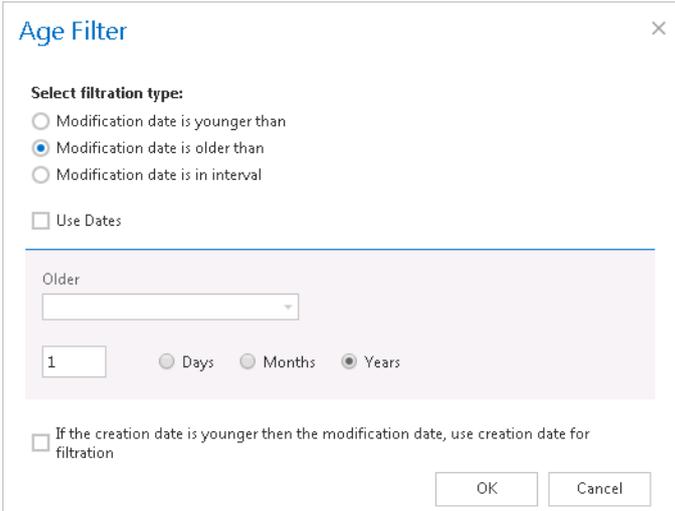
any of these criteria, activate the filter button by checking the checkbox next to it, then click on the activated button.

▪ **Age filter:**

With this filter the user may configure, how old files should be processed by the shortcutting job. The user has multiple choices here; he can a) use either the **Use dates** option and pick up a date from the calendar, or b) he can enter a value into days/months/years textbox to process the files which are younger than/older than or fall into time interval set here.

The shortcutting job is checking if the modification date of the remote files is the same as the modification date of the data center files. If the dates are the same, the job replaces the remote files with a shortcut; if the dates are different, it skips the remote files and writes this information into the .log file.

As we would like to replace remote files older than 1 year with shortcuts, we set “**Modification date is older than**” **1 year** in the **Age filter** repository window.

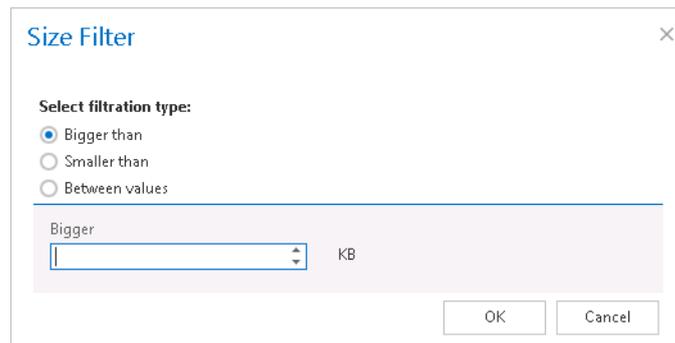


Screenshot: Remote files older than 1 year will be replaced with shortcuts

▪ **Size filter:**

This filter can be used if you would like to replace with shortcuts only files of a certain size. To use it, activate **Size filter** button by checking the checkbox next to it, then click on the active button.

In the **Size filter** dialog choose from the filtering types (**Bigger then**, **Smaller then**, or **Between values**), enter the size (in kilobytes) and click **OK**.



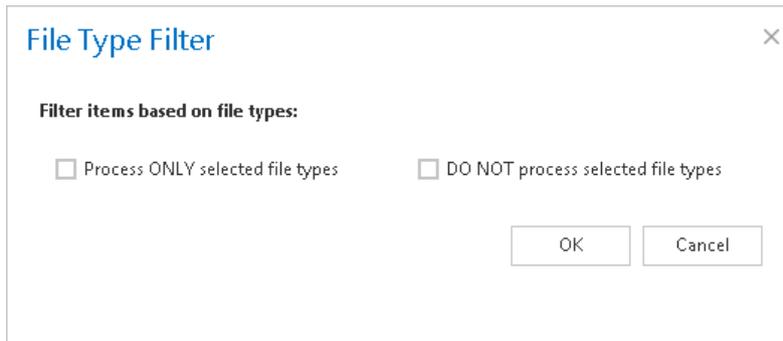
If the user would like to process all files of the remote share, he can skip this filter settings (like in this use case as well).

Important!!!: When the user changes the file content, e.g. deletes a picture from the file and saves it to the original location, (and thus the file size will be reduced e.g. from 110 to 85 kB) and file size filter is set on >100 kB, then the shortcutting job will not process the newly created item by the next processing. The newly created item will be saved in the remote location and the old shortcut will be present in the remote location, too, which will still link to the old file without any changes.

For this reason, it is recommended to always check the size filter settings, if a file has not been replaced by a shortcutting job.

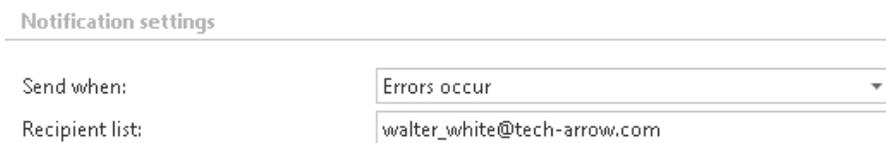
- **File type filter:** This filter was improved to select certain file types for processing. For filtering between documents according to this criteria, activate **File Type filter** button by checking the checkbox next to it, then click on the active button.

In the **File Type filter** dialog the user may select the file types that need to be processed (option **Process ONLY selected file types**), or he may specify file types that should be excluded from the processing (**DO NOT process selected file types**). The file types selected in the whitelist/blacklist are displayed below the grid in a read-only text box. Any file types (also file types that are not included in the whitelist and/or blacklist) can be specified in the **Custom file types** text box (in this use case “dwg”). If nothing is selected/deselected from the file types, then every file type will be processed automatically. If you need to process all files on the remote share, skip these settings.



✓ **Notification settings.** Select here, if you need to get notification emails from the **Remote shortcutting** job, and in which cases you would like to get such email message.

Into the **Recipient list** textbox insert the email addresses of the people, whom you would like to send these emails to.



✓ **Resource settings.** Set the value, which will determine how many items will be processed simultaneously by the job. The recommended value is 2, as in our case.



Never forget to save your job configurations at the end: click on **Save** in the left upper corner of UI.

File system remote shortcutting job description

All the numbers and descriptions in the job’s progress have a particular meaning. In this section, we are going to explain the numbers and descriptions of a **File system remote shortcutting job**.

Description	Explanation
x folders processed	x folders and their files have been processed, no further work on the folder required



x folders failed	x folders' processing failed, no items have been processed from this folder
x documents processed	x documents have been processed
x skipped	x documents have been skipped
x shortcuts created	x documents have been converted to shortcuts



Active/inactive documents in File system archive

Definition of terms: file = file on the file system; item = archived file in the archive

To avoid displaying duplicate items in the archive, the user has the choice to filter between active and inactive items in the contentACCESS archive (contentWEB). A duplicated item is created when a file is processed multiple times and is saved into the archive multiple times. A typical use case might be when a user copies a file from one source folder to a target folder in his file system and then deletes the file from the source folder. Let's assume that the archive job meanwhile caught and processed both files (created duplicates in the archive). To avoid the user from getting confused, the files processed in the source and target folder need to be differentiated from each other in the archive. The file archived from the source location will be inactive in the archive (the file in the source location is not available on the user's side, the user deleted it); the file archived from the target location will be active in the archive (the file in the target location is available for the user). The contentWEB active/inactive filter makes it easy to display the actual (last touched) files in the archive.

When is an item/folder inactive in the archive? An item/folder gets an **inactive status** in the archive if it **no longer exists in the file system (neither the original, nor the shortcut to it)**. Once the item is touched (e.g. versions were created, it was restored by a job, or recovered), its status will turn to active.

When an archive job is running, it is synchronizing the current state of the archive with the state of the file system. The following tables will give an overview to a user about when an item is active/inactive in the archive. The light blue cells contain the files/folders that are found by an archive/restore/recovery job in the file system (on the user's side), the grey cells inform the reader about the action that the job performs when it finds this particular file/folder.



Archive with shortcutting method

File system (user's side)	Is item in archive in the same location?	
A) Shortcut was found by the archive job	YES: the job does not touch the shortcut. The item will be ACTIVE .	NO: the job will duplicate the item to the new location. The shortcut will be updated with a new ID. The new item will be ACTIVE (the old item is not touched).
B) File was found by the archive job	Is item in the archive?	
	YES: If the file was changed, a new version will be created in the archive, and the file will be converted to shortcut. The item will be ACTIVE in the archive.	NO: The file will be archived and converted to shortcut; the item will be ACTIVE in the archive.
C) No shortcut, no file was found by the archive job	YES: the item will be INACTIVE in the archive.	NO: no action will be performed by the job
D) Folder no longer exists	Is folder in the archive?	
	YES: folders will be INACTIVE (recursively); items will be INACTIVE	
E) Folder exists	Is folder in the archive?	
	YES: permissions will be actualized and the folder will be set to ACTIVE	NO: it will be archived and set to ACTIVE

Archive with the "Keep original" method

File system (user's side)	Is item in archive in the same location?	
A) Shortcut was found by the archive job	YES: the job does not touch the shortcut. The item will be ACTIVE .	NO: the job will duplicate the item to the new location. The shortcut will be updated with a new ID. The new item will be ACTIVE (the old item is not touched).
B) File was found by the archive job	Is item in the archive?	
	YES: If the file was changed, a new version will be created in the archive and the file will	NO: The file will be archived and the original will be kept; the item will be ACTIVE in the archive.



	be kept in the file system. The item will be ACTIVE in the archive.	
C) No shortcut, no file was found by the archive job	YES: the item will be INACTIVE in the archive.	NO: no action will be performed by the job.
D) Folder no longer exists	Is folder in the archive?	
	YES: folders will be set to INACTIVE (recursively); items will be set to INACTIVE .	
E) Folder exists	Is folder in the archive?	
	YES: permissions will be actualized and the folder will be set to ACTIVE ,	NO: it will be archived and will be set to ACTIVE .

Archive with the “Delete original” method

File system (user’s side)	Is item in archive in the same location?	
A) Shortcut was found by the archive job	YES: the job does not touch the shortcut. The item will be ACTIVE .	NO: the job will duplicate the item to the new location. The shortcut will be updated with a new ID. The new item will be ACTIVE (the old item is not touched).
B) File was found by the archive job	Is item in the archive?	
	YES: If the file was changed, a new version will be created in the archive and the file will be deleted from the file system. The item will be INACTIVE in the archive.	NO: The file will be archived and the original will be deleted; the item will be INACTIVE in the archive.
C) No shortcut, no file was found by the archive job	YES: the item will be INACTIVE in the archive.	NO: no action will be performed by the job.
D) Folder no longer exists	Is folder in the archive?	
	YES: folders will be set to INACTIVE (recursively); items will be set to INACTIVE .	
E) Folder exists	Is folder in the archive?	
	YES: permissions will be actualized and the folder will be set to ACTIVE .	NO: it will be archived and will be set to ACTIVE .

Note: The user may browse for his archived items either in contentWEB, or on Virtual drive. By default, Virtual drive displays the active items only, but this is configurable on the Virtual drive's configuration page (System → Client applications → Virtual drive configuration).

Automatic restore from shortcut

File system (user's side)	Action performed by the restore job
a) Shortcut found	The job restores the original into the file system location; the item in the archive will be set to ACTIVE .
b) No shortcut found	No action.

Automatic recovery

File system (user's side)	Action performed by the recovery job
A) File found	No action, file will be skipped.
B) Shortcut found	No action, shortcut will be skipped.
C) Nothing found	C/1) If the job configuration requires to recover original: the original will be created in the file system; the item will be ACTIVE in the archive.
	C/2) If the job configuration requires to recover shortcut; the shortcut will be created in the file system; the item will be ACTIVE in the archive.

Manual recovery from contentWEB

File system (user's side)	Action performed by the manual recovery
D) File found	No action, file will not touched, it will be skipped. The item will be ACTIVE in the archive.
E) Shortcut found	Shortcut will be replaced by the original file in the file system; it will be ACTIVE in the archive.
F) Nothing found	New file will be created in the file system; the item in the archive will be ACTIVE .

Other use cases:

- ✓ The shortcut is deleted from file system: nothing happens in the archive during the archiving process, the items change to **INACTIVE** if they were active before.



- ✓ The shortcut is moved: the item is duplicated to the new location. The new item is ACTIVE. The old item will be INACTIVE if there is no file or shortcut at the old location.

Email Archive

Nowadays, companies have a growing need to create a safe archive for storing their company documents (mainly accountant documents). The reason for this growing demand is that these documents must be accessible during a certain period of time, which is determined by the regulations of the country and of the company itself. contentACCESS Email Archive solution offers long-term storage of emails with easy search (over contentWEB) and retrieval capabilities, therefore saving space on the Exchange server. The following store types are supported at the moment: Disk Store, inPoint, iTernity, Easy and Perceptive. Processing is ensured from the local Exchange servers and also from the cloud (O365). Public folders can be also archived. The archived documents can be also accessed/restored/recovered from the archive in case of need. Restore and recovery functions are ensured either with automatically running jobs, or they can be restored manually. contentACCESS is a brilliant solution for archiving emails into supported or any implemented third party storages.

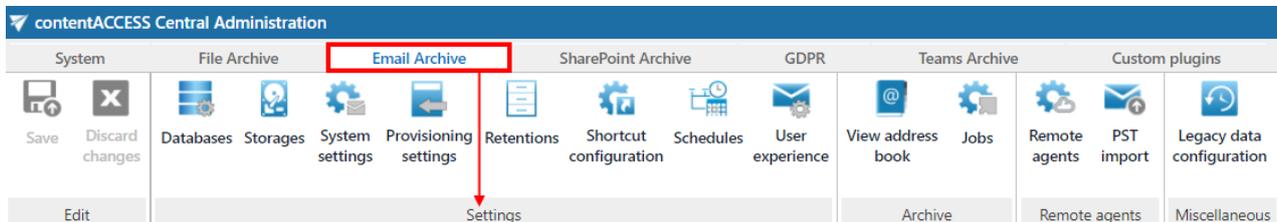
There are **two main methods of archiving** available with contentACCESS Email Archive:

- ✓ **Archiving by scheduled jobs**, which are configurable in the contentACCESS Central Administration – archiving process running in the background according to pre-defined settings.
- ✓ **Manual archiving/restore directly from MS Outlook** with the help of **Mail app** feature (in case of Exchange 2013 or higher) or **OWA 2010 extension** (if Exchange 2010 is used).

The following **processing types** are available when archiving from the Exchange server:

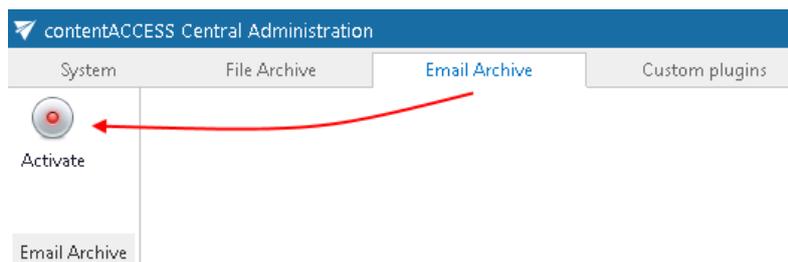
- ✓ **Archive with keeping the original item** in the source location – this processing method is generally used to archive emails younger than 1 year.
- ✓ **Archive with shortcutting method** (transparent shortcuts in case that MS Outlook is used; HTML shortcuts in case that MS Outlook can't be used (OWA) – shortcuts are used for archiving mailbox items, which are older than 1 year, but younger than 2 years and must be easily accessed without a need to search for them in the archive; it also helps to save storage space.
- ✓ **Archive with delete method** – the mailbox items older than 2 years are usually deleted from the source location (but they are stored in the archive during the required retention time).

The mandatory email archive settings can be done directly from **Email archive** tab → **Settings** group (Screenshot A).



Screenshot A: Required settings in email archive

The steps described in section “[Important settings before creating an Email Archive job](#)” will lead you through the settings that need to be done before starting to configure an Email archive job. When navigating to the **Email archive** tab for the first time, the user needs to activate Email archive with a click on **Activate** button (Screenshot B).



Screenshot B

With this action, a provisioning job, which will perform necessary synchronizations in the background, will be automatically created.

Important settings before creating an Email Archive job

- 1) It is required to install the contentACCESS Proxy.
- 2) Make sure that the needed tenant database(s) are created (for more information refer to section “[SMTP Mappings](#)”).
- 3) [The SMTP mappings page can be](#) found under **System -> Services** section in Central Administration. On this page the user can define new SMTP mappings, edit the existing ones (the listening address cannot be changed) and/or delete them using their context menu. Upon adding a new mapping, editing or deleting an existing one, the new list of the mappings is synchronized to the SMTP servers immediately.



The columns in the grid are the following:

Email address: the address the SMTP server listening on for incoming emails

Folder name: the name of the folder in the target mailbox, to which the emails archived by the SMTP server will be saved

Model name: the name of the model, where the selected target entity lives (the Email archive model enabled for SMTP based archiving)

Entity name: name of the target entity - the email address of the target mailbox



SMTP Mappings

System > Services > SMTP Mappings

+ new smtp mapping

Email address	Folder name	Model name	Entity name
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
mne.testing@tech-arrow.com	*** SMTP	Email archive	dne@ta.internal
john.smith@microsoft.com	*** SMTPmapping	Email archive	SNE@ta.internal
andrew.tech@tech-arrow.com	*** Mappings	Email archive	ANE@ta.internal

Page 1 of 1 (3 items)



To add a new SMTP mapping, click on the **+ new smtp mapping** and specify the following:

Email address: the address that the SMTP server is listening on for incoming emails. The domain part is a dropdown list and contains the domains specified in the **SMTP domains** section in the SMTP Servers page

Folder name: the name of the folder in the target mailbox, to which the emails archived by the SMTP server will be saved

Model name: the name of the model, where the selected target entity lives (the Email archive model enabled for SMTP based archiving)

Entity name: name of the target entity - the email address of the target mailbox. For a mailbox to show up here, it must have an archive database and an index zone assigned.



SMTP Mapping ✕

SMTP mapping

Email address:	<input type="text" value="jack.bolton"/>	@	<input type="text" value="tech-arrow.coi"/>
Folder:	<input type="text" value="SMTP mails"/>		
Model:	<input type="text" value="Email archive"/>		
Entity:	<input type="text" value="dne@ta.internal"/>		

Note: If the email address is not specified in any of the mappings, it cannot be processed by the SMTP server.

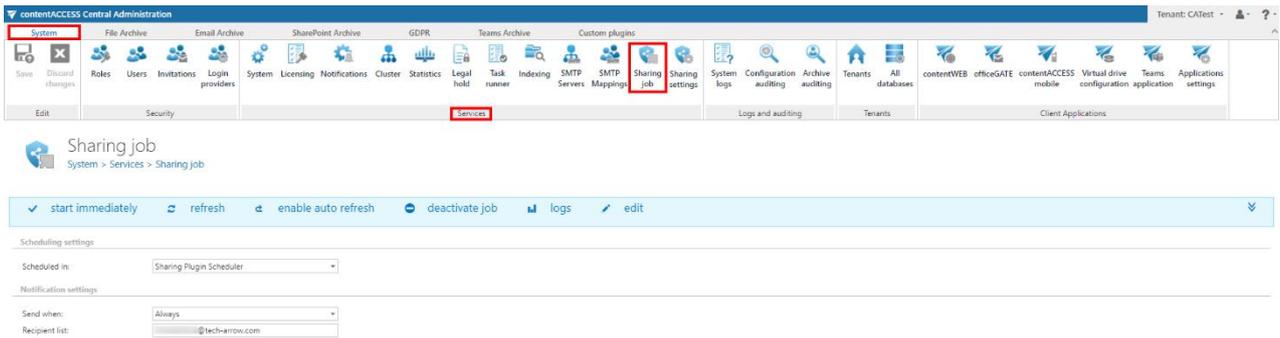
Important: One **Email address** can be associated only with one **Entity**! However, one **Entity** can be associated with multiple **Email addresses**.

- 4) Sharing job
- 5) The sharing job is a system-wide job that handles asynchronous post-processing and management of the shared files and all sharing inside the system.

This job does the following tasks:

- updates and synchronizes channel and chat memberships for the files that were shared through **contentACCESS Teams app**
- deletes the expired files from the store

To configure the sharing job, navigate to **System -> Services -> Sharing job**.



On this page, you will be able to set the following:

✓ **Scheduling settings:**

In this step the running times of the sharing job must be selected. It is possible either to select a scheduler from the list or to create a new scheduler via create new option. For more information about how to set schedulers please refer to the section Schedules above.

Scheduling settings

Scheduled in:

✓ **Notification settings:**

The user may select here, in which cases he needs to get notifications from the sharing job. It is possible to set here that the notification emails will be sent only in case of errors or warnings, or they can be sent in all cases, too. Into the **Recipient list** textbox, insert the email addresses of the people, whom these emails should be sent to. Notifications emails may be used as tools of the troubleshooting process.

Notification settings

Send when:

Recipient list:

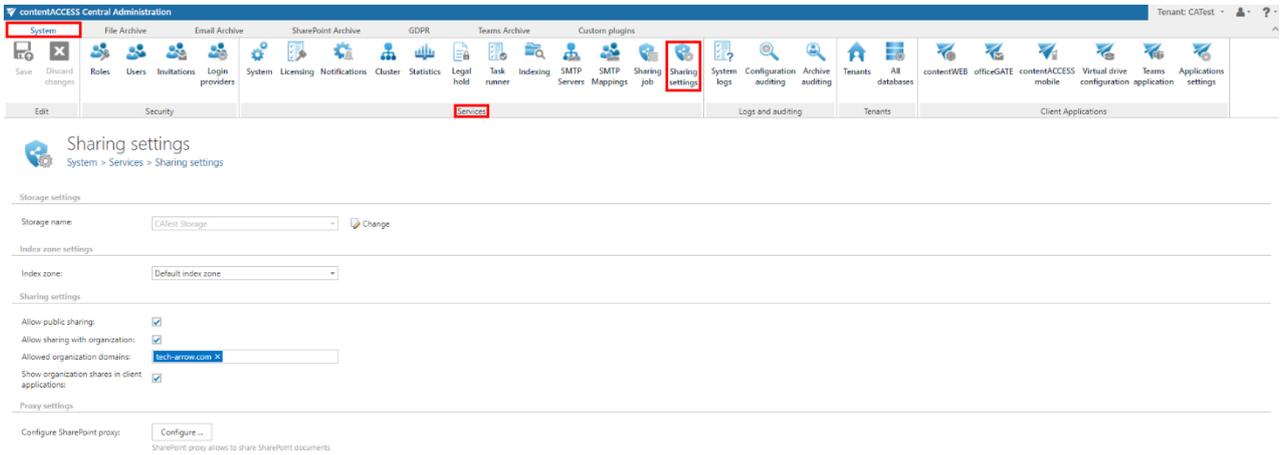
Sharing settings

The sharing **feature allows** the user to specify the restriction and retention to be applied for the shared items when sharing them. It also automates the user **invitation process** in case the items are shared with



an external recipient and sends an email with links pointing to the shared items. Full Auditing logs are provided about the sharing and file downloads, too.

More settings for the **Sharing** module can be configured here. Navigate to **System -> Services -> Sharing settings**.



On this page, you will be able to set the following:

✓ **Storage settings:**

Choose an already configured storage from the dropdown list. The binaries for the files that were directly uploaded during the sharing will be stored here, items shared from the archive won't be duplicated into this storage. For more information on how to set storages check section [Storages](#) above.

Storage settings

Storage name:

✓ **Index zone settings:**

Pick the Index zone that will be assigned to the **shared items** from the dropdown list. If you want to configure a new one, navigate to **System ⇒ Services ⇒ Index zones**.

Index zone settings

Index zone:



✓ Sharing settings:

In this part, you can set the following:

- **Allow public sharing** – if checked, you will be able to share archived items from contentWEB with anyone, even the people the sharing link or email is forwarded to will be able to open it; in case of public sharing, no authentication is required, therefore the Auditing is not able log the identity of the user that downloaded the item
- **Allow sharing with organization** – by checking this checkbox, the next two options will get enabled; the organization sharing will enable you to easily allow access to a file for everyone inside the organization. This is very useful when sharing company-wide documents.
- **Allowed organization domains** – in this textbox you can specify organization domain(s), which will be then used when selecting the option to share with “My organization” in contentWEB - the system will be checking the user’s login name for the domains. In case the organization owns multiple domains, all domains must be specified here for the users to be able to download the files.
- **Show organization shares in client applications** – if the option mentioned above was used, the organization shares will be visible in client applications; The files shared with organization access will be displayed for all users inside the organization.

Sharing settings

Allow public sharing:	<input checked="" type="checkbox"/>
Allow sharing with organization:	<input checked="" type="checkbox"/>
Allowed organization domains:	<input type="text" value="tech-arrow.com X"/>
Show organization shares in client applications:	<input checked="" type="checkbox"/>

✓ Proxy settings:

It is possible to also share not only archived, but also **live SharePoint files** that are not in the archive. By using the **SharePoint proxy**, all extra features (date/download restrictions, common view about the shared files,...) provided by contentACCESS are applied, while the files stay in SharePoint. The file download and access is done by a superuser, but during the sharing process, the permissions of the user that is sharing the file(s) are verified, if the user really has access to the file(s).

Requirement: O365 SharePoint is needed, and the sharing user must have O365 login in contentACCESS.



To **Configure SharePoint proxy**, click on the **Configure...** button.

Sharing settings
System > Services > Sharing settings

Storage settings

Storage name: Change

Index zone settings

Index zone:

Sharing settings

Allow public sharing:

Allow sharing with organization:

Allowed organization domains:

Show organization shares in client applications:

Proxy settings

Configure SharePoint proxy:

SharePoint proxy allows to share SharePoint documents

First, you will need to activate the SharePoint proxy by clicking on the **Activate proxy** button. In our case, it is already activated, that is why only the **Deactivate proxy** button is enabled.

Note: by deactivating the SharePoint proxy, any previously shared file will be unavailable. By re-activating the proxy, the files will be available again.

SharePoint proxy
SharePoint Archive > Settings > SharePoint proxy

Activation status

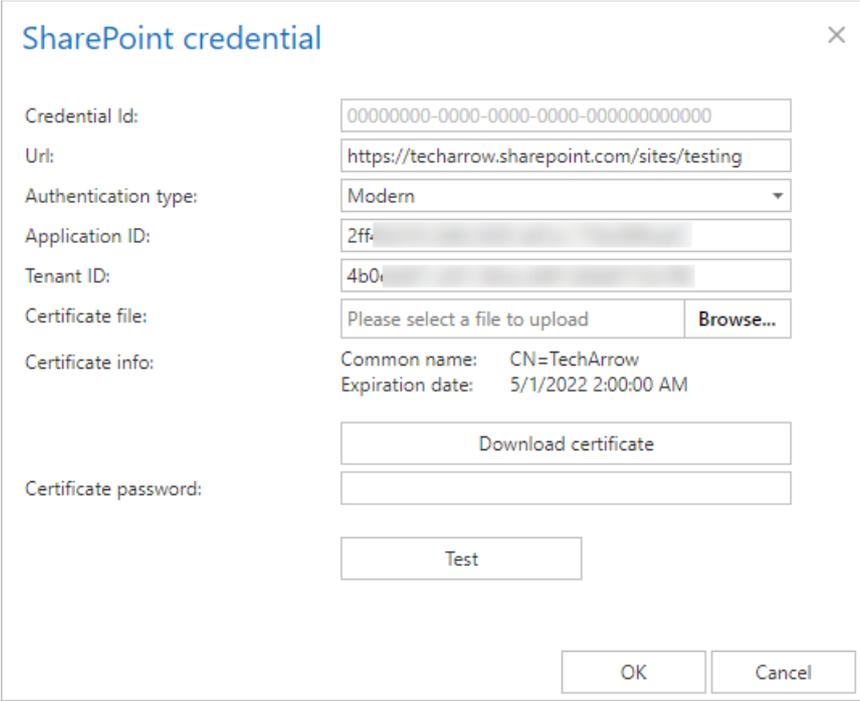
SharePoint proxy activation status: Activated

SharePoint credentials

[+ new](#)

Uri	Authentication	User
https://techarrow.sharepoint.com/sites/testing	▲ Modern	

Each site collection you would like to share files from needs to be specified separately. To specify a new site collection, click on **+new**. The **SharePoint credential** window opens. Enter the **URL** and choose the **Authentication type** from the dropdown list – **Integrated**, **Basic** or **Modern**. All the authentication types are explained in this section.



- 6) How to create/configure databases — All databases”).
- 7) Under **System** → **Services** → **System** check if the Database, FQDN and LDAP settings are well configured (for more information navigate here: [“System”](#)).

Configure the mandatory settings accessible in the **Email Archive** → **Settings** group. The configuration logic is from left to right. If you follow this logic, then all the necessary configuration will be done for the next step.

If you want to archive public folders as well, it is necessary to set it in the Email archive System settings (Email archive tab → Settings → System settings, section General settings).

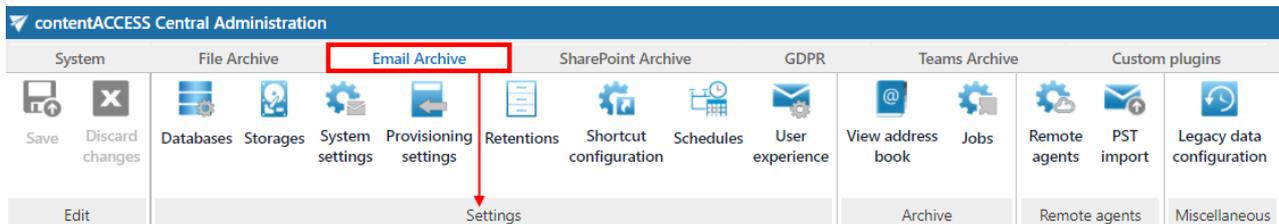
Note: These configurations are described in the details in this section below.



8) Assign a database and storage to the mailbox that will be archived (for more information refer to section “Database and store assignment in email archiving”; if a database and storage have not been assigned manually, the first running email archive job will assign them to the mailbox.

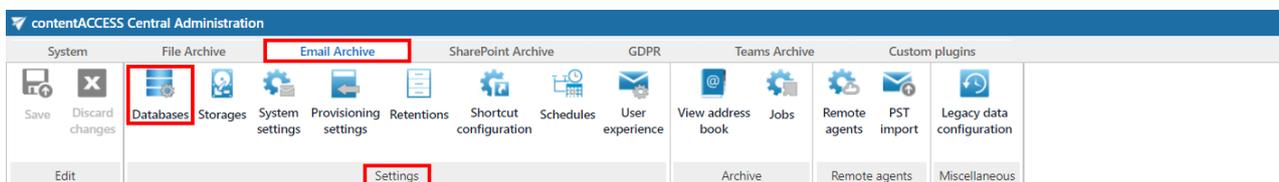
Email archive settings: Navigate to **Email Archive** → **Settings** group. The mandatory settings and many useful criteria for automated email archiving can be set here:

- ✓ Tenant database connections can be configured;
- ✓ System settings can be performed;
- ✓ Provisioning settings can be set;
- ✓ Retentions can be created; the retentions configured here can be selected on the jobs’ configuration page;
- ✓ Shortcuts and further processing types can be configured; the processing types configured here can be selected on the jobs’ configuration page;
- ✓ Schedulers can be set; the schedulers configured here can be selected on the jobs’ configuration page;
- ✓ User experience configurations can be accessed from here, too.



Database settings

Navigate to **Email Archive** → **Settings** → **Databases**:



Databases

Email Archive > Settings > Databases

+ configure existing ? manage access

Connection name	Server	Type	Database	Schema	User	Is default
PROD-FULTEXTDEMOCA-SQLDB	*** .\sqlexpress	MSSQL	PROD-FULTEXTDEMOCA-SQLDB	dbo	sa	Yes
PROD-FULTEXTDEMOCA-TEA	*** .\sqlexpress	MSSQL	PROD-FULTEXTDEMOCA-TEA	dbo	sa	No
TeamsDemo	*** .\sqlexpress	MSSQL	TeamsDemo	dbo	sa	No



Here you can find the full list of all accessible databases, which are configured for the tenant. The destination for storing processed metadata can be set as **on premise** or **cloud** on the **Database settings** page. For further information on how to add new databases and perform database settings, please refer to section "[Databases](#)".

Email archive System settings

General Email archive system settings are available on the **System settings** page. To configure these settings, navigate to **Email Archive** → **Settings** → **System settings** on the ribbon:



contentACCESS Central Administration Tenant: TECH-ARROW

System | File Archive | **Email Archive** | SharePoint Archive | GDPR | Teams Archive | Custom plugins

Save | Discard changes | Databases | Storages | **System settings** | Provisioning settings | Retentions | Shortcut configuration | Schedules | User experience | View address book | Jobs | Remote agents | PST import | Legacy data configuration

Edit | **Settings** | Archive | Remote agents | Miscellaneous

System settings

Email Archive > Settings > System settings

a) Database settings

Database connection: ✔

b) Exchange connection settings

Exchange server type:

Region:

Exchange server interface version:

EWS Uri:

Use impersonation:

EWS authentication mode:

PowerShell Uri:

PowerShell auth:

Max connection count:

Ignore SSL errors:

Keep connection alive:

Use explicit credentials:

User name:
administrator@domain.com or domain\administrator

Password:

c) Hybrid Exchange settings

Use hybrid Exchange environment

d) General settings

Use forest wide queries:

Allow to re-link mailboxes:

Allow to archive public folders:

Public folder access:

Retention reference date:

Allow to archive one-off emails:

e) Message class handling

Exclude message classes: Mails Posts Documents Appointments Contacts Distribution list Tasks Reports

Exclude custom message classes:

Custom message classes

No data to display

Shortcutting of non-email types:
Allow or disable shortcut creation for non email items like appointment, contact, task, post. The exact shortcut configuration is taken from job settings.

Rights protected messages: Allow converting to shortcut

[Online help](#)



a) **Database settings:** Select the Email archive database, that you have previously configured on **Email Archive** → **Settings** → **Databases** page (in our case it is database “Email Archive DB”), from the dropdown list. This selected database will be used by the provisioning job. The provisioning job will store here the metadata during the synchronization process.

b) **EWS settings:**

Under **Exchange server type** and **Exchange server interface version** select the type and version of the server, where your email provider is running.

In case of the user having/using a [German cloud](#) (dedicated and isolated Microsoft Azure version for Germany), **Germany** must be selected in the **Region** dropdown list.

In case that the predefined settings for **O365** and **PowerShell** don't match your expectation and/or needs, it is possible to select the **Custom** option from the **Region** dropdown list and specify your own values.

Exchange connection settings

Exchange server type:	Exchange Online (O365)	
Region:	Custom	
Exchange server interface version:	Exchange 2013	←
EWS Url:	https://outlook.office365.abcde/EWS/Exchange.asmx	←
Use impersonation:	<input checked="" type="checkbox"/>	
EWS authentication mode:	Basic	
PowerShell Url:	https://ps.outlook.abcde/PowerShell	←

Enter the **EWS URL**. Choose whether you want to **Use impersonation** or not. By default, this checkbox is turned off. If it is turned on, the **Email archive** will use **Impersonation** instead of **delegation** (more information in [this](#) section).

Impersonation allows the superuser account to impersonate any other user's account and access their mailboxes.

Note: Only accounts with the **ApplicationImpersonation** role can use impersonation. For more information about how to configure impersonation for your account, please check [this](#) page.



If the O365 user has “desktopless” license, his account **can't be used** for impersonation. The problem is that EWS access is disabled for such user (he is unable to connect to EWS).

Select one **EWS authentication mode** from the dropdown list. There are 2 options: **Basic** and **Modern**. **Basic** authentication method was used by default in previous versions and it wasn't possible to select another authentication type. **Modern** authentication is more secure and complex and requires the app (Email archive in this case) to be registered on **Azure portal**. How to register it and gain the necessary **IDs** and **client secret** is described in [this](#) section. The app can be registered by using [this](#) PowerShell script too.

EWS authentication mode:	Modern
OAuth application ID:	72c73
OAuth tenant ID:	4b0e
OAuth client secret:

Specify the **PowerShell URL** and select the **PowerShell authentication** type. **PowerShell** can use **Basic** and **Modern** authentication type, too.

The **EWS** and **PowerShell** data must be requested from the email provider you are using (the configuration properties are the same for On-premise and Hosted Exchange).

Note: If **On-premise** is selected under **Exchange server type**, the **Email archive Provisioning job** will create contentWEB users with **Windows** login provider. If **Exchange Online** is selected, the **Email archive Provisioning job** will create contentWEB users with **Office 365** login provider. If **Hosted Exchange** is selected, the **Email archive Provisioning job** will create contentWEB users with **Microsoft Exchange** login provider.

EWS settings	
<u>Exchange server type:</u>	On-premise
Region:	On-premise
Exchange server interface version:	Exchange Online (O365)
EWS Url:	Hosted Exchange
PowerShell Url:	https://tadc01/PowerShell
PowerShell auth:	Basic
Max connection count:	10



Under **Max. connection count** option, the user may define how many parallel connections will be maintained by the system when connecting to PowerShell.

If you do not have a valid certificate, you can check the **Ignore SSL errors** checkbox.

Keep connection alive: If it is turned on, then the connection between contentACCESS and the Exchange server is cached, which increases the performance. If the Exchange is load balanced, some requests can land on another Exchange and therefore cause errors in contentACCESS. In these cases, unchecking the keep alive option will destroy the connection after each request and will rebuild it on the next request.

- If you are communicating with **one Exchange server: turn it on** to increase the performance
- If you have a **load balanced Exchange environment** and there are **communication problems** with the Exchange: it is recommended to **turn it off**

Further enter the applicable **User name** and **Password** to connect to the Exchange (use explicit credentials or log in under service-credentials).

We recommend to run a test connection via **Test** button.

Important!!! The user set under *Exchange connections* must have a full access to the mailbox(es) that he/she would like to archive (in case of not using **Impersonation**). Provisioning job requires to have “View-Only Organization Management” right on the Exchange. If [Mail app](#) will be also used, then roles **Org Custom Apps, Org Marketplace Apps** and **User Options** must be assigned for the EWS user in the **EWS settings**. These roles enable an administrator to install and manage custom apps for the organization (read more about the roles [here](#)).

In case of the user having **cloud environment**, it is possible to set **Office 365 “SuperUser”** under Exchange connections. To learn what to configure for the “SuperUser” mailbox, please check [this](#) section of our documentation.

Note: In case the user who has MFA enabled is also Admin for email archiving, the user must use the app password instead of the regular password in the **Email archive -> System settings -> EWS settings**.



c) Hybrid Exchange settings:

In order to support **Hybrid exchange environment**, please check this checkbox and configure the settings. In that case, contentACCESS will connect to both On-premise and Office 365, which are configured separately.

Note: For **Office 365** alone, this option is not visible. **On-premise Exchange** and **Hosted Exchange** will show this option and it will be possible to set up **Hybrid Exchange**.

d) General settings:

Use forest wide queries: This option allows to list the users and groups in other child domains. The option is available by On-premise Exchange server type only.

Many big companies are separating the users from resources into multiple child domains. Without that option, the email provisioning will search only the current domain (where the MS Exchange is installed), but not the others. Using this option, the searching will be extended to look into other domains too. This option has some impact on the provisioning performance.

Allow to re-link mailboxes: By default this option is turned off. If this option is turned on, the provisioning job will be able to detect that a mailbox was deleted and replaced by a new one. The new mailbox (even if the mailbox GUID is changed) will be linked to the deleted (old) entry. If this option is turned off, the provisioning job will not attempt to re-link the mailbox, however, the mailbox will be marked with a warning flag in the [Address book](#).

Default restore method: The administrator may decide the default restore method here. The data can be restored either into the existing shortcut (in-place restore), or a new item can be created. The default setting is used by the Email archive restore and Shortcut synchronization jobs.

Allow to archive public folders: The default contentACCESS behavior is not to archive the public folders; if you want to archive them, this option must be selected, otherwise they will be ignored. If public folder archiving is turned on and later off, the existing archived public folder mailbox is not removed (nor disabled). It will be simply not archived further, but the existing data remain in the archive.



Public folder access: When connecting using the Exchange Web Services, a mailbox (any mailbox) must be opened. This mailbox is defined here. It is recommended to use the superuser mailbox. If this value is changed, it is necessary to run the email provisioning job.

Retention reference date: If **Sent date** is set here, then the option **Reference date** when creating a new retention will use the **Sent date** value.

Retention repository ✕

Retention name:

Description:

Calculated from:

Protected retention time in months:

Has unprotected retention time

Allow to archive one-off emails: One-off items are emails with special message class and custom code (for example a contentACCESS shortcut) that is disconnected from the custom form (i.e. the message class is reverted, and the custom code is included in the mail).

By default, the option to archive such emails is **unchecked**, because these are not correct emails. These emails were reported as **errors** in the [System logs](#) before, now they are reported as **information**.

By **checking** this option, the system will archive these emails (may be necessary in journal archiving). The one-offed emails will be archived "as-is" - with no warranty that it will be possible to open them in Outlook.

e) **Message class handling:** Enables to exclude certain message classes from the email archiving process **on the level of the tenant**. This feature can be quite useful for companies that have a policy stating that certain message classes, e.g. Contacts, Tasks etc. mustn't be archived. Here you can also **exclude custom message classes**. E.g. if your company already has a third party archive, then you can exclude these already archived emails from the re-archiving process. Wildcards are also supported in the exclude message class list. Supported formats are: contains: *Test*; EndsWith: *Test; StartsWith: IPM*.



Shortcutting of non email items (appointment, task, post, contact) is also allowed. The message class of these items won't be changed by the job, only the body and attachments will be. The shortcut type is taken from job settings. If you wish to process these items, select **Create shortcut** from the dropdown list, if not, select **Do not create shortcut**.

Shortcutting of non-email types:

Allow or disable shortcut creation for non email items like appointment, contact, task, post. The exact shortcut configuration is taken from job settings.

Important: In case of **custom Exchange solution(s)** used for emails, the **custom email properties will not be archived!** The recommended solution: do not archive these emails and/or use the exclude feature (in [Email archive System settings](#)) for these custom message classes.

Important: It is important to bear in mind that the message class settings performed within **Email Archive** → **Settings** → **System settings** under section **Exclude message classes** will always take priority over the message class filtering configurations of an archiving job.

The **Allow converting to shortcut** checkbox for **Rights protected messages** enables the administrator to allow this kind of emails to be shortcutted on a tenant level – this option is disabled/unchecked by default. You can read more about the archiving of rights protected messages in [this](#) section.

Rights protected messages: Allow converting to shortcut

Hybrid exchange settings

Important: Active Directory integration settings in **System** => **Services** => **System** must point to the On-premise system.

If your company plans to use **Office 365 together with the existing On-premise Exchange infrastructure** or plans to **migrate to Office 365**, the **Email archive** is also supporting the **Hybrid Exchange environment**.

The transition period (moving from on-premise to cloud) can take a lot of time. During this time **both on-premise and cloud mailboxes can be archived**.

The following configuration changes must be performed to support the **Hybrid environment**:



- The domain controller settings must point to an **On-premise domain controller**
- The **Use hybrid Exchange environment** checkbox must be checked - it allows configuring the connection to the Office 365 of your organization
- The mailboxes should be grouped to groups that are available on the On-premise Exchange
- The Office 365 login provider must be configured

Note: The **Hybrid Exchange** option is visible only for **On-premise Exchange** and **Hosted Exchange** configurations. The option is not available if your archive is already configured for **Office 365**.

Region: If you are using a [German cloud](#), **Germany** needs to be picked in this dropdown list.

In case that the predefined settings for **O365** and **PowerShell** don't match your expectation and/or needs, it is possible to select the **Custom** option from the **Region** dropdown list and specify your own values.

Region:	<input type="text" value="Custom"/>	
EWS Url:	<input type="text" value="https://outlook.office365.abcde/EWS/Exchange.asmx"/>	←
EWS authentication mode:	<input type="text" value="Basic"/>	
PowerShell Url:	<input type="text" value="https://ps.outlook.abcde/PowerShell"/>	←

PowerShell auth: Pick the proper PowerShell authentication from the dropdown list. Recommended is to use the **Basic** authentication. It is also possible to select **Modern** authentication – in that case, the **PowerShell authentication** will be automatically extended by the necessary parameters (more info in [this](#) section).

Max connection count: Specify the maximum number of parallel connections the archive is allowed to use when connecting to Office 365 PowerShell. Office 365 throttling policies are applying for these connections, therefore it is recommended to use the account exclusively for archiving, otherwise the email archive might not receive a free connection from Office 365.

Ignore SSL errors: Use this option only if the connection can't be established because of SSL errors. The Office 365 certificates should be trusted by default, so there is no other reason to check this option.

Keep connection alive: If it is turned on, then the connection between contentACCESS and the Exchange server is cached, which increases the performance.

Use explicit credentials: If explicit credentials need to be used to connect to the Exchange, check the Use explicit credentials checkbox and enter the applicable **User name** and **Password**.

Note: It is recommended to use the same SuperUser for both systems (On-premise, Office 365).

Hybrid Exchange settings

Use hybrid Exchange environment

Region:	Global
EWS Url:	https://outlook.office365.com/EWS/Exchange.asmx
EWS authentication mode:	Modern
OAuth application ID:	72c7
OAuth tenant ID:	4b0e
OAuth client secret:
PowerShell Url:	https://ps.outlook.com/PowerShell
PowerShell auth:	Basic
Max connection count:	2
Ignore SSL errors:	<input type="checkbox"/>
Keep connection alive:	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/> Use explicit credentials	
User name:	companyadmin@tech-arrow.com administrator@domain.com or domain\administrator
Password:
	<input type="button" value="Test connection"/>

After the checkbox is checked and everything is configured, contentACCESS will be able to connect to both **On-premise** and **Office 365** systems, which are configured separately.

Which groups are visible for provisioning?

In **hybrid environments**, the **Email archive** is processing only the groups that are available on the on-premise Exchange servers. These groups can contain both on-premise mailboxes and cloud mailboxes. It is recommended to **set up an Exchange group (or groups)** containing all mailboxes to be archived and provision only the group.



Exchange servers

Please choose servers or groups you decided to process by provisioning job. If a server is selected, all the groups in it will be processed.

Servers: select

Name	Server DN
EX	*** /o=exTA/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Configuration/cn=Servers/cn=EX

Exchange groups

Groups: select add

Name	Group DN
OnPrem_GroupTest	*** CN=OnPrem_GroupTest,CN=Users,DC=TA,DC=local

How to distinguish between On-premise and cloud mailboxes in Address book?

The column **Server name** shows the server that is hosting the mailbox. For cloud mailboxes, the server name will be **Office365**, on-premise mailboxes will show the name of the **on-premise Exchange server**.

Name	Email	Create content/WEB access	Associate with role	Enable mail app	Archive database	Store	Active	server name	Disconnected	Process as journal	Warning	Index zone
ad min	*** admin@techybrid1.onmicrosoft.com	Inherit		Inherit	TestingDB	EmailArchiveStorage	Yes	EX	No	No		Default index zone
Christiano Ronaldo	*** ronaldo@techybrid1.onmicrosoft.com	Inherit		Inherit	TestingDB	EmailArchiveStorage	Yes	Office365	No	No		Default index zone
[blurred]	*** [blurred]	Inherit		Inherit			Yes	EX	No	No		
Emily Blunt	*** blunt@techybrid1.onmicrosoft.com	Inherit		Inherit	TestingDB	EmailArchiveStorage	Yes	EX	No	No		Default index zone
h.y.	*** hybrid.com@techybrid1.onmicrosof	Inherit		Inherit			Yes	EX	No	No		
Lionel Messi	*** messi@techybrid1.onmicrosoft.com	Inherit		Inherit	TestingDB	EmailArchiveStorage	Yes	Office365	No	No		Default index zone

How logins are created?

In **Email archive Provisioning settings** (Email archive => Settings => Provisioning settings => User creation options), it is possible to configure what type of login will be associated with the users. For every on-premise and cloud mailbox, a **Windows** login is created. **Office 365** login is created for every Office 365 mailbox, but can be additionally created for on-premise mailboxes.



User creation options

Create users with:

Create additional Azure login:

What to do after a mailbox is moved from On-premise to cloud (also vice-versa)?

If the mailbox is still in the group after the move, only the [Email archive Provisioning job](#) needs to be started.

After a mailbox is moved from on-premise to cloud, the mailbox should remain a member of one of the groups configured for provisioning. The next provisioning job will actualize the mailbox information and switch the on-premise mailbox to cloud mailbox type. The same procedure applies when a mailbox is moved from cloud to on-premise.

View address book
[Email Archive](#) > [Archive](#) > [View address book](#)

Mailboxes										
Name	Email	Distinguished Name	Create content	WEB access	Associate with role	Enable mail app	Archive database	Store	Active	Server name
OnPrem_Palko	OnPrem_Palko@techhybrid1.onmicrosoft.com	CN=OnPrem_Palko,OU=techhybrid1.onmicrosoft.com,Exchange Hosted Organizations,DC=EURPR03A007,DC=PROD,DC=	Inherit		Inherit	Inherit			Yes	Office365
✓ OnPrem_Petike	OnPrem_Petike@techhybrid1.onmicrosoft.com	CN=OnPrem_Petike,CN=Users,DC=TA,DC=local	Enable		Inherit	Enable	TestingDB	EmailArchiveStore	Yes	EX ←
OnPrem_Piroska	OnPrem_Piroska@techhybrid1.onmicrosoft.com	CN=OnPrem_Piroska,CN=Users,DC=TA,DC=local	Enable		Inherit	Inherit	TestingDB	EmailArchiveStore	Yes	EX
OnPrem_Pistike	OnPrem_Pistike@techhybrid1.onmicrosoft.com	CN=OnPrem_Pistike,CN=Users,DC=TA,DC=local	Enable		Inherit	Enable	TestingDB	EmailArchiveStore	Yes	EX
OnPrem_Samu	OnPrem_Samu@techhybrid1.onmicrosoft.com	CN=OnPrem_Samu,CN=Users,DC=TA,DC=local	Enable		Inherit	Inherit			Yes	EX
t.t.	ta.local@techhybrid1.onmicrosoft.com	CN=t.t.,CN=Users,DC=TA,DC=local	Inherit		Inherit	Inherit			Yes	EX
t.u.	testuser2@techhybrid1.onmicrosoft.com	CN=t.u.,CN=Users,DC=TA,DC=local	Inherit		Inherit	Inherit			Yes	EX
ta.com t.a	ta.com@techhybrid1.onmicrosoft.com	CN=ta.com t.a,CN=Users,DC=TA,DC=local	Inherit		Inherit	Inherit			Yes	EX
Tom Cruise	cruise@techhybrid1.onmicrosoft.com	CN=Tom Cruise,OU=techhybrid1.onmicrosoft.com,OU=MI,Exchange Hosted Organizations,DC=EURPR03A007,DC=PROD,DC=	Inherit		Inherit	Inherit	TestingDB	EmailArchiveStore	Yes	Office365



Mailbox details

Details
Statistics
Groups
Tools

Basic information

Mailbox name:	OnPrem_Petike
Email address:	OnPrem_Petike@techybrid1.onmicrosoft.com
Server:	EX
Distinguished name:	CN=OnPrem_Petike,CN=Users,DC=TA,DC=local
Database:	TestingDB
Store:	EmailArchiveStorage
Index zone:	Default index zone
Is disconnected:	No
Is active:	Yes
Process as journal:	No
Mailbox guid:	f2d8b2f3-2cef-46f5-9a95-c9a7a31c15e6
Active mailbox guid:	f2d8b2f3-2cef-46f5-9a95-c9a7a31c15e6

Close

Screenshots: Mailbox before moving to cloud

View address book
[Email Archive](#) > [Archive](#) > [View address book](#)

Mailboxes	Public folders	Groups	Servers					
import mailboxes manually + add mailbox manually								
Name	Email	Create contentWEB access	Associate with role	Enable mail app	Archive database	Store	Active	Server name
OnPrem								
onprem journal	*** onprejournal@techybrid1.onmicr	Inherit		Inherit			Yes	EX
OnPrem_Palko	*** OnPrem_Palko@techybrid1.onmicr	Inherit		Inherit			Yes	Office365
<input checked="" type="checkbox"/> OnPrem_Petike	*** OnPrem_Petike@techybrid1.onmicr	Enable	Inherit	Enable	TestingDB	EmailArchiveStor	Yes	Office365 ←
OnPrem_Piroska	*** OnPrem_Piroska@techybrid1.onmicr	Enable	Inherit	Inherit	TestingDB	EmailArchiveStor	Yes	EX
OnPrem_Pistike	*** OnPrem_Pistike@techybrid1.onmicr	Enable	Inherit	Enable	TestingDB	EmailArchiveStor	Yes	EX
OnPrem_Samu	*** OnPrem_Samu@techybrid1.onmicr	Enable	Inherit	Inherit			Yes	EX

Page 1 of 1 (6 items) ⏪ 1 ⏩

Mailbox details ✕

Details
Statistics
Groups
Tools

Basic information

Mailbox name:	OnPrem_Petike
Email address:	OnPrem_Petike@techhybrid1.onmicrosoft.com
Server:	Office365
Distinguished name:	CN=OnPrem_Petike,OU=techhybrid1.onmicrosoft.com,OU=Microsoft Exchange Hosted Organizations,DC=EURPR03A007,DC=PROD,DC=OUTLOOK,DC=COM
Database:	TestingDB
Store:	EmailArchiveStorage
Index zone:	Default index zone
Is disconnected:	No
Is active:	Yes
Process as journal:	No
Mailbox guid:	f2d8b2f3-2cef-46f5-9a95-c9a7a31c15e6
Active mailbox guid:	f2d8b2f3-2cef-46f5-9a95-c9a7a31c15e6

Screenshots: Mailbox after moving to cloud

Important: If an on-premise Exchange group is used in a job configuration, the job configuration needs to be updated after the group is moved to the cloud, since the group identifier changes and the job is still using the old identifier.

Steps to take:

- open job's configuration page
- remove the group from the list of **Address book objects to process**
- select the group and re-add it to the list
- save the job configuration

How to reconfigure the system after On-premise is turned off?

If you decide to keep only your cloud system running and turn off the On-premise one, the following steps need to be done for your environment to work correctly:



- the **Use hybrid Exchange environment** checkbox in **Email archive => Settings => System settings => Hybrid Exchange settings** must get unchecked
- EWS settings under **Email archive => Settings => System settings** must be rewritten to point to the cloud system
- old server and groups need to be deleted from **Email archive Provisioning job** configuration and added newly

Email archive registration on Azure portal for Modern authentication

For modern authentication, Email archive must be first registered on the Azure portal. We will describe the necessary part of the process in this section.

Navigate to **portal.azure.com**. Go to **All services -> App registrations -> + New registration**. Register the app.

All services > App registrations > Register an application

Register an application

* Name

The user-facing display name for this application (this can be changed later).

contentACCESS Email archive ✓

Supported account types

Who can use this application or access this API?

Accounts in this organizational directory only (contentACCESS EarlyAccessDE only - Single tenant)

Accounts in any organizational directory (Any Azure AD directory - Multitenant)

Accounts in any organizational directory (Any Azure AD directory - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox)

[Help me choose...](#)

Redirect URI (optional)

We'll return the authentication response to this URI after successfully authenticating the user. Providing this now is optional and it can be changed later, but a value is required for most authentication scenarios.

Web ▼ e.g. https://myapp.com/auth



After the app is successfully registered, you will be able to see the **Application ID** and **Directory ID** in the app's **Overview**. These are used in Teams archive System settings to connect contentACCESS with the Teams application.

The screenshot shows the 'Overview' page for the 'contentACCESS Email archive' application in the Azure portal. The left-hand navigation pane includes sections for 'Manage' (Branding, Authentication, Certificates & secrets, Token configuration, API permissions, Expose an API, Owners, Roles and administrators, Manifest) and 'Support + Troubleshooting' (Troubleshooting, New support request). The main content area displays the following details:

- Display name:** contentACCESS Email archive
- Application (client) ID:** 4124 [redacted] (indicated by a red arrow)
- Directory (tenant) ID:** 9bab [redacted] (indicated by a red arrow)
- Object ID:** 517005 [redacted]
- Supported account types:** My organization only
- Redirect URIs:** Add a Redirect URI
- Application ID URI:** Add an Application ID URI
- Managed application in ...:** contentACCESS Email archive

Below the details, there is a 'Call APIs' section with a 'View API permissions' button and a 'Documentation' section with links to Microsoft identity platform resources.

Next, go to **Certificates & secrets** and add a new client secret by clicking on the **+ New client secret** button.

The screenshot shows the 'Certificates & secrets' page for the 'contentACCESS Email archive' application. A blue banner at the top contains a warning: 'Copy the new client secret value. You won't be able to retrieve it after you perform another operation or leave this blade.' Below this, the 'Certificates' section is empty, with a message: 'No certificates have been added for this application.' The 'Client secrets' section contains a '+ New client secret' button, which is highlighted with a red box. Below the button is a table of existing client secrets:

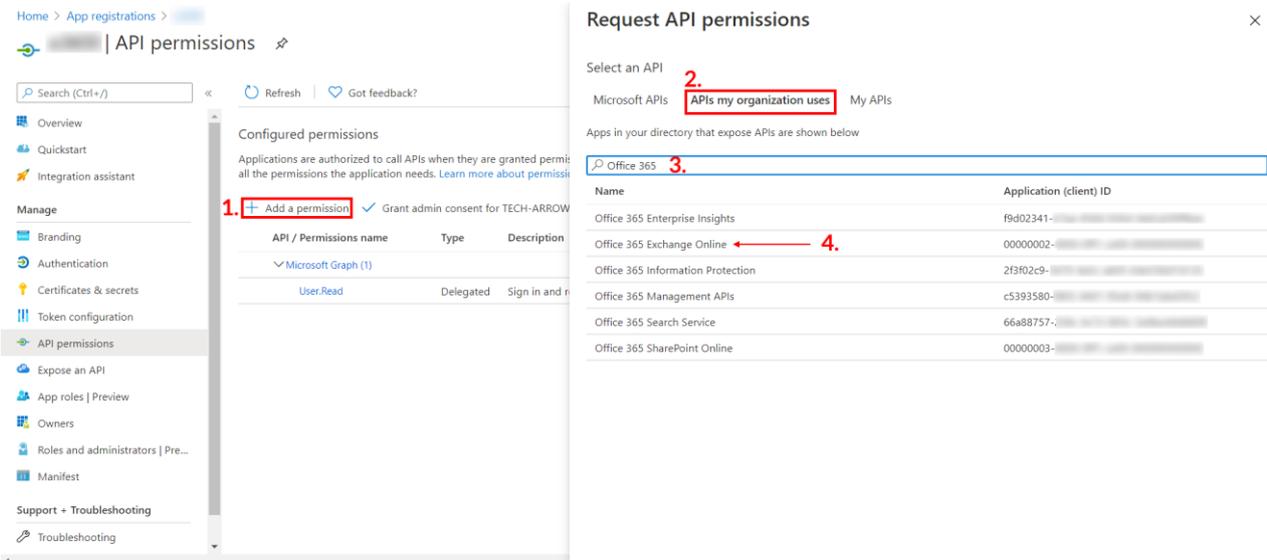
Description	Expires	Value
Email Archive Secret	12/31/2299	4FQ6 [redacted]

Next, you need to define the **API permissions** by adding the following permissions:

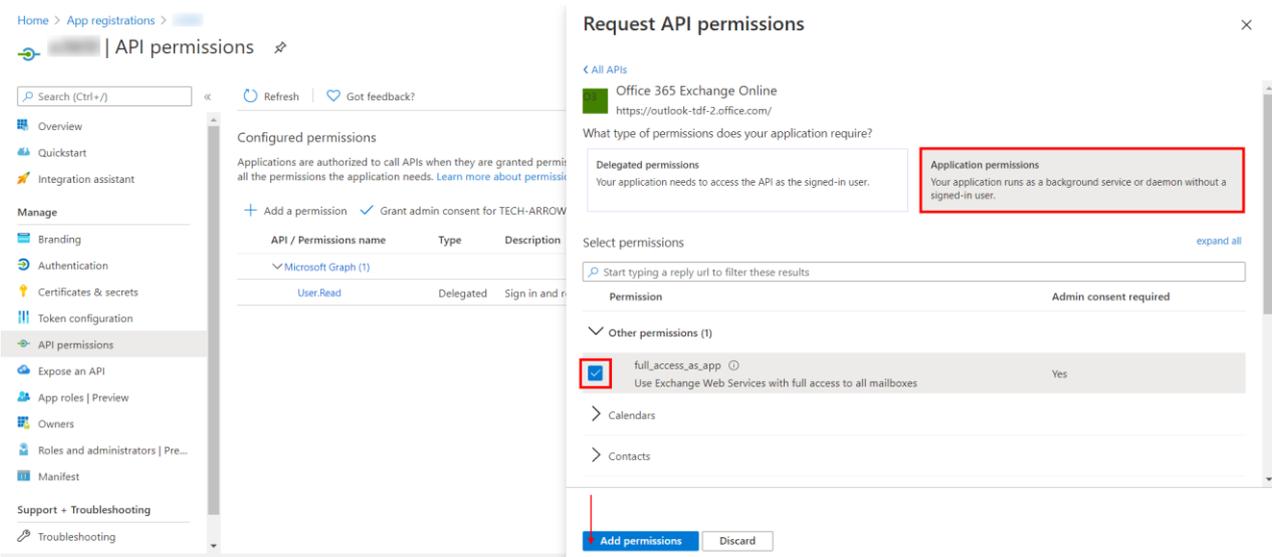
- Office 365 Exchange Online - full_access_as_app

- Microsoft.Graph - User.Read

To add the **Office 365 Exchange Online** permission, click on the **Add a permission** button. Next, switch to the **APIs my organization uses** tab. Start writing „Office 365“ to the search field and then click on **Office 365 Exchange Online** option.

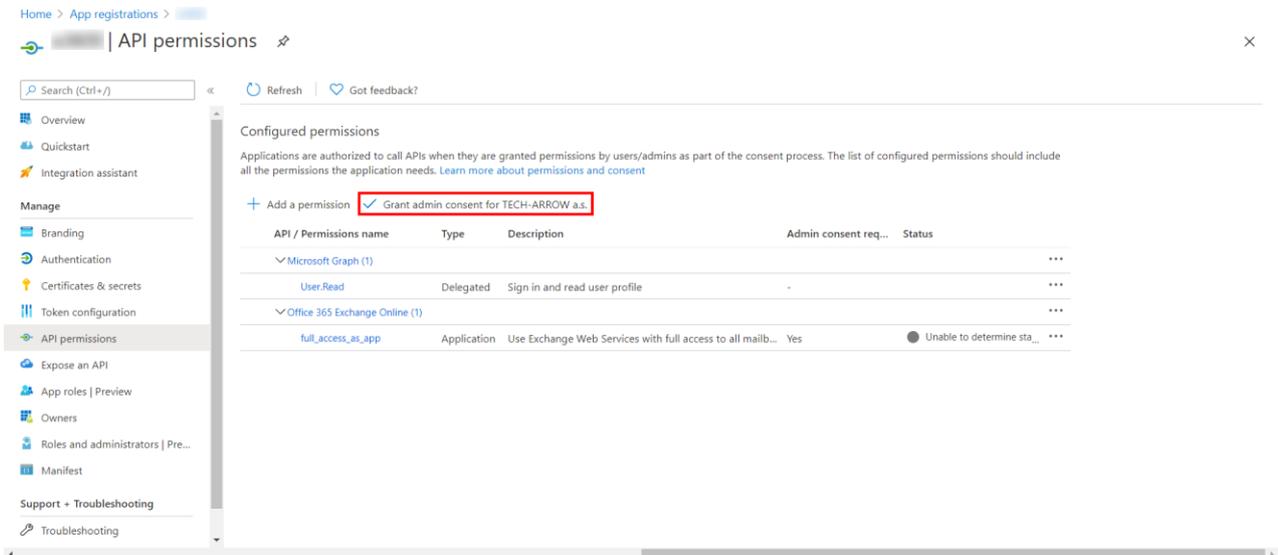


Select the **Application permissions** type. Check the **full_access_as_app** checkbox and then click on **Add permissions**.





After that, click on the **Grant admin consent** button. This will grant consent for the permissions assigned to the application.



Email archive Provisioning settings

The provisioning job:

- Synchronizes the Exchange server objects specified on the **Provisioning settings** page to the contentACCESS **Address book**
- Verifies the user's permissions on the mailboxes on the Exchange server and synchronizes these permissions to contentACCESS
- If contentWEB user creation is turned on in the Address book for an object (Exchange mailbox/group/server), it creates a contentWEB user for mailboxes with an authentication type **Windows, Office 365** or **Microsoft Exchange** based on the EWS settings (for more info please refer to [Email archive System settings](#), section **EWS settings**)
- If [MailApp](#) activation is allowed (or inherited from parent group/server), it activates MailApp for the selected mailbox/group/server
- Based on the roles assigned in the Address book, it gives permissions on the specific archive mailbox(es)

The mailbox provisioning job is an elementary job, which is intended to extract Exchange groups and subgroups from the Exchange server and synchronize their changes with contentACCESS. For example, if a new user has been added to an Exchange group which is under archiving process, the provisioning job will



“point out” this change and the mailbox of this new user will be crawled/archived automatically. Provisioning job will synchronize the mailbox permissions as well.

In contentACCESS, a provisioning job is created automatically when activating email archive for the first time.

Email Archive provisioning settings are available on the **Provisioning settings** page (**Email Archive → Settings → Provisioning settings**):



contentACCESS Central Administration Tenant: TECH-ARROW

System | File Archive | **Email Archive** | SharePoint Archive | GDPR | Teams Archive | Custom plugins

Save | Discard changes | Databases | Storages | System settings | **Provisioning settings** | Retentions | Shortcut configuration | Schedules | User experience | View address book | Jobs | Remote agents | PST import | Legacy data configuration

Edit | Settings | Archive | Remote agents | Miscellaneous

Provisioning settings

Email Archive > Settings > Provisioning settings

start immediately
 refresh
 disable auto refresh
 deactivate job
 logs
 edit

Status: **Idle**
 Progress: 20 mailboxes processed (13 mailboxes not changed, 7 mailboxes updated, 10 groups not changed) (completed 5 days ago)

a) Force full crawl (Click to maintain a full crawl for the next provisioning run.)

b) Scheduling settings

Scheduled in:

c) Notification settings

Send when:

Recipient list:

d) Exchange servers

Please choose servers or groups you decided to process by provisioning job. If a server is selected, all the groups in it will be processed.

Servers:

Name	Server DN
No data to display	

e) Exchange groups

Groups:

Name	Group DN
...	*** CN=...,CN=Users,DC=ta,DC=internal
2	*** CN=...,2,CN=Users,DC=ta,DC=internal
3	*** CN=...,3,CN=Users,DC=ta,DC=internal
wolvesX	*** CN=wolvesX,CN=Users,DC=ta,DC=internal
wolvesW	*** CN=wolvesW,CN=Users,DC=ta,DC=internal
...	*** CN=...,CN=Users,DC=ta,DC=internal
wolves	*** CN=wolves,CN=Users,DC=ta,DC=internal
decgroup	*** CN=decgroup,OU=VWE_TEST,DC=ta,DC=internal

f) Archive settings

Mailbox owner role:
Warning! The role will be assigned to mailboxes only if the Create contentWEB access option is turned on for a mailbox, group or server in Addressbook.

Shared mailboxes role:

Assign to mailbox:

Database connection:
Warning! Multiple databases available, and the selected one will be automatically assigned.

Storage name:

Index zone:

Create contentWEB user:

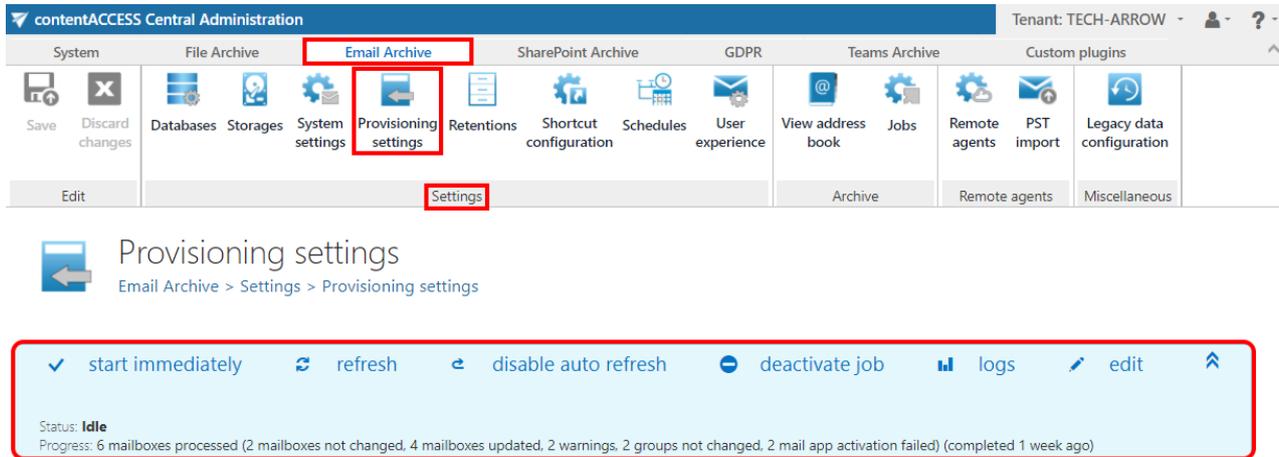
g) User creation options

Create users with:

h) Resource settings

Worker thread count:

The **status bar** of the provisioning job offers the following options:



If a scheduler has not been selected, the provisioning job can be still started (and also stopped) manually with the “start immediately/stop” control button. For manual refresh of provisioning progress information, click on “refresh” button. To enable/disable auto refresh in every 5 seconds, click on “enable auto refresh”/“disable auto refresh” button. The provisioning job can be also deactivated with the “deactivate job” button. A deactivated job will not start neither automatically, nor can be started manually. The “edit” button is used to select the node, where provisioning job will be run. The user may also rename the provisioning job from here. To view further event details of provisioning job (and also to detect any potential failures/errors in the provisioning events), click on “logs” button. This will redirect you to the System logs page, where the last run of the provisioning job will be preselected, and the last events will be shown in the events table.

#	Start date	End date	Date	Title	Description
1	8/10/2015 5:33 PM	8/10/2015 5:34 PM	8/10/2015 5:34 PM	Plugin is finished successfully	Plugin.MailboxProvisioning
2	8/3/2015 1:39 PM	8/3/2015 1:39 PM	8/10/2015 5:34 PM	contentACCESS user skipped from permission sync	User 'new user' permissions can't be set because the user SID could not be resolved.
3	7/31/2015 12:39 PM	7/31/2015 12:39 PM	8/10/2015 5:34 PM	contentACCESS user skipped from permission sync	User 'MA' permissions can't be set because the user SID could not be resolved.
4	7/15/2015 10:54 AM	7/15/2015 10:54 AM	8/10/2015 5:34 PM	contentACCESS user skipped from permission sync	User 'sa' permissions can't be set because the user SID could not be resolved.
5	7/15/2015 10:52 AM	7/15/2015 10:52 AM	8/10/2015 5:34 PM	contentACCESS user skipped from permission sync	User 'administrator' permissions can't be set because the user SID could not be resolved.
6			8/10/2015 5:34 PM	Updating mailbox:	Updating mailbox: '26 (#vladimir.werskov@tech-arrow.com)' in DB.
7			8/10/2015 5:34 PM	Updating mailbox:	Updating mailbox: '25 (#tfs@TECHARROW.onmicrosoft.com)' in DB.

With the arrows mark () at the right side of the status bar the user may collapse or expand the progress information about the provisioning job’s running. The status bar’s last state is always stored, and the last state will be opened by navigating to the page again.

The following configuration sections are available on the **Provisioning settings** page:

- a) **Force full crawl:** The Exchange provisioning job is performing an incremental crawl of the Exchange objects (mailboxes and groups). This means that if an object is not changed, it is not necessary to access



it. This makes the provisioning job faster and helps to use less resources. In some situations, however, it is necessary to perform a full crawl of the objects – need to synchronize every object independently, whether it was changed or not from the last synchronization. This can be done with a single click on the „force full crawl“ button, which is located under the status bar of the provisioning job.

Provisioning settings

Email Archive > Settings > Provisioning settings

- b) **Scheduling settings:** Select the running times of the provisioning job or create a new scheduler. For more information on how to configure scheduler settings please refer to section [Schedules](#) described above.
- c) **Notification settings:** If the provisioning job could not run properly due to some reasons, contentACCESS can send a warning about the problem. The notification email message will be sent to the email address that is set here under **Recipient list** option. Here you can also choose, when these email messages should be sent: only if errors occur, or when errors or warnings occur, or always, regardless of the faultless running of the provisioning job.
- d) **Exchange servers:** click on **select** option and select the Exchange servers to synchronize from the list of **Select Exchange Server** dialog.

Drag a column header here to group by that column	
Name	Server DN
<input type="checkbox"/> Office365	Office365

If you select a server, then all mailboxes falling under this server and also all Exchange groups within the organization will be permanently processed by the provisioning job. This will eventually mean that if a



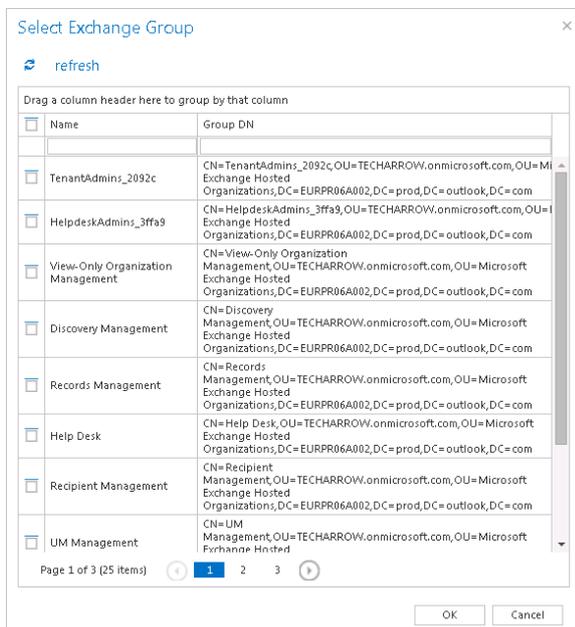
server is selected, then it makes no sense to select an Exchange group as well. If all settings are done, click on **OK**. The selected server can be deleted from its context menu:



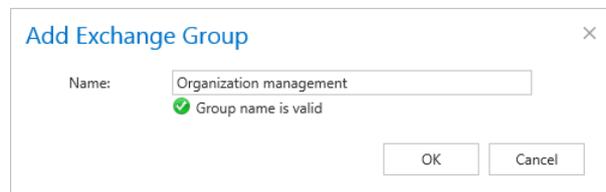
e) **Exchange groups:** all users of an Exchange server fall under an Exchange group (or can belong to even more Exchange groups simultaneously). In this section it is possible specify one or more Exchange groups to be synchronized by the provisioning job.

Group(s) can be

- **selected from the list** of all groups available on the Exchange – Click on **select** option and select the groups in the **Select Exchange Group** dialog’s list (Screenshot 1).
- **added manually** to the groups to be provisioned – Click on **+ add** and fill the group to the **Add Exchange Group** dialog manually (Screenshot 2).



Screenshot 1



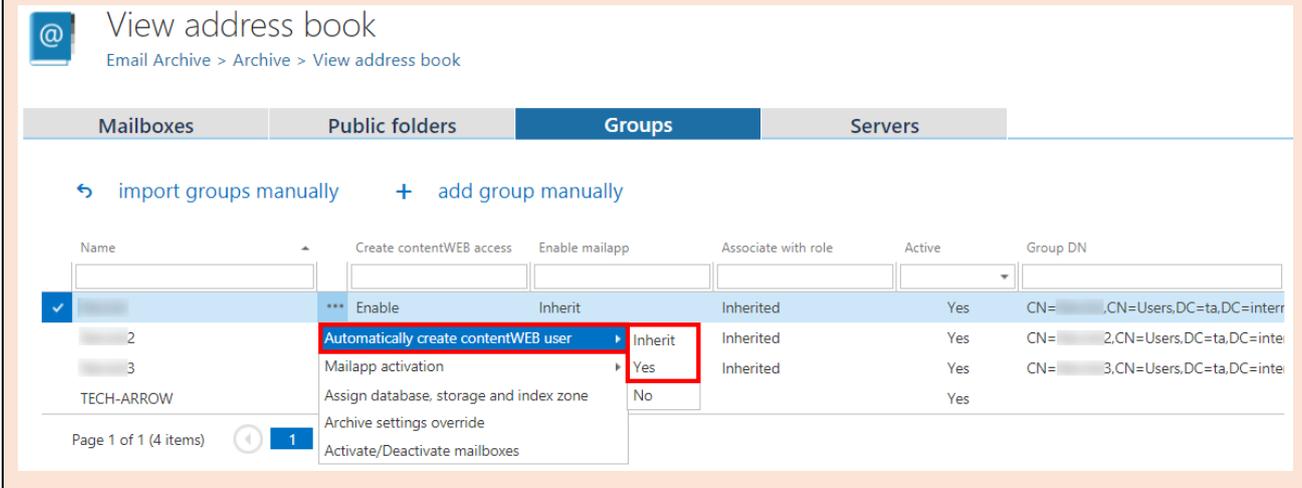
Screenshot 2

Note: If you selected a server one step earlier, then all groups falling under this server will be processed and it makes no sense to select groups as well.

f) **Archive settings:** This configuration section allows to assign default contentWEB user roles. The provisioning job will assign the role defined here for the Exchange objects, which are already synchronized to the Address book and contentWEB user creation is allowed for them (option “Automatically create contentWEB user” in the Address book). It is recommended to specify here a default role with less contentWEB permissions, e.g. a role without permissions to recover from the archive. The roles to be assigned must be created on the [Roles](#) page.

Important: If there are multiple roles assigned for the same Exchange object (e.g. one role with less permissions in the provisioning settings, another role with more permissions in the Address book), then the following rule applies: The role with more permissions always wins.

Important: To be able to assign roles using the provisioning job, first the contentWEB user(s) creation must be allowed in the Address book or inherited from a parent that has contentWEB user(s) creation allowed, otherwise the role will not be assigned.



The screenshot shows the 'View address book' interface with the 'Groups' tab selected. A table lists group configurations with columns for Name, Create contentWEB access, Enable mailapp, Associate with role, Active, and Group DN. A dropdown menu is open for the 'Automatically create contentWEB user' setting, showing options: 'Inherit', 'Yes', and 'No'. The 'Inherit' option is highlighted with a red box.

Name	Create contentWEB access	Enable mailapp	Associate with role	Active	Group DN
2	*** Enable	Inherit	Inherited	Yes	CN=...,CN=Users,DC=ta,DC=interr
3	Automatically create contentWEB user	Inherit	Inherited	Yes	CN=...,2,CN=Users,DC=ta,DC=inte
TECH-ARROW	Mailapp activation	Yes	Inherited	Yes	CN=...,3,CN=Users,DC=ta,DC=inte
	Assign database, storage and index zone	No		Yes	
	Archive settings override				
	Activate/Deactivate mailboxes				

Roles containing Manage system and/or Manage tenant permissions are unavailable in the default roles' dropdown list. If the role is changed in this configuration section, the next run of the email provisioning job will replace the previously assigned user permissions with the permissions defined in the newly assigned role.



In the **Archive settings** configuration section you need to set:

Mailbox owner role: this is a default role, which will be assigned for the Exchange objects (mailboxes/groups/entire server) if the “Use the role defined in the provisioning job” option is selected for the given Exchange object in the Address book.

Shared mailboxes role: select a role, which will define the user’s permissions on the shared mailboxes on the Exchange server.

Archive settings

Mailbox owner role:	<div style="border: 1px solid #ccc; padding: 2px;"> ▼ Limited user </div> <small>Warning! The role will be assigned to mailboxes only if the Create contentWEB access option is turned on for a mailbox, group or server in Addressbook</small>
Shared mailboxes role:	<div style="border: 1px solid #ccc; padding: 2px;"> ▼ Limited user </div>

If you check the **Assign to mailbox** checkbox, 3 dropdowns and the **Create contentWEB user** checkbox will appear. With the dropdowns it is possible to select the default **Database, Store and Index zone** for the mailboxes.

During the run of the provisioning job, if there are new mailboxes provisioned, the selected **Database, Store and Index zone** will be automatically assigned to them.

If you want to assign **Database, Store and Index zone** to already provisioned mailboxes that don't have them assigned yet, you need to enable **Force full crawl** before executing the provisioning job.

If a database is already assigned to the mailbox, it will not be updated.

If a store is already assigned to the mailbox, it will not be updated.

If an index zone is already assigned to the mailbox, it will not be updated.

If you check the **Create contentWEB user** checkbox, then a contentACCESS user will be created with the selected **Mailbox owner role** in case that **Create contentWEB access** is set to **Inherit** in the **Address book** for that mailbox **AND**:

- the mailbox is **not** in any group and **Create contentWEB access is not set to Forbidden** for the server in Address book, **OR**
- for all the groups the mailbox is a member of, the **Create contentWEB access** is set to **Inherit** in Address book and **Create contentWEB access is not set to Forbidden** for the server in Address book, **OR**



- for at least one of the groups the mailbox is a member of, the **Create contentWEB access** is set to **Enable**

Assign to mailbox:

Database connection: 
Warning! Multiple databases available, and the selected one will be automatically assigned.

Storage name:

Index zone:

Create contentWEB user:

For more information on how to assign explicit permissions for newly created contentWEB users and how to change these explicit permissions, please refer to chapter [Creating contentWEB users.](#)

- g) **User creation options:** In this section, the login type of the users created by the provisioning job is displayed.

User creation options

Create users with:

- h) **Resource settings:** Set the value, which will determine how many items will be processed simultaneously by the provisioning job. The recommended value is "2".

Resource settings

Worker thread count:

Email archive provisioning job description

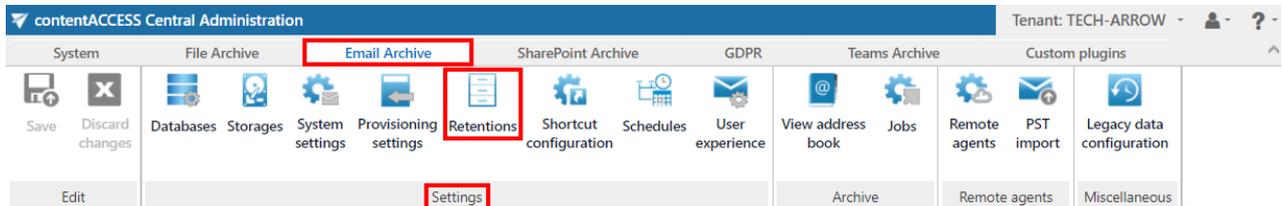
All the numbers and descriptions in the job's progress have a particular meaning. In this section, we are going to explain the numbers and descriptions of an **Email archive provisioning job**.



Description	Explanation
x mailboxes processed	x mailboxes were scanned and processed
x mailboxes added	x mailboxes have been added to the address book (new)
x mailboxes not changed	x mailboxes have been skipped
x mailboxes updated	x mailboxes have been updated in the address book
x mailboxes failed	x mailboxes failed to process
x warnings	x warnings in the processing
x groups added	x new groups were added to the address book
x groups not changed	x groups were not changed, therefore skipped
x groups updated	x groups were updated in the address book
x contentWEB accesses granted	contentweb access has been granted for x number of mailboxes
x mail app accesses granted	the mail app was installed for x mailboxes
x mail app accesses revoked	the mail app was uninstalled for x mailboxes
x mail app activation failed	the mail app failed to install for x mailboxes
x mail app deactivation failed	the mail app failed to uninstall for x mailboxes

Retention settings

Navigate to **Email Archive** → **Settings** → **Retentions**:



contentACCESS Central Administration Tenant: TECH-ARROW

System | File Archive | **Email Archive** | SharePoint Archive | GDPR | Teams Archive | Custom plugins

Save | Discard changes | Databases | Storages | System settings | Provisioning settings | **Retentions** | Shortcut configuration | Schedules | User experience | View address book | Jobs | Remote agents | PST import | Legacy data configuration

Edit | **Settings** | Archive | Remote agents | Miscellaneous

Retentions

Email Archive > Settings > Retentions

+ new | manage access

Retention name	Protected retention time in months	Has unprotected retention time	Unprotected retention time in months	Is default	Calculated from	Description
5 years	60	No	-	Yes	Archivation date	
No retention	0	No	-	No	Archivation date	

Retention settings enable to specify the time period, during which the email message will be stored. To add a new retention attribute, click on **+ new** and refer to section “**Retentions**” above for further configurations.

Shortcuts in email archiving

In contentACCESS’s email archive solution the emails can be archived with one of the following archiving methods. They can be

- replaced by shortcut; there are 2 shortcut types that can be used: normal shortcut and HTML shortcut;
- completely deleted;
- kept in the original file location.

Mailbox items younger than 1 year are archived continuously on a daily basis, but the originals are kept in the original mailbox folder. From 1 to 2 year old items are usually archived with the shortcutting method to ensure an easy access to them in case of need. They allow to open the already archived items directly from the mailbox without a need to browse for them in the archive. Another advantage of shortcuts is the spared storage space. They help to unburden Exchange servers from numbers of redundant documents that are not in use any more. If the mailbox items are older than 2 years, then they are usually deleted. It depends on the customer how he combines these processing methods.

Important: The encrypted S/MIME emails are not converted to shortcut during the archiving process. The encrypted emails are archived, but they are **not converted to shortcut**, with the following applying:



- no message class is changed
- no text body or HTML body is modified
- category can be added to the email
- attachments are **not removed** from the email

Note: There are situations when mails are archived with a shortcut type that later turns out to be incorrect. This is usually because of incorrect planning or bad decisions. If there are already shortcuts created and they need to be replaced, the Shortcut repair job type can easily solve this problem. Read more in chapter [Shortcut repair job](#).

Note: If an email was archived with shortcutting method and a category was added, the category will be still present even after running the [Email restore job](#).

These archive methods and shortcut types can be configured on the **Shortcut configuration** page. Navigate to **Email Archive** → **Settings** → **Shortcut configuration** control button to open it. On this page, under **Shortcut configuration** section you may find the full list of already configured shortcuts. The grid also contains the configuration information of the respective shortcuts. The bold color of a shortcut means that it was set as default (i.e. if they are used by manual archiving).

Under the **HTML Templates** section you may see all HTML templates configured for the HTML shortcuts. The date of creation, modification and the modified by information can be viewed in the templates' grid, too.

The shortcuts that the admin configures on this page can be selected when configuring an email archive job instance on the job's configuration page.

The listed items can be deleted/edited from their context menu with a click on the ellipses (...).



contentACCESS Central Administration Tenant: TECH-ARROW

System File Archive Email Archive SharePoint Archive GDPR Teams Archive Custom plugins

Save Discard changes Databases Storages System settings Provisioning settings Retentions Shortcut configuration Schedules User experience View address book Jobs Remote agents PST Import Legacy data configuration

Shortcut configuration
Email Archive > Settings > Shortcut configuration

+ new manage access

Name	Description	Change message class	Html template	Keep formatted body	Truncate	Remove attachments	Keep inline attachments	Add category	Category name	Is default
Normal	Normal	Yes		No	No	No	No	No		Yes
HTML	HTML	Yes	Default template	No	No	No	No	No		No
Keep original	Keep original	No		No	No	No	No	No		No
Journal	Journal	No		No	No	No	No	No		No
HTML formatted		Yes	Office 365 V2 formatted template	Yes	No	No	No	Yes	Green category	No

HTML Templates

+ new

Name	Description	Creation date	Modification date	Modified by
Default template	Default template	11/3/2017 1:04:53 PM	11/3/2017 1:04:53 PM	Administrator
Office 365 formatted template	Use this template with keep formatted body option	11/8/2018 2:45:12 PM	11/8/2018 2:45:12 PM	Administrator
Office 365 template	Office 365 template	3/15/2018 3:33:27 PM	11/8/2018 1:45:12 PM	Administrator
Office 365 V2 formatted template	Use this template with keep formatted body option	11/8/2018 2:45:12 PM	11/8/2018 2:45:12 PM	Administrator
Office 365 V2 template	Office 365 V2 template	11/8/2018 2:45:12 PM	11/8/2018 2:45:12 PM	Administrator

Online help

To create a new shortcut, click on **+ new** under the **Shortcut configuration** section and select a shortcut type from the **Type** list of the **Shortcut configuration** dialog.

Note: The “+ new” option is unavailable for the logged on user if the “Add repository items” permission on the tenant is not allowed in his role assignment.

The “manage access” option allows to grant access permissions on the selected shortcut configuration for a second user. This “manage access” option is available for the logged on administrator if his role assignment contains the Edit repository item – All allowed permission on the tenant. Read more in [Managing access to contentACCESS objects](#).

There are 4 types of shortcuts in contentACCESS’s Email Archive, namely:

- ✓ **Normal shortcut**
- ✓ **HTML shortcut**
- ✓ **Journal shortcut**
- ✓ **Keep original shortcut**



Shortcut configuration ✕

Name:

Description:

Type:

Normal shortcut

HTML shortcut

Journal shortcut

Keep original

Change message class:

Remove attachments:

Attachment placeholder name:

Add category:

Normal shortcut

Normal shortcut is completely transparent with the original message, after restoring/reopening the user cannot see any change between the original email and the shortcut version. This is the recommended shortcut type if the end user uses MS Outlook. This type of shortcut works in:

Normal shortcut			
	Installed prerequisites	Are attachments directly accessible? (direct preview)	Is email body accessible?
Outlook 2013 or higher	Mail app* or Outlook forms	Yes	Yes
	Nothing installed	No	Yes
OWA 2013 or higher	Mail app	Yes	Yes
	Nothing installed	No	Yes
Outlook 2010	Outlook forms	Yes	Yes
	Nothing installed	No	Yes
OWA 2010	OWA 2010 extension	Yes	Yes
	Nothing installed	No	Yes

*Exchange 2013 (or higher) requirements

MS Outlook 2013 or higher: To display archived attachments, the user needs to have the contentACCESS Outlook form **or** the Mail app (refer to section [User experience](#)) installed in Outlook. If not installed, the email body will be still accessible.



MS Outlook 2010: To display archived attachments, the user needs to have the contentACCESS Outlook form installed in Outlook. If not installed, the email body will be still accessible.

For more information on how to install contentACCESS Outlook forms please refer to installation guide accessible [here](#). Regarding system requirements: MS Outlook 2010 or 2013 is needed. The form should work on both 32 and 64 bit Outlook versions. On mobile devices the form is not supported.

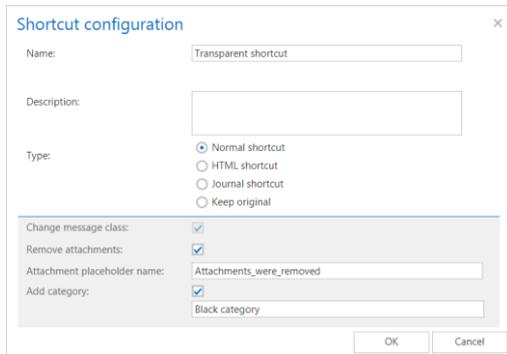
OWA 2013 or higher: To display archived attachments, the user needs to have Mail app installed. For more information refer to section [User experience](#). If not installed, the email body will be still accessible.

OWA 2010: To display archived attachments, the user needs to have contentACCESS OWA integration installed. For more information refer to section [User experience](#). If not installed, the email body will be still accessible.

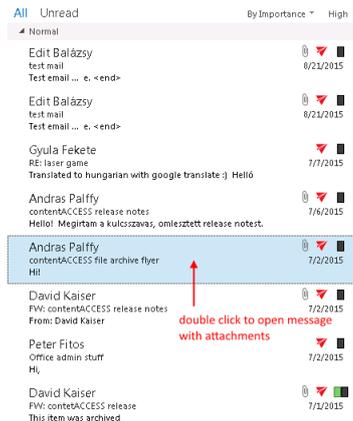
If the **Remove attachments** function was turned on during the configuration of the shortcut, the attachments will be still accessible by a double click on the archived message in the compose window. (In case if the correct extension – Outlook forms, Mail app or OWA 2010 extension – is installed.)

On the normal shortcut's configuration dialog the **Change message class** checkbox is selected by default. With this setting the restore from shortcuts is ensured.

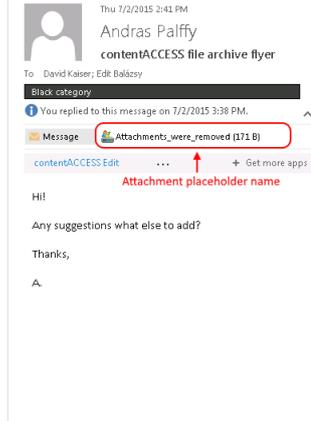
It is also possible to set here, if the attachment of the processed email should be removed (check **Remove attachments**) or should be kept (leave **Remove attachments** unchecked). Removed attachments can be retrieved by double clicking on the archived email in the compose window. The **Attachment placeholder name** can be also specified here. If you check the **Add category** option in the **Shortcut configuration** window and enter a category into the textbox, then archived emails will be marked with this category (e.g. if Black category is selected, then emails will be marked with black color). After filling all required data in the **Shortcut configuration** window, click **OK**.



Screenshot A:
Normal shortcut used by an email archive job



Screenshot B:
Original email replaced with the normal shortcut in the user's mailbox



HTML shortcut

If the user is archiving with a job using an HTML shortcut, then:

1) If the HTML shortcut doesn't have the Keep formatted body option checked

the body of the original email message will be replaced by an HTML file containing 2 links to the original email message and the attachment(s); one link opens the original email as an .msg, second opens it as .eml. The **Keep formatted body** option is explained below in this section.

Note: The .eml link ensures the compatibility with a wide range of applications and operating systems (compatibility with MAC OS is also ensured).

2) If the HTML shortcut does have the Keep formatted body option checked

the shortcut template will be injected into the original body and the original formatted body will be kept. The **Keep formatted body** option is explained below in this section.

Important: The digitally signed (S/MIME) emails can be converted to shortcut with the following limitations - **inline images can't be kept in the shortcut**. Even if you select the **Keep formatted body** option, the formatted text will be kept in the shortcut, but the inline images will be missing from the shortcut.



Important: If the email message is archived with the HTML shortcut method and it contains embedded .msg, then there will be no link in the body to access the embedded message as attachment.

In certain situations, it is not possible to use Outlook to check our emails. In these circumstances the user cannot use normal shortcuts to access emails. However, HTML-shortcuts can be still used to access email bodies and also attachments with the help of links. Emails can be checked for example with OWA. To ensure an easy access to the archived items in any cases, it is highly recommended to use this shortcut type.

The following table gives a general overview on how the archived emails and attachments can be accessed with the HTML shortcuts if MS Outlook or OWA (Outlook Web Access) is used:

HTML shortcut				
	A) The following prerequisites are installed	The attachments are accessible	B) The prerequisites are not installed	The attachments are accessible
Outlook 2013 (or higher)	Mail app* or Outlook forms	In direct preview	-	Over links
OWA 2013 (or higher)	Mail app	In direct preview	-	Over links
Outlook 2010	Outlook forms	In direct preview	-	Over links
OWA 2010	OWA 2010 extension	In direct preview	-	Over links

*Exchange 2013 or higher requirements

MS Outlook 2013 or higher: To transparently view the archived items (the body and the attachment), the user needs to have the contentACCESS Outlook forms or the Mail app installed in Outlook.

MS Outlook 2010: To transparently view the archived items (the body and the attachment), the user needs to have the contentACCESS Outlook form installed in Outlook.

OWA 2013 or higher: To transparently view the archived items (the body and the attachment), the user needs to have Mail app installed. For more information refer to section "[User experience](#)".

OWA 2010: To transparently view the archived items (the body and the attachment), the user needs to have contentACCESS OWA integration installed. For more information refer to section "[User experience](#)".

If the extensions are not installed, then the body and the attachment are still accessible over the shortcut links.



If the **Remove attachments** function was turned on, the attachments are still accessible by a double click on the archived message in the compose window.

Note: contentACCESS Outlook add-in catches changes when replying or forwarding an HTML and/or Normal shortcut. Read more about the contentACCESS Outlook forms in [this](#) section.

Before you start to configure the HTML shortcut, HTML template(s) must be created. You can use one of the pre-configured templates, or create your own. If you want to create your own template, we **highly recommend** to download one of the pre-configured ones and customize it. If you want to use a more flexible template (for example because of localizations), download and customize a **V2** template; if you want to keep the original formatted body, download and customize a **V2 formatted** template.

The 5 predefined HTML templates are the following:

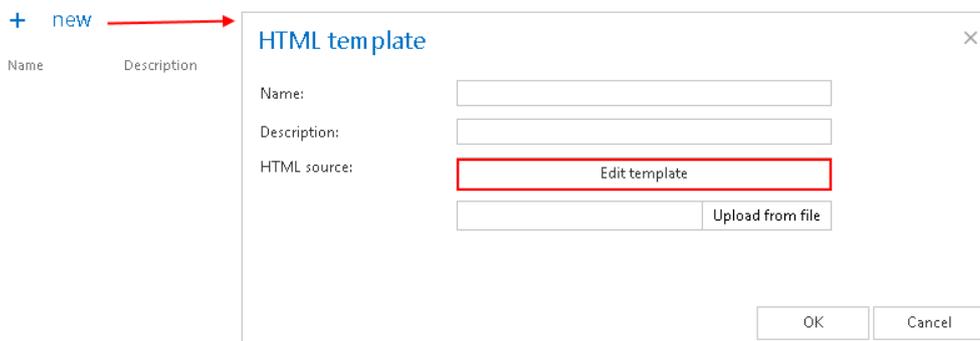
- Default
- Office 365 template
- Office 365 formatted template
- Office 365 V2 template
- Office 365 V2 formatted template

The **formatted** templates are used when creating a HTML shortcut with the **Keep formatted body** option checked (the **Keep formatted body** option is explained below in this section).

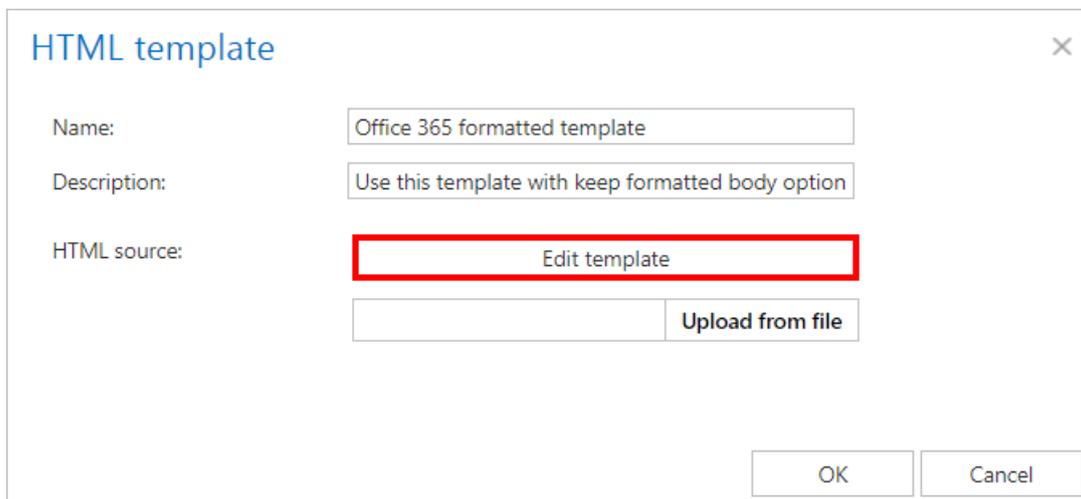
The **V2** templates have had their syntax changed to **mustache** – this allows much more flexibility when creating the template. All text included in them can be changed, which also means that the templates can be **fully localized**.

a) The default HTML template can be downloaded automatically with a click on **+ new** under the **HTML Templates** section and then by clicking on the **Edit template** button in the **HTML template** dialog.

HTML Templates



b) A pre-configured template can be downloaded by selecting **Edit** from its context menu and then clicking on **Edit template**.



c) To create a custom HTML template, download a pre-configured template first, as described above. Save it somewhere on your disc. Download an HTML editor from the web and edit your template, then save it.

Upload the default/custom HTML template to the template list: Under **HTML Templates** section click on **+new**. The **HTML template** dialog will open. Here give a **Name** for the HTML and fill the **Description** field (not required), then click on **Upload from file** and browse for the desired template that you have created. Upload it to the template list.

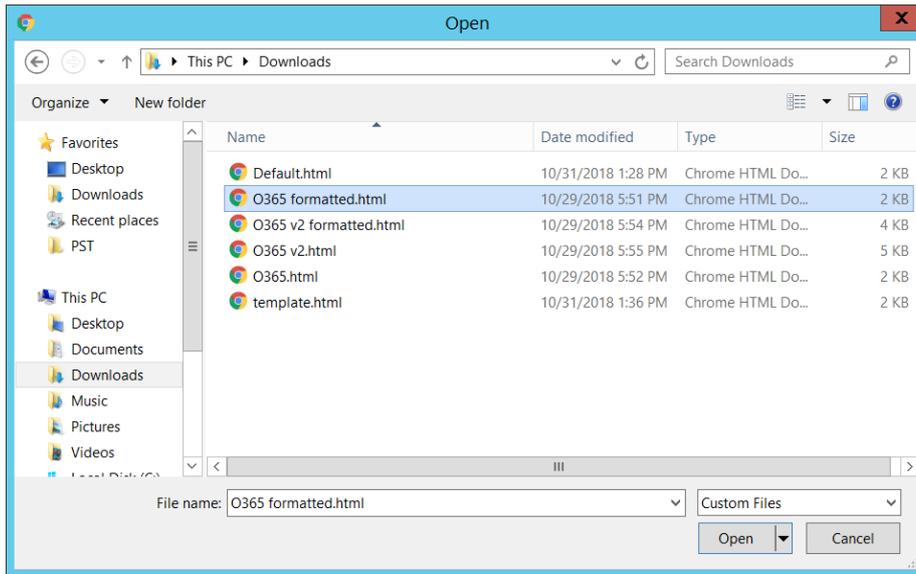


HTML template

Name:

Description:

HTML source:



Once your desired template is uploaded, a custom HTML shortcut can be configured. Navigate to **Email Archive** → **Settings** → **Shortcut configuration** and click on **+ new** under the **Shortcut configuration** section.

contentACCESS Central Administration Tenant: TECH-ARROW

System | **Email Archive** | SharePoint Archive | GDPR | Teams Archive | Custom plugins

Save | Discard changes | Databases | Storages | System settings | Provisioning settings | Retentions | **Shortcut configuration** | Schedules | User experience | View address book | Jobs | Remote agents | PST import | Legacy data configuration

Edit | **Settings** | Archive | Remote agents | Miscellaneous

Shortcut configuration

Email Archive > Settings > Shortcut configuration

+ new | manage access

Name	Description	Change message class	Html template	Keep formatted body	Truncate	Remove attachments	Keep inline attachments	Add category	Category name	Is default
Normal	Normal	Yes		No	No	No	No	No		Yes
HTML	HTML	Yes	Default template	No	No	No	No	No		No
Keep original	Keep original	No		No	No	No	No	No		No
Journal	Journal	No		No	No	No	No	No		No
HTML formatted		Yes	Office 365 V2 formatted template	Yes	No	No	No	Yes	Green category	No



The **Shortcut configuration** dialog opens. Enter a name for the shortcut into the **Name** field. In the **Use html template** dropdown list select the HTML template that you have created.

If you check the **Keep formatted body** checkbox, the original HTML body won't be converted to plain text during the shortcut creation, but the system will try to inject the attachment links into the existing message body. The user will be warned that he must select a template, which supports this formatting option. It will also become possible to keep inline attachments in the mail body by checking the **Keep inline attachments** checkbox. The **Truncate body** option will be disabled.

The **Change message class** textbox is checked by default and cannot be unchecked. This enables to restore the archived emails from the shortcuts. If you want a certain number of characters to be included in the shortcut, check the **Truncate body** option and enter a value here. The **Remove attachments** checkbox is checked by default for HTML shortcuts. Removed attachments can be later retrieved by double clicking on the archived email in the compose window. It is also possible to specify here the **Attachment placeholder name**, like when configuring a **Normal shortcut**. In the HTML shortcut configuration, the user can set how the archived emails will be marked. They will be marked with the category specified under option **Add category**.

Shortcut configuration ✕

Name:

Description:

Type:
 Normal shortcut
 HTML shortcut
 Journal shortcut
 Keep original

Use html template:

Keep formatted body:

Please verify that you have selected an HTML template which supports the keep formatted body option!

Change message class:

Truncate body:

(Number of characters)

Remove attachments:

Keep inline attachments:

Attachment placeholder name:

Add category:

Screenshot: Configuring a new HTML shortcut



Search Dominik (Ctrl+E)

Arrange By: Date | Newest on top

Today

Microsoft pictures 8:03 PM

Older

- 8/28/2018
- 8/28/2018
- 8/28/2018
- 8/28/2018
- 8/28/2018
- 8/28/2018
- Administrator 7/6/2018
contentACCESS license error
- Administrator 4/10/2018
contentACCESS license warning

Microsoft pictures

Green category

Sent: Wed 10/31/2018 8:03 PM
To: [redacted]

Message Attachments_were_removed (147 B)

This item was archived
[View original email](#) [View as eml](#)

Attachments:

microsoft-building.jpg	36 KB
microsoft-e1452011064246.jpg	230 KB
microsoft-european-union.jpg	70 KB
microsoft-office-365-logo-100630074-primary.idge -300x200.jpg	9 KB
microsoft-office-365-logo-100684405-large.jpg	21 KB
Microsoft-OneDrive-logo-official-1-696x385.jpg	13 KB
ms-office.jpg	21 KB
office-101-badge.png	4 KB
office-365-1024x640.jpg	27 KB

Hello!

I am sending the Microsoft pictures for the social media posts, as you requested. If you need any additional pictures, please let me know immediately!

Best regards
Monika

Screenshot: Email replaced by the HTML formatted shortcut in the user's mailbox



Microsoft logo

Green category

Sent: Wed 4/3/2019 3:50 PM
To: [redacted]

This item was archived
[View original email](#) [View as eml](#)

Attachments:

[image001.jpg](#) 8 KB

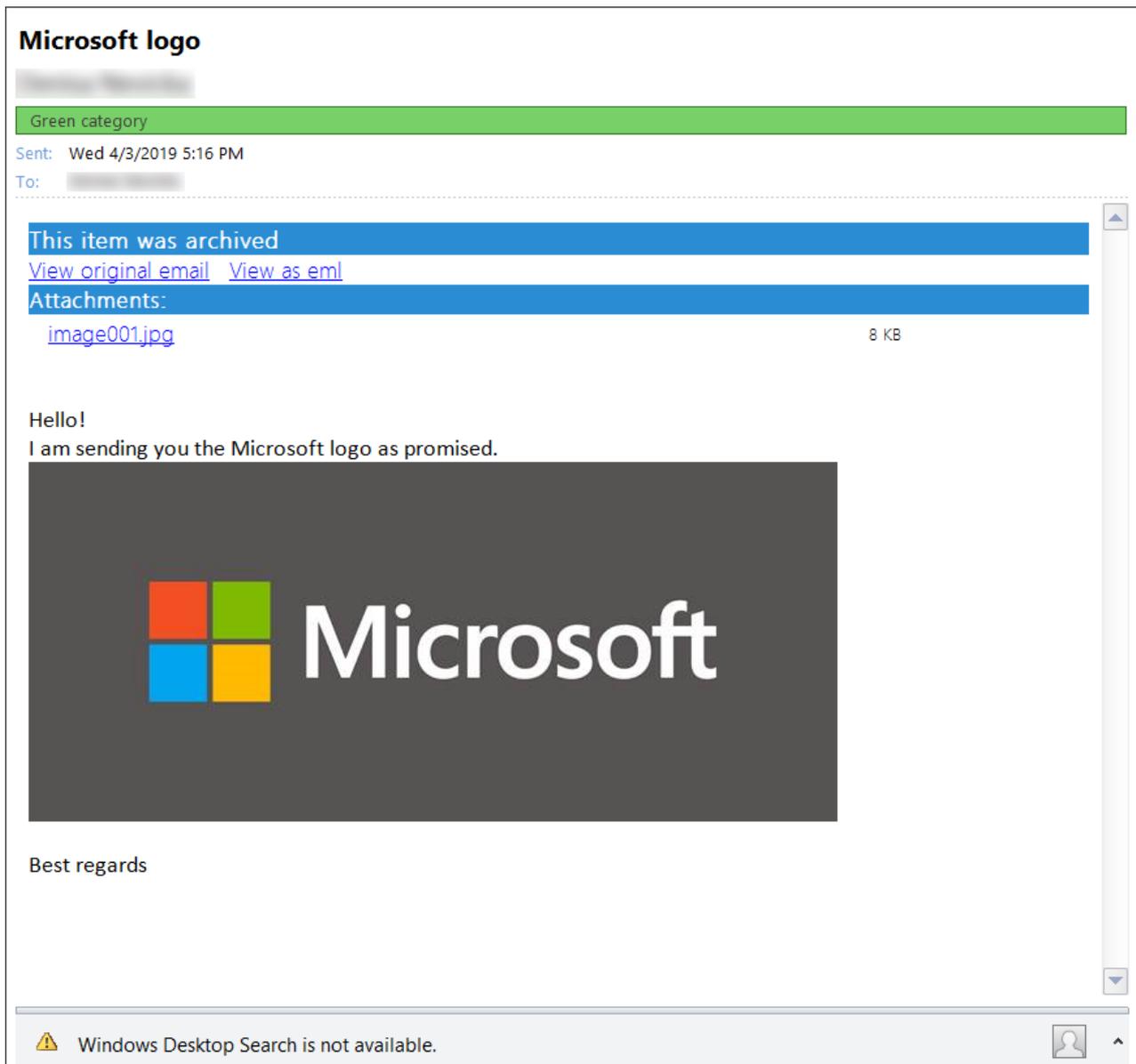
Hello!
I am sending you the Microsoft logo as promised.

 The linked image cannot be displayed. The file may have been moved, renamed, or deleted. Verify that the link points to the correct file and location.

Best regards

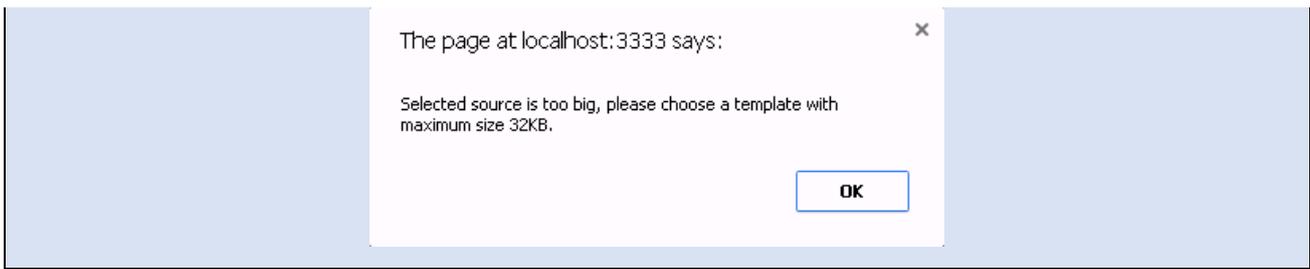
 Windows Desktop Search is not available.

Screenshot: Email archived with Keep inline attachments **unchecked**

Screenshot: Email archived with Keep inline attachments **checked**

After filling all required data in the **Shortcut configuration** window, click **OK**.

Note: Always keep in mind that the size of a HTML-template cannot exceed **32 kB**. If the template is edited with MS WORD, then numbers of redundant informations will be included in the template, which might easily cause the filesize to exceed the maximum. For this reason, it is not recommended to use MS WORD for editing the HTML-templates. If you got a Warning such as this one below, then delete the template and try to edit a new default one with an alternative HTML-editor.

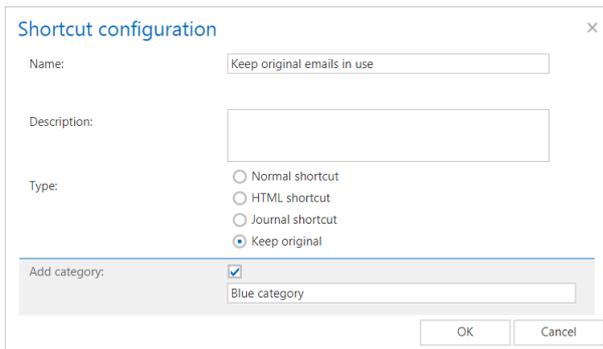


Journal shortcut

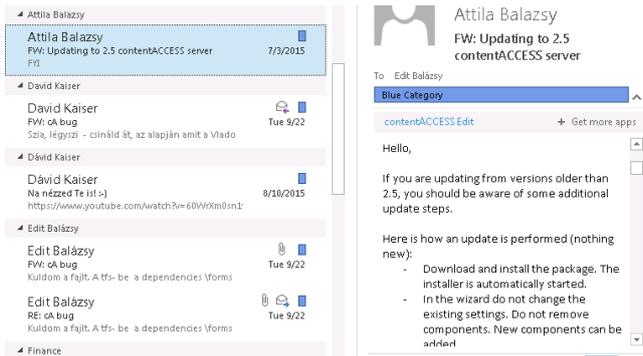
By using this option, the original message will be automatically deleted from the original location. The **Delete original** checkbox is inactive and selected here by default. This processing type is commonly used when archiving mailbox(es), which won't be used in the future (e.g. if the mailbox user/employee leaves the company), or the mailbox items are older than 2 years. It is commonly used for archiving Exchange server journal mailboxes as well.

Keep original method

By using this option, the original document will be kept in the original location/folder. It is recommended to select this processing type for archiving emails younger than 1 year. By checking the **Add category** checkbox and specifying a custom category, the user may set up a custom category for the archived email message (e.g. if the “Blue category” is set as on the screenshot B below, then email will be marked with this color).



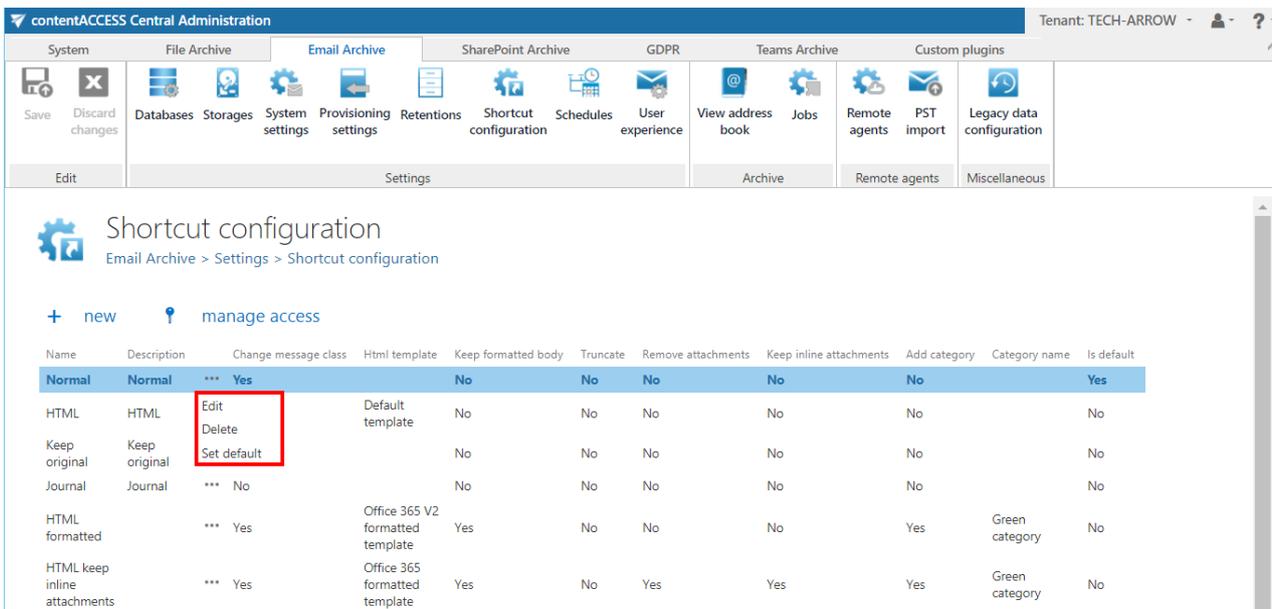
Screenshot A:
Keep original method used for archiving 2+ year old emails



Screenshot B:
Untouched originals marked with blue

Editing of shortcuts

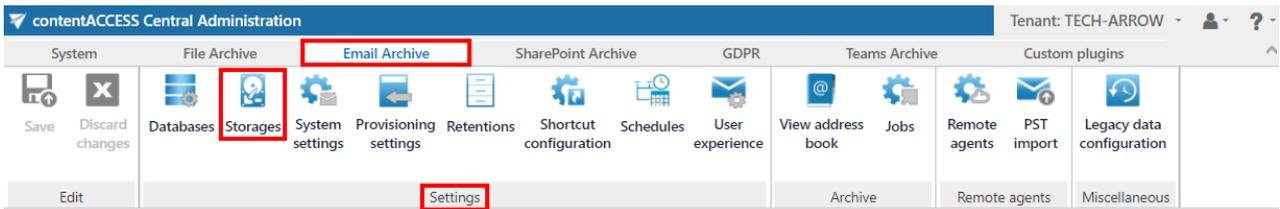
Select the shortcut, which you would like to modify, from the grid and open its context menu.



To modify shortcut settings, click on **Edit** and change the settings in the **Shortcut configuration** dialog, so that the shortcut contains the information that you require. You can also set the selected shortcut as default from the shortcut's context menu. This is a must-to setting if you want to archive/restore the emails manually using the Mail app or OWA integration (more information [here](#)).

Storing of archived emails

Navigate to **Email Archive** → **Settings** → **Storages**. The grid of already configured email archive storages can be found on this page. Here you can set up a new storage, where the binaries will be stored during the archiving process. For further information on how to set new storages check section "**Storages**" above.



Storages

Email Archive > Settings > Storages

+ new manage access

Storage Name	Storage Type	Is default
AzureStore	Store.Azure	Yes
AzureStore TEA	Store.Azure	No

LoboDMS storage

The LoboDMS storage is used only by the Email archive plugin. The storage can be configured in Email archive → Settings → Storages. Click on **+new**. The **Storage repository** window will open. Enter the following:

Storage repository

Storage settings

Store name:

Store type:

LoboDMS server: :// :

Username:

Password:

Repository:

Document type:

Attachment type:

✔ Connection successful!



- **Store name** - A display name for the store.
- **Store type** - Select LoboDMS – it should be available if your license is valid.
- **LoboDMS server** - Server where LoboDMS is installed - [Protocol://ServerName:Port](#)
- **Username** - The name of the user who has access to LoboDMS.
- **Password** - Password provided for the user mentioned above.
- **Repository** - LoboDMS instance can contain more repositories. The repository where the system will archive emails has to be provided here.
- **Document type** - The name of the type defined in LoboDMS, where the metadata of the mail will be archived. The types are defined like this:
- **Attachment type** – The name of the type defined in LoboDMS, where the binaries will be archived.

Click on the Test button to check if your connection with the LoboDMS works. If a green table appears, then everything should be working fine. Save your settings.

Creating email archive schedulers

Navigate to **Email Archive** → **Settings** → **Schedules**:

The screenshot shows the 'contentACCESS Central Administration' interface. The 'Email Archive' tab is selected in the top navigation bar. Below it, the 'Schedules' sub-tab is highlighted. The main content area displays the 'Schedules' page with a breadcrumb 'Email Archive > Settings > Schedules'. There are two buttons: '+ new' and 'manage access'. Below these is a table of existing schedulers:

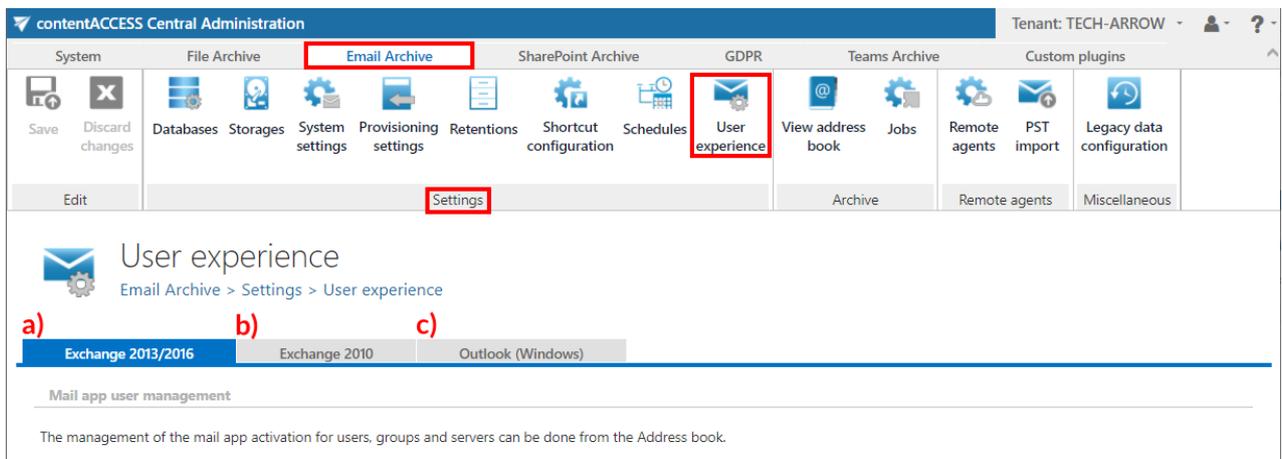
Name	Type	Description
Every 2 minutes	*** AlwaysRun	Always running in every X minutes
Every hour	*** AlwaysRun	Always running in every X minutes
Manually	*** OneTime	Running on 4/2/2017 12:00:00 AM
TaskRunnerScheduler	*** AlwaysRun	Always running in every X minutes

The already configured schedulers for automatized email archiving are listed on this page in the scheduler's grid. By clicking on the **+ new** option, it is possible to create a new scheduler. (For more information about how to set schedulers refer to the section "[Schedules](#)" above.)

User experience

contentACCESS Email Archive may archive the emails either from Exchange 2010 or Exchange 2013 or higher. The exact Exchange version, which is configured on the Email Archive's **System settings** page under section **EWS settings**, is used. The items archived and replaced with shortcuts can be accessed both from MS Outlook desktop version and OWA if the right extensions (*OWA 2010 integration* for OWA 2010 and *Mail app* for OWA 2013 (or higher) or MS Outlook desktop version 2013 or higher) are installed. Items archived with Metalogix Archive Manager Exchange Edition (MAM EE) and Email Lifecycle Manager (ELM) can be retrieved as well. To retrieve MAM EE and ELM shortcuts, the given legacy retrieve service must be also installed and configured in contentACCESS. (Read more in [Legacy email archive connectors](#).)

OWA 2010 integration, Mail app and office GATE can be installed on the **User experience** page of the Central Administration. Open the **User experience** page by navigating to **Email Archive** → **Settings** → **User experience** on the ribbon.



The screenshot shows the contentACCESS Central Administration interface. The ribbon is set to 'Email Archive', and the 'Settings' group is selected. The 'User experience' option is highlighted. Below the ribbon, the 'User experience' page is displayed, showing the breadcrumb 'Email Archive > Settings > User experience'. Three tabs are visible: 'Exchange 2013/2016' (labeled 'a)'), 'Exchange 2010' (labeled 'b)'), and 'Outlook (Windows)' (labeled 'c)'). The 'Exchange 2013/2016' tab is currently selected.

There are 3 tabs that can be opened from this page:

- a) **Exchange 2013/2016** - If this version is used, you may **use Mail app** with OWA 2013 or higher and MS Outlook desktop version (2013 or higher) directly. This allows manual archiving of mailbox items/manual restoring of shortcuts directly from the mailbox. Emails and attachments archived with MAM EE and ELM can be opened from the legacy shortcuts as well if the legacy retrieve service is installed and configured. (Read more in [Legacy email archive connectors](#).)
- b) **Exchange 2010** – If this version is used, you may integrate contentACCESS **with OWA 2010** and allow transparent opening of the shortcuts in OWA. The extension allows manual archiving of mailbox



items/manual restoring of contentACCESS shortcuts directly from the mailbox. Emails and attachments archived with MAM EE and ELM can be opened from the legacy shortcuts as well if the legacy retrieve service is installed and configured. (Read more in [Legacy email archive connectors.](#))

c) **Outlook (Windows)** – On this tab it is possible to **download the Forms.zip (1)** – this ZIP file includes the [Outlook forms](#) installer and pdf installation manual; and **request officeGATE for free (2)** – after clicking on this, you will be redirected to the [officeGATE](#) download request page.



Exchange 2013/2016	Exchange 2010	Outlook (Windows)
Outlook forms installer download		
Download url:		Click here to get it for free 1
officeGATE download		
officeGATE is a Microsoft Outlook add-in connecting Microsoft Outlook with local file-systems and also contentACCESS, OneDrive, SharePoint, etc. The add-in enables the user to Drag&Drop not only archived files from/to email messages directly in Microsoft Outlook, without the need to switch to other applications.		
Learn more about officeGATE here .		
Download url:		Click here to get it for free 2

For more information about these settings read the corresponding sections below:

Exchange 2013+: Mail app in OWA 2013+ or on MS Outlook 2013+ desktop version

Mail app is a simple end-user friendly contentACCESS feature, which was designed to manually archive/restore from/to mailboxes directly in MS Outlook desktop version or OWA 2013 or higher, without any need to use an email archive job.

Mail app is running on the following platforms:

- Desktop (Windows, Macintosh – on Macintosh MS Outlook 2015+ is required)
- OWA (desktop computer, android, iOS, phone, tablet)
- Native MS Outlook app on tablets

Native Outlook app on mobiles doesn't support Mail app.

Important: To read more about Mail app (installation, configuration and usage), please check [this](#) manual.

If the user wants to use Mail app, **Exchange permissions** for **OrgCustomApps** must be also granted. To read about how to grant them, please check [this](#) section.

Exchange 2010: OWA 2010 integration

With the Exchange 2010 user experience you may deploy the OWA (Outlook Web Access) support to your Exchange server. **This allows transparent opening of contentACCESS and legacy (MAM and ELM) shortcuts in OWA 2010. The mailbox items can be manually archived and the contentACCESS shortcuts can be restored directly from the mailbox too.**

The OWA integration feature requires to have:

- 1) **Proxy with HTTPS connection installed** – it can be installed on the CAS 2010 (Client Access Role) server as well. The proxy will be used by the OWA to retrieve emails from the shortcuts.
- 2) A **HTTPS alias** configured on the **System** page, under **External accessibility settings** section (more information [here](#));
- 3) A **default shortcut**, which will be used by archiving from the mailbox (more information [here](#));
- 4) A **default retention** (more information [here](#));

Installing the OWA integration on the CAS 2010 (Client Access Role) server(s).

Go to your CAS server(s). The OWA integration setup can be accessed on the **User experience** page of the Central Administration. Open this page by navigating to **Email Archive → Settings → User experience** in the contentACCESS Central Administration. If you have Exchange 2010 configured in the Email Archive's **System settings**, the right tab will be automatically preselected on this page. Use the link below to download the **contentACCESS OWA Installer** tool and start it on your CAS server(s).



Exchange 2013/2016

Exchange 2010

Outlook (Windows)

To activate Outlook Web Access 2010 integration, please follow the steps below:

- Go to your Client Access Servers (CAS)
- Download and start the **contentACCESS OWA Installer** tool on your Client Access Servers (CAS)
- Fill the OWA url - Exchange 2010 CAS must be targeted (Your current OWA url is: **https://tadc01.ta.internal/OWA**)
- Fill the contentACCESS Proxy url (Your current proxy url is: **https://tacatest.ta.internal**)
- Click the install button

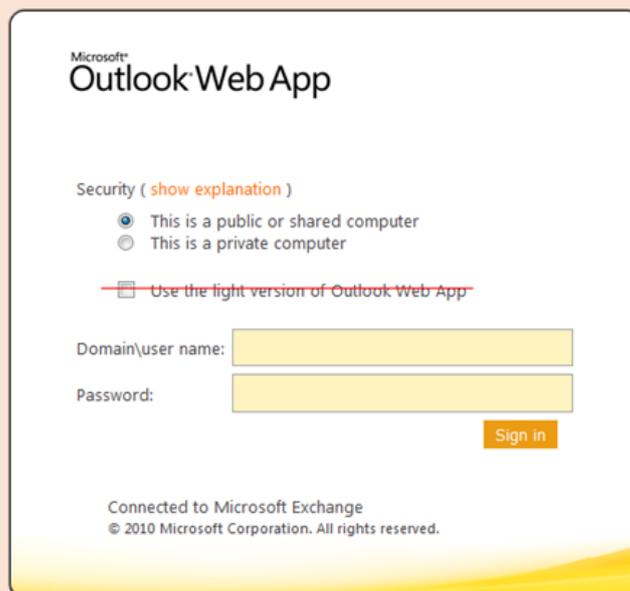
The OWA installer requires to:

- Fill the **OWA URL** (the value is prepopulated in the **OWA 2010 installer** window on the **User experience** page)
- Fill the **contentACCESS Proxy URL** (the value is prepopulated in the **OWA 2010 installer** window on the **User experience** page)
- Click the **Install** button.

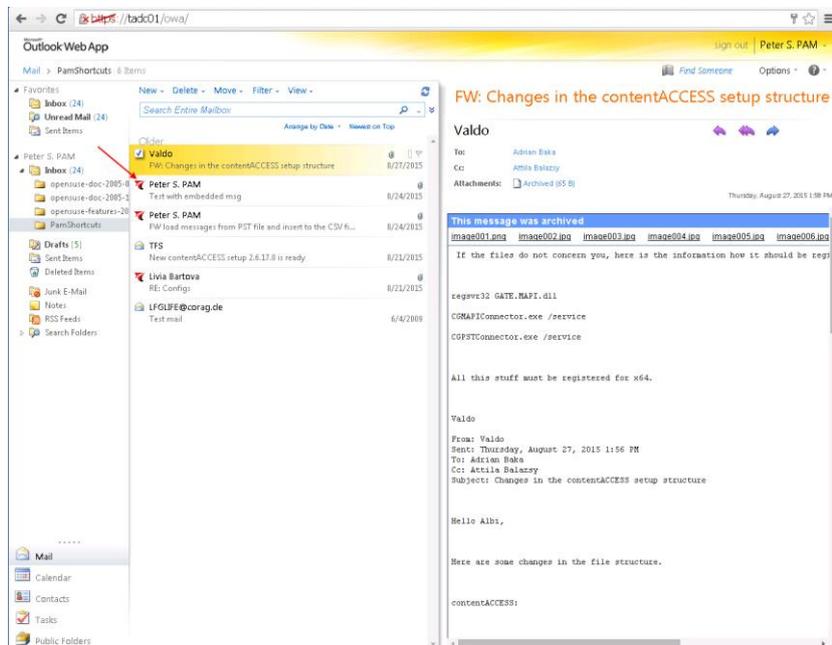


Screenshot: OWA 2010 installer (sample)

Important!!! The shortcuts in OWA 2010 do not work with the light version of OWA, so do not select this option when signing in:

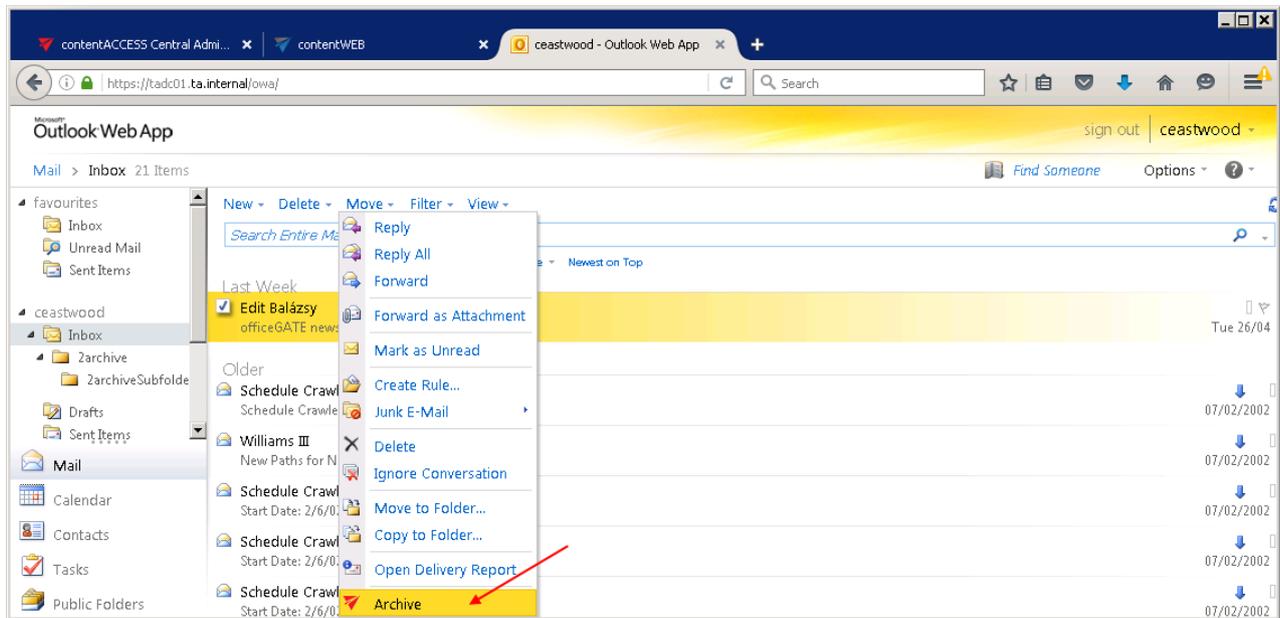


The contentACCESS icons in your mailbox will show that the OWA 2010 integration has been successfully installed on your CAS server. By uninstalling OWA 2010 support, these icons will be removed automatically. Legacy shortcuts are marked with an icon containing “L” letter, as on the screenshot below.

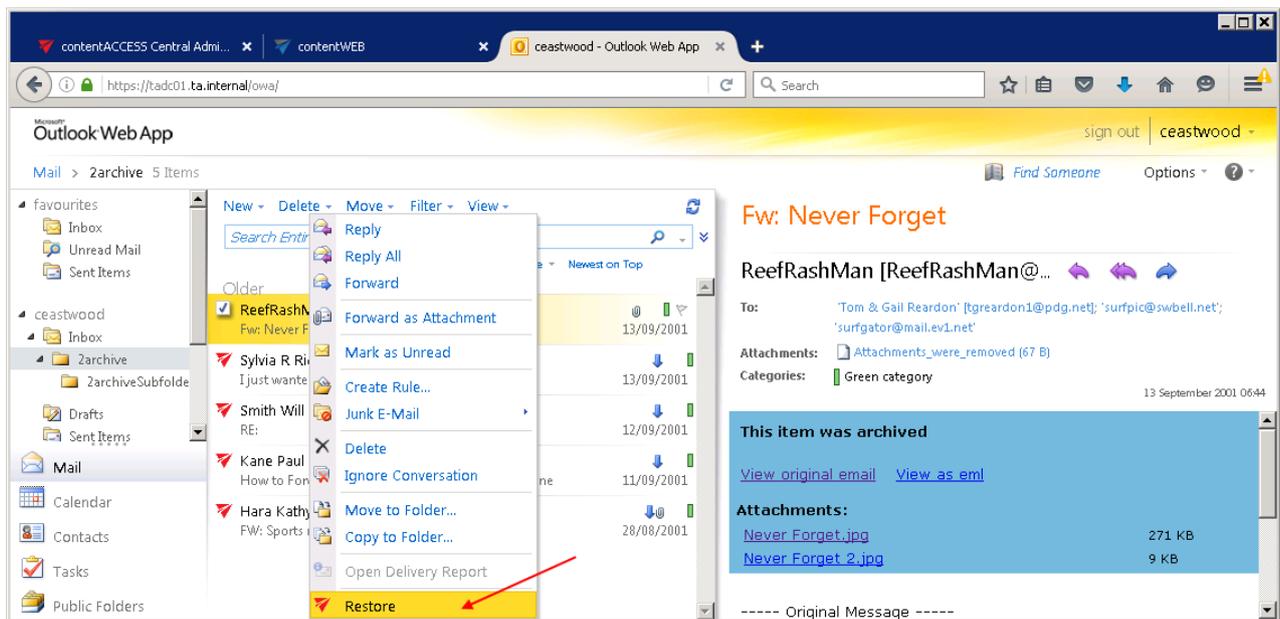


If OWA 2010 is used, the following operations are available in the contentACCESS mailbox items context menu:

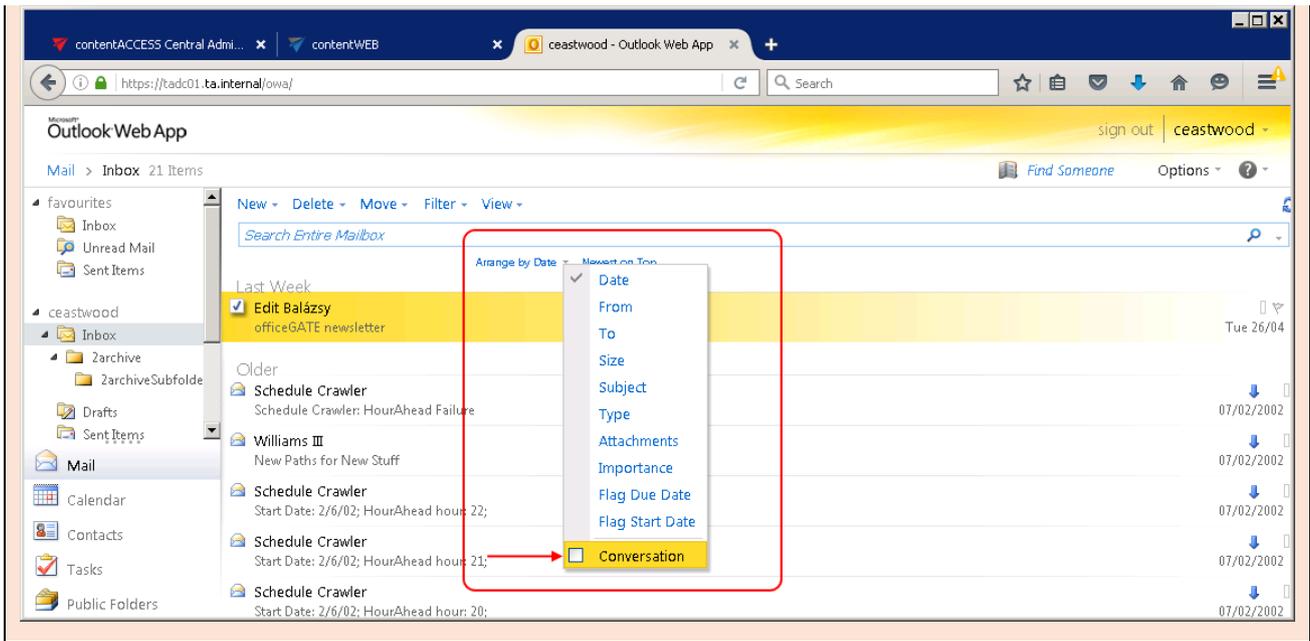
Manual archiving: Mailbox items that **have not been archived yet can be archived manually**; it is possible to archive multiple items at once;



- **Manual restoring:** Already archived emails can be restored using the email's context menu;



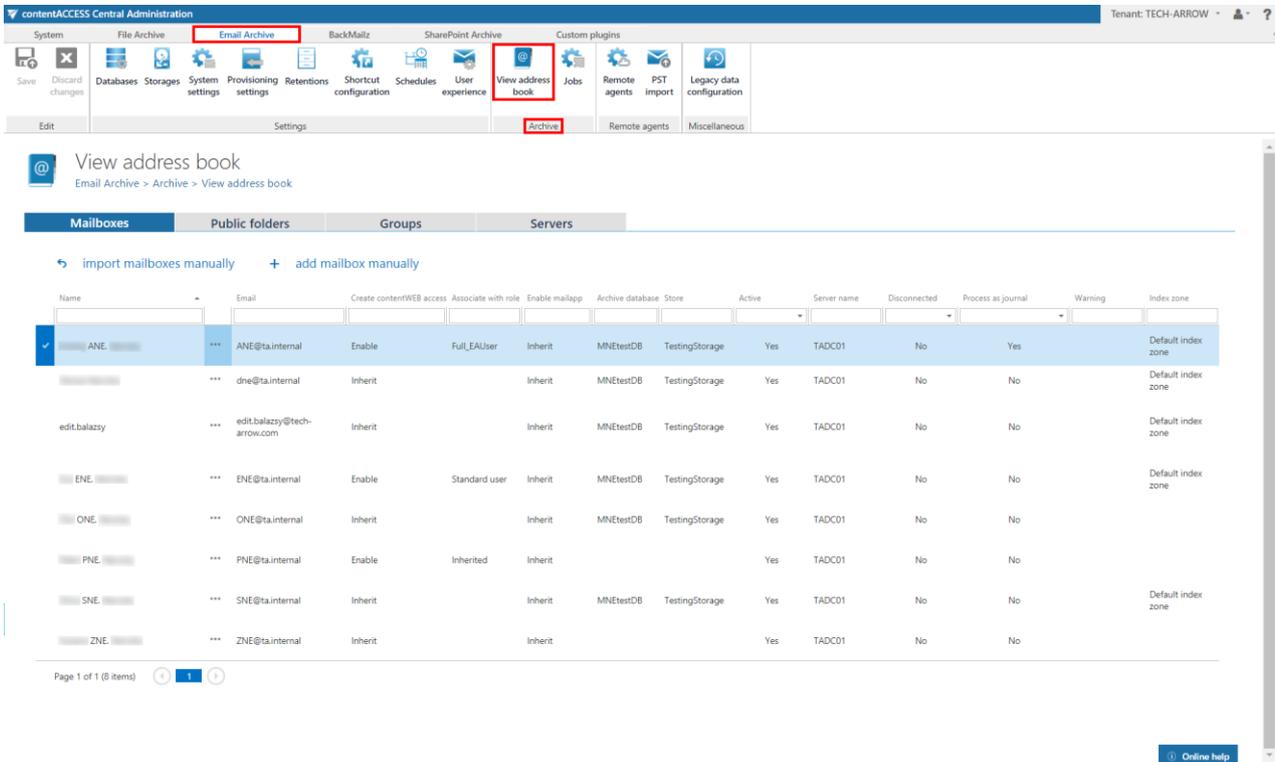
Hint: The conversation mode must be turned off, otherwise the manual archiving/manual restoring is not available in the context menu.



- In case of **contentACCESS shortcuts**: **all operations** (forward, reply, manual restoring) are available (restoring of multiple items is also supported), **except of forwarding AS attachment**;
- In case of **legacy MAM and legacy ELM shortcuts**: forwarding and replying are available, but manual restoring and forwarding AS attachments are **unavailable**.

Address book objects

Navigate to **Email Archive** → **Archive** → **View Address Book** to open the **View address book** page:



The screenshot shows the 'View address book' page in the contentACCESS Central Administration interface. The 'Email Archive' menu item is highlighted in red, and the 'View address book' option is also highlighted in red. The page displays a table of mailbox objects with columns for Name, Email, Create contentWEB access, Associate with role, Enable mailapp, Archive database, Store, Active, Server name, Disconnected, Process as journal, Warning, and Index zone.

Name	Email	Create contentWEB access	Associate with role	Enable mailapp	Archive database	Store	Active	Server name	Disconnected	Process as journal	Warning	Index zone
ANE	ANE@ta.internal	Enable	Full_EAUser	Inherit	MNEtestDB	TestingStorage	Yes	TADC01	No	Yes		Default index zone
dne	dne@ta.internal	Inherit		Inherit	MNEtestDB	TestingStorage	Yes	TADC01	No	No		Default index zone
edit.balazy	edit.balazy@tech-arrow.com	Inherit		Inherit	MNEtestDB	TestingStorage	Yes	TADC01	No	No		Default index zone
ENE	ENE@ta.internal	Enable	Standard user	Inherit	MNEtestDB	TestingStorage	Yes	TADC01	No	No		Default index zone
ONE	ONE@ta.internal	Inherit		Inherit	MNEtestDB	TestingStorage	Yes	TADC01	No	No		Default index zone
PNE	PNE@ta.internal	Enable	Inherited	Inherit			Yes	TADC01	No	No		Default index zone
SNE	SNE@ta.internal	Inherit		Inherit	MNEtestDB	TestingStorage	Yes	TADC01	No	No		Default index zone
ZNE	ZNE@ta.internal	Inherit		Inherit			Yes	TADC01	No	No		Default index zone

The address book contains a read-only list of objects that are provisioned in the address book. The objects can be added to the address book:

- by the Email Archive provisioning job – read more [here](#)
- manually – using the **import manually** (read more [here](#)) or **add manually** (read more [here](#)) options on all tabs, **except Public folders**

The address book objects are organized on the page into four tabs: **Mailboxes**, **Public folders**, **Groups** and **Servers**. Read more about public folders in [this](#) chapter.

The **Create contentWEB access** columns indicates if there is a command for the provisioning job to create contentWEB users for the selected object (mailbox, group or server). If the **Create contentWEB access** column displays **Inherit**, the object will inherit the **Create contentWEB access** option from its parent. Once a contentWEB access is granted (provisioning job must be run), every user of the provisioned object will be able to access the archived content of the mailboxes, which he is able to access also on the Exchange server.



The **Associate with role** column displays the role assigned/to be assigned for the Exchange object by the next running Email provisioning job. By default, the Exchange server mailboxes inherit the default role specified in the Email archive Provisioning settings, but the administrator can decide to assign custom roles for the objects. Such custom roles can be selected, when contentWEB user is created for the Exchange object (more information [here](#)).

View address book
Email Archive > Archive > View address book

Mailboxes												
Public folders												
Groups												
Servers												
import mailboxes manually + add mailbox manually												
Name	Email	Create contentWEB access	Associate with role	Enable mailapp	Archive database	Store	Active	Server name	Disconnected	Process as journal	Warning	Index zone
ANE	ANE@ta.internal	Enable	Full_EAUser	Inherit	MNEtestDB	TestingStorage	Yes	TADC01	No	Yes		Default index zone
	dne@ta.internal	Inherit		Inherit	MNEtestDB	TestingStorage	Yes	TADC01	No	No		Default index zone
edit.balazsy	edit.balazsy@tech-arrow.com	Inherit		Inherit	MNEtestDB	TestingStorage	Yes	TADC01	No	No		Default index zone
ENE	ENE@ta.internal	Enable	Standard user	Inherit	MNEtestDB	TestingStorage	Yes	TADC01	No	No		Default index zone
ONE	ONE@ta.internal	Inherit		Inherit	MNEtestDB	TestingStorage	Yes	TADC01	No	No		Default index zone
PNE	PNE@ta.internal	Enable	Inherited	Inherit			Yes	TADC01	No	No		Default index zone
SNE	SNE@ta.internal	Inherit		Inherit	MNEtestDB	TestingStorage	Yes	TADC01	No	No		Default index zone
ZNE	ZNE@ta.internal	Inherit		Inherit			Yes	TADC01	No	No		Default index zone

Screenshot: Columns **Create contentWEB access** and **Associate with role** in the **Mailboxes** tab

Mailboxes							Public folders							Groups							Servers						
import groups manually + add group manually																											
Name	Create contentWEB access	Enable mailapp	Associate with role	Active	Group DN																						
	Enable	Inherit	Inherited	Yes	CN=...,CN=Users,DC=ta,DC=internal																						
2	Enable	Inherit	Inherited	Yes	CN=...2,CN=Users,DC=ta,DC=internal																						
3	Enable	Inherit	Inherited	Yes	CN=...3,CN=Users,DC=ta,DC=internal																						
TECH-ARROW	Inherit	Inherit		Yes																							

Screenshot: Columns **Create contentWEB access** and **Associate with role** in the **Groups** tab

Mailboxes						Public folders						Groups						Servers					
import servers manually + add server manually																							
Name	EWS version	Create contentWEB access	Enable mail app	Associate with role	Server DN																		
TADC01	Exchange2010_SP2	Enable	Not set	Inherit	/o=First Organization/ou=Exchange																		

Screenshot: Columns **Create contentWEB access** and **Associate with role** in the **Servers** tab

Column **Enable mail app** shows, if Mail app was allowed for the respective mailbox, group or server. By default, the Exchange server mailboxes and groups inherit the Mail app access from the parent, but the administrator can decide to explicitly allow/forbid the access for the objects.

Mailboxes												
Name	Email	Create contentWEB access	Associate with role	Enable mailapp	Archive database	Store	Active	Server name	Disconnected	Process as journal	Warning	Index zone
ANE	ANE@ta.internal	Enable	Full_EAUser	Inherit	MNEtestDB	TestingStorage	Yes	TADC01	No	Yes		Default index zone
	dne@ta.internal	Inherit		Inherit	MNEtestDB	TestingStorage	Yes	TADC01	No	No		Default index zone
edit.balazy	edit.balazy@tech-arrow.com	Inherit		Inherit	MNEtestDB	TestingStorage	Yes	TADC01	No	No		Default index zone
ENE	ENE@ta.internal	Enable	Standard user	Inherit	MNEtestDB	TestingStorage	Yes	TADC01	No	No		Default index zone
ONE	ONE@ta.internal	Inherit		Inherit	MNEtestDB	TestingStorage	Yes	TADC01	No	No		
PNE	PNE@ta.internal	Enable	Inherited	Inherit			Yes	TADC01	No	No		
SNE	SNE@ta.internal	Inherit		Inherit	MNEtestDB	TestingStorage	Yes	TADC01	No	No		Default index zone
ZNE	ZNE@ta.internal	Inherit		Inherit			Yes	TADC01	No	No		

Screenshot: Column **Enable mail app** in the **Mailboxes** tab

Groups						
Name	Create contentWEB access	Enable mail app	Associate with role	Active	Group DN	
	Enable	Inherit	Inherit	Yes	CN= ,CN=Users,DC=ta,DC=internal	
2	Enable	Inherit	Inherit	Yes	CN= 2,CN=Users,DC=ta,DC=internal	
3	Enable	Inherit	Inherit	Yes	CN= 3,CN=Users,DC=ta,DC=internal	
TECH-ARROW	Inherit	Inherit		Yes		

Screenshot: Column **Enable mail app** in the **Groups** tab

Servers					
Name	EWS version	Create contentWEB access	Enable mail app	Associate with role	Server DN
TADC01	Exchange2010_SP2	Enable	Not set	Inherit	/o=First Organization/ou= /cn=Configuration/cn=Servers/cn=TADC01

Screenshot: Column **Enable mail app** in the **Servers** tab



Column **“Active”** shows, if the respective mailbox or group is active in contentACCESS. With this feature it is possible to deactivate no longer used mailboxes, keeping the licenses under control. Deactivated mailboxes/groups are neither touched by the Email archive/Email restore, Email recovery and/or by the Shortcut synchronization jobs, nor they are counted to the licensed mailboxes. To set a group or mailbox to active/inactive, the telemetry job must be run, too. It is running automatically every day or can be started manually on the **Licensing** page (**System** tab → **Services** group → **Licensing**, option **“update telemetry”**). Please note that you can't have more **active** mailboxes than the license allows. If you have already reached the limit, it won't be possible to add more mailboxes for archiving.

Mailboxes													
Public folders													
Groups													
Servers													
import mailboxes manually + add mailbox manually													
Name	Email	Create contentWEB access	Associate with role	Enable mail app	Archive database	Store	Active	Server name	Disconnected	Process as journal	Warning	Index zone	
ANE	ANE@ta.internal	Enable	Full_EAUser	Inherit	MNEtestDB	TestingStorage	Yes	TADC01	No	Yes		Default index zone	
dne	dne@ta.internal	Inherit		Inherit	MNEtestDB	TestingStorage	Yes	TADC01	No	No		Default index zone	
edit.balazy	edit.balazy@tech-arrow.com	Inherit		Inherit	MNEtestDB	TestingStorage	Yes	TADC01	No	No		Default index zone	
ENE	ENE@ta.internal	Enable	Standard user	Inherit	MNEtestDB	TestingStorage	Yes	TADC01	No	No		Default index zone	
ONE	ONE@ta.internal	Inherit		Inherit	MNEtestDB	TestingStorage	Yes	TADC01	No	No		Default index zone	
PNE	PNE@ta.internal	Enable	Inherited	Inherit			Yes	TADC01	No	No		Default index zone	
SNE	SNE@ta.internal	Inherit		Inherit	MNEtestDB	TestingStorage	Yes	TADC01	No	No		Default index zone	
ZNE	ZNE@ta.internal	Inherit		Inherit			Yes	TADC01	No	No		Default index zone	

Screenshot: Column **Active** in the **Mailboxes** tab

Mailboxes						
Public folders						
Groups						
Servers						
import groups manually + add group manually						
Name	Create contentWEB access	Enable mail app	Associate with role	Active	Group DN	
2	Enable	Inherit	Inherit	Yes	CN=2,CN=Users,DC=ta,DC=internal	
3	Enable	Inherit	Inherit	Yes	CN=3,CN=Users,DC=ta,DC=internal	
TECH-ARROW	Inherit	Inherit		Yes		

Screenshot: Column **Active** in the **Groups** tab

Mailboxes						
Public folders						
Groups						
Servers						
No data to display						



Screenshot: Column **Active** in the **Public folders** tab

Note: The mailbox is ready for archiving if it's associated with a database and storage and is set as **active**. If license allows it, the mailbox will be archived. After reaching the limit of **active** mailboxes of the license it won't be possible to archive more mailboxes.

Important: If the limit was already reached, the existing email jobs are not able to start. In order to fix the problem, it is necessary to deactivate some mailboxes until the number of **active mailboxes** drops under the number of **licensed mailboxes**, and then run the **telemetry job**.

The email archive database, storage and index zone assigned/to be assigned to the Exchange mailbox(es) are displayed in the **Archive database**, **Store** and **Index zone** columns. Database and storage is assigned automatically either by the provisioning job or by the first running archive job, or manually using the mailbox context menu. Index zone can be assigned by the provisioning job or archive job, not manually.

View address book
Email Archive > Archive > View address book

Mailboxes													
Public folders													
Groups													
Servers													
import mailboxes manually + add mailbox manually													
Name	Email	Create content	WEB access	Associate with role	Enable mailapp	Archive database	Store	Active	Server name	Disconnected	Process as journal	Warning	Index zone
ANE	ANE@ta.internal	Enable		Full_EAUUser	Inherit	MNEtestDB	TestingStorage	Yes	TADC01	No	Yes		Default index zone
	dne@ta.internal	Inherit			Inherit	MNEtestDB	TestingStorage	Yes	TADC01	No	No		Default index zone
edit.balazsy	edit.balazsy@tech-arrow.com	Inherit			Inherit	MNEtestDB	TestingStorage	Yes	TADC01	No	No		Default index zone
ENE	ENE@ta.internal	Enable		Standard user	Inherit	MNEtestDB	TestingStorage	Yes	TADC01	No	No		Default index zone
ONE	ONE@ta.internal	Inherit			Inherit	MNEtestDB	TestingStorage	Yes	TADC01	No	No		Default index zone
PNE	PNE@ta.internal	Enable		Inherited	Inherit	MNEtestDB	TestingStorage	Yes	TADC01	No	No		Default index zone
SNE	SNE@ta.internal	Inherit			Inherit	MNEtestDB	TestingStorage	Yes	TADC01	No	No		Default index zone
ZNE	ZNE@ta.internal	Inherit			Inherit	MNEtestDB	TestingStorage	Yes	TADC01	No	No		Default index zone

Screenshot: **Archive database**, **Store** and **Index zone** columns in the **Mailboxes** tab

Mailboxes												
Public folders												
Groups												
Servers												
Name	Access email					Index zone	Archive database	Store	Active	Server name		
No data to display												

Screenshot: **Archive database**, **Store** and **Index zone** columns in the **Public folders** tab

The **Process as journal** column shows if the mailbox will be processed as journal when selected in **Address books objects to process** in email archive job configuration (read more [here](#)).

Mailboxes												
Public folders												
Groups												
Servers												
import mailboxes manually + add mailbox manually												
Name	Email	Create contentWEB access	Associate with role	Enable mailapp	Archive database	Store	Active	Server name	Disconnected	Process as journal	Warning	Index zone
ANE	ANE@ta.internal	Enable	Full_EAUser	Inherit	MNEtestDB	TestingStorage	Yes	TADC01	No	Yes		Default index zone
	dne@ta.internal	Inherit		Inherit	MNEtestDB	TestingStorage	Yes	TADC01	No	No		Default index zone
edit.balazsy	edit.balazsy@tech-arrow.com	Inherit		Inherit	MNEtestDB	TestingStorage	Yes	TADC01	No	No		Default index zone
ENE	ENE@ta.internal	Enable	Standard user	Inherit	MNEtestDB	TestingStorage	Yes	TADC01	No	No		Default index zone
ONE	ONE@ta.internal	Inherit		Inherit	MNEtestDB	TestingStorage	Yes	TADC01	No	No		Default index zone
PNE	PNE@ta.internal	Enable	Inherited	Inherit			Yes	TADC01	No	No		Default index zone
SNE	SNE@ta.internal	Inherit		Inherit	MNEtestDB	TestingStorage	Yes	TADC01	No	No		Default index zone
ZNE	ZNE@ta.internal	Inherit		Inherit			Yes	TADC01	No	No		Default index zone

Page 1 of 1 (8 items)

Screenshot: Column **Process as journal** in the **Mailboxes** tab

Using the server's/group's/mailbox's context menu the administrator with the necessary permissions is allowed to

- View mailbox details
- Automatically create contentWEB user also with custom permissions (read more [here](#)) or disable the creating
- Mail app activation – read more [here](#)
- Assign database, storage and index zone for Exchange groups and mailboxes (read more [here](#))
- Activate/deactivate mailbox licenses
- Archive settings override – read more about the option below in this section
- Manage access for second users to the selected archive mailbox(es) (read more [here](#))
- Move mailbox (read more [here](#))
- Disconnect mailbox
- Change server settings (read more [here](#))
- Select the mailbox to be processed as journal/normal (read more [here](#))

Mailboxes Public folders Groups Servers

↶ import mailboxes manually + add mailbox manually

Name	Email	Distinguished	Create contentWEB access	Associate with role
ANE. [redacted]	*** ANE@ta.internal	CN= [redacted] ANE.	Enable	Full_EAUser
[redacted]	[redacted]	[redacted] CN=	[redacted]	[redacted]
edit.balazsy	[redacted]	[redacted] dc1c- 408f- - a6a19e2	Inherit	[redacted]
ENE. [redacted]	[redacted]	[redacted]	Enable	Standard user
ONE. [redacted]	[redacted]	[redacted] CN=	[redacted]	[redacted]

- Show mailbox details
- Automatically create contentWEB user
- Mail app activation
- Assign database, storage and index zone
- Deactivate mailbox license
- Archive settings override
- Manage access ...
- Move mailbox ...
- Disconnect mailbox
- Process as normal mailbox

After clicking on **Show mailbox details**, a pop-up opens. Here it is possible to see the mailbox details, archive statistics and the list of groups of the user.

Mailbox details ✕

Details
Statistics
Groups
Tools

Basic information

Mailbox name:	██████████
Email address:	██████████@tech-arrow.com
Associated user:	██████████
Server:	Office365
Distinguished name:	CN=██████████,OU=TECHARROW.onmicrosoft.com,OU=Microsoft Exchange Hosted Organizations,DC=EURPR06A002,DC=prod,DC=outlook,DC=com
Database:	██████████_database
Store:	██████████
Index zone:	Default index zone
Is disconnected:	No
Is active:	Yes
Process as journal:	No
Mailbox guid:	cf03127b-7d8f-44a0-9b11-ce723f31e6c8
Active mailbox guid:	cf03127b-7d8f-44a0-9b11-ce723f31e6c8
In-Place archive mailbox available:	Yes
In-Place archive mailbox guid:	7a3bf28c-0ce9-4003-ae50-8d632b383589

On the **Statistics** tab, it is possible to see **Folder count**, **Email count**, total **Size** of the emails, whether the mailbox has some **Imported PST files** or not and **Document count** processed by the **Indexing job**.



Mailbox details ✕

- Details
- Statistics**
- Groups
- Tools

Archive statistics

Folder count:	17
Email count:	864
Size:	157.9 MB
Has imported PST files:	No

Index statistics

Document count:	0
-----------------	---

On the **Tools** tab, it is possible to see if **Create contentWEB access** was allowed, if **Mail app activation** was allowed, if **Mail app** was already activated and details about the **Group** and **Server** that the mailbox belongs to.



Mailbox details ✕

Details
Statistics
Groups
Tools

Effective statuses

Generate contentWEB user:	Yes
Activate mail app:	Enable
Mail app activated:	No

Groups

Group name	Distinguished name	Generate contentWEB user	Enable mail app
[REDACTED]	CN=[REDACTED],CN=Users,DC=ta,DC=internal	Inherit	Inherit

Server

Name	Server DN	Generate contentWEB user	Enable mail app
TADC01	/o=First Organization/ou=Exchange Administrative Group [REDACTED]/cn=Configuration/cn=Servers/cn=TADC01	Enable	Inherit

Close

After clicking on **Show details** from a group’s context menu, a pop-up opens. On the **Details** tab, it is possible to see basic information and details of the selected group.



Group details ✕

Details
Members

Basic information

Group name:	█_subsite_█-b70f7e7bca81
Distinguished name:	CN=█_subsite_█-b70f7e7bca81,OU=TECHARROW.onmicrosoft.com,OU=Microsoft Exchange Hosted Organizations,DC=EURPR06A002,DC=prod,DC=outlook,DC=com
Create contentWEB access:	Inherit
User role:	Inherit
Enable mailApp:	Inherit
Is active:	Yes

On the **Members** tab, it is possible to see the list of the members of the currently selected group and some information about them.

Group details ✕

Details **Members**

Display name	Type	📍	Email address	Has In-Place archive mailbox
	Mailbox			Yes

You should only use the **Disconnect mailbox** option if the mailbox no longer exists and you want to re-use the email address for a new user/mailbox. By disconnecting the mailbox, the email address will be changed - allowing to use the email address for a new user.

Message from webpage ✕

Are you sure you want to disconnect the mailbox? The smtp address will be renamed and the mailbox will not be further archived.

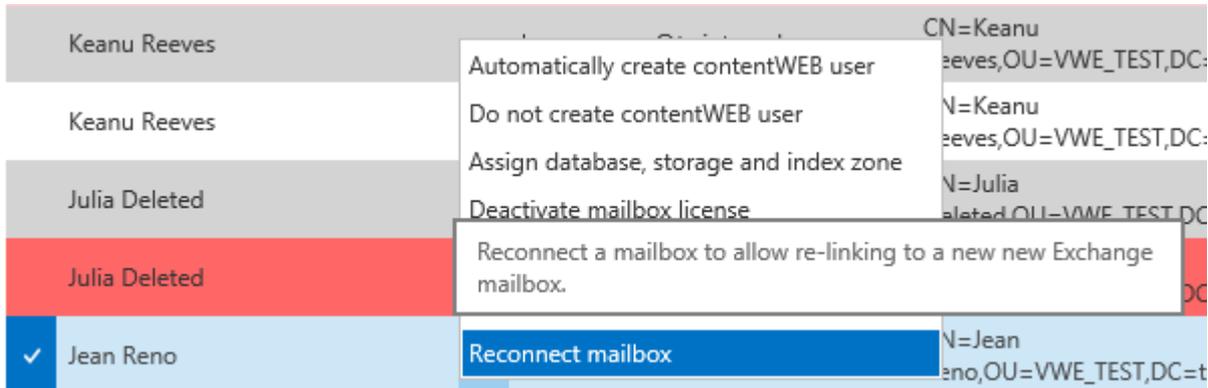
After you disconnect a mailbox, the email address is prefixed with #.

✓

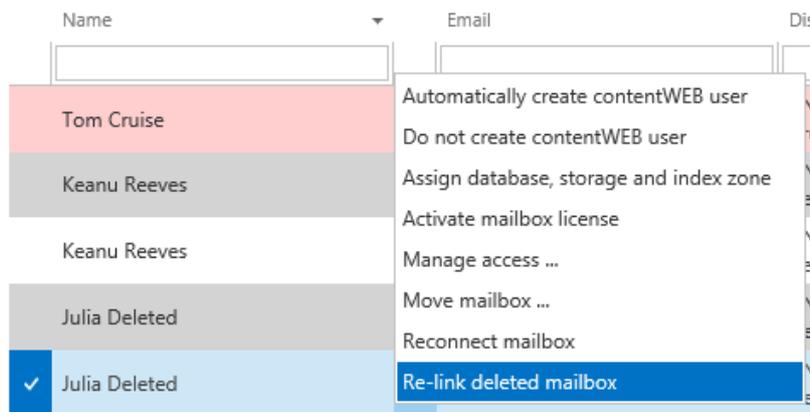
Jean Reno

#reno@ta.internal

If the mailbox was not re-used yet, you can undo the operation and **Reconnect** the mailbox.



If the mailbox is marked with the warning **Guid changed** (read at the end of this section), a new menu option (Re-link deleted mailbox) appears. By using this option it is possible to locate the new mailbox, which was created for the user.



The **search textboxes** (A) and **page listing** (B) options at the top and bottom of each section ensure an easier handling with the address book objects.



View address book

Email Archive > Archive > View address book

Mailboxes	Public folders	Groups	Servers
-----------	----------------	--------	---------

[import mailboxes manually](#) + [add mailbox manually](#)

Name	Email	Create contentWEB access	Associate with role	Enable
ane				
<input checked="" type="checkbox"/> ANE. [redacted]	*** ANE@ta.internal	Enable	Full_EAUser	Inherit

Page 1 of 1 (1 items) 1 B

It is also possible to assign specific storage, retention and shortcutting type to selected **mailboxes** and **groups** on **folder level** by clicking on the **Archive settings override** option from their context menu – these setting will be always prioritized.

Mailboxes	Public folders	Groups	Servers
-----------	----------------	--------	---------

[import groups manually](#) + [add group manually](#)

Name	Create contentWEB access	Enable mail app	Associate with role	Active	Group DN
[redacted]	*** Enable	Inherit	Inherit	Yes	CN=[redacted],CN=Users,DC=ta,DC=internal
[redacted] 2	Automatically create contentWEB user		Inherit	Yes	CN=[redacted] 2,CN=Users,DC=ta,DC=internal
[redacted] 3	Mail app activation		Inherit	Yes	CN=[redacted] 3,CN=Users,DC=ta,DC=internal
TECH-ARROW	Assign database, storage and index zone			Yes	
	Archive settings override				
	Activate/Deactivate mailboxes				

Page 1 of 1 (4 items) 1

The selected mailbox(es) will be displayed in the **Mailboxes** section. If you want to overwrite already existing settings for the mailbox(es), check the **Overwrite if already exists** checkbox. Fill in the path of the mailbox folder, select shortcut, storage and retention from the respective dropdown lists and click on **Add**. The rule will be added to the list below. Click **Save**. Once this is done, the official archiving (live mail and offline mail) will check for each item to be archived if there is a folder override for that item.

Archive settings override ✕

Apply specific settings for mailbox folders.

Mailboxes:

Overwrite if already exists

Folder path:

Shortcut:

Storage:

Retention:

Rules to override:

<input type="checkbox"/>	Folder	Shortcut	Storage	Retention
<input type="checkbox"/>	Inbox\Personal	Keep original	TestingStorage	1 year

Important: The [Shortcut repair job](#) will **NOT** take the shortcut settings from **Archive settings override**.

Change server settings

To change server settings, switch to **Servers** tab in **Address book**. Select a server and pick **Change server settings** from its context menu. In this window, it is possible to change the EWS version or specify custom EWS URL.

Server configuration ✕

EWS version:

Custom EWS Url:

Warning flags

In the Address book, the objects may be displayed with different colors:

Name	Email	Distinguished Name	Create contentWEB access	Associate with role	Archive database	Store	Active	Server name	Disconnected	Warning	Index zone
Tom Cruise	*** cruise@ta.internal	CN=Tom Cruise,OU=VWE_TEST,DC=ta,DC	No				No	TADC01	No		
Keanu Reeves	*** keanureeves@ta.internal	CN=Keanu Reeves,OU=VWE_TEST,DC=ta,DC	No				Yes	TADC01	No	Deleted	
Keanu Reeves	*** keanu@ta.internal	CN=Keanu Reeves,OU=VWE_TEST,DC=ta,DC	No				Yes	TADC01	No		
Julia Deleted	*** julia@ta.internal	CN=Julia Deleted,OU=VWE_TEST,DC=ta,DC	No				Yes	TADC01	No	SID changed	
Julia Deleted	*** #julia@ta.internal	CN=Julia Deleted,OU=VWE_TEST,DC=ta,DC	No				No	TADC01	Yes	Deleted; Guid changed	
Jean Reno	*** reno@ta.internal	CN=Jean Reno,OU=VWE_TEST,DC=ta,DC	No				Yes	TADC01	No		
Emily Blunt	*** blunt@ta.internal	CN=Emily Blunt,OU=VWE_TEST,DC=ta,DC	No				Yes	TADC01	No		

Screenshot: different warning flags on mailboxes

- the object is ok
- selected object
- the object has a warning, the warning is displayed in the **Warning** column
- the object is not active (or set to inactive at the next provisioning run), the license was removed
- the object was deleted, Guid changed – displayed in the **Warning** column

The warnings may be:

- Deleted – the object was detected as deleted
- SID changed – the owner of the mailbox was changed (the mailbox was assigned to a different Windows user)
- Guid changed – the mailbox was manually deleted and a new mailbox was created for the user

Based on the status of the object, different context menu is displayed.

Adding address book objects manually

All objects can be added in **Basic** or **Advanced** mode. The settings that must be specified are marked with *****.

Basic mode

Adding mailboxes



The basic mode is used for creating virtual mailboxes, which can be later used by the SMTP server based archiving. The advanced mode allows the user to add a mailbox, which is needed to be archived from a real Exchange server, with all of its options.

Add mailbox manually ✕

Basic mode
 Advanced mode

Mailbox options

Mailbox address *:	<input type="text" value="ane@ta.internal"/>
Server *:	<input type="text" value="TADC01"/>
Add mailboxes to group:	<input checked="" type="checkbox"/>
Group:	<input type="text" value=""/>
	Note: Please start typing the group name
Associate with storage:	<input type="text" value="TestingStorage"/>
Associate with email archive database:	<input type="text" value="MNEtestDB"/>
Associate with index zone:	<input type="text" value="Default index zone"/>

In the **Server** option the user can select an existing Exchange server from the dropdown list or he can type in any server name and a model server with that name will be created. If the **Add mailboxes to group** checkbox is unchecked, the **Group** dropdown list will be disabled.



Adding groups

Add group manually

Basic mode
 Advanced mode

Group name:

Display name:

Adding servers

Add server manually

Basic mode
 Advanced mode

Server name:

Advanced mode

Adding mailboxes

The advanced mode allows the user to add a mailbox, which needs to be archived from a real Exchange server, with all of its options.



Add mailbox manually ✕

Basic mode
 Advanced mode

Mailbox options

Mailbox GUID *:	<input type="text" value="fbf600a2-30f9-4efc-97cd-f9ec5d69c975"/>
Name *:	<input type="text" value="john.smith"/>
Display name:	<input type="text" value="John Smith"/>
SAM account name *:	<input type="text" value="SampleDomain\johnsmith"/>
User principal name *:	<input type="text" value="john.smith@sampledomain.com"/>
Mailbox address *:	<input type="text" value="john.smith@sampledomain.com"/>
Linked master account:	<input type="text" value="NT AUTHORITY\SELF"/>
Is linked:	<input type="checkbox"/>
Is mailbox enabled:	<input type="checkbox"/>
Is resource:	<input type="checkbox"/>
Is shared:	<input type="checkbox"/>
Quota:	<input type="text" value="0"/>
Use database quota defaults:	<input type="checkbox"/>
Archive GUID:	<input type="text" value="1cb94597-375d-4db7-a46c-f44965ec08c6"/>
Email addresses:	<input type="text" value="SMTP;john.smith@sampledomain.com"/>
Mailbox DN:	<input type="text" value="/o=Tech-Arrow/ou=Exchange Administrative Group"/>
Distinguished name *:	<input type="text" value="CN=testXX,CN=Users,DC=testdomain,DC=com"/>
When created:	<input style="border-bottom: none;" type="text" value="1/23/2018"/> ▼
When changed:	<input style="border-bottom: none;" type="text" value="1/23/2018"/> ▼
Associated user SID *:	<input type="text" value="S-1-2-21-1218810553-3938697923-1081931466-10"/>
Server *:	<input style="border-bottom: none;" type="text" value="TADC01"/> ▼
Add mailboxes to group:	<input type="checkbox"/>
Group:	<input style="border-bottom: none;" type="text" value=""/> ▼
	Note: Please start typing the group name
Associate with storage:	<input style="border-bottom: none;" type="text" value="TestingStorage"/> ▼
Associate with email archive database:	<input style="border-bottom: none;" type="text" value="MNEtestDB"/> ▼
Associate with index zone:	<input style="border-bottom: none;" type="text" value="Select an index zone"/> ▼
Exchange mailbox database *:	<input type="text"/>
Exchange archive database:	<input type="text"/>

Adding groups

Add group manually ✕

Basic mode
 Advanced mode

Group name:

Display name:

SID:

Distinguished name:

When created:

When changed:

Adding servers

Add server manually ✕

Basic mode
 Advanced mode

Server name:

Server distinguished name:

Settings:

The **Settings** have to be copied from the actual settings of the Office365 Exchange server.

Removing groups and mailboxes from the Address book

It is possible to remove groups and mailboxes that weren't archived before from the Address book.

Removing a mailbox

To remove a mailbox from the **Address book**, click on **Remove mailbox** from its context menu.



View address book

Email Archive > Archive > View address book

Mailboxes

Public folders

Groups

Servers

← import mailboxes manually

+ add mailbox manually

Name	Email	Distinguished	Create contentWEB access	Associate with role
ANE.	*** ANE@ta.internal	CN= ANE.	Enable	Full_EAUser
dec		dec,CN=	Inherit	
dec_test_1		dec_test	Inherit	
		,CN=	Enable	Inherit
edit.balazsy		dc1c-408f-	Inherit	
		a6a19e2		
ENE.			Enable	Standard user

- Show mailbox details
- Automatically create contentWEB user
- Mail app activation
- Assign database, storage and index zone
- Deactivate mailbox license
- Archive settings override
- Manage access ...
- Move mailbox ...
- Disconnect mailbox
- Process as normal mailbox
- Remove mailbox

The system will warn you that only mailboxes without archived data can be deleted. Click **OK**.

Are you sure you want to remove the mailbox? Only mailboxes without archived data will be deleted.

OK

Zrušit

If everything went successfully, the mailbox got removed from the **Address book**, otherwise an alert pops up.



Operation is unable to delete the mailbox

Failed to remove mailbox ANE@ta.internal. The mailbox contains archived emails.

OK

Removing a group

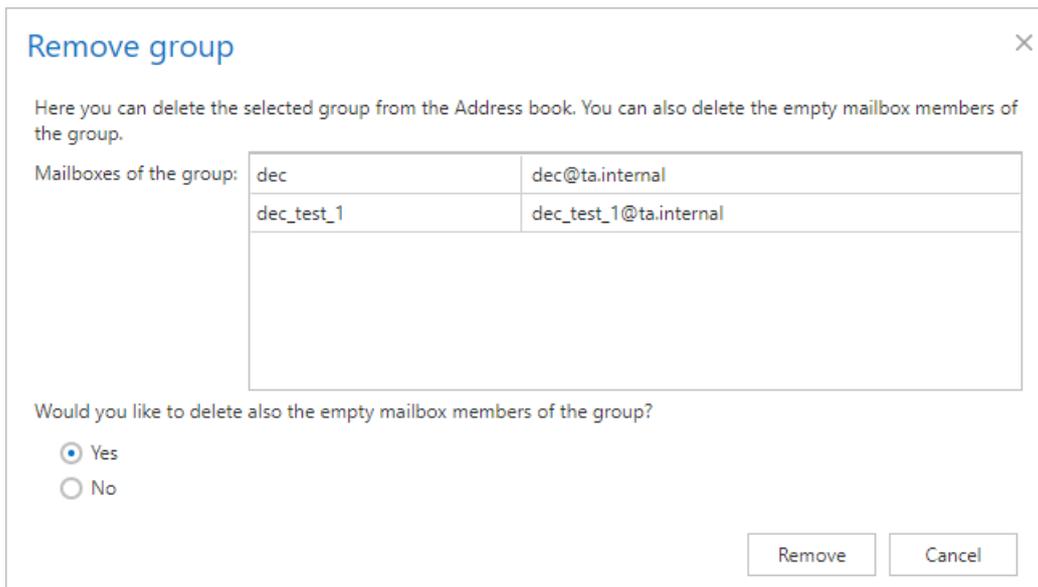
To remove a group from the **Address book**, click on **Remove group** from its context menu.

 View address book
Email Archive > Archive > View address book

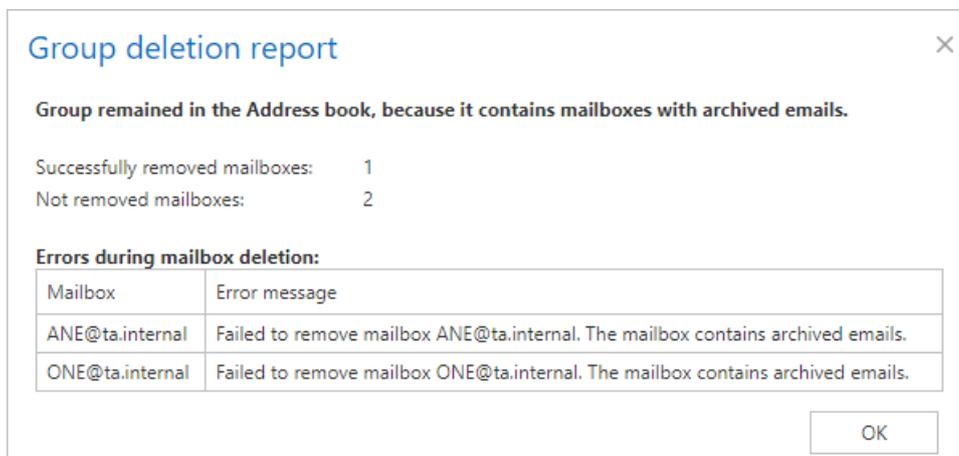
Mailboxes	Public folders	Groups	Servers	
← import groups manually		+ add group manually		
Name	Create contentWEB access	Enable mail app	Associate with role	Active
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
<input checked="" type="checkbox"/> decgroup	*** Inherit <ul style="list-style-type: none"> Automatically create contentWEB user Mail app activation Assign database, storage and index zone Archive settings override Activate/Deactivate mailboxes Remove group 	Inherit		Yes
Special	*** Inherit	Inherit		Yes

This will open a dialog with the list of the group members. You can choose whether **only the group** will be deleted from the Address book, or **also its empty mailboxes**. If you chose to delete also the mailboxes, the system will try to remove all mailboxes of the group and if everything can be deleted, the group gets deleted from the Address book as well. Click on **Remove**.

Important: The subgroups and subgroup members are **not** deleted.



If at least one of the mailboxes of the group can't be deleted, the group will remain in the **Address book** and only empty mailboxes will get deleted. A pop-up window with **Group deletion report** will appear.



Granting access rights for mailbox users and explicit users to view the mailbox archive

The archived emails can be viewed by an end user in contentWEB, which is the user interface for contentACCESS archive.

There are 2 ways how a contentWEB access can be created. The administrator can:



- 1) Create a **contentWEB user for one mailbox user or for multiple mailbox users** of the selected Exchange server/group
- 2) He can **give explicit rights to any contentACCESS user to access any archive mailbox(es)** associated with one main mailbox user on the Exchange server.

The following chapters of the guide will show you how to manage access to contentWEB using these options.

Creating contentWEB users (option 1):

The **Create contentWEB user** method should be used if the administrator would like to grant access rights **to multiple mailbox users** for their own associated mailbox archives. contentWEB users (with permissions to access the associated email archives in contentWEB) can be created on 3 levels. It is possible to:

- create contentWEB users to all mailbox users of the Exchange server - by selecting **Automatically create contentWEB user** option from the server's context menu and picking **Yes**;

Mailboxes	Public folders	Groups	Servers	
import servers manually + add server manually				
Name	EWS version	Create contentWEB access	Enable mail app	Associat
✓ TADC01	*** Exchange2010_SP2	Enable	Not set	Inherit
Page 1 of 1 (1 items) 1		Automatically create contentWEB user Not set Mail app activation Yes Change server settings No		

- create contentWEB users to mailbox users of the selected Exchange group - by selecting **Automatically create contentWEB user** option from the group's context menu and picking **Yes** or **Inherit** (if the parent has the contentWEB user creation turned on);



Mailboxes Public folders **Groups** Servers

↶ import groups manually + add group manually

Name	Create contentWEB access	Enable mail app	Associate with role	Active
TECH-ARROW	*** Enable	Inherit	Inherit	Yes
2	Automatically create contentWEB user	Inherit	Inherit	Yes
3	Mail app activation	Yes	Inherit	Yes
	Assign database, storage and index zone	No		Yes
	Archive settings override			
	Activate/Deactivate mailboxes			

Page 1 of 1 (4 items) 1

- create one contentWEB user to one selected mailbox - by selecting **Automatically create contentWEB user** option from the context menu of the selected mailbox and picking **Yes** or **Inherit** (if the parent has the contentWEB user creation turned on);

Mailboxes **Public folders** Groups Servers

↶ import mailboxes manually + add mailbox manually

Name	Email	Create contentWEB access	Associate with role	Enable r
ANE.	ANE@ta.internal	Enable	Full_EAUser	Inherit
				Inherit
edit.balazsy				Inherit
ENE.			Standard user	Inherit
ONE.				Inherit

When you allow to create a contentWEB user, the **contentWEB user role** pop-up dialog opens. Here you need to specify the contentWEB user role (containing user permissions) to be assigned to the contentWEB user. There are 2 options which role to define here:

- you can use the (default) role (e.g. with read-only permissions only) defined in the email archive provisioning job (read more in section [Email Archive Provisioning Settings](#))



- or you can assign a custom role (e.g. Standard user role with more permissions like manual recovery, preview etc.) to the user in the **Archive settings** (read more about Archive settings [here](#)) section of the **contentWEB user role** dialog.

contentWEB user role ✕

The user will be created with Windows login provider.

Use the role defined in the provisioning job
 Select a custom role you want to assign to the created user(s)

Archive settings

Mailbox owner role:

Assign to mailbox:

Database connection: ✔

Warning! Multiple databases available, and the selected one will be automatically assigned.

Storage name:

Index zone:

Create contentWEB user:

Standard user role is a system level role, it is present in contentACCESS (and therefore in the contentWEB user role dialog's dropdown list) by default. Other types of Email archive user roles must be created manually based on the steps described in section "[Roles](#)".

Important: If there are multiple roles assigned to the same Exchange object (e.g. one role with less permissions in the provisioning settings, another role with more permissions in the Address book), then the following rule applies: The role with more permissions always wins.

Now, in this use case, we will create contentWEB users with default Standard user permissions in the archive for the whole TADC01 server, but our mailbox user "ANE" will have also full rights on all archive mailboxes of TECH-ARROW tenant in contentWEB. We presume that Standard user role is selected in the email archive provisioning job.



1. First we need to create a role with “All allowed” permissions on our tenant’s email archive (read more is section “Roles”). This role will be later assigned for “ANE”.

Role details ×

Role display name:

Permissions

Plugin.Datengut

View Datengut DDCs: Not allowed All allowed ?

Plugin.EmailArchive

View mailboxes:	<input type="radio"/> Not allowed	<input checked="" type="radio"/> All allowed	<input type="radio"/> Specific allowed	?
Export:	<input type="radio"/> Not allowed	<input checked="" type="radio"/> All allowed	<input type="radio"/> Specific allowed	?
Manual archive:	<input type="radio"/> Not allowed	<input checked="" type="radio"/> All allowed	<input type="radio"/> Specific allowed	?
Manual recovery:	<input type="radio"/> Not allowed	<input checked="" type="radio"/> All allowed	<input type="radio"/> Specific allowed	?
Manual restore:	<input type="radio"/> Not allowed	<input checked="" type="radio"/> All allowed	<input type="radio"/> Specific allowed	?
Preview:	<input type="radio"/> Not allowed	<input checked="" type="radio"/> All allowed	<input type="radio"/> Specific allowed	?
View all public folders:	<input type="radio"/> Not allowed	<input checked="" type="radio"/> All allowed	<input type="radio"/> Specific allowed	?

Plugin.EPO

View EPO SAP: Not allowed All allowed ?

Select a tenant, where the role will be available

Tenant:

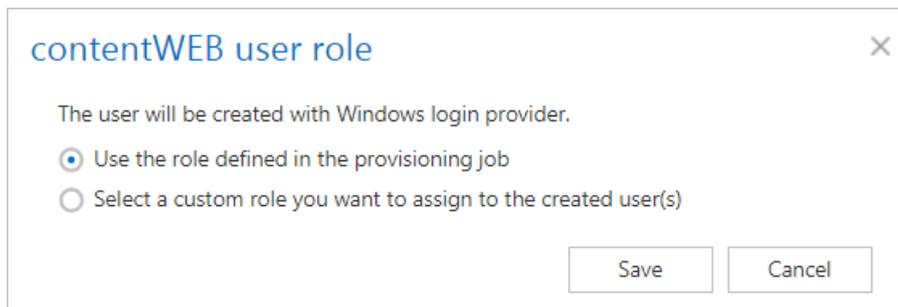
Now we go the Address book:

2. We open the server’s context menu with a click on the ellipses, choose **Automatically create contentWEB user** from the list and select **Yes**.



Mailboxes	Public folders	Groups	Servers		
import servers manually		+ add server manually			
Name	EWS version	Create contentWEB access	Enable mail app	Associate with role	
<input type="checkbox"/> TADC01	*** Exchange2010_SP2	Enable	Not set	Inherit	
Page 1 of 1 (1 items)		1			
		Automatically create contentWEB user	Not set		
		Mail app activation	Yes		
		Change server settings	No		

- The **contentWEB user role** dialog, where we select “Use the role defined in the provisioning job” option, opens. As already mentioned above, the Standard role is defined in the provisioning job.



- There will appear an “Enabled” command in the “Create contentWEB access” column, which means that contentWEB users to all mailboxes of the server will be created at next run of the provisioning job. Associate with role is “Inherit”, i.e. the (default) role defined on server level is inherited from the email archive provisioning job.

Mailboxes	Public folders	Groups	Servers		
import servers manually		+ add server manually			
Name	EWS version	Create contentWEB access	Enable mail app	Associate with role	
<input checked="" type="checkbox"/> TADC01	*** Exchange2010_SP2	Enable	Not set	Inherit	
Page 1 of 1 (1 items)		1			

- Now we search for our mailbox “ANE...” and create contentWEB user for him as well. This user will have full permissions on all archive mailboxes of the tenant. These permissions are defined in role “Full_EAUser” from the first step, so we select it in the pop-up window.



Mailboxes Public folders Groups

↶ import mailboxes manually + add mailbox manually

Name	Email	Create contentWEB
ane		
ANE.	ANE@ta.internal	Enable

Page 1 of 1 (1 items) 1

- Show mailbox details
- Automatically create contentWEB user**
 - Inherit
 - Yes**
 - No
- Mail app activation
- Assign database, storage and index zone
- Deactivate mailbox license
- Archive settings override
- Manage access ...
- Move mailbox ...
- Disconnect mailbox
- Process as normal mailbox

contentWEB user role

The user will be created with Windows login provider.

Use the role defined in the provisioning job
 Select a custom role you want to assign to the created user(s)

Archive settings

Mailbox owner role:

Assign to mailbox:

Database connection: ✔

Warning! Multiple databases available, and the selected one will be automatically assigned.

Storage name:

Index zone:

Create contentWEB user:

6. Now we start the provisioning job, which will create our contentWEB users with the assigned roles (or we wait until it begins to run according to the provisioning scheduler).



To apply the new settings, the provisioning job needs to be started. You can wait for the scheduled run or you can [start it now.](#)



View address book

Email Archive > Archive > View address book

- Mailboxes
- Public folders
- Groups
- Servers

[↶ import mailboxes manually](#) [+ add mailbox manually](#)

Name	Email	Create contentWEB access	Associate with role	Enable mail
ane				
<input checked="" type="checkbox"/> ANE. [REDACTED]	*** ANE@ta.internal	Enable	Full_EAUser	Inherit

Page 1 of 1 (1 items) 1

Provisioning job points out which mailbox user is associated with which mailbox(es) on the Exchange server and synchronizes these permissions with contentACCESS. The rights on the Exchange server will be synchronized with contentACCESS and new contentWEB users will be created for each mailbox user on the server. Each contentWEB user will have an Automatical flag. In case of O365, an Azure user login will be created; in case of on-premise Exchange server, a Windows user login will be created for each mailbox user on the server. With these accounts, the contentWEB email archive will be accessible for these mailbox users. The contentWEB user created for “ANE” will be able to access the archive mailboxes of the assigned tenant as defined in his role.



User details

System > Security > Users > User details

User details

Display name:

Tenant:

Is system admin: No

Status: Offline ●

Security information

+ Assign role

User name	Role name	Flags	Description
[redacted] ANE.	*** Standard user	Automatic (100)	[redacted] ANE. [redacted] has Standard user rights on Email archive mailbox [redacted] ANE. [redacted] [ANE@ta.internal] on tenant TECH-ARROW
[redacted] ANE.	*** Full_EAUser	Automatic (100)	[redacted] ANE. [redacted] has Full_EAUser rights on Email archive mailbox [redacted] ANE. [redacted] [ANE@ta.internal] on tenant TECH-ARROW

User logins

+ new

Login type	Login name	External id
Windows	*** TA\ANE	S-1-5-21-1454735840-2720631597-1747903052-3298

What happens if you select **No** after clicking on **Automatically create contentWEB user** in the context menu of a group/server? If it was formerly set to **Yes** and the administrator changes this setting to **No**, then the already existing contentWEB user(s) will NOT be deleted. However, if new mailbox users are added on the Exchange server, they will NOT get contentWEB access rights on the mailbox archive.

How to find Exchange groups/Exchange mailboxes with or without contentWEB users? In the Groups/Mailboxes tab, click to the **Create contentWEB access** search box and type in **Enable** to filter out all groups/mailboxes, for which contentWEB users will be/were created. If you would like to find all groups/mailboxes without contentWEB users, type in **Inherit**.

Mailboxes	Public folders	Groups	Servers		
import groups manually + add group manually					
Name	Create contentWEB access	Enable mail app	Associate with role	Active	Group DN
[redacted]	*** Enable	Inherit	Inherit	Yes	CN=[redacted],CN=Users,DC=ta,DC=internal
[redacted] 2	*** Enable	Inherit	Inherit	Yes	CN=[redacted] 2,CN=Users,DC=ta,DC=internal
[redacted] 3	*** Enable	Inherit	Inherit	Yes	CN=[redacted] 3,CN=Users,DC=ta,DC=internal
TECH-ARROW	*** Inherit	Inherit		Yes	

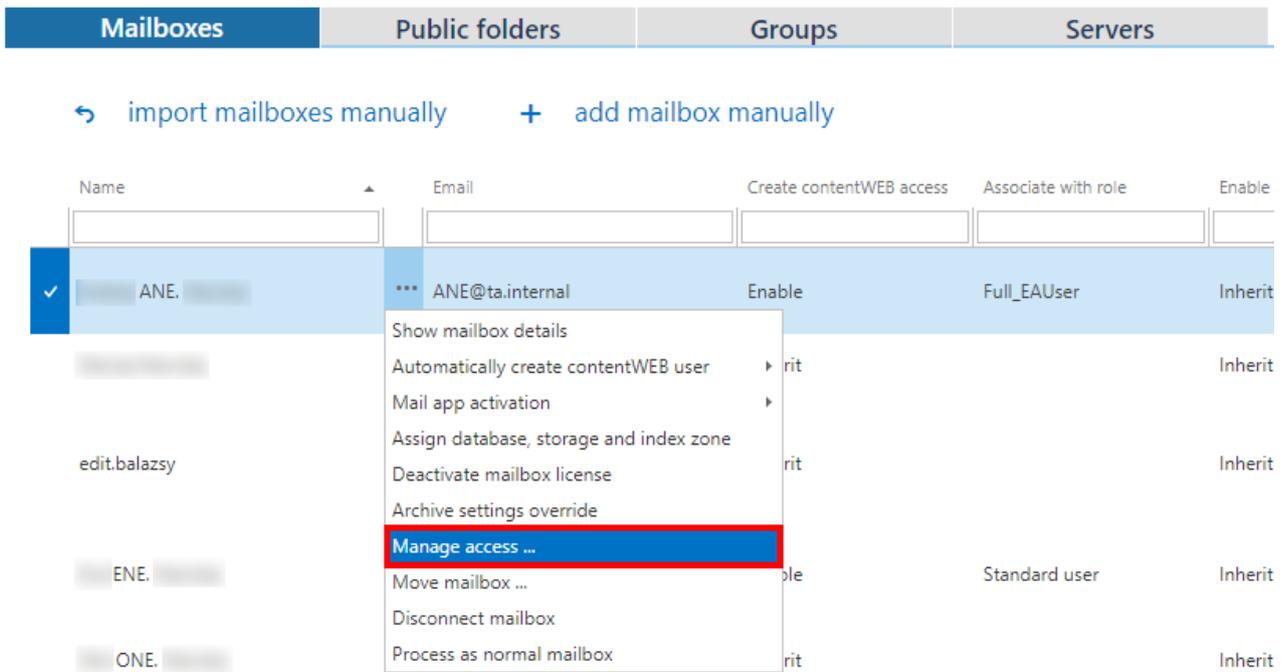
Manage access to a mailbox archive (option 2)

It can happen that the administrator is asked to grant access permissions to the mailbox archive for a second (explicit) user. An explicit user can be anybody – a user who has never used contentACCESS before and now he has to view the archived emails, a colleague who stood in for somebody else during vacation time and needs to access the archive, somebody from the company who got a claim regarding older stuff and needs to access the already archived email attachments, invoices etc. In such cases, this (second) user must get rights to the mailbox archive(s) associated with the main mailbox user.

In this use case we will show you how to grant explicit rights to the archive mailboxes associated with mailbox “ane@ta.internal” for a user. To achieve this, the administrator should follow the next steps:

Navigate to the Email Archive tab → Archive → View Address book control on the ribbon. Under **Mailboxes** tab choose the desired mailbox, click “...” (ellipsis mark) and select **Manage access** option in the context menu.

Note: This “manage access” option is available for the logged on administrator if his role assignment contains Manage tenant permission on the tenant and also View archive mailbox – All allowed rights on the tenant. Read more in [Managing access to contentACCESS objects](#).



The screenshot shows the 'Mailboxes' tab in a management console. At the top, there are navigation options: 'import mailboxes manually' and '+ add mailbox manually'. Below this is a table with columns: Name, Email, Create contentWEB access, Associate with role, and Enable. A row for a mailbox named 'ANE.' is selected, and a context menu is open over it. The menu items are: Show mailbox details, Automatically create contentWEB user, Mail app activation, Assign database, storage and index zone, Deactivate mailbox license, Archive settings override, **Manage access ...** (highlighted with a red box), Move mailbox ..., Disconnect mailbox, and Process as normal mailbox. The table row for 'ANE.' shows 'ANE@ta.internal' in the Email column, 'Enable' in the Create contentWEB access column, 'Full_EAUser' in the Associate with role column, and 'Inherit' in the Enable column.

Name	Email	Create contentWEB access	Associate with role	Enable
ANE.	ANE@ta.internal	Enable	Full_EAUser	Inherit
edit.balazsy				Inherit
ENE.			Standard user	Inherit
ONE.				Inherit

On the **Manage access** page click on **+ new**. The **Create new role association** dialog will open. Select a role (Standard user role or any explicit role created on the **Roles** page) that this user will have. Further select



the invitation type (invite new user/search for existing contentACCESS user/create new user), specify the login provider and the login credentials (if required).

Create new role association ✕

Tenant information

Role: Standard user

Invitation type: Create new

Create new user

Display name: TA archive user

Default tenant: TECH-ARROW

Login provider: Forms

Login name: Andy

Login password:

Confirm password:

OK Cancel

As this user was created manually, he got a **Manual flag**, which can be viewed on his **User details** page. It is also possible edit the user's login data, or to delete the user login. If the administrator deletes the user login, the user won't be able to log in to contentWEB with this user login anymore. These actions are accessible from the context menu of the provider, under **User logins** section.



User details

System > Security > Users > User details

User details

Display name:

Tenant:

Is system admin: No

Status: Offline ●

Security information

+ Assign role

User name	Role name	Flags	Description
TA archive user	... Standard user	Manual	TA archive user has Standard user rights on Email archive mailbox Andrej ANE. Nevicky [ANE@ta.internal] on tenant TECH-ARROW

User logins

+ new

Login type	Login name	External id
Forms	... Andy	Andy



Database and store assignment in email archiving

What is the meaning of “mailbox assigned to a database and storage”? When the provisioning job synchronizes contentACCESS with the Exchange server, it adds the mailboxes to the contentACCESS’s address book. In this moment, these mailboxes are unassigned, i.e. they do not belong to any archive – they are not archived yet. If the database and storage fields are empty, this indicates that these mailboxes have never been archived by contentACCESS. Before the email archiving process is started, a database and storage should be assigned to the mailbox. There are multiple possibilities on how to assign a mailbox:

- Go to the jobs and start the jobs (it will assign the mailboxes associated with the job to the store and database that are configured in this job);
- Navigate to **Email Archive** → **Archive** → **View address book** and manually assign the mailboxes to databases/storages.

When something is archived from the mailbox for the very first time, the first job automatically assigns the mailbox to the database and storage, which are configured in this job. From this point onward, the mailbox will belong to the database/storage and anything newly archived will go to the same database/storage. It does not matter if the job settings are changed later on: the mailbox is already assigned and will always go to the assigned database/storage, no matter how the job is configured. This might be confusing for the administrator, but contentACCESS is preventing a disaster here: the mailbox should not have a part of the data in a different database/storage. This also means that it is possible now to safely move the mailboxes between the groups without a possibility that the same mailbox will be archived into two different databases/storages. You can associate a database and a storage to Exchange groups (or to a single mailbox as well).

The administrator can see in the address book which mailbox is in which database/storage. This information can be found at the right side of the particular mailbox row.



Mailboxes		Public folders	Groups	Servers			
import mailboxes manually + add mailbox manually							
Name	Email	Create contentWEB access	Associate with role	Enable mail app	Archive database	Store	Act
ANE.	*** ANE@ta.internal	Enable	Full_EAUser	Inherit	MNEtestDB	TestingStorage	
	*** dne@ta.internal	Inherit		Inherit	MNEtestDB	TestingStorage	
edit.balazsy	*** edit.balazsy@tech-arrow.com	Inherit		Inherit	MNEtestDB	TestingStorage	

It is also possible to change this assignment as it is described below, but it is not recommended! The reasons why the reassignment of mailboxes is still allowed are the following:

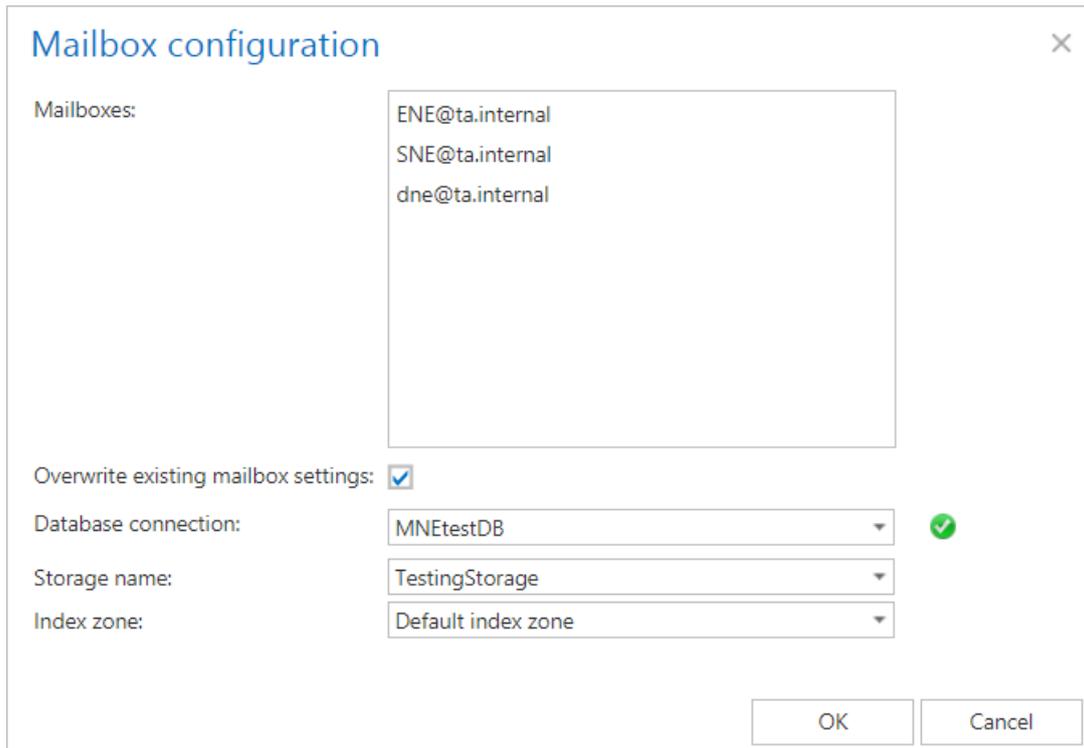
- ✓ It makes possible to manually set the unassigned mailboxes if an archiving job is not currently running.
- ✓ It is a must-have tool if you would like to select one (or just a few) mailbox(es) from a group, which will be associated with another database. In this case (before starting the archiving process), you can assign one database to the whole Exchange group and select a mailbox (or a few mailboxes) from this group and assign it to another database manually.

How to assign database, storage and index zone to an Exchange group?

Navigate to **Email Archive** → **Archive** → **View address book**, select a group, click on ... (ellipses) and then on **Assign database, storage and index zone** (Screenshot A) in the context menu. Fill the database, storage and index zone into the **Mailbox configuration** repository window (Screenshot B).

Mailboxes	Public folders	Groups	Servers	
import groups manually + add group manually				
Name	Create contentWEB access	Enable mail app	Associate with role	Active
<input checked="" type="checkbox"/>	*** Inherit	Inherit		Yes
2	Automatically create contentWEB user		Inherit	Yes
3	Mail app activation		Inherit	Yes
TECH-ARROW	Assign database, storage and index zone			Yes
Page 1 of 1 (4 items)				

Screenshot A

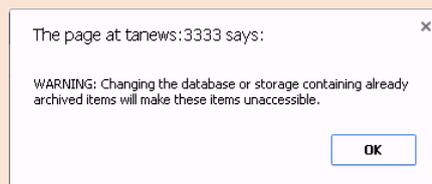


Screenshot B

Next to **Mailboxes** all mailboxes falling under this certain Exchange group can be seen.

Database, Storage, Index zone: Assign a database, storage and index zone to the mailboxes of the Exchange group.

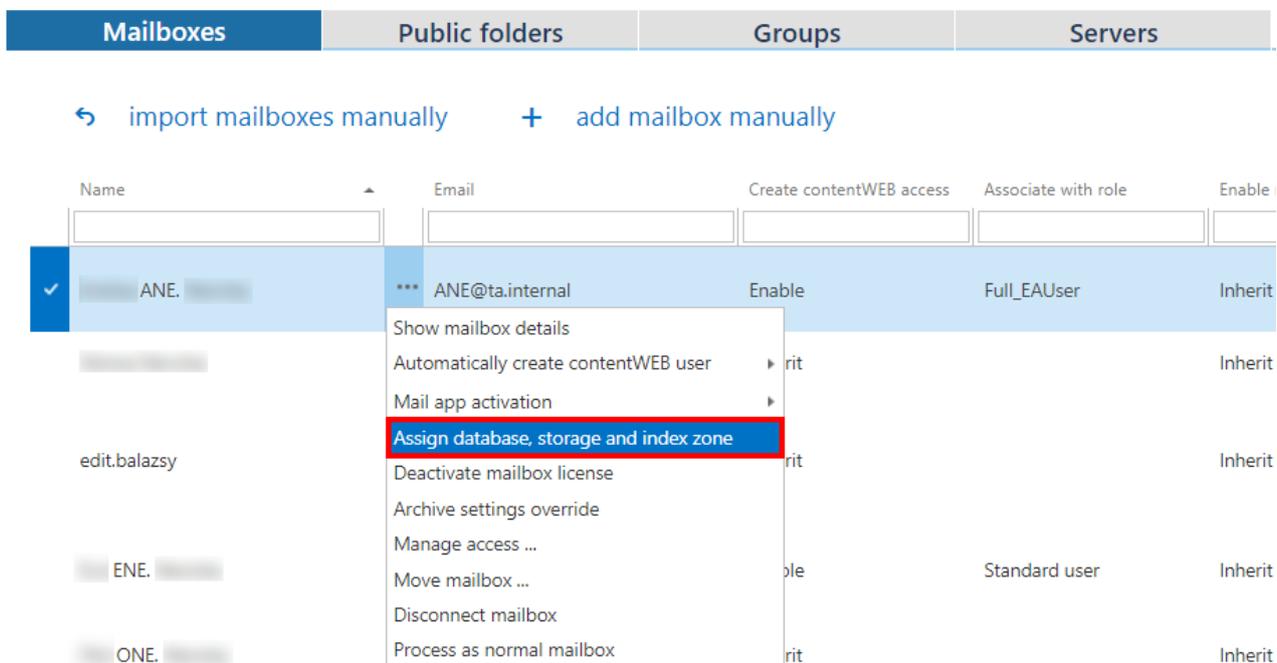
Overwrite existing settings: It is very important to keep in mind that by checking this checkbox the mailboxes (who already have their own database, storage and index zone settings) will not have an access to the items that were previously archived into another database, storage and with another index zone. A contentACCESS pop-up window (like the one below) will warn the administrator about this fact. If you leave the “Overwrite existing mailbox settings” checkbox unchecked, then the newly assigned database, storage and index zone will be assigned only to those mailboxes, which are not associated with any DB, storage and index zone.



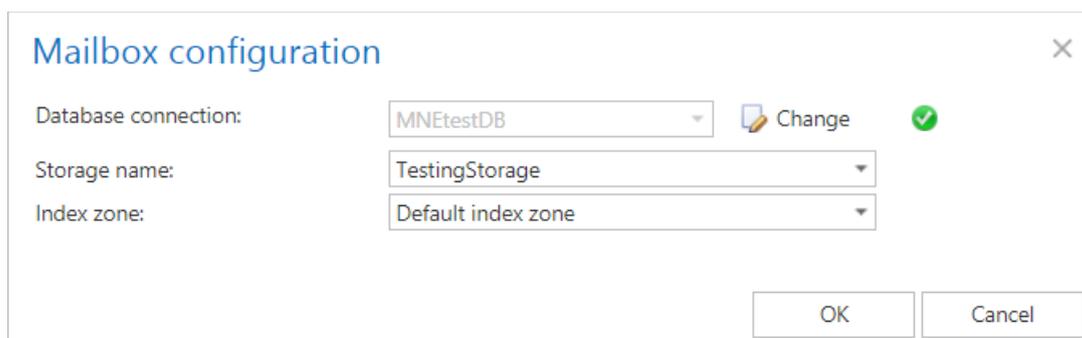
Note: If the mailbox database, storage and index zone **have not been selected manually** in the View address book, then **by the next run** of an email archive job **the database, storage and index zone will be automatically assigned to the mailbox according to the settings of this job.**

How to assign database and storage to a mailbox?

It is also possible to assign a database, storage and index zone to a single mailbox. Select a mailbox under the **Exchange mailboxes**, click on ... and select **Assign database, storage and index zone** option from the list.



Fill out the **Mailbox configuration** window (Screenshot A). If you want to edit these settings in the future, a pop-up window will warn you that changing the database containing already archived items will make these items inaccessible for the user(s) (Screenshot B).



Screenshot A



Screenshot B

The information about the assigned database, storage and index zone will be located in the columns:

Mailboxes												Public folders		Groups		Servers	
import mailboxes manually + add mailbox manually																	
Name	Email	Distinguished Name	Create content	WEB access	Associate with role	Enable mail app	Archive database	Store	Active	Server name	Disconnected	Process as journal	Warning	Index zone			
ANE	ANE@ta.internal	CN=ANE, CN=Users	Enable		Full_EAUser	Inherit	MNEtestDB	TestingStorage	Yes	TADC01	No	Yes		Default index zone			

How to move data from source database/storage into a second (target) database/storage?

The mailbox mover feature allows to move one or more mailboxes into different database and different storage. This is possible by creating a new job directly from the address book. On the **View address book** page (Email Archive → Archive → View address book), Mailboxes tab, click on the ellipses (...) of the particular mailbox containing the archive data that need to be moved, and select **Move mailbox** from the context menu.



View address book

Email Archive > Archive > View address book

- Mailboxes
- Public folders
- Groups
- Servers

↶ import mailboxes manually + add mailbox manually

Name	Email	Distinguished Name	Create contentWEB access	Associate with role	Enable mail app
ANE. [redacted]	ANE@ta.internal	CN=ANE, CN=Users, [redacted]	Enable	Full_EAUser	Inherit
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
edit.balazsy	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
ENE. [redacted]	[redacted]	[redacted]	Enable	Standard user	Inherit
ONE. [redacted]	[redacted]	[redacted]	Inherit	[redacted]	Inherit
PNE. [redacted]	[redacted]	[redacted]	Enable	Inherit	Inherit

For more information on how to set a mailbox move job, please refer to section **Mailbox move** in section [“Creating Email archive jobs: archive, restore, recovery, mailbox move”](#).

Mail app access

Important: To be able to activate Mail app via EA Provisioning job, the roles **Org Custom Apps**, **Org Marketplace Apps** and **User Options** must be assigned for the EWS user on the [Email archive System settings](#) page in section **EWS settings**.

It is possible to allow Mail app activation from Central administration. To do this, navigate to **Email archive** -> **Archive** -> **View address book**. In the column **Enable mail app** it is possible to see if the Mail app activation was allowed for the selected object. By default, **the objects inherit the Mail app activation from their parent**, so if the parent has it set to enable/forbid, so will the child.



View address book

Email Archive > Archive > View address book

Mailboxes Public folders **Groups** Servers

import groups manually + add group manually

Name	Create contentWEB access	Enable mail app	Associate with role	Active	Group DN
[selected]	*** Inherit	Inherit		Yes	CN=[selected],CN=Users,DC=ta,DC=internal
[selected]-2	*** Enable	Enable	Inherit	Yes	CN=[selected]-2,CN=Users,DC=ta,DC=internal
[selected]-3	*** Enable	Forbid	Inherit	Yes	CN=[selected]-3,CN=Users,DC=ta,DC=internal
TECH-ARROW	*** Inherit	Inherit		Yes	

Page 1 of 1 (4 items) 1

The Mail app activation can be set from the context menu of the selected object to:

- Inherit
- Explicitly allow
- Explicitly forbid.



View address book

Email Archive > Archive > View address book

Mailboxes Public folders **Groups** Servers

import groups manually + add group manually

Name	Create contentWEB access	Enable mail app	Associate with role	Active	Group DN
[selected]	*** Inherit	Inherit		Yes	CN=[selected],CN=Users,DC=ta,DC=internal
[selected]-2	*** Enable	Enable	Inherit	Yes	CN=[selected]-2,CN=Users,DC=ta,DC=internal
[selected]-3	*** Enable	Forbid	Inherit	Yes	CN=[selected]-3,CN=Users,DC=ta,DC=internal
TECH-ARROW	*** Inherit	Inherit		Yes	

Page 1 of 1 (4 items) 1

Context menu for selected item:

- Automatically create contentWEB user
- Mail app activation**
 - Inherit
 - Explicitly allow
 - Explicitly forbid
- Assign database, storage and index zone
- Archive settings override
- Activate/Deactivate mailboxes

If you selected **Explicitly allow**, the contentWEB user role pop-up will open. Here you need to specify the contentWEB user role (containing user permissions) to be assigned to the contentWEB user(s). It is possible to select a **custom role** from the dropdown list or you can use the role defined in the [Email archive Provisioning job](#).



contentWEB user role ✕

The user will be created with Windows login provider.

Use the role defined in the provisioning job
 Select a custom role you want to assign to the created user(s)

Archive settings

Mailbox owner role:

Assign to mailbox:

Database connection: ✔

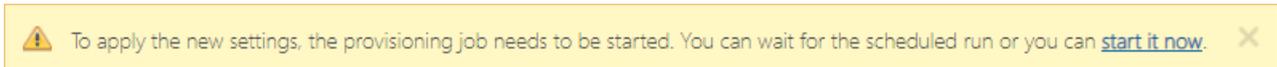
Warning! Multiple databases available, and the selected one will be automatically assigned.

Storage name:

Index zone:

Create contentWEB user:

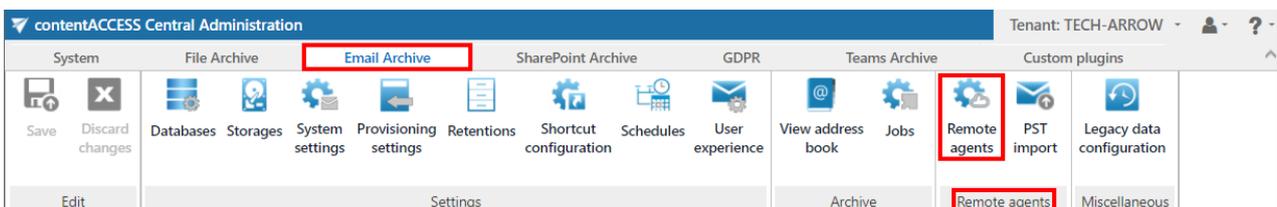
After the changes have been made, it is necessary to start the **Provisioning job** to apply them.



Remote agents (email archive)

Go to **Email Archive -> Remote agents -> Remote agents**.

The list of remotely installed agents, which are archiving files located on network shares or uploading PST files, can be found on this tab.



It is possible to download the [Remote File Archiving](#) agent (application) and contentACCESS web services (Proxy) setup or agent configuration (.XML file) [here](#).



Remote agents

Email Archive > Remote agents > Remote agents



refresh



download agent



download proxy



download agent configuration

Refresh

Refresh the list of remote agents.

Remote File Archiving agent

The Remote File Archiving agent is used to archive files that are not accessible to contentACCESS server, and thus no regular archiving job can be defined to archive them; or to upload PST files to be later used for PST import. After it was installed and configured on a computer (for more info please read the [Remote File Archiving](#) manual), the agent will appear in the agent's list and can be configured either from the Remote File Archiving client application locally or by using the contentACCESS Central Administration.

contentACCESS Proxy

The contentACCESS proxy is a web service which ensures communication between front-end applications and the contentACCESS server through secure channel (using https protocol, if configured that way). It forwards application requests to contentACCESS server and isolates the server from the outer world.

Agent configuration

Since you can download the agent configuration file from central administration, it is very easy to install remote agents with GPO.

You have to select the user and the models. The RFA will be logged in under the selected user and will support the features based on the selected models. It is possible to disable the logout option by checking the **Disable logout** checkbox. It is also possible to pick a **Database**, **Storage** and **Index zone** from the respective dropdown lists.



Agent configuration ✕

Service url:

User:

Model: File system archive
 Email archive

Disable logout:

Database: ✔

Store:

Index zone:

Remote File Archiving configuration

Note: First, the agent must be installed and registered, otherwise the list will be empty.

After clicking on the context menu of the selected agent, list of the rules, which are assigned to that agent, will appear. The RFA rule is identical to the [File archive job](#) configuration. The context menu of the agent also allows to Assign database, storage and index zone; enable/disable it or create a new rule.



Remote agents

Email Archive > Remote agents > Remote agents

[refresh](#) [download agent](#) [download proxy](#) [download agent configuration](#)

Status	Server name	Server IP	Enabled	Last ping	Database	Store	Index zone
Offline	TACATEST	192.168.190.96	Yes	1/10/2019 8:49:46 PM	MNEtestDB	TestingStorage	Default index zone
<div style="border: 1px solid #ccc; padding: 5px; margin-top: 5px;"> Assign database, store and index zone Enable Disable Create rule </div>							
12	Rule 01	RFA	Local	Yes	Finished successfully	Newly archived files: 11. Processed folders: 1.	
13	PST to cA importing	PST	Local	Yes	Finished successfully	Processed folders: 1. New PST files found: 3.	
14	PST to cA test	PST	Local	Yes	Finished successfully	Processed folders: 1.	
15	Schedule test	RFA	Local	Yes	Finished with errors		
8	PST import	PST	Global	Yes	Finished successfully	Skipped files: 10. Processed folders: 4. Uploaded PST files: 4.	
9	TECH-ARROW files	RFA	Global	Yes	Finished successfully	Processed folders: 1.	
Offline	VMDJODEV	192.168.190.104	Yes	5/25/2018 12:34:47 PM	-	-	-
Offline	TACATEST05	192.168.190.106	Yes	6/14/2018 3:32:51 PM	-	-	-

The context menu of the rule allows to edit it, configure its settings or delete it (PST rule can be only configured).



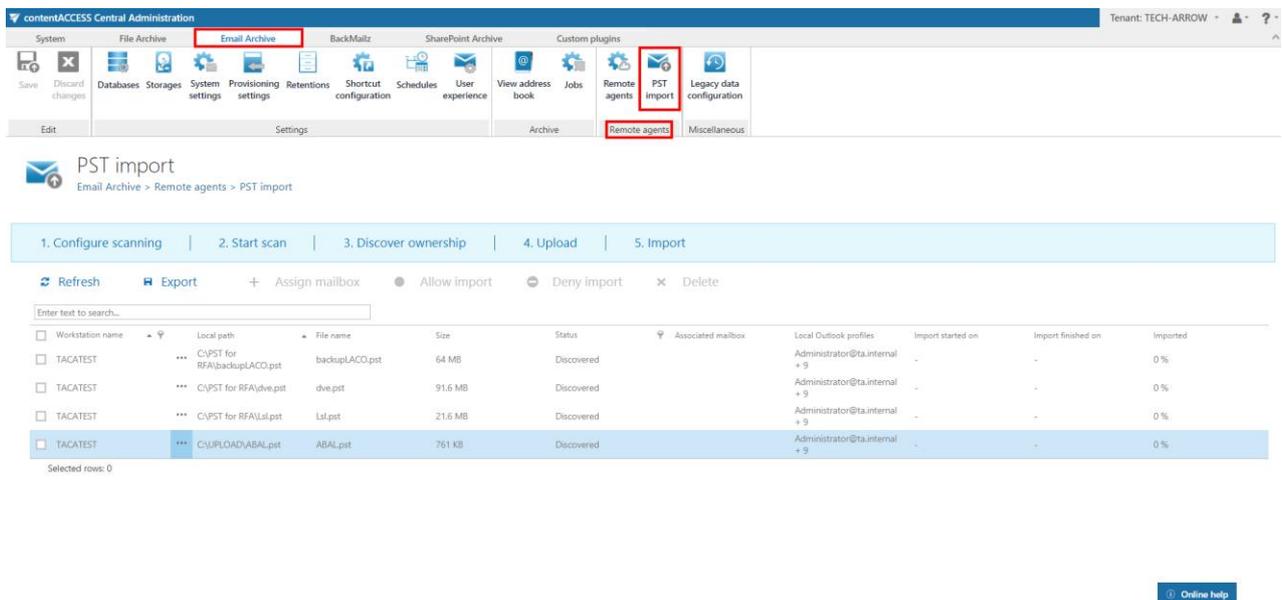
Rule ID	Name	Type	Is readonly	Enabled
1	Rule04	RFA	No	Yes
2	Archive local	Edit	No	Yes
3	Archive share	Configure	No	Yes
6	DaniTest	Delete	No	Yes
7	PST import to cA	*** PST	No	Yes
10	PST 2	*** PST	No	Yes

Note: For more information about Remote agents and Remote File archiving, please check out [this manual](#).

PST import

Go to **Email archive -> Remote agents -> PST import**.

On this page it is possible to manage the PST files that were uploaded by Remote File archiving agent (read more [here](#)). The PST files are stored in the resource storage.



To make PST files appear on this list (and be able to manage them), one of the following needs to be done as the first step:

1) Upload PST files via RFA

If the PST files are uploaded this way, they can be managed right away.

2) Use the 1. Configure scanning and 2. Start scan options

First, click on the **1. Configure scanning** button. The configuration page of the global PST import rule opens. On this page it's possible to add new folders to the rule, assign it to remote agents, disable it or view its statistics.



Assign to agents Disable rule Rule statistics

Remote locations

+ new

Path	User
C:\PST for import	*** ta\administrator
C:\PST for RFA	*** ta\administrator
C:\UPLOAD	*** ta\administrator

To add new folders to be scanned to the global PST import rule, click on **+ new**. Enter the path of the folder, where the remote agents have their PST files to be imported located. Specify explicit user credentials if necessary and click OK.

File Path ✕

File location settings

Path:

Use explicit credentials: Use explicit credentials

User name:

Password:

Confirm Password:



Click on the rule and then on **Assign to agents**. The agent selection window will open. Pick the agent(s) whom you want to assign the rule to or check the **Automatically assign to all workstations** checkbox. Click on **Select**.



Scanning configuration

Email Archive > Remote agents > Scanning configuration

Assign to agents

Disable rule

Rule statistics

Remote locations

+ new

Path	User
C:\PST for import	*** ta\administrator
C:\PST for RFA	*** ta\administrator
C:\UPLOAD	*** ta\administrator
C:\Global PST	*** ta\administrator

Agent selection ✕

Automatically assign to all workstations

Assign rule to the following workstations:

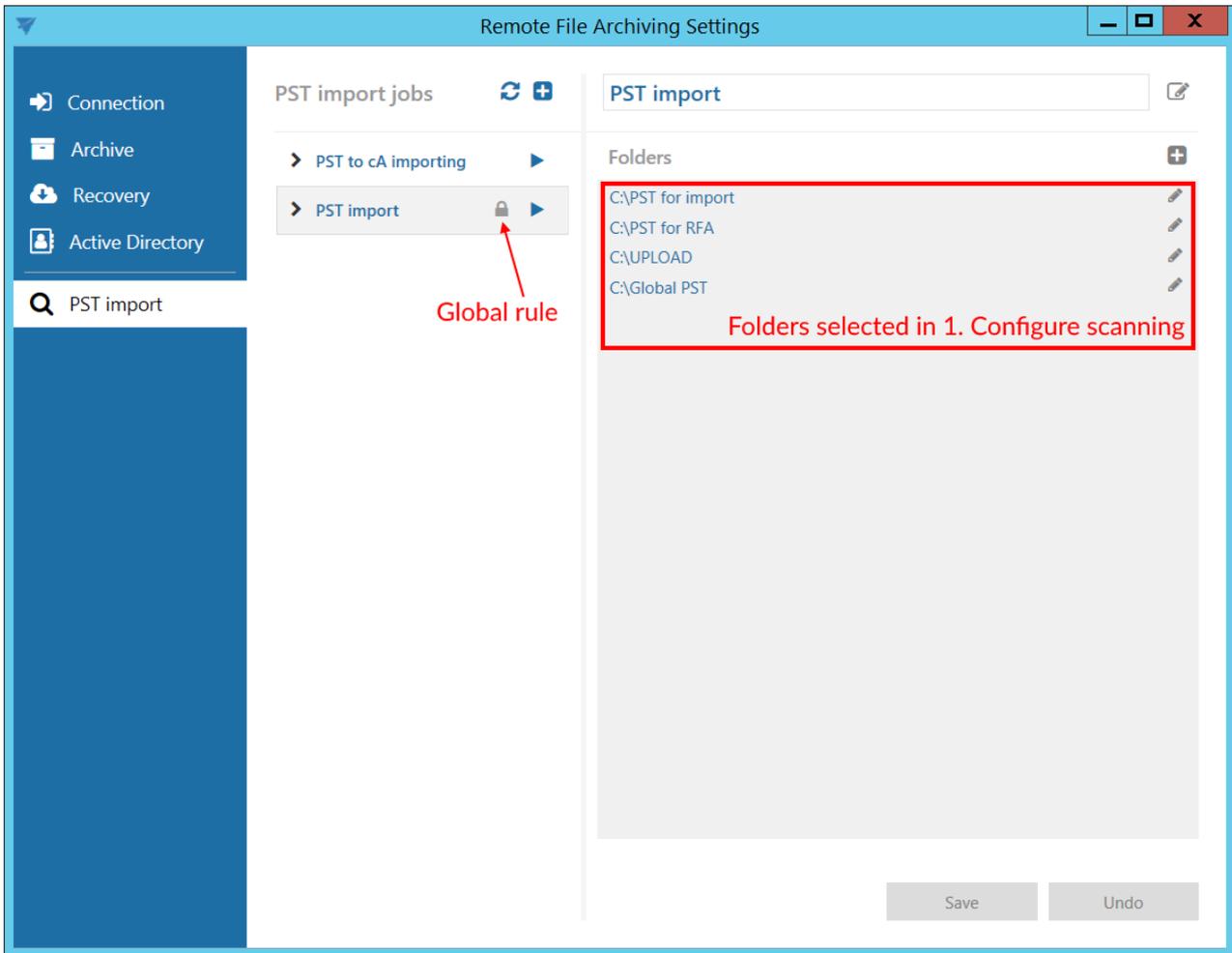
Workstation name ▲

<input checked="" type="checkbox"/>	TACATEST
<input type="checkbox"/>	TACATEST05
<input type="checkbox"/>	VMDJODEV

[refresh agents list](#)

Save your changes using the **Save** button in the upper left corner.

Go back to the **PST import** page. Click on the **2. Start scan** button. This will make the global rule appear in the list of PST import jobs for the selected remote agents.



The remote agents now have to start the job (rule). After the rule is finished, the PST files from the global rule folders will appear in the list of PST files in **PST import** tab and the administrator will be able to manage them.

PST import
Email Archive > Remote agents > PST import

1. Configure scanning | 2. Start scan | 3. Discover ownership | 4. Upload | 5. Import

Refresh Export + Assign mailbox ● Allow import ● Deny import ✕ Delete

Enter text to search...

<input type="checkbox"/>	Workstation name	Local path	File name	Size	Status	Associated mailbox	Local Outlook profiles	Import started on	Import finished on	Imported
<input type="checkbox"/>	TACATEST	*** C:\Global PST\ABAL.pst	ABAL.pst	761 KB	Discovered		Administrator@ta.internal +9	-	-	0%
<input type="checkbox"/>	TACATEST	*** C:\Global PST\..._inbox.pst	..._inbox.pst	38.3 MB	Discovered		Administrator@ta.internal +9	-	-	0%
<input type="checkbox"/>	TACATEST	*** C:\Global PST\Lsl.pst	Lsl.pst	21.6 MB	Discovered		Administrator@ta.internal +9	-	-	0%
<input type="checkbox"/>	TACATEST	*** C:\PST for import\ABAL.pst	ABAL.pst	761 KB	Discovered		Administrator@ta.internal +9	-	-	0%
<input type="checkbox"/>	TACATEST	*** C:\PST for import\apa4.pst	apa4.pst	121.4 MB	Discovered		Administrator@ta.internal +9	-	-	0%
<input type="checkbox"/>	TACATEST	*** C:\PST for import\Lsl.pst	Lsl.pst	21.6 MB	Discovered		Administrator@ta.internal +9	-	-	0%
<input type="checkbox"/>	TACATEST	*** C:\PST for RFA\ABAL.pst	ABAL.pst	761 KB	Discovered		Administrator@ta.internal +9	-	-	0%
<input type="checkbox"/>	TACATEST	*** C:\PST for RFA\backupLACO.pst	backupLACO.pst	64 MB	Discovered		Administrator@ta.internal +9	-	-	0%
<input type="checkbox"/>	TACATEST	*** C:\PST for RFA\dve.pst	dve.pst	91.6 MB	Discovered		Administrator@ta.internal +9	-	-	0%

[Online help](#)



Note: The PST files will **NOT** be uploaded to contentACCESS yet, only loaded to the list. The upload will come in a later step.

The **second step** is to match the PST files with target mailboxes. This can be done by one of the following:

1) Manually assigning the mailboxes

Select the desired PSTs by checking their checkbox on the left, then click on the **+ Assign mailbox** button (or select the option from the context menu of a file). The mailbox selection window will open. Pick one of the available mailboxes and click **Select**.



Mailbox selection ✕

refresh

#		Name	Type	Email address
<input type="checkbox"/>		ENE. [redacted]	Mailbox	ENE@ta.internal
<input type="checkbox"/>		SNE. [redacted]	Mailbox	SNE@ta.internal
<input type="checkbox"/>		[redacted]	Mailbox	dne@ta.internal
<input type="checkbox"/>		[redacted] ZNE. [redacted]	Mailbox	ZNE@ta.internal
<input checked="" type="checkbox"/>		[redacted] ANE. [redacted]	Mailbox	ANE@ta.internal
<input type="checkbox"/>		[redacted] PNE. [redacted]	Mailbox	PNE@ta.internal
<input type="checkbox"/>		[redacted] ONE. [redacted]	Mailbox	ONE@ta.internal
<input type="checkbox"/>		edit.balazsy	Mailbox	edit.balazsy@tech-arrow.com

2) Automatically assigning the target mailbox

By selecting a PST and clicking on the **3. Discover ownership** button, the system will try to match the selected PST with one of the available mailboxes based on its name.

PST import

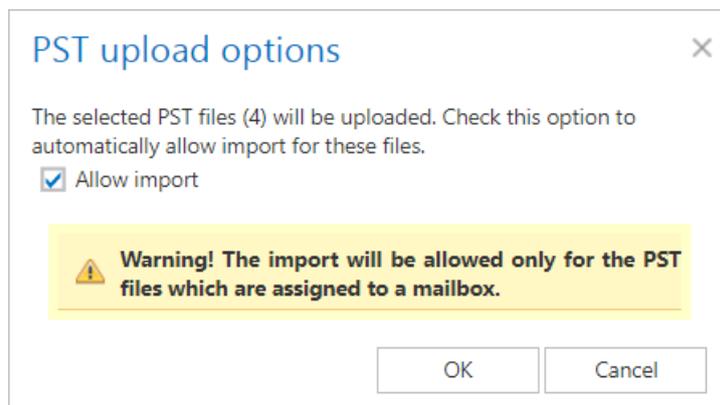
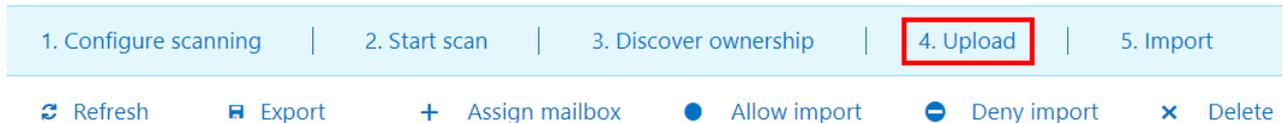
Email Archive > Remote agents > PST import

1. Configure scanning
2. Start scan
3. Discover ownership
4. Upload
5. Import

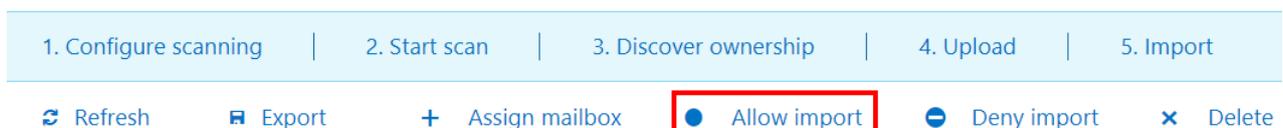
Refresh
 Export
 Assign mailbox
 Allow import
 Deny import
 Delete



The **third step** is to upload the files to contentACCESS. This can be done by using the **4. Upload** button. It is also possible to **Allow import** by checking the corresponding checkbox in this step. Click **OK**.



If the import was not allowed in the third step, it needs to be allowed in the **fourth step** by selecting the desired PST file(s) and clicking on the **Allow import** button.



The **fifth step** is to configure the PST import job. This can be done by clicking on the **5. Import** button. The job will assign [Database](#) and [Storage](#) to those mailboxes that are associated with at least one PST file and don't have a database and/or storage assigned yet. Database, storage and index zone can be assigned also from the context menu of the mailbox in [Address book](#).



PST import

Email Archive > Remote agents > PST import

1. Configure scanning

2. Start scan

3. Discover ownership

4. Upload

5. Import

Refresh

Export

Assign mailbox

Allow import

Deny import

Delete

The job configuration page opens. Here, the following has to be set:

✓ Database settings

Select an already configured connection from the dropdown list. Here the metadata will be stored. For further information on how to set database connections please refer to section [Databases](#).

Database settings

Database connection:

MNEtestDB



✓ Scheduling settings

In this step, the running time(s) of the PST import job must be selected. It is possible either to select a scheduler from the list or to create a new scheduler via **create new ...** option from the dropdown list. For more information about how to set schedulers refer to the section [Schedules](#).

Scheduling settings

Scheduled in:

Manual

✓ Storage settings

Choose an already configured storage from the dropdown list. The processed binaries will be stored here. For more information on how to set storages check section [Storages](#).

Storage settings

Storage name:

TestingStorage

✓ Retention settings

Choose an already configured retention time from the dropdown list. The processed PSTs will be stored during this time in the storage, and it will be impossible to delete them from there. It is highly recommended to select a retention time that is required by the law of your country. For more information about how to set retentions check section [Retentions](#).

Retention settings

Retention:

✓ Include folders

PST import job is crawling the entire mailbox or recursive folder structures from the PST files for further processing. Before you enter the folder name(s) to be crawled, it is necessary to select the folder filtering type. The folder filtering type is described in more details in [this](#) section.

Include folders

Folder filtering type:

- Entire PST
- One single folder
- Recursive, starting from a single folder
- Multiple folders
- Multiple recursive, starting from a single folder

✓ PST processing settings

Root folder – if you specify a folder here, emails from the root folders will be imported into the folder defined here.

Prefix - all of the PST files will be imported into a folder defined here.

PST processing settings

Root folder:

Prefix:



✓ Exclude folders

With this function, you may set which folders/subfolders should not be imported. If you would not like to exclude any folder from the process, you can skip these settings.

The folders may be excluded using one of the available methods: a) They may be **added manually** via the **+** **new** option; b) they may be **imported** in one of the available file formats via the **import** option. Folder excluding is described in more details in [this](#) section.

Exclude folders

+ new **↶** import

Pattern

%OUTBOX%

✓ Filtering settings

Click on the **Change filter** button and set the filtering according to your needs and/or regulations. To learn more about how to work with filtering settings, please, check [this](#) section of our documentation.

Filter settings
✕

visual
text

A N D ▼	Has attachment ▼	= ▼	Yes ▼	✕
	Body ▼	Contains ▼	Microsoft	✕

+add group
+add condition

+add new group

OK

Cancel

✓ Notification settings

Select here, when you will need to get notification emails from the PST import job. It is possible to set here if you need such a notification email always/never, or you need it only in case that an error/warning occurred during the importing process – for example, if the import of one or more items failed, then you may get a notification email about this error. Into the **Recipient list** textbox insert the email address(es) of the person(s), who will get such notifications. Notifications should be used if the administrator does not use the **System logs** feature.



Notification settings

Send when:

Recipient list:

✓ Resource settings

Set the value, which will determine how many items will be processed simultaneously by the PST import job. The recommended value is "2".

Resource settings

Worker thread count:

Save your changes and start the job! The PST files will now be imported to the associated mailboxes.

If the import was allowed for a PST file, but the user then decided not to import that file, it can be denied by clicking on **Deny import** button (or select the option from the context menu of a file).



PST import

Email Archive > Remote agents > PST import

1. Configure scanning | 2. Start scan | 3. Discover ownership | 4. Upload | 5. Import

Refresh Export Assign mailbox Allow import **Deny import** Delete

In case a PST file is not needed anymore, it can be deleted from the list by clicking on the **Delete** button (or select the option from the context menu of a file).



PST import

Email Archive > Remote agents > PST import

1. Configure scanning | 2. Start scan | 3. Discover ownership | 4. Upload | 5. Import

Refresh Export Assign mailbox Allow import Deny import **Delete**

It is possible to export the list of available (or just selected) PST files to **XLS** or **CSV** file.



1. Configure scanning | 2. Start scan | 3. Discover ownership | 4. Upload | 5. Import

 Refresh  Export  Assign mailbox  Allow import  Deny import  Delete

PST import job description

All the numbers and descriptions in the job's progress have a particular meaning. In this section, we are going to explain the numbers and descriptions of a **PST import job**.

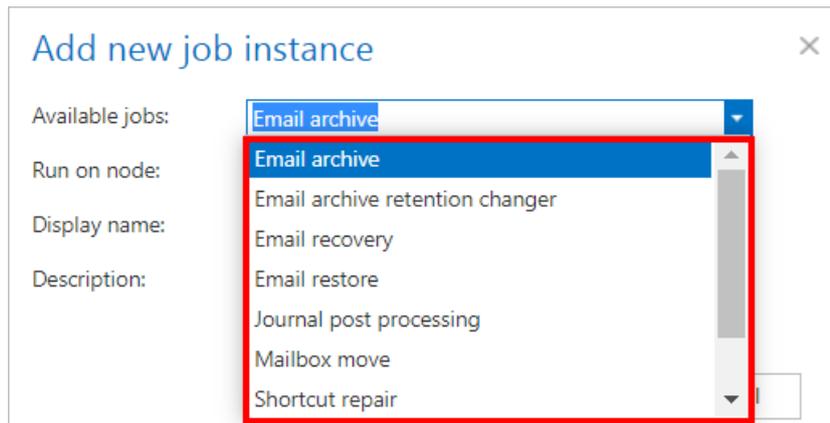
Description	Explanation
x PST files processed	x PST files were finished by the job
(y failed)	y PST files failed (out of the x PST files)
x emails imported	x emails were imported from the PST files
(x folders skipped)	x folders were skipped from the processing because of folder exclude settings
(x skipped)	x emails have been skipped because of filtering or because they were already imported
(x failed)	x emails failed to import

Creating Email archive jobs: archive, restore, recovery, delete, mailbox move, shortcut synchronization, shortcut repair

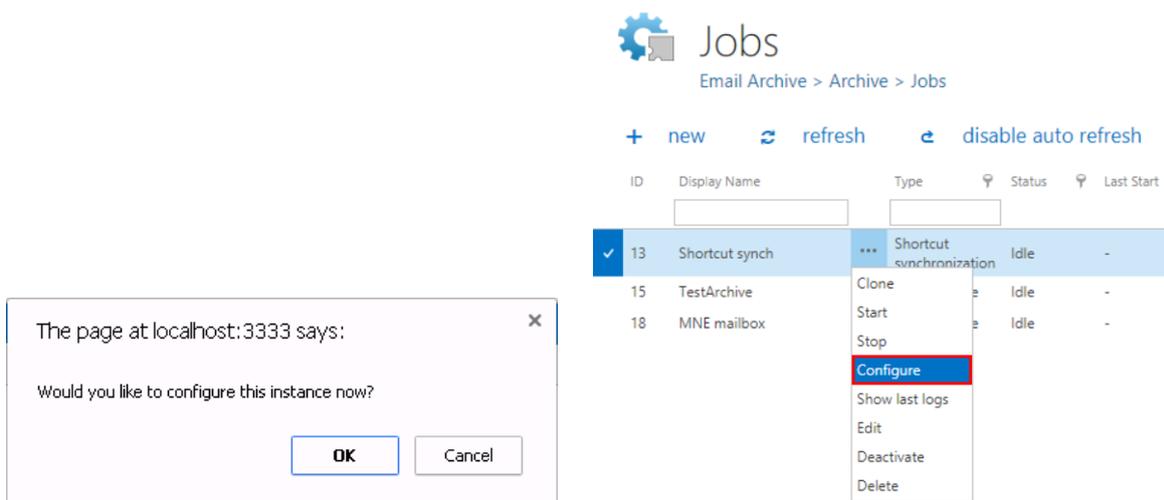
As previously mentioned, automated archiving is managed by automated jobs that are configured on the job's configuration page. Here you can define the exact configurations (i.e. database, schedulers, storage, address book objects to process etc.) of an archive/restore/recovery/mailbox move/shortcut synchronization/ shortcut repair job.

Creating jobs from email archive plugins:

Navigate to **Email archive** → **Archive** on the ribbon and click on the **Jobs** button. The **Jobs** page of Email Archive will open. Click here on **+ new** option. In the **Add new job instance dialog** choose one from the list of available jobs (Email archive/Email restore/Email recovery/Mailbox move/Shortcut synchronization/Shortcut repair), select the node where the job will run (option **Run on node**) and fill a **Display name** into the **Add new job instance** popup-window. Then click on **Add**.



If you want to configure the job immediately, then click **OK** in the pop-up window and the job configuration page opens immediately. The configuration page is accessible any time using the “Configure” menu item in the given job’s context menu (2nd picture below).



The following subchapters will describe the functionality and configuration of the following email archive job types in more details:

- [Email archive job](#)



- [Email archive retention changer job](#)
- [Email restore job](#)
- [Email recovery job](#)
- [Delete job](#)
- [Journal post processing job](#)
- [Mailbox move job](#)
- [Shortcut synchronization job](#)
- [Shortcut repair job](#)
- [Public folder archiving](#)
- [SMTP archiving](#)



Email archive job

This job type archives the configured mailbox items into the selected archive storage. The items that are archived with shortcuts or with the “Keep original” method will be retrievable from the respective mailboxes; items archived with the journal shortcut will be accessible only in the archive. Automated email archive jobs are usually running out of working hours.

Note: The HTML shortcut, which replaces the archived email, also contains a link in .eml format, which is compatible with MAC OS, too.



Email archive job configuration

In this use case, we will configure an email archive job, which will archive the mailbox items of mailbox “edit.balazsy@tech-arrow.com” that are older than 1 year, but younger than 2 years. The archived items will be replaced by HTML shortcuts. The archiving process will run each working day from 5 PM CET till midnight. For this processing type, it is a must to configure the following sections on the job’s configuration page:

✓ Report mode settings:

If the **Use report mode** checkbox is checked, the job will run in report mode. After the job finishes its run in this mode, the user will be able to download a .csv report file here in this section. The file will contain a list of emails that belong to the entities selected in section **Address book objects to process** of the job and some information to them, including whether they will be processed or not.



Report mode settings

Use report mode:



Generated report file:

File name: JobReport_7779b902-c4eb-49f0-b7de-6eed8313a926.csv

Size: 1.3 KB

Date: 4/4/2019 3:01:51 PM

A	B	C	D	E
Subject	SentDate	Sender	Status	Filter
Microsoft logo	4/3/2019 15:15	dne@ta.internal	will be skipped - Shortcut	
Indexing 10	8/28/2018 14:48	dne@ta.internal	will be skipped	no filter
Indexing 09	8/28/2018 14:47	dne@ta.internal	will be skipped	no filter
Indexing 08	8/28/2018 14:47	dne@ta.internal	will be skipped	no filter
Indexing 07	8/28/2018 14:46	dne@ta.internal	will be skipped	no filter
Indexing 06	8/28/2018 14:38	dne@ta.internal	will be skipped	no filter
Indexing 05	8/28/2018 14:38	dne@ta.internal	will be skipped	no filter
Indexing 04	8/28/2018 14:38	dne@ta.internal	will be skipped	no filter
Indexing 03	8/28/2018 14:38	dne@ta.internal	will be skipped	no filter
Indexing 02	8/28/2018 14:37	dne@ta.internal	will be skipped	no filter
Indexing 01	8/28/2018 14:35	dne@ta.internal	will be skipped	no filter

Screenshot: Report file preview

✓ Processing settings:

From the Archive dropdown list, the administrator has to choose what will be archived by the Archiving job.

There are 3 options:

- Mailboxes
- In-Place Archives
- Mailboxes and In-Place Archives

The administrator may select here if he would like to use MAPI protocol to communicate with the Exchange server. EWS (Exchange Web Services) connection is selected by default if MAPI is not selected here. It is important to know that **O365 Exchange server does not support MAPI connection**. Another requirement to use MAPI is to have Exchange server 2013 or earlier version.

Note: MAPI can be selected only in case **Mailboxes** option is selected in the **Archive** dropdown list, since MAPI is **not supported by In-Place Archive**.

The **Use journal archive to build folder structures of mailboxes** option will allow the job to update the folder IDs and create the correct folder structure. The job goes through a mailbox, searches for the email in the archive and updates its folder ID (creates also the folder in the archive if it hasn't existed yet). Read more about journal processing [here](#).

If you check the **Archive email if journal didn't archive it yet** sub-option, the archive job will also archive the email if it was not yet archived using the journal processing. Read more about journal processing [here](#).

Note: At least one mailbox must be set as **Process as journal mailbox** from its context menu in the **Address book**, otherwise the **Use journal archive to build folder structures of mailboxes** and **Archive email if journal didn't archive it yet** options won't appear in the job's configuration.

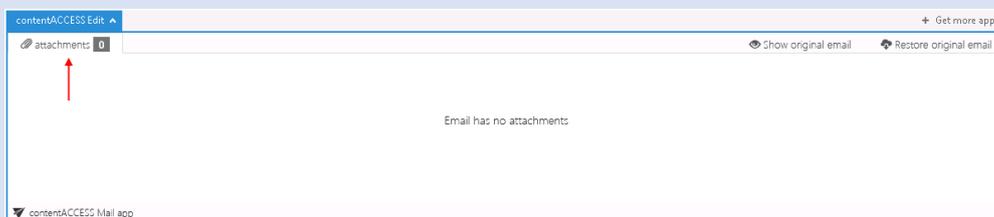
Processing settings

Archive:

Processing settings:

- Use MAPI to communicate with Exchange Server (Supported only for versions up to Exchange 2013)
- Use journal archive to build folder structures of mailboxes
- Archive email if journal didn't archive it yet

Note: The **Split attachments** option is active (checked) by default. That means that the body of the email and the attachment are stored separately. If the email message containing attachments has been archived by a job, where this option **was not checked**, our apps ([MailApp](#), [officeGATE](#), [contentACCESS Mobile](#)) will show 0 attachments. However, if you open the original email, the attachments are shown.



If this option **was checked**, but the email was containing embedded email (.msg attachment), this embedded email won't be displayed between the attachments in our apps.



✓ Database settings:

Select an already configured connection from the dropdown list. Here the metadata will be stored. We have configured for our archived emails the database named “Email Archive DB”, so we set it here. (For further information on how to set database connections please refer to section [Databases.](#))

Database settings

Database connection:

✓ Scheduling settings:

In this step, the running time(s) of the Email archive job must be selected. It is possible either to select a scheduler from the list or to create a new scheduler via **create new ...** option from the dropdown list. For an email archive job, it is recommended to set a Week schedule with repeat, which will start the job at the same time every day. In our use case, we set a scheduler which starts the archive job every day after the business hours (starts at 5 PM CET and ends at midnight). (For more information about how to set schedulers refer to the section [Schedules](#) above.)

Scheduling settings

Scheduled in:

✓ Storage settings:

Choose an already configured storage from the dropdown list. The processed binaries will be stored here. On the screenshot below we selected our already configured disk type store: “Email Archive store”). (For more information on how to set storages check section [Storage](#) above.)

Storage settings

Storage name:

- ✓ **Shortcutting.** In the mailbox, the emails will be replaced by the shortcut that is set in the “Apply to NOT ARCHIVED items” section. You can use any previously configured shortcut type that was configured in section **Shortcut configuration** above. If the mailbox items have not been archived yet (are archived for the 1st time), check the “Apply to NOT ARCHIVED items” checkbox. It is recommended to use HTML shortcut for emails/attachments that are 1 to 2 years old.

Shortcutting

Shortcut types:

Apply to NOT ARCHIVED items

Use shortcut **HTML emails 1-2 years** for items where filter is **not set** [\[Change\]](#)

Apply to ALREADY ARCHIVED items with keep original shortcutting method

Use shortcut **HTML formatted** for items where filter is **not set** [\[Change\]](#)

Apply to ALREADY ARCHIVED items with keep original shortcutting method
 Use shortcut **HTML emails 1-2 years** for items where filter is **not set** [\[Change\]](#)

Apply to ALREADY ARCHIVED items with keep original shortcutting method
 Use shortcut **HTML formatted** for items where filter is **not set** [\[Change\]](#)

Apply to ALREADY ARCHIVED items with keep original shortcutting method
 Use shortcut **Journal** for items where filter is **not set** [\[Change\]](#)

Apply to ALREADY ARCHIVED items with keep original shortcutting method
 Use shortcut **Keep original** for items where filter is **not set** [\[Change\]](#)

Apply to ALREADY ARCHIVED items with keep original shortcutting method
 Use shortcut **Normal** for items where filter is **not set** [\[Change\]](#)

Note: If the items are already archived (e.g. with the “Keep original” method), but they need to be replaced with shortcuts, check the second checkbox and specify a previously configured shortcut type that should be used. It should be mentioned that these 2 processes will always run in 2 stages (even if both processes are configured within one job). By the 1st run of the job the items will be archived, by the 2nd run of the job the (archived) items will be replaced by the selected shortcuts.

If an email has been shortcutted before, but was then restored or recovered, the "Apply to ALREADY ARCHIVED items with keep original shortcutting method" checkbox must be checked if the user wants the email to be processed by the job.

Click on the **Change** button and set the filtering according to your needs and/or regulations. To learn more about how to work with filtering settings, please, check [this](#) section of our documentation.

Note: Email archive size filter is limited to 2 GB (gigabytes). Size filter uses the message size acquired from EWS (Exchange web service). This message size can be different from the value displayed in Outlook.

Filter settings ✕

+ add custom property

visual
text

AND ▼	Sent date ▼	>	▼	2Y	📅 ✕
	Sent date ▼	<	▼	1Y	📅 ✕
+add group +add condition					

+add new group

Note: Shortcutting methods can be also combined when configuring an Email Archive job. For more information refer to section “**Combining the shortcutting methods**”.

Note: The message classes excluded in the [Email archive System settings](#) take always priority over the **filtering settings** defined in the archive job.



Important: In case of **custom Exchange solution(s)** used for emails, the **custom email properties will not be archived!** The recommended solution: do not archive these emails and/or use the exclude feature (in [Email archive System settings](#)) for these custom message classes.

Use case: archive emails older than 1 year

In this use case, we would like to archive emails older than 1 year and replace them with a shortcut. We are configuring the option “Apply to NOT ARCHIVED items” only.

Shortcutting

Shortcut types:

Apply to NOT ARCHIVED items
Use shortcut for items where filter is **(Sent date < "1Y")** [\[Change\]](#)

Apply to ALREADY ARCHIVED items with keep original shortcutting method
Use shortcut for items where filter is not set [\[Change\]](#)

The mails will be archived and immediately replaced by a shortcut.

Use case: archive immediately, create shortcut later

In this use case, we will configure the archiving job to archive all emails (regardless of age) with the shortcut type **Keep original**. This will ensure that all emails are archived, but the mailbox is kept intact. Emails older than 3 months will be further processed – after these are archived, they will be converted to **HTML** shortcuts.

Shortcutting

Shortcut types:

Apply to NOT ARCHIVED items
Use shortcut for items where filter is not set [\[Change\]](#)

Apply to ALREADY ARCHIVED items with keep original shortcutting method
Use shortcut for items where filter is **(Sent date < "3M")** [\[Change\]](#)

Note: By using a “Journal shortcut” type you can delete the shortcuts completely from the mailbox.

Shortcutting

Shortcut types:

Apply to NOT ARCHIVED items
Use shortcut for items where filter is not set [\[Change\]](#)

Apply to ALREADY ARCHIVED items with keep original shortcutting method
Use shortcut for items where filter is **(Sent date < "3M")** [\[Change\]](#)



✓ **Retention settings:**

Choose an already configured retention time from the dropdown list. The archived emails will be stored during this time in the storage, and it will be impossible to delete them from there. It is highly recommended to select a retention time that is required by the law of your country. (For more information about how to set retentions check section [Retentions](#) above.)

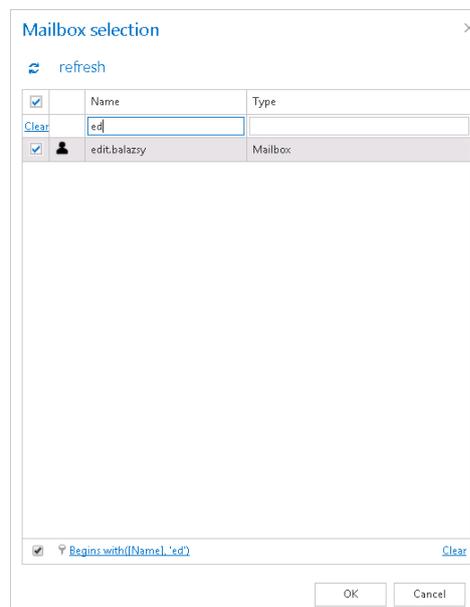
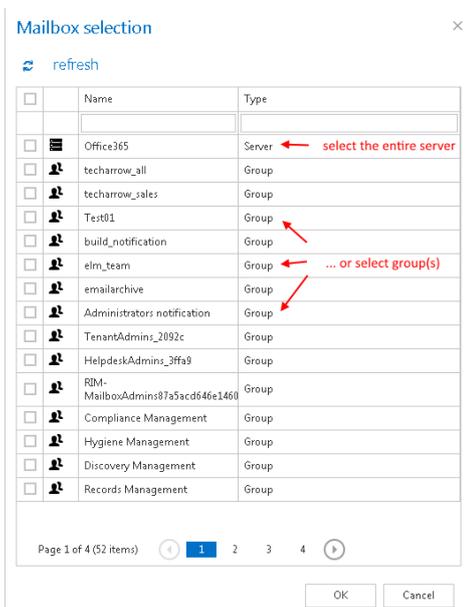


✓ **Address book objects to process**

Here the administrator may select the mailboxes, groups or the entire Exchange server, which will be processed by the archive job. Click on the **select** option and check the desired groups or servers in the **Mailbox selection** window, then click on **OK**.

Note: If the **In-Place Archives** option is selected in the **Archive** dropdown list in **Processing settings**, this warning will pop up for the **Address book objects**. In this case, only servers, groups and In-Place Archive mailboxes can be selected after clicking on the **Select** option.

In this use case, we will archive mailbox “edit.balazsy@tech-arrow.com”, so we select it from the list:





Note: It is possible to archive journal mailboxes as well. Just select this option in the Mailbox selection window and in the “Include folders” configuration section set %INBOX%.

- When a journal message is retrieved in the mailbox, the inner message is retrieved;
- When a journal message is restored, the whole envelope is restored;
- When a journal message is previewed (in contentWEB archive), the inner message is displayed;
- When a journal message is exported to PST, the inner message is exported.

Important: If an on-premise Exchange group is used in a job configuration, the job configuration needs to be updated after the group is moved to the cloud, since the group identifier changes and the job is still using the old identifier.

Steps to take:

- open job’s configuration page
- remove the group from the list of **Address book objects to process**
- select the group and re-add it to the list
- save the job configuration

✓ **Include folders:**

Email archive job is crawling the entire mailbox or recursive folder structures from the mailbox for further processing. Before you enter the folder name(s) to be crawled, it is necessary to select the folder filtering type.

Include folders

Folder filtering type:

One single folder

Entire mailbox

One single folder

Recursive, starting from a single folder

Multiple folders

Multiple recursive, starting from a single folder

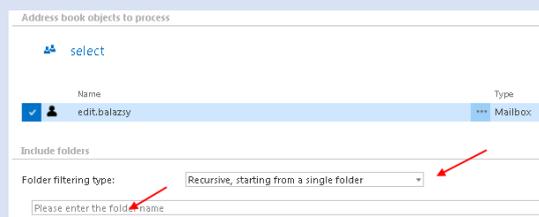
If you set **Entire mailbox**, then the whole mailbox including all folders will be processed. If you set **One single folder** type, then only one pre-selected folder will be processed (e.g. if you set %INBOX%\Subfolder1, then only Subfolder1 will be processed). If you set **Recursive, starting from a single folder** filtering type, then all folders starting from the defined folder will be processed (e.g. if you set %INBOX%\Subfolder1, then starting from Subfolder1, every subfolder will be processed in the structure). The same rule applies to the



Multiple folders and to the **Multiple recursive, starting from a single folder**, too, but in this case we can work with more folders simultaneously (e.g.: %INBOX%, %OUTBOX%\Folder name 5...or...%TASKS%, %CALENDARS%\Folder name 6).

Important: It is highly recommended to specify the root mailbox folders using wildcards (%). Wildcards ensure that the given mailbox folder (e.g. the "INBOX" folder) will be processed, regardless of the language settings of the mailbox. This is important mainly for companies who archive mailboxes using different languages. Subfolders must be added to a root folder with a backslash (\). Since the backslash "\" is used as path separator, it can't be used in folder name. If you want to include or exclude a folder which contains backslash in its name, enter it with "_|_" instead of "\".

Note: It is important to bear in mind that by selecting "Recursive, starting from a single folder" filtering type under "Include folders" section and leaving the folder path textbox empty, the whole selected mailbox will be archived:



In our use case, we select the whole "INBOX" to archive:



✓ Exclude folders

With this function, you may set which folders/subfolders should not be archived. If you would not like to exclude any folder from the archive process, you can skip these settings.

The folders may be excluded using one of the available methods: a) They may be **added manually** via the **+** **new** option; b) they may be **imported** in one of the available file formats via the **import** option.

Important: Due to different language settings in the user mailboxes, it is highly recommended to specify the root folders using wildcards (%). Subfolders must be added to a root folder with a backslash (\).

Since the backslash “\” is used as path separator, it can't be used in folder name. If you want to include or exclude a folder which contains backslash in its name, enter it with “_|_” instead of “\”.

Exclude folders

a) + new b) ↶ import

a) Add exclude folders manually:

Click on + new option. In the **Exclude folder** dialog's textbox specify the folder(s) to be excluded. Use the hints that are featured in the same dialog. %INBOX%\TECH-ARROW pattern on the picture below means that “TECH-ARROW” folder on the “INBOX” root folder will be excluded.

Exclude folder ✕

Exclude folder settings

Pattern: %INBOX%\TECH-ARROW

Test pattern

Hint:

\Example	Exclude the folder Example on the root
Example	Exclude all folders with name Example
\Example\Example	Exclude subfolder 'Example' of the folder Example on the root
Example\Example	Exclude subfolder Example of folders with name Example
\Example*	Exclude subfolders of the folder Example on the root
Example*	Exclude all subfolders of folders with name Example
\Example**Example*	Exclude subfolder *Example* of the folder Example on the root
Example**Example*	Exclude subfolder *Example* of folders with name Example
\Ex*	Exclude all folders that start with Ex on the root
Ex*	Exclude all folders that start with Ex
\Ex**	Exclude all subfolders of folders that start with Ex on the root
Ex**	Exclude subfolders of all folders that start with Ex

Special characters *, +, ?, |, , { }, [], (), ^, \$, ., # need to be escaped by backslash \

Example: Folder\Folder \ (John\) will exclude the path Folder\Folder (John). If the folder divider \ is followed by subfolders pattern * or with any escaped special character it must be escaped, too. E.g. the folder Test\#abc# is excluded with using a pattern Test\\#abc#.

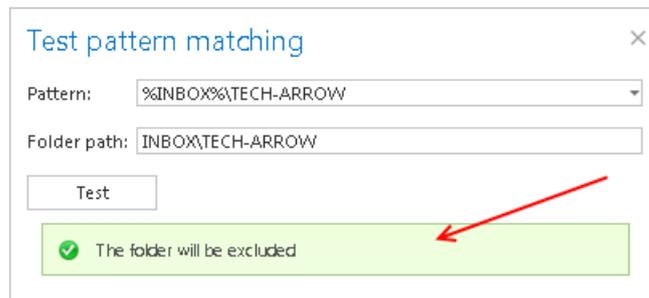
The entered pattern is case-insensitive

Save
Cancel

Test pattern button

This button is used to check if the entered pattern will be suitable for the path that the user would like to exclude from the archiving process. Open the **Test pattern matching** window by clicking on the **Test pattern** button. Enter the folder path into the **Folder path** field (this time without the % sign) and click on **Test** button.

The test will be successful if the **Pattern** was entered correctly into the **Exclude folder** window.



b) Import the list of folders to be excluded:

The list of folders to be excluded may be imported from files in one of the available formats: CSV, XML, Tab delimited files or Space delimited file. The file to be imported must contain the list of the folders. **Important:** Root folders must be specified in wildcards (%) in the import files. Subfolders must be added to a root folder with a backslash (\). To import such a file with the list of folders refer to chapter [Importing contentACCESS configurations from files](#) of this guide.

Excluding folders with special characters

The folders containing special characters like brackets, hyphens, question marks etc. can be excluded from the archiving process. To exclude such folders from the archiving process, the special characters included in the folder(s) name must be excluded **using the backslash “\” escape character**. The **escape character must be added before the special character** to be excluded, in the **Exclude settings** of the archive job’s configuration page.

E.g. you have such a structure in the mailbox: `INBOX\Important (folder)`

and the **“Important (folder)”** must be excluded (the special characters are the brackets), then you must specify the folder to be excluded like this: `INBOX\Important\(folder\)`

This information is available at the bottom of the **Exclude folder** window:

Exclude folder ✕

Exclude folder settings

Pattern:

Hint:

\Example	Exclude the folder Example on the root
Example	Exclude all folders with name Example
\Example\Example	Exclude subfolder 'Example' of the folder Example on the root
Example\Example	Exclude subfolder Example of folders with name Example
\Example*	Exclude subfolders of the folder Example on the root
Example*	Exclude all subfolders of folders with name Example
\Example**Example*	Exclude subfolder *Example* of the folder Example on the root
Example**Example*	Exclude subfolder *Example* of folders with name Example
\Ex*	Exclude all folders that start with Ex on the root
Ex*	Exclude all folders that start with Ex
\Ex**	Exclude all subfolders of folders that start with Ex on the root
Ex**	Exclude subfolders of all folders that start with Ex

Special characters *, +, ?, [, { }, [], (), ^, \$, ., # need to be escaped by backslash \

Example: Folder\Folder \ (John\) will exclude the path Folder\Folder (John). If the folder divider \ is followed by subfolders pattern * or with any escaped special character it must be escaped, too. E.g. the folder Test\#abc# is excluded with using a pattern Test\\#abc#.

The entered pattern is case-insensitive

- ✓ **Notification settings.** Select here, when you will need to get notification emails from the Email archive job. It is possible to set here if you need such a notification email always/never, or you need it only in case that an error/warning occurred during the archiving process – for example, if the archiving of one or more items failed, then you may get a notification email about this error. Into the **Recipient list** textbox insert the email address(es) of the person(s), who will get such notifications. Notifications should be used if the administrator does not use the **System logs** feature.



Notification settings

Send when:	<input type="text" value="Never"/>
Recipient list:	<input type="text" value="john.doe@example.com,peter.white@example.com,..."/>

- ✓ **Resource settings.** Set the value, which will determine how many items will be processed simultaneously by the email archive job. The recommended value is “2”.

Resource settings

Worker thread count:	<input type="text" value="2"/>
----------------------	--------------------------------

- ✓ **Save your changes!!**

Combining the shortcutting methods in an Email archive job

What are the advantages of combining the shortcutting methods for the user?

Companies use the “Keep original” archiving method on a daily basis. This archiving method ensures that the emails and their attachments are ready at hand during the time when they are still in use. After certain time period (usually after 6 months), it is pointless to keep these emails in the mailbox(es), as they take up too much space. However, these emails must be still easily accessible at any time. For this reason, it is recommended to replace them with shortcuts, which save space in the mailboxes and guarantee easy access to the older mailbox items. By combining the shortcut methods the end user will easily achieve the desired result.

This use case will demonstrate how to configure an Email Archiving job, which will archive the items older than 10 days, while keeping them in the original file location. The job will also replace these items with shortcuts after 6 months. The job combines the “Keep original” archiving method with the shortcutting after the item reaches a certain age (6 months in this use case). The size of the items to be archived and shortcutted can be set as well.

Note: If two archive processes are combined (as in this use case), then the archive process will run in two stages, too. By the first job running the emails will be archived while keeping the original, by the 2nd job running these items will be replaced by shortcuts.

The following steps should be executed to set up an email archive job using the advantages of this method:

- ✓ **Set up a new Email Archiving job and open its configuration page.**
- ✓ **Set all required sections on the job’s configuration page.**



- ✓ On the configuration page of the Email Archiving job **navigate to the “Shortcutting”** section and check the **“Apply to NOT ARCHIVED items”** checkbox.

Shortcutting

Shortcut types:

Apply to NOT ARCHIVED items
Use shortcut for items where filter is **(Sent date < "10D")** [\[Change\]](#)

Apply to ALREADY ARCHIVED items with keep original shortcutting method
Use shortcut for items where filter is **(Sent date < "6M" AND Size >= "100KB")** [\[Change\]](#)

- ✓ Set the **“Keep original”** archive method for items that are older than 10 days. Choose the “Keep original” option from the dropdown menu and set that all items older than 10 days will be archived.

Shortcutting

Shortcut types:

Apply to NOT ARCHIVED items
Use shortcut for items where filter is **(Sent date < "10D")** [\[Change\]](#)

Apply to ALREADY ARCHIVED items with keep original shortcutting method
Use shortcut for items where filter is **(Sent date < "6M" AND Size >= "100KB")** [\[Change\]](#)

- ✓ Apply the shortcutting to the items archived with the **“Keep original”** method, which are older than 6 months and larger than 100 kB. Choose HTML shortcut type, which will be used by the job.

Check the “Apply to ALREADY ARCHIVED items with keep original shortcutting method” checkbox.

Choose the already configured “HTML” shortcut from the dropdown list. Set the sent date to 6 months and the size to “larger than 100 kB”.

Shortcutting

Shortcut types:

Apply to NOT ARCHIVED items
Use shortcut for items where filter is **(Sent date < "10D")** [\[Change\]](#)

Apply to ALREADY ARCHIVED items with keep original shortcutting method
Use shortcut for items where filter is **(Sent date < "6M" AND Size >= "100KB")** [\[Change\]](#)

USE CASE: How to set up the shortcutting if all items should be archived and items under 100 kB should be kept in the original location, while items over 100 kB should be replaced by shortcuts? In this use case set the size filter in the 2nd!!!! row only (refer to screenshot above) to >100 kB and do not set a size filter in the 1st row.



Shortcutting

Shortcut types:

Apply to NOT ARCHIVED items
 Use shortcut for items where filter is (Sent date < "10D") [\[Change\]](#)

Apply to ALREADY ARCHIVED items with keep original shortcutting method
 Use shortcut for items where filter is (Sent date < "6M" AND Size >= "100KB") [\[Change\]](#)

✓ **Save your settings and wait until the job starts to run** according to the configured scheduler.

Email archive job description

All the numbers and descriptions in the job’s progress have a particular meaning. In this section, we are going to explain the numbers and descriptions of an **Email archive job**.

Description	Explanation
x mailboxes processed	x mailboxes were finished by the job
(y failed)	y mailboxes failed (out of the x mailboxes)
x emails archived	x emails were archived with the selected shortcut
x (y) emails archived	x emails were archived in total, but only (x-y) were archived with the selected shortcut, y emails were archived with keep original shortcut
(x folders skipped)	x folders were skipped from the processing because of exclude folder settings
(x skipped)	x emails have been skipped because of filtering settings, or the emails were already archived
(x failed)	x emails failed to archive (due to permissions or invalid emails)

Email archive journal processing

Journal based archiving is the most efficient way of archiving that fully solves the economical and compliancy requirements.



Journaling is the ability of an email server to record all (inbound and outbound) email communication in an organization. This email communication can be directly stored in a dedicated mailbox or can be forwarded to contentACCESS SMTP server.

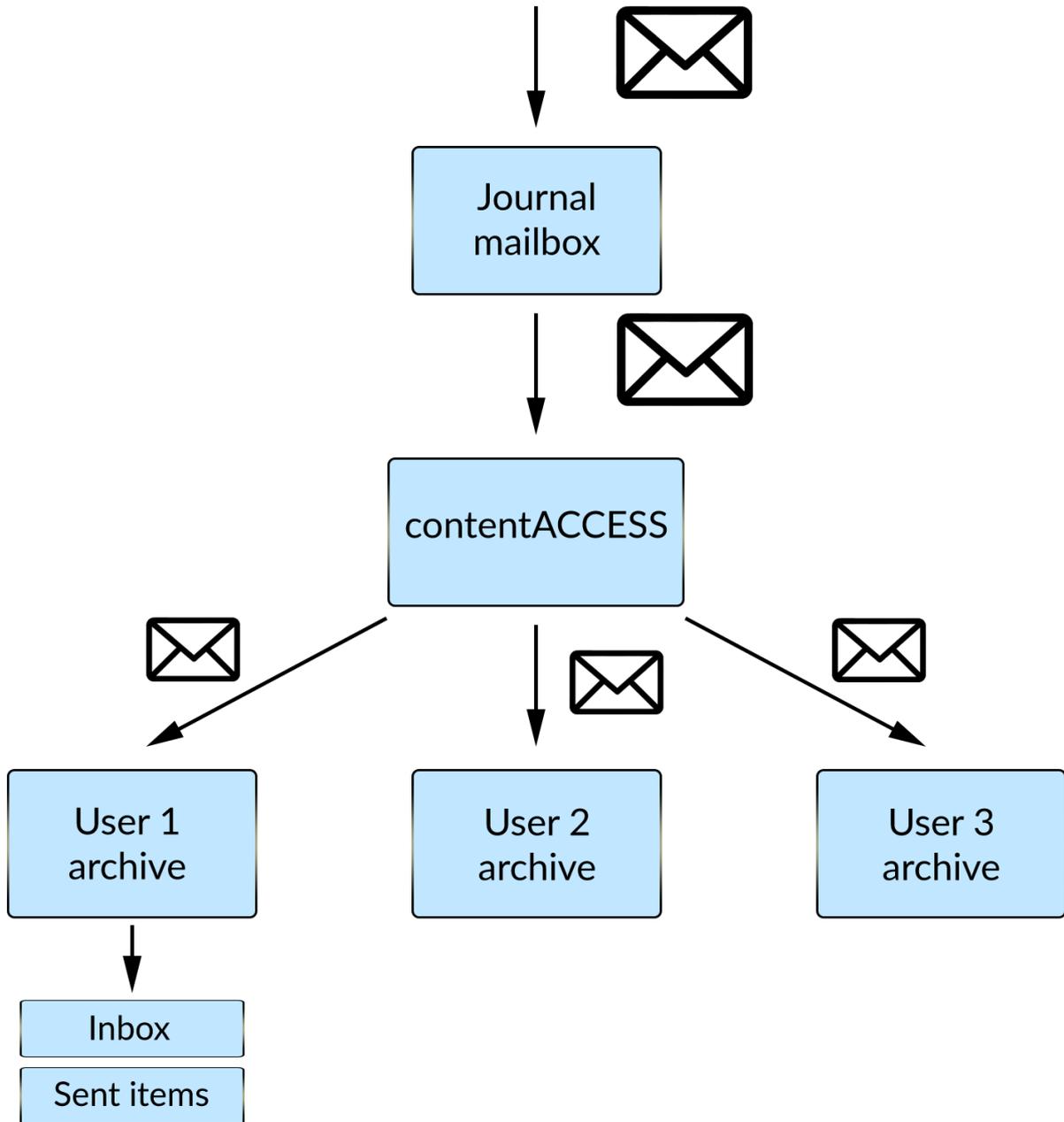
- In case of a **dedicated mailbox**, contentACCESS will periodically monitor that mailbox and will process emails from it.
- In case of the **journal forwarding**, the built-in contentACCESS SMTP server will receive the emails and will forward them to the archiving module. The SMTP forwarding is very useful for O365 tenants, as Microsoft does support creating a dedicated journal mailbox, but allows only forwarding of the journal emails.

The result will be the same in both cases (the dedicated mailbox and the SMTP forwarding).

In a **standard journal archiving case**, the company will have only one mailbox in the archive - the journal one. This mailbox can be used for legal, regulatory and organizational compliance purposes, but standard users will not have access to it.

In an **advanced journal archiving case**, contentACCESS will not archive the email only into a single journal mailbox, but will also duplicate (link) that email to all recipients. In such case, **each user participating in the email conversation will get a separate copy of that email**. Unfortunately, the emails delivered through journal processing do not contain the folder information (in which folder the users will have the final email). To solve this, the standard contentACCESS email archive job can run in a special mode, where it synchronizes the user's folder structure, will find the emails duplicated (linked) through journal in the user's mailbox and will place them into the correct folder inside the archive. By doing this, contentACCESS can achieve the same result as for standard email archiving case, but in a more efficient way.

Note: The shortcutting functionality is also supported during the advanced journaling.



Screenshot: Workflow of the journal processing



<ul style="list-style-type: none"> ▲ Journal <li style="background-color: #cccccc;">Inbox 	MyEmail
---	---------

<ul style="list-style-type: none"> ▲ Joe <li style="background-color: #cccccc;">Inbox Sent items 	MyEmail
---	---------

<ul style="list-style-type: none"> ▲ Mary Inbox <li style="background-color: #cccccc;">Sent items 	MyEmail
--	---------

Screenshot: Results in contentWEB before (on the left) and after the archive job "archive based on journal" (on the right)

Configuring the journal processing

First, you need to select **Process as journal mailbox** from the context menu of the selected mailbox in **Address book**.



View address book

Email Archive > Archive > View address book

Mailboxes Public folders Groups Servers

import mailboxes manually + add mailbox manually

Name	Email	Distinguish	Create contentWEB access	Associate with role
ANE.	ANE@ta.internal	CN= ANE.	No	
ENE.		N= NE.	Yes	Standard user
ONE.		N= NE.	No	
PNE.		N= NE.	Yes	Inherited

Show mailbox details

Automatically create contentWEB user

Do not create contentWEB user

Assign database, storage and index zone

Deactivate mailbox license

Manage access ...

Move mailbox ...

Disconnect mailbox

Process as journal mailbox

Phase 1

In this phase the archiving process will create

- mailboxes in the archive for all users, who are recipients or senders on a journal email
- "Inbox" and "Sent items" folders in the archive for these mailboxes

Note: All mailboxes must have a **Database** and **Store** assigned in the **Address book**, otherwise the job will skip them.

Archive the journal mailbox by one of the following ways:

- 1) directly, by creating an **Email archive job** and selecting the journal mailbox in **Address book objects to process**



Address book objects to process

 select

Name	Type
 ANE.	Mailbox

- 2) via SMTP archiving – to learn how to configure this way of archiving, please, refer to the section [SMTP archiving](#)

The job archives the mails in the journal mailbox and also automatically duplicates the archived email for all the recipients and senders:

- in case of sender, it creates a "Sent items" folder in the archive for the sender mailbox and duplicates the email there
- in case of recipient, it creates an "Inbox" folder in the archive for the recipient(s) mailbox(es) and duplicates the email there

Phase 2

Important: This option is not working for Exchange 2010 or earlier.

In this phase the archiving process will create the correct folder structure in the archive for the mailboxes that were archived in **Phase 1** and will move each email into the correct folder.

First, you need to have a job configured based on **Phase 1** (see above).

Now, create an archive job and enable the **Use journal archive to build folder structures of mailboxes** option in **Processing settings**. This will allow the job to create the correct folder structure.

Note: At least one mailbox must be set as **Process as journal mailbox** from its context menu in the **Address book**, otherwise the **Use journal archive to build folder structures of mailboxes** and **Archive email if journal didn't archive it yet** options won't appear in the job's configuration.



Processing settings

- Use MAPI to communicate with Exchange Server (Supported only for versions up to Exchange 2013)
- Split attachments
- Use journal archive to build folder structures of mailboxes
- Archive email if journal didn't archive it yet

In section **Address books object to process**, select all the mailboxes except the journal one (you can simply select the whole server or group and exclude the journal mailbox in section **Exclude addresses**).

Address book objects to process

select

Name	Type
TADC01	Server

Include folders

Folder filtering type:

Exclude folders

new import

Pattern

No data to display

Exclude addresses

new import

Address to exclude	Exclude type
ane@ta.internal	All

When the job runs, it goes through a mailbox, searches for the email in the archive and moves it to the correct folder (creates also the folder in the archive if it hasn't existed yet).



If you check the **Archive email if journal didn't archive it yet** sub-option, the archive job will also archive the email if it was not yet archived using the journal processing (**Phase 1** did not duplicate it for the sender or recipient mailbox).

Processing settings

- Use MAPI to communicate with Exchange Server (Supported only for versions up to Exchange 2013)
- Split attachments
- Use journal archive to build folder structures of mailboxes
- Archive email if journal didn't archive it yet ←

Recommendations after turning on journal archive

In this section, we would like to talk about some actions that we would recommend doing after turning on journal archive.

Additional tasks after turning on journal archive

Turning on the journal archiving or SMTP archiving applies only to emails sent/received **after the feature is turned on**. The emails that were sent/received prior to this feature need to be archived differently. This section will help you to configure the archive.

What to do with emails prior to Journal activation?

Definition of term: Journal activation is the date/time when the journaling or SMTP archiving was activated.

If the older emails do not need to be archived

No additional configuration is needed.

If the older emails need to be archived as well

We recommend creating a new email archive job for these emails, with a filter: **archive emails older than the Journal activation date**. This archive job **should NOT use** the option "Use journal archive to build folder structures of mailboxes". By turning this option off, the archive job will process all emails prior to **Journal activation** as regular user emails.



contentACCESS Central Administration

System	File Archive	Email Archive	SharePoint Archive	GDPR	Teams Archive	Custom plugins
Save Discard changes	Databases Storages	System settings Provisioning settings Retentions	Shortcut configuration Schedules	User experience	View address book Jobs	Remote agents PST import Legacy data configuration
Edit	Settings			Archive	Remote agents	Miscellaneous



Archiving older emails

Email Archive > Archive > Jobs > Archiving older emails

start immediately
 refresh
 disable auto refresh
 deactivate job
 logs
 edit

Status: **Idle**
Progress:

Report mode settings

Use report mode:

Processing settings

Processing settings:

- Use MAPI to communicate with Exchange Server (Supported only for versions up to Exchange 2013)
- Use journal archive to build folder structures of mailboxes **← do NOT check this option**
- Archive email if journal didn't archive it yet

Database settings

Database connection: DemoDB

Scheduling settings

Scheduled in: Manual

Storage settings

Storage name: Disk store

Shortcutting

Shortcut types:

- Apply to NOT ARCHIVED items
 - Use shortcut HTML for items where filter is **Sent date older than "2021-05-14"** **← our Journal activation date** [\[Change\]](#)
- Apply to ALREADY ARCHIVED items with keep original shortcutting method
 - Use shortcut Select from the repository for items where filter is not set [\[Change\]](#)

Once the older emails are covered, the journal-based archive jobs will cover the new emails.



contentACCESS Central Administration

System		File Archive		Email Archive			SharePoint Archive		GDPR	Teams Archive		Custom plugins		
Save	Discard changes	Databases	Storages	System settings	Provisioning settings	Retentions	Shortcut configuration	Schedules	User experience	View address book	Jobs	Remote agents	PST import	Legacy data configuration
Edit		Settings							Archive		Remote agents		Miscellaneous	



Journal archiving

Email Archive > Archive > Jobs > Journal archiving

start immediately
 refresh
 disable auto refresh
 deactivate job
 logs
 edit

Status: **Idle**
Progress:

Report mode settings

Use report mode:

Processing settings

Processing settings:

- Use MAPI to communicate with Exchange Server (Supported only for versions up to Exchange 2013)
- Use journal archive to build folder structures of mailboxes ←
- Archive email if journal didn't archive it yet

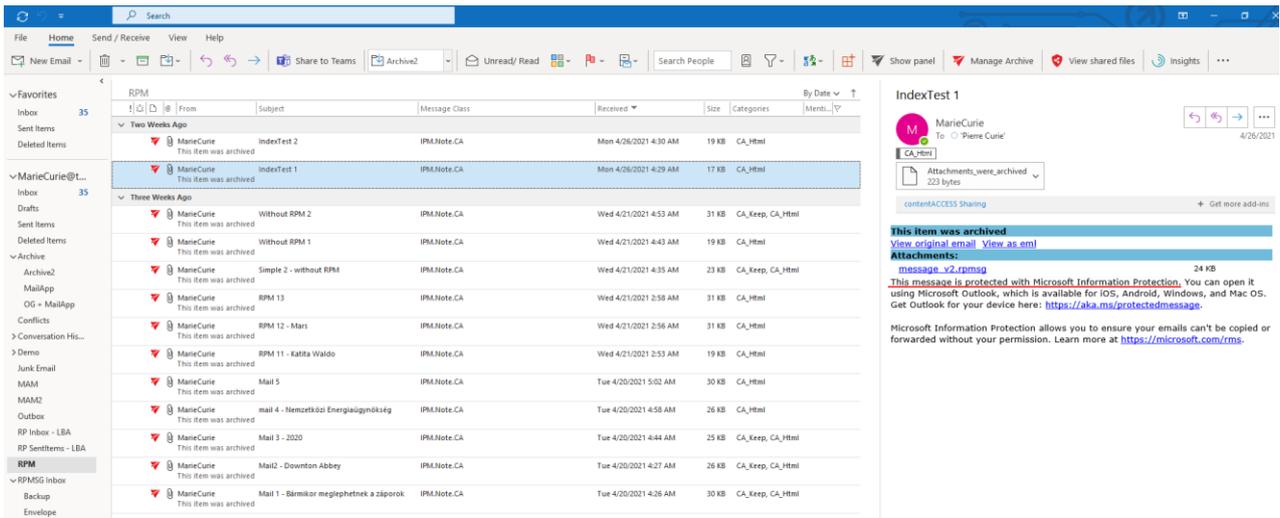
Note: If you miss this step, the job in **report mode** will not be able to distinguish between the mails prior and after the **Journal activation**, resulting in misleading numbers in the report.

Archiving of rights protected messages

User mailbox archiving

Office 365 allows the users to send encrypted emails using the **Azure Rights Management** cloud service. These rights protected messages (RPM) can be archived by contentACCESS with the following limitations:

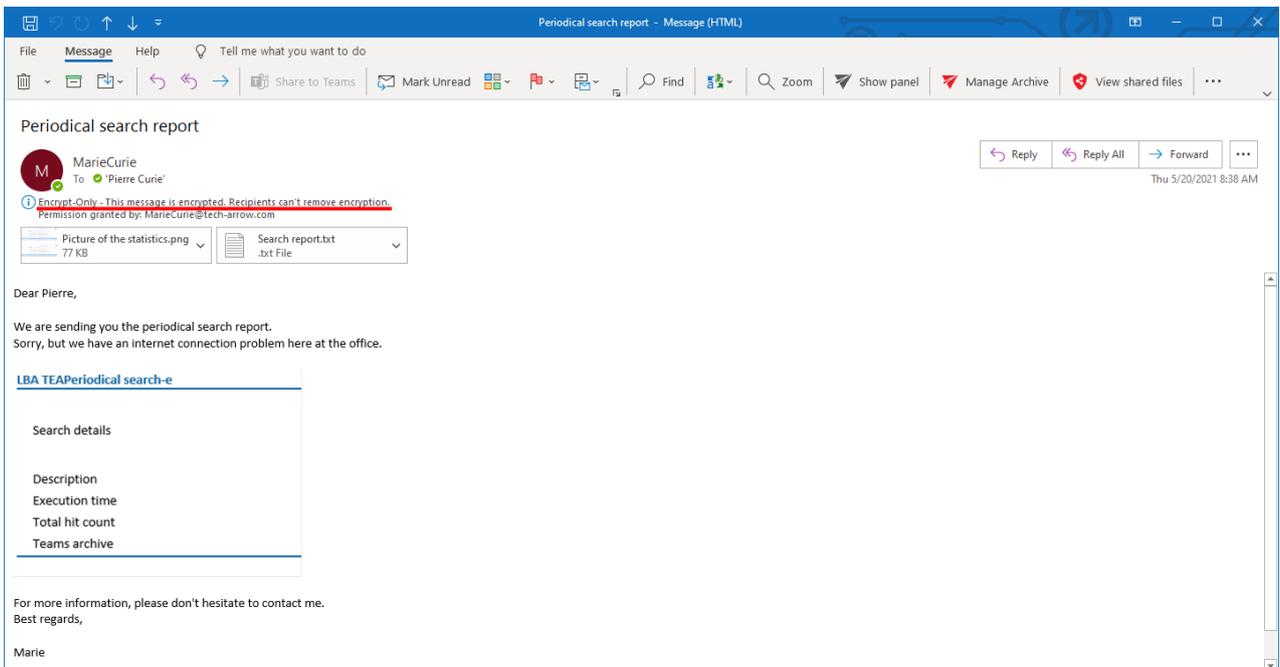
- the email is stored in encrypted form
- contentACCESS is not able to access, display nor fulltext index the email body nor its attachments



Screenshot: An archived RPM email in the mailbox

- contentACCESS can convert the email to shortcut, but it is not recommended (needs to be allowed first by checking the **Allow converting to shortcut** checkbox in [Email archive System settings](#)). If the emails are converted to shortcut, only Outlook users will be able to access the archived email. Mobile and OWA users will not be able to open the email.

To work with archived rights protected messages, the user requires Outlook and an Office 365 account. Outlook automatically decrypts the email when it is opened from **.msg** or **.eml** format.



Screenshot: An RPM email opened



Journal mailbox archiving

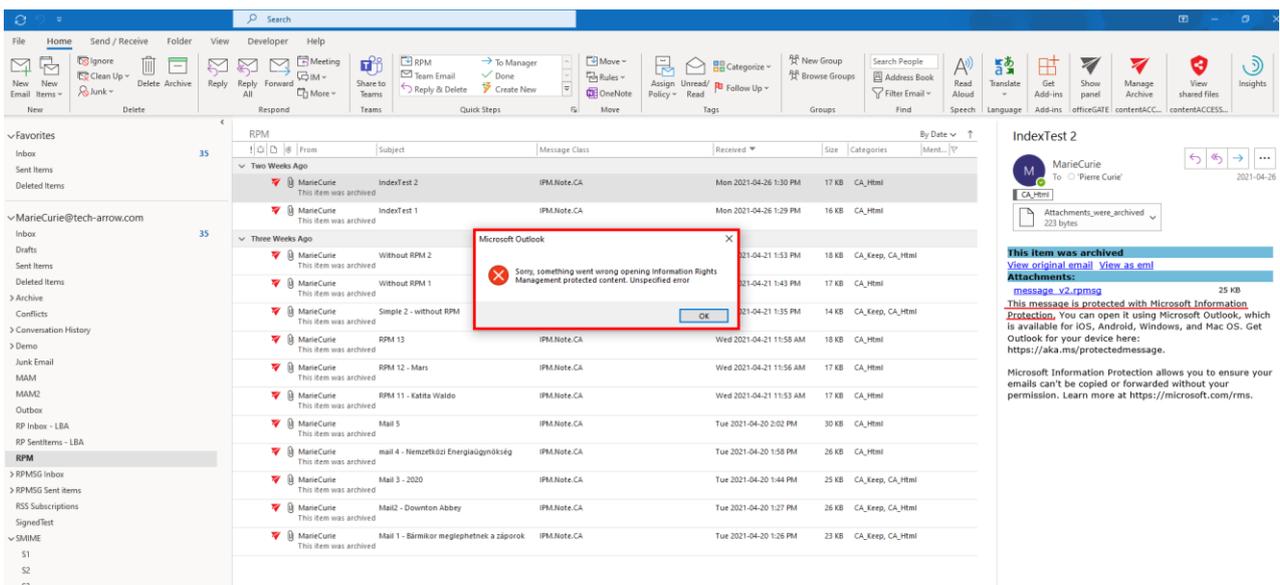
If contentACCESS is archiving the Office 365 journal mailbox (requires a configured contentACCESS SMTP server), contentACCESS is receiving envelope journal message. These envelopes contain the decrypted email alongside the encrypted email. contentACCESS archives **both the encrypted and the decrypted version** of the email. This allows the administrators to search and access the contents of the rights protected emails, but only in the journal mailbox.

Processing settings

- Processing settings:
- Use MAPI to communicate with Exchange Server (Supported only for versions up to Exchange 2013)
 - Use journal archive to build folder structures of mailboxes
 - Archive email if journal didn't archive it yet

Screenshot: Archiving a mailbox as a journal mailbox

The end user still will not be able to access the encrypted emails directly but needs to open them in Outlook for them to be decrypted automatically.

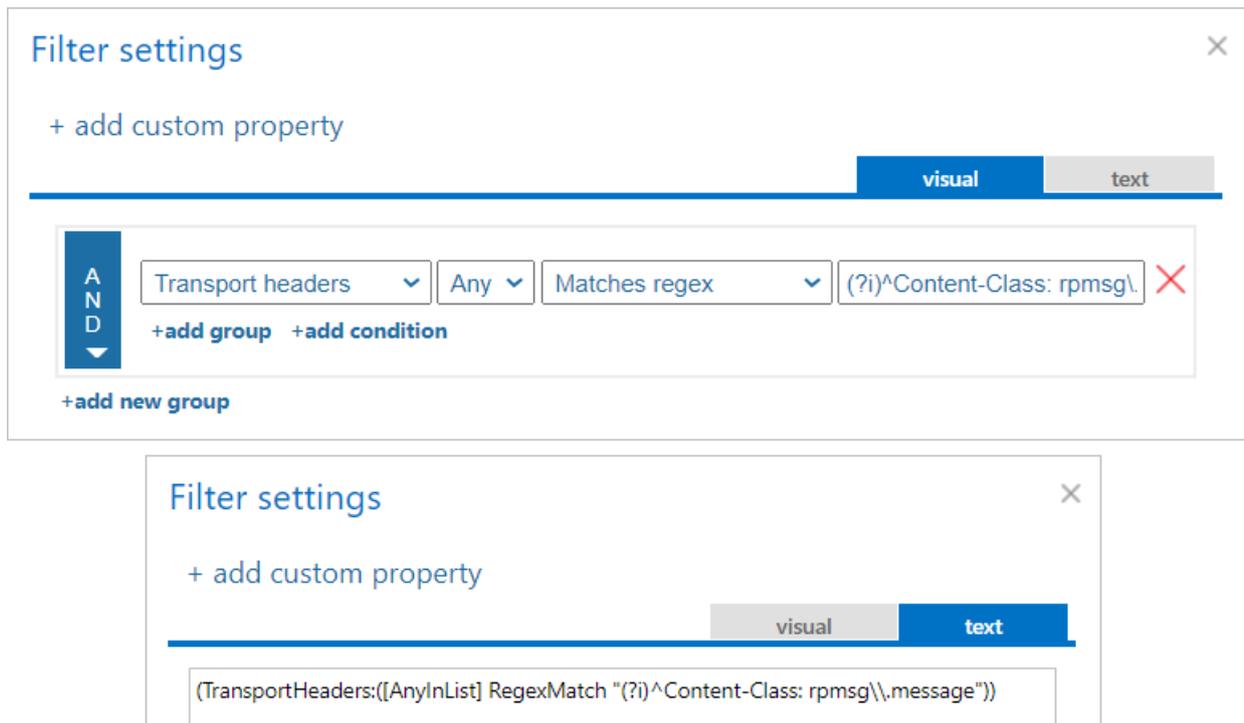


Screenshot: Opening an archived RPM email without the necessary permissions

Configuration

The rights protected messages are archived by contentACCESS archive jobs. If you want to exclude the rights protected emails from archiving, it is necessary to filter out these messages using the following filter:

(TransportHeaders:([AnyInList] RegexMatch "(?i)^Content-Class: rpsmg\\.message"))



Screenshot: Excluding rights protected messages from archiving - both visual and text filtering is shown on the screenshot

The administrator can control the shortcutting of rights protected emails on the **Tenant level**. The shortcut creation is disabled by default and can be enabled in **Email archive -> System settings -> Message class handling** by checking the following checkbox:

Rights protected messages: Allow converting to shortcut

Email archive retention changer job

This job changes the retention time of emails of the selected mailbox(es) if it's allowed to change the retention on storage level. Storages that support this change are: Disk, Azure, Amazon S3.

Go to Jobs -> click on **+new** -> select **Email archive retention changer**.



Add new job instance ✕

Available jobs:

Run on node:

Display name:

Description:

On the job's configuration page go through the following sections:

✓ Running mode settings (mandatory)

The job can be run in 3 modes:

- 1) **Immediate processing** -> collects the emails and changes their retention.

Running mode settings

Run in mode:

- 2) **Create report** -> collects the emails and provides a csv file with a list of emails. The administrator can review and edit the list of affected documents.

Running mode settings

Run in mode:

Generated report file:

File name:	GeneratedRC_12_16_2019 7_42_18 PM.csv
Size:	2.6 KB
Date:	12/16/2019 7:42:18 PM

- 3) **Apply report** -> a csv file with a list of emails to be processed must be uploaded. The administrator can delete emails from the list before running the job (only emails which are in the list will be processed). The job reads the list and changes the retention of the emails that are on the list.



Running mode settings

Run in mode:	<input type="text" value="Apply report"/>
Reviewed report file:	<input type="text" value="Please upload a csv file"/> ...
File name:	GeneratedRC_12_16_2019 7_42_18 PM.csv
Size:	2.6 KB
Date:	12/16/2019
<input type="button" value="Get uploaded file"/>	

✓ Scheduling settings (mandatory)

In this section the running times of the **retention changer job** must be selected. It is possible either to select a scheduler from the list or to create a new scheduler via the **“Create new ...”** option.

Scheduling settings

Scheduled in:	<input type="text" value="Manual"/>
	<input type="button" value="Create new ..."/> <input checked="" type="button" value="Manual"/> <input type="button" value="TaskRunnerScheduler"/>

✓ Retention settings (mandatory)

Select the new retention to be applied for the emails.

Retention settings

Target retention:	<input type="text" value="5Y"/>
-------------------	---------------------------------

✓ Address book objects to process (mandatory)

Here the administrator may select the mailboxes, groups or the entire Exchange server, which will be processed by the **retention changer job**. Click on the  **select** option and check the desired mailboxes, groups or servers in the **Mailbox selection** window, then click on **OK**.

Mailbox selection ✕

 refresh

<input type="checkbox"/>		Name	Type
		<input type="text"/>	<input type="text"/>
<input type="checkbox"/>		TADC01	Server
<input type="checkbox"/>		[blurred]	Group
<input type="checkbox"/>		E [blurred]	Mailbox
<input type="checkbox"/>		S [blurred]	Mailbox
<input type="checkbox"/>		De [blurred]	Mailbox

Important: If an on-premise Exchange group is used in a job configuration, the job configuration needs to be updated after the group is moved to the cloud, since the group identifier changes and the job is still using the old identifier.

Steps to take:

- open job's configuration page
- remove the group from the list of **Address book objects to process**
- select the group and re-add it to the list
- save the job configuration

✓ Include folders (mandatory)

Email retention changer job is crawling the entire mailbox or recursive folder structures from the mailbox for further processing. Before you enter the folder name(s) to be crawled, it is necessary to select the folder filtering type.

Include folders

Folder filtering type: One single folder

- Entire mailbox
- One single folder
- Recursive, starting from a single folder
- Multiple folders
- Multiple recursive, starting from a single folder

If you set **Entire mailbox**, then the whole mailbox including all folders will be processed. If you set **One single folder** type, then only one pre-selected folder will be processed (e.g. if you set %INBOX%\Subfolder1, then only Subfolder1 will be processed). If you set **Recursive, starting from a single folder** filtering type, then all folders starting from the defined folder will be processed (e.g. if you set %INBOX%\Subfolder1, then starting from Subfolder1, every subfolder will be processed in the structure). The same rule applies to the **Multiple folders** and to the **Multiple recursive, starting from a single folder**, too, but in this case we can work with more folders simultaneously (e.g.: %INBOX%, %OUTBOX%\Folder name 5...or...%TASKS%, %CALENDARS%\Folder name 6).

Important: It is highly recommended to specify the root mailbox folders using wildcards (%). Wildcards ensure that the given mailbox folder (e.g. the "INBOX" folder) will be processed, regardless of the language settings of the mailbox. This is important mainly for companies who archive mailboxes using different languages. Subfolders must be added to a root folder with a backslash (\).

Note: It is important to bear in mind that by selecting "Recursive, starting from a single folder" filtering type under "Include folders" section and leaving the folder path textbox empty, the whole selected mailbox will be processed:

Address book objects to process

[select](#)

Name	Type
<input checked="" type="checkbox"/> edit.balazsy	Mailbox

Include folders

Folder filtering type: Recursive, starting from a single folder



✓ Filtering settings (optional)

Click on the **Change filter** button and set the filtering according to your needs and/or regulations. To learn more about how to work with filtering settings, please, check [this](#) section of our documentation.

Filter settings

×

visual text

AND	Creation date	Older than	1Y		
	Creation date	Younger than	2Y		

[+add group](#) [+add condition](#)

[+add new group](#)

OK Cancel

✓ Notification settings (mandatory)

Select here, when you will need to get notification emails from the **Retention changer job**. It is possible to set here if you need a notification email always/never, or you need it only if an error/warning occurred



during the process – for example, if the retention change of one or more items failed, then you may get a notification email about this error. Into the **Recipient list** textbox insert the email addresses of the people whom you would like to send these emails to – if there are multiple recipients, the addresses must be separated by “,” or “;”.

Notification settings

Send when:	<input type="text" value="Errors or warnings occur"/>
Recipient list:	<input type="text" value="walter_white@tech-arrow.com"/>

✓ **Resource settings (mandatory)**

Set the value, which will determine how many items will be processed simultaneously by the **Retention changer job**. The recommended value is 2, as in our case.

Resource settings

Worker thread count:	<input type="text" value="2"/>
----------------------	--------------------------------

At the end never forget to save your job configurations: click on **Save** in the left upper corner of UI.



Email restore job

This job type is used to restore the original mailbox items from the shortcuts back into the mailbox. A restore job relocates the already archived original back into the original location only in case that it was archived with the shortcutting method (i.e. it has a shortcut in the mailbox with the same parameters). The age filter and message class filter settings will be considered as well. If the restore job finds in the source location (mailbox):

1. the original mailbox item – it will not touch it;
2. a shortcut with the same parameters – it will restore the original item to the source folder;
3. nothing (neither a shortcut, nor the original) – nothing will happen, the source folder will remain empty.

There are 2 restore methods that can be used by the restore job. The administrator may decide if

1. the data will be restored to the existing shortcut.
2. a new item will be created and the shortcut will be replaced by this new item.

The default restore method can be set on the [Email archive System settings](#) page (**Email Archive** tab → **Settings** group → **System settings** button, section “**General settings**”).

Restore jobs are run rarely, so it is recommended to set either a “One time scheduler” for them, or to start them manually from the grid.

Email restore job configuration

For this processing type the following sections must be configured:

✓ **Report mode settings:**

If the **Use report mode** checkbox is checked, the job will run in report mode. After the job finishes its run in this mode, the user will be able to download a .csv report file here in this section. The file will contain a list of emails that belong to the entities selected in section **Address book objects to process** of the job and some information to them, including whether they will be processed or not.



Report mode settings

Use report mode:

Generated report file: File name: JobReport_7779b902-c4eb-49f0-b7de-6eed8313a926.csv
 Size: 1.3 KB
 Date: 4/4/2019 3:01:51 PM

Download report

A	B	C	D	E
Subject	SentDate	Sender	Status	Filter
Microsoft logo	4/3/2019 13:50		will be processed	no filter
Indexing 10	8/28/2018 14:48		will be processed	no filter
Indexing 09	8/28/2018 14:47		will be processed	no filter
Indexing 08	8/28/2018 14:47		will be processed	no filter
Indexing 07	8/28/2018 14:46		will be processed	no filter
Indexing 06	8/28/2018 14:38		will be processed	no filter
Indexing 05	8/28/2018 14:38		will be processed	no filter
Indexing 04	8/28/2018 14:38		will be processed	no filter
Indexing 03	8/28/2018 14:38		will be processed	no filter
Indexing 02	8/28/2018 14:37		will be processed	no filter
Indexing 01	8/28/2018 14:35		will be processed	no filter

Screenshot: Report file preview

✓ **Processing settings:**

From the Restore dropdown list, the administrator must choose what will be restored by the Restore job.

There are 3 options:

- Mailboxes
- In-Place Archives
- Mailboxes and In-Place Archives

The administrator may select here if he would like to use MAPI protocol to communicate with the Exchange server. EWS (Exchange Web Services) connection is selected by default if MAPI is not selected here. It is important to know that **O365 Exchange server does not support MAPI connection**. Another requirement to use MAPI is to have Exchange server 2013 or earlier version.

Note: MAPI can be selected only in case **Mailboxes** option is selected in the **Restore** dropdown list, since MAPI is **not supported by In-Place Archive**.



Processing settings

Restore:

Processing settings: Use MAPI to communicate with Exchange Server (Supported only for versions up to Exchange 2013)

✓ Scheduling settings:

In this step the running time(s) of the restore job must be selected. It is possible either to select a scheduler from the list or to create a new scheduler via create new option. Restore jobs are usually scheduled with “one time schedulers”. Our restore job will run on 1st of October, with a start date 6 PM CET and will run until it finishes the restore process. (For more information about how to set schedulers refer to the section “[Schedules](#)” above.)

Scheduling settings

Scheduled in:

✓ Address book objects to process

Here you can select the mailboxes, groups or the entire Exchange server that will be processed by the restore job. In this use case, we will restore the mailbox of “edit.balazsy”, so we select it from the list. To find it, we click on the  **select** option and start to write the mailbox name into the **Mailbox selection** search field:

Note: If the **In-Place Archives** option is selected in the **Restore** dropdown list in **Processing settings**, this warning will pop up for the **Address book objects**. In this case, only servers, groups and In-Place Archive mailboxes can be selected after clicking on the **Select** option.

Address book objects to process

 Only mailboxes having In-Place Archive will be processed.



Mailbox selection

refresh

<input type="checkbox"/>	Name	Type
<input type="checkbox"/>	Office365	Server
<input type="checkbox"/>	techarrow_all	Group
<input type="checkbox"/>	techarrow_sales	Group
<input type="checkbox"/>	Test01	Group
<input type="checkbox"/>	build_notification	Group
<input type="checkbox"/>	elm_team	Group
<input type="checkbox"/>	emailarchive	Group
<input type="checkbox"/>	Administrators notification	Group
<input type="checkbox"/>	TenantAdmins_2092c	Group
<input type="checkbox"/>	HelpdeskAdmins_3ffa9	Group
<input type="checkbox"/>	RIM-MailboxAdmins87a5acd646e1460	Group
<input type="checkbox"/>	Compliance Management	Group
<input type="checkbox"/>	Hygiene Management	Group
<input type="checkbox"/>	Discovery Management	Group
<input type="checkbox"/>	Records Management	Group

Page 1 of 4 (52 items) 1 2 3 4

OK Cancel

Mailbox selection

refresh

<input checked="" type="checkbox"/>	Name	Type
<input checked="" type="checkbox"/>	edit	
<input checked="" type="checkbox"/>	edit.balazsy	Mailbox

Begins with((Name),_ed) Clear

OK Cancel

Important: If an on-premise Exchange group is used in a job configuration, the job configuration needs to be updated after the group is moved to the cloud, since the group identifier changes and the job is still using the old identifier.

Steps to take:

- open job's configuration page
- remove the group from the list of **Address book objects to process**
- select the group and re-add it to the list
- save the job configuration

✓ **Include folders:**

Email restore job is crawling the entire mailbox or recursive folders from the mailbox. Before you enter the folder name(s) to be crawled, it is necessary to select the folder filtering type.



Include folders

Folder filtering type:

One single folder

Entire mailbox

One single folder

Recursive, starting from a single folder

Multiple folders

Multiple recursive, starting from a single folder

If you set **Entire mailbox**, then the whole mailbox including all folders will be restored. If you set **One single folder** type, then only one pre-selected folder will be processed (e.g. if you set %INBOX%\Subfolder1, then only Subfolder1 will be processed). If you set **Recursive, starting from a single folder** filtering type, then all folders starting from this folder will be processed (e.g. if you set %INBOX%\Subfolder1, then starting from Subfolder1 every subfolder will be processed in the structure). The same rule applies to the **Multiple folders** and to the **Multiple recursive, starting from a single folder**, too, but in these cases we can work with more folders simultaneously (e.g.: %INBOX%, %OUTBOX%\Folder name 5...or...%TASKS%, %CALENDARS%\Folder name 6).

Important: Due to different language settings in the user mailboxes, it is highly recommended to specify the root folders using wildcards (%). Subfolders must be added to a root folder with a backslash (\).

How to restore the whole mailbox? It is important to bear in mind that by selecting “Recursive, starting from a single folder” filtering type under “Include folders” section and leaving the folder path textbox empty, the whole selected mailbox will be restored:

Address book objects to process

select

Name	Type
edit.balazsy	Mailbox

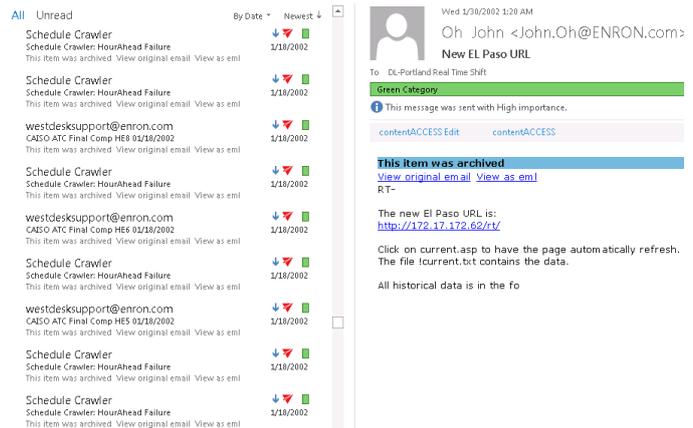
Include folders

Folder filtering type:

Now we will restore the content of single folder “Subfolder 1” on the “INBOX” root (check screenshot).



Screenshot A: Folder filter of the restore job



Screenshot B: Content of "Subfolder 1" before restore

✓ Exclude folders

With this function, you may set which folders/subfolders should not be restored. The same rules apply for the restore job as for the archive job. The folders may be

- a) **added (via the + new option)** as it is described in the Email archive job configuration or
- b) **imported (via the import option).**

To learn more about these settings refer to chapter [Importing contentACCESS configurations from files](#) of this guide.

Exclude folders

- a) + new
- b) ↶ import

Important: Due to different language settings in the user mailboxes, it is highly recommended to specify the root folders using wildcards (%). Subfolders must be added to a root folder with a backslash (\).

✓ Filtering settings

Click on the **Change filter** button and set the filtering according to your needs and/or regulations. To learn more about how to work with filtering settings, please, check [this](#) section of our documentation.

Filter settings ✕

visual
text

AND	Sent date ▼	> ▼	10M	📅 ✕
	Importance ▼	Equals ▼	High ▼	✕
	Body ▼	Contains ▼	Microsoft	✕
+add group +add condition				
+add new group				

OK
Cancel

- ✓ **Notification settings.** The user may select here, when to send notification emails from the restore job regarding the successfulness of the restore process. It is possible to set here if you need a notification email always/never, or you need it only in case when an error/warning occurred during the restoring process. Into the **Recipient list** textbox insert the email address(es) of the person(s), whom such notifications will be sent to. Notification emails may be useful if the **System logs** feature is not used to detect possible failures of job running.

Notification settings

Send when:	<input style="width: 100%;" type="text" value="Never"/>
Recipient list:	<input style="width: 100%;" type="text" value="john.doe@example.com,peter.white@example.com,..."/>



- ✓ **Resource settings.** Set the value, which will determine how many items will be processed simultaneously by the email archive job. The recommended value is “2”.
- ✓ **Save your changes!**
- ✓ **Wait until the job starts to run according to the schedule.** If the job finished processing, the shortcuts linking to the matching items will be replaced by originals in your “Subfolder 1” folder.

Email restore job description

All the numbers and descriptions in the job’s progress have a particular meaning. In this section, we are going to explain the numbers and descriptions of an **Email restore job**.

Description	Explanation
x mailboxes processed	x mailboxes were finished by the job
(y failed)	y mailboxes failed (out of the x mailboxes)
x emails restored	x shortcuts were restored
(x folders skipped)	x folders were skipped from the processing because of exclude folder settings
(x skipped)	x emails have been skipped because of filtering
(x failed)	x emails failed to restore

Email recovery job

The function of this job is to re-generate the Exchange mailbox from the archive. This processing type is useful in the following cases:

- The entire mailbox was deleted,
- One or more folders were deleted,
- One or more items were deleted,

and the user would like to get back these already archived items from the archive storage.



The mailbox recovery is able to reconstruct the mailbox from the archive: the items that were already archived will be put back to the mailbox exactly into the source location. The mailbox recovery will also create the folder if it no longer exists in the mailbox. It will try to keep the folder type as well (if the information is available in the archive). Since all filtering options are active, it is possible to recover any part of the mailbox:

- One folder
- Multiple folders
- Recursive folder structure
- Whole mailbox (structure)
- Mails older than/Younger than/Between dates ...
- Different message classes (mails, documents, contacts etc.)

This processing type is also checking for duplicates, (so it is safe to run the same job multiple times, as duplicates will not be created):

- If there is a shortcut (for the recovered mail) in the folder – the mail will not be recovered.
- If the same mail is already in the folder – the mail will not be recovered.
- If the same mail was archived multiple times to the same folder (archive-restore-archive) – only the youngest mail will be recovered.

Note: It is important to bear in mind that duplicate checking is active only on folder level. Mails without internet message ID might be duplicated.

Note: There are also some limitations of the recovery technology, namely:

- Contacts can be recovered only into a contacts folder;
- Appointments can be recovered only into an appointment folder;
- Tasks can be recovered only into a tasks folder.

To create a new Email system recovery job, click on **+ new** on the page of the email archive jobs. The **Add new job instance** dialog opens. Select “Email recovery” from the dropdown list, enter the job’s name, select a node where it should run and click **OK**.



Add new job instance ✕

Available jobs:

Run on node:

Display name:

Description: Re-create mailbox hierarchy from archive. Use this job if you have lost the full or part of the mailbox and want to recover the archived mails to the original mailbox.

Email recovery job configuration

On the job’s configuration page the user is required to configure the following settings:

✓ **Report mode settings:**

If the **Use report mode** checkbox is checked, the job will run in report mode. After the job finishes its run in this mode, the user will be able to download a .csv report file here in this section. The file will contain a list of emails that belong to the entities selected in section **Address book objects to process** of the job and some information to them, including whether they will be processed or not.

Report mode settings

Use report mode:

Generated report file: File name: JobReport_7779b902-c4eb-49f0-b7de-6eed8313a926.csv
Size: 1.3 KB
Date: 4/4/2019 3:01:51 PM

A	B	C	D	E
Subject	SentDate	Sender	Status	Filter
Microsoft logo	4/3/2019 13:50		will be processed	no filter
Indexing 10	8/28/2018 14:48		will be processed	no filter
Indexing 09	8/28/2018 14:47		will be processed	no filter
Indexing 08	8/28/2018 14:47		will be processed	no filter
Indexing 07	8/28/2018 14:46		will be processed	no filter
Indexing 06	8/28/2018 14:38		will be processed	no filter
Indexing 05	8/28/2018 14:38		will be processed	no filter
Indexing 04	8/28/2018 14:38		will be processed	no filter
Indexing 03	8/28/2018 14:38		will be processed	no filter
Indexing 02	8/28/2018 14:37		will be processed	no filter
Indexing 01	8/28/2018 14:35		will be processed	no filter

Screenshot: Report file preview

✓ Processing settings

In this section, the user configures what will be recovered and how it will be recovered:

Process

From the Process dropdown list, the administrator must choose what will be recovered by the Recovery job. There are 3 options:

- Mailboxes
- In-Place Archives
- Mailboxes and In-Place Archives

Processing settings

Connection: Use MAPI to communicate with Exchange Server (Supported only for versions up to Exchange 2013)

Process: **In-Place Archives**

Recover In-Place Archive items to: Mailboxes

Recover: **In-Place Archives**

What to do: Mailboxes and In-Place Archive

What to recover: Last known version

Shortcut processing type: Recover original

If **In-Place Archives** or **Mailboxes and In-Place Archives** is selected, the administrator must choose where the In-Place Archive items will be recovered to. There are 2 options:

- In-Place Archive
- Mailbox

Processing settings

Connection: Use MAPI to communicate with Exchange Server (Supported only for versions up to Exchange 2013)

Process: In-Place Archives

Recover In-Place Archive items to: **In-Place Archive**

Recover: Mailbox

What to do: **In-Place Archive**

What to recover: Last known version

Shortcut processing type: Recover original

Note: If you are recovering emails from **IN-PLACE** archive to **MAILBOX**, the flag "**Is in in-place archive**" might be modified:

- > if recover to the same mailbox and same folder => the flag is removed
- > if recover to the same mailbox but different folder => the flag is NOT removed
- > if recover to a different mailbox and same folder => the flag is NOT removed
- > if recover to a different mailbox and different folder => the flag is NOT removed

The administrator may select here if he would like to use MAPI protocol to communicate with the Exchange server. EWS (Exchange Web Services) connection is selected by default if MAPI is not selected here. It is important to know that **O365 Exchange server does not support MAPI connection**. Another requirement to use MAPI is to have Exchange server 2013 or earlier version.

Note: MAPI can be selected only in case **Mailboxes** option is selected in the **Recover** dropdown list, since MAPI is **not supported by In-Place Archive**.

Recover – what will be recovered

- **Files and structure** – the recovery job will create the archived folder structure and recover the emails from the archive
- **Structure only** – the recovery job will create the archived folder structure, but no emails will be recovered

Processing settings

Connection:	<input type="checkbox"/> Use MAPI to communicate with Exchange Server (Supported only for versions up to Exchange 2013)
Process:	Mailboxes
Recover:	Items and structure
What to do:	Items and structure
What to recover:	Structure only
Shortcut processing type:	Recover original

What to do

- **Recover items not in the target folder** – only the non-existing emails can be recovered

What to recover

- **Last known version** – the job will recover the latest version of the item from archive



- **Version at specific date** – the job will recover the version that was valid at the specific time. It means the version having modification date older or equal to the specific date

Shortcut processing type

- **Recover original** – the job will recover the original email
- **Recover shortcut** – the job will recover the shortcut. If the administrator would need to recover items as shortcuts, then the already configured shortcut selected right here will be used to recover them. If the administrator selected above to recover the original item, this configuration option will be then hidden.

Processing settings

Connection:	<input type="checkbox"/> Use MAPI to communicate with Exchange Server (Supported only for versions up to Exchange 2013)
Process:	Mailboxes
Recover:	Items and structure
What to do:	Recover items not in the target folder
What to recover:	Version at specific date
	09/08/2021 09:58 AM
Shortcut processing type:	Recover shortcut
Shortcut name:	HTML

✓ Scheduling settings

Specify a scheduler to determine, when the recovery job will run. It is possible either to select a scheduler from the list or to create a new scheduler via **Create new** option. (For more information about how to set schedulers refer to the section [Schedules](#) above.) It is recommended to set here a **One time** scheduler, or to start the job manually.

Scheduling settings

Scheduled in: On 7th of Sept

✓ Notification settings

Select here, when you will need to get notifications from the job regarding the successfulness of the recovery process. It is possible to set here, if you will get a notification email always/never, or you get it only in case when an error/warning occurred during the archiving – for example, if the recovery of one or more items failed, then you may get a notification email about this error. Into the **Recipient list** textbox insert the email address(es) of the person(s), to whom these emails should be sent.



Notification settings

Send when:

Recipient list:

✓ **Address book objects to process**

Here you can select the mailboxes, groups or the entire Exchange server, which will be processed by the recovery job. First, click on the **select** option and check the groups or servers in the **Mailbox selection** window, then click on **OK**:

Note: If the **In-Place Archives** option is selected in the **Recover** dropdown list in **Processing settings**, this warning will pop up for the **Address book objects**. In this case, only servers, groups and In-Place Archive mailboxes can be selected after clicking on the **Select** option.

Address book objects to process

Only mailboxes having In-Place Archive will be processed.

Mailbox selection ✕

refresh

<input type="checkbox"/>	Name	Type
<input type="checkbox"/>	<input type="text"/>	<input type="text"/>
<input type="checkbox"/>	Office365	Server ← select the entire server
<input type="checkbox"/>	techarrow_all	Group
<input type="checkbox"/>	techarrow_sales	Group
<input type="checkbox"/>	Test01	Group
<input type="checkbox"/>	build_notification	Group
<input type="checkbox"/>	elm_team	Group ← ... or select group(s)
<input type="checkbox"/>	emilarchive	Group
<input type="checkbox"/>	Administrators notification	Group
<input type="checkbox"/>	TenantAdmins_2092c	Group
<input type="checkbox"/>	HelpdeskAdmins_3ffa9	Group
<input type="checkbox"/>	RIM-MailboxAdmins:87a5acd646e1460	Group
<input type="checkbox"/>	Compliance Management	Group
<input type="checkbox"/>	Hygiene Management	Group
<input type="checkbox"/>	Discovery Management	Group
<input type="checkbox"/>	Records Management	Group

Page 1 of 4 (52 items) ⏪ 1 2 3 4 ⏩

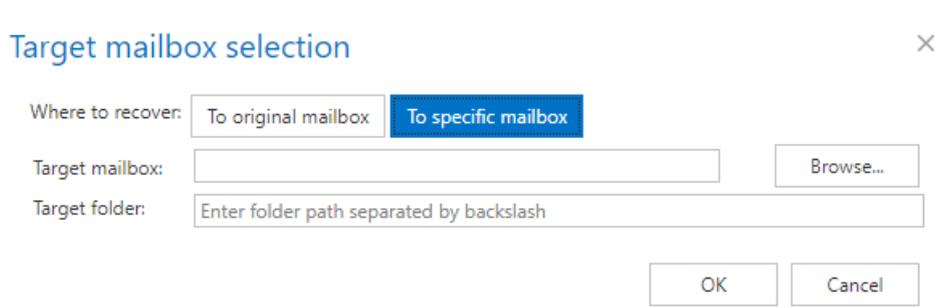
Important: If an on-premise Exchange group is used in a job configuration, the job configuration needs to be updated after the group is moved to the cloud, since the group identifier changes and the job is still using the old identifier.

Steps to take:

- open job's configuration page
- remove the group from the list of **Address book objects to process**
- select the group and re-add it to the list
- save the job configuration

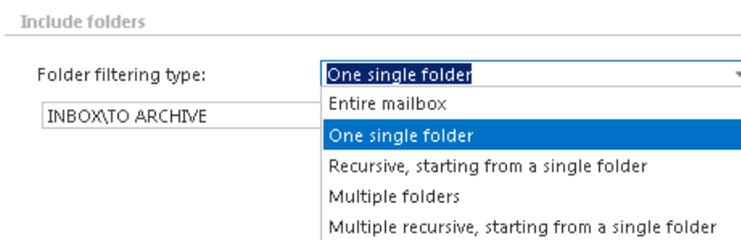
Next, select where the emails from the folder will be recovered:

- **To original location** – items will be recovered to the place where they were archived from. The target folder can be added manually, then click on OK.
- **To specific location** – items can be recovered to a **different folder in the same mailbox**, or to a **different folder in a different mailbox**. Click on the **To specific location** button. A new dropdown list will appear. Here you can select the destination folder for the recovery.



✓ Include folders

Recovery job is able to recover any folders of the mailbox; the entire mailbox, one single folder, multiple folders, recursive folder structures etc. Before you enter the folder name(s) to be crawled, it is necessary to select the folder filtering type.



If you set **Entire mailbox**, then the whole mailbox including all folders will be recovered. If you set **One single folder** type, then only one predefined folder will be processed (e.g. if you set INBOX\Subfolder1, then only Subfolder1 will be processed). If you set **Recursive, starting from a single folder** filtering type, then all folders starting from this folder will be processed (e.g. if you set INBOX\Subfolder1, then starting from

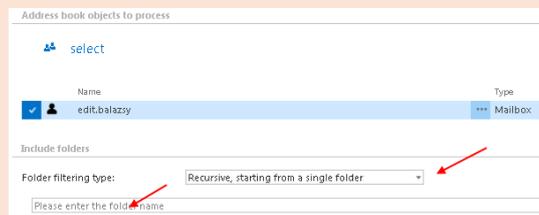


Subfolder1, every subfolder will be processed in the structure). Subfolders must be added to a root folder with a backslash (\).

The same rule applies to the **Multiple folders** and to the **Multiple recursive, starting from a single folder** too, but in this case we can work with more folders simultaneously (e.g.: INBOX, OUTBOX\Folder name 5...or...TASKS, CALENDARS\Folder name 6).

Important!! It is **not required to specify the root folder with wildcards** (percent signs) for the recovery processing type. If any wildcard is specified, the recovery process will not be successful. E.g. instead of %INBOX% use form INBOX, instead of %TASK% use form TASK etc. The same rule applies to **Exclude folder** configurations, too.

How to recover whole mailbox? It is important to bear in mind that by selecting “Recursive, starting from a single folder” filtering type under “Include folders” section and leaving the folder path textbox empty, the whole selected mailbox will be recovered:



✓ Exclude folders

With this function you may set, which folders/subfolders should not be recovered. The folders that should not be recovered may be

- a) Added via the “+ new” button – The settings are the **same as for the Email archive job with ONE EXCEPTION:** for the Email recovery job you can't use %INBOX% to use the language independent default folders.
- b) Imported from a file via the **import** button - For more information refer chapter [Importing contentACCESS configurations from files](#) of this guide.



Exclude folders

a) + new b) ↶ import

✓ Filtering settings

Click on the **Change filter** button and set the filtering according to your needs and/or regulations. To learn more about how to work with filtering settings, please, check [this](#) section of our documentation.

Filter settings

×

visual text

AND	Sent date	>	10M	📅	×
	Importance	Equals	High		×
	Body	Contains	Microsoft		×

+add group +add condition

+add new group

OK Cancel



- ✓ **Resource settings.** Set the value, which will determine how many items will be processed simultaneously by the recovery job. The recommended value is “2”.
- ✓ **Save your changes!!**
- ✓ **Wait until the scheduler starts the job.**

Email recovery job description

All the numbers and descriptions in the job’s progress have a particular meaning. In this section, we are going to explain the numbers and descriptions of an **Email recovery job**.

Description	Explanation
x mailboxes processed	x mailboxes were finished by the job
(y failed)	y mailboxes failed (out of the x mailboxes)
x emails recovered	x emails were recovered
(x recoveries failed)	x emails failed to recover
(x existing mails)	x emails have been skipped because a shortcut is already in the folder
(x filtered out)	x emails were skipped because of filter
(x folders skipped)	x folders were skipped from the processing because of folder exclude settings

Configuration of Delete job in Email archive

This job type deletes data, which have been archived, from the archive.

Note: First, you need to mark files/emails for delete in contentWEB (read more in [this](#) section).

Go to Jobs -> Add new -> Delete from archive.

Add new job instance ✕

Available jobs:

Run on node:

Display name:

Description: Removes the documents from the archive, with expired retention time.

On the job's configuration page go through the following sections; most of them are mandatory, filtering settings are optional:

✓ Running mode settings

The job can be run in 3 modes:

- 1) **Immediate deletion** -> collects the expired documents and deletes them.

Running mode settings

Run in mode:

- 2) **Create report** -> collects the expired documents and provides a csv file with a list of documents. The administrator can delete documents from the list.

Running mode settings

Run in mode:

Generated report file:

File name:	Generated_8_3_2017 7_27_25 PM.csv
Size:	120 B
Date:	8/3/2017 7:27:25 PM

- 3) **Apply report** -> a csv file with a list of documents to be deleted must be uploaded. The administrator can delete documents from the list before running the job (only documents which are in the list will be processed). The job reads the list and if the documents are expired, deletes them.



Running mode settings

Run in mode:

Reviewed report file: ...

File name: Generated_8_3_2017 7_27_25 PM.csv
 Size: 120 B
 Date: 8/3/2017

✓ **Address book objects to process**

Here the administrator may select the mailboxes, groups or the entire Exchange server, which will be processed by the delete job. Click on the **select** option and check the desired mailboxes, groups or servers in the **Mailbox selection** window, then click on **OK**.

Mailbox selection ✕

refresh

		Name	Type
<input type="checkbox"/>		<input type="text"/>	<input type="text"/>
<input type="checkbox"/>		TADC01	Server
<input type="checkbox"/>		<input type="text"/>	Group
<input type="checkbox"/>		Eva E <input type="text"/>	Mailbox
<input type="checkbox"/>		Silvia <input type="text"/>	Mailbox
<input type="checkbox"/>		Denisa <input type="text"/>	Mailbox



Important: If an on-premise Exchange group is used in a job configuration, the job configuration needs to be updated after the group is moved to the cloud, since the group identifier changes and the job is still using the old identifier.

Steps to take:

- open job's configuration page
- remove the group from the list of **Address book objects to process**
- select the group and re-add it to the list
- save the job configuration

✓ **Processing settings**

In this section, you may check the **Delete even if not marked for delete** checkbox. If you do so, the **Delete job** will delete the expired item without them needing to be marked for delete.

Processing settings

Delete even if not marked for delete:

✓ **Filtering settings**

Click on the **Change filter** button and set the filtering according to your needs and/or regulations. To learn more about how to work with filtering settings, please, check [this](#) section of our documentation.

Filter settings ✕

visual
text

AND	Sent date ▼	> ▼	10M	📅 ✕
	Importance ▼	Equals ▼	High ▼	✕
	Body ▼	Contains ▼	Microsoft	✕
+add group +add condition				
+add new group				

OK
Cancel

✓ Notification settings

Select here, when you will need to get notification emails from the Delete job. It is possible to set here if you need a notification email always/never, or you need it only if an error/warning occurred during the process – for example, if the deletion of one or more items failed, then you may get a notification email about this error. Into the **Recipient list** textbox insert the email addresses of the people whom you would like to send these emails to – if there are multiple recipients, the addresses must be separated by “,” or “;”.



Notification settings

Send when:	Errors or warnings occur
Recipient list:	walter_white@tech-arrow.com

✓ Resource settings

Set the value, which will determine how many items will be processed simultaneously by the delete job. The recommended value is 2, as in our case.

Resource settings

Worker thread count:	2
----------------------	---

At the end never forget to save your job configurations: click on **Save** in the left upper corner of UI.

When does the document expire?

Retention repository ✕

Retention name:	<input type="text" value="1 year"/>
Description:	<input type="text" value="1 year"/>
Calculated from:	<input type="text" value="Reference date"/>
Protected retention time in months:	<input type="text" value="12"/>
<input checked="" type="checkbox"/> Has unprotected retention time	
Unprotected retention time in months:	<input type="text" value="12"/>

- 1) **If the protected retention has expired** (archive date / reference date + protected retention is in the past) and the document is not under legalhold and the document is marked for deletion
- 2) **If the unprotected retention is defined and has expired** (archive date / reference date + unprotected retention is in the past)



Email delete job description

All the numbers and descriptions in the job's progress have a particular meaning. In this section, we are going to explain the numbers and descriptions of an **Email delete job**.

Description	Explanation
x mailboxes scanned	x mailboxes have been scanned for deletable documents
(x failed)	x mailboxes failed to process
(x warning)	x mailboxes finished with warnings
x documents purged	x documents have been purged, or if the job ran in report mode x documents have been added to the report
x skipped	x documents skipped, or in case of report mode x documents have not been added to the report because of the filtering settings
x failed	x documents' deletion failed

Journal post processing job

The journal post processing job processes the mailboxes marked as **Process as journal**.

View address book
Email Archive > Archive > View address book

Mailboxes Public folders Groups Servers

import mailboxes manually + add mailbox manually

Name	Email	Create contentWEB access	Associate with role	Enable mail app	Archive database	Store	Active	Server name	Disconnected	Process as journal	Warning	Index zone
edit.balazy	edit.balazy@tech-arrow.com	Inherit		Inherit	MNEtestDB	TestingStorage	Yes	TADC01	No	Yes		Default index zone
PNE	*** PNE@ta.internal	Enable	Inherit	Inherit			Yes	TADC01	No	Yes		
ANE	*** ANE@ta.internal	Enable	Full_EAUser	Enable	MNEtestDB	TestingStorage	Yes	TADC01	No	Yes		Default index zone
ZNE	*** ZNE@ta.internal	Inherit		Inherit			Yes	TADC01	No	Yes		
ONE	*** ONE@ta.internal	Inherit		Inherit	MNEtestDB	TestingStorage	Yes	TADC01	No	No		
dne	*** dne@ta.internal	Enable	Inherit	Enable	MNEtestDB	TestingStorage	Yes	TADC01	No	No		Default index zone

It is reading all emails from the mailbox(es) selected in the section **Address book objects to process** of the job. It checks the recipients of the email (To, Cc, Bcc) and if the recipient mailbox is present in the [Address](#)



[book](#), the mail is duplicated into that mailbox. The group membership is also resolved - when the recipient is a group, the mails are duplicated into the mailboxes of the group.

Important: The duplicating is based on the **actual** group membership = not checking if the user was a member of the group when the email was sent.

The job uses bookmarking - if an email has been already processed, it will not be processed again, even if there are new mailboxes provisioned. To duplicate the already processed emails to the newly provisioned mailboxes, the bookmark has to be deleted from the database table `[JOURNAL_POSTPROCESSING_SETTINGS]`.

Journal post processing job configuration

Go to Jobs -> Add new -> Journal post processing.

Add new job instance
×

Available jobs:

Run on node:

Display name:

Description: Creates duplicates from the journal mailbox emails.

On the job's configuration page go through the following sections:

✓ **Scheduling settings**

In this step, the running time(s) of the job must be selected. It is possible either to select a scheduler from the list or to create a new scheduler via **create new ...** option from the dropdown list.

✓ Address book objects to process

Here the administrator may select the mailboxes that will be processed by the job. Only the mailboxes marked as **Process as journal** are listed in the selection dialog. Click on the  **select** option and check the desired mailboxes in the **Mailbox selection** window, then click on **OK**.

Mailbox selection ✕

 refresh

<input type="checkbox"/>		Name	Type	Email address
<input checked="" type="checkbox"/>		ZNE. [redacted]	Mailbox	ZNE@ta.internal
<input type="checkbox"/>		ANE. [redacted]	Mailbox	ANE@ta.internal
<input checked="" type="checkbox"/>		PNE. [redacted]	Mailbox	PNE@ta.internal
<input type="checkbox"/>		edit.balazsy	Mailbox	edit.balazsy@tech-arrow.com

✓ Notification settings

Select here, when you will need to get notification emails from the job. It is possible to set here if you need a notification email always/never, or you need it only if an error/warning occurred during the process. Into



the **Recipient list** textbox insert the email addresses of the people whom you would like to send these emails to – if there are multiple recipients, the addresses must be separated by “,” or “;”.

Notification settings

Send when:

Recipient list:

✓ Resource settings

Set the value, which will determine how many items will be processed simultaneously by the job. The recommended value is 2, as in our case.

Resource settings

Worker thread count:

At the end never forget to save your job configurations: click on **Save** in the left upper corner of UI.

Mailbox move job

This job allows to move archived mailbox data (archived emails) between stores and databases.

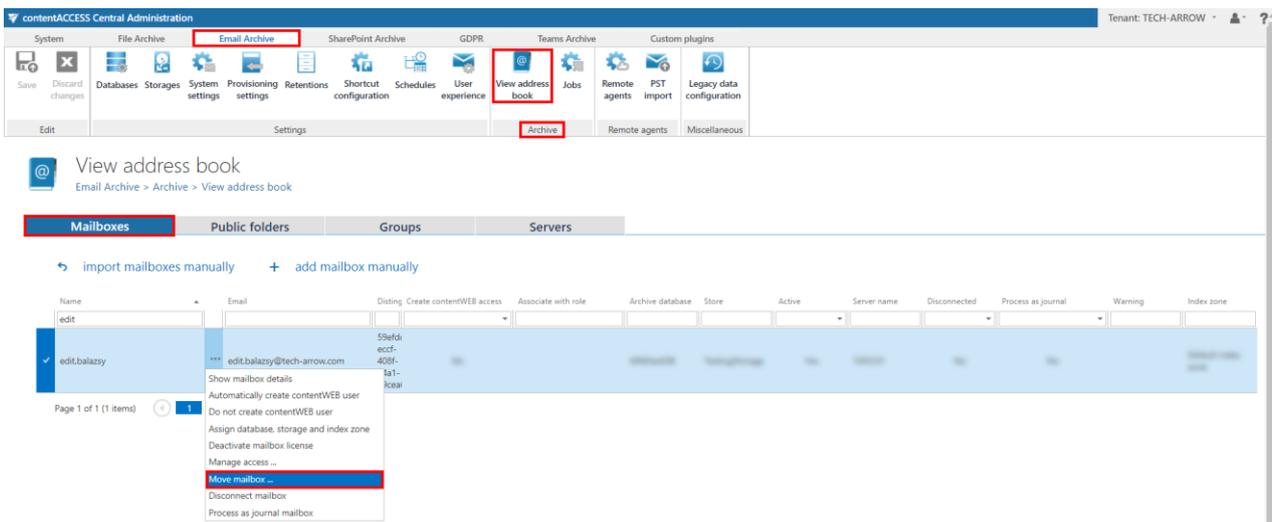
Typical use cases:

- **If you did a mistake and you've archived the same mailbox into 2 different databases**, then you will be able to access only the archived items of the actually associated database (configured in **Email Archive → Archive → View address book**). You can easily troubleshoot such a problem with using the “consolidate” option of the Move mailbox job. This moves the items from the wrong database to the correct one.
- A typical use case of a database/storage move can be if one company **employee was dismissed and his mailbox archive data need to be moved** into another storage/database.
- If the already associated database/storage has **no more storage capacity thanks to the big volume of the archived items**, then the administrator may move the archived mailbox data somewhere else.
- The **mailbox move is also enabled on the level of tenants** (cross-tenant move), e.g. if one company affiliate will be closed and its mailboxes (archived emails) need to be moved into the database/storage of another affiliate (tenant) etc.

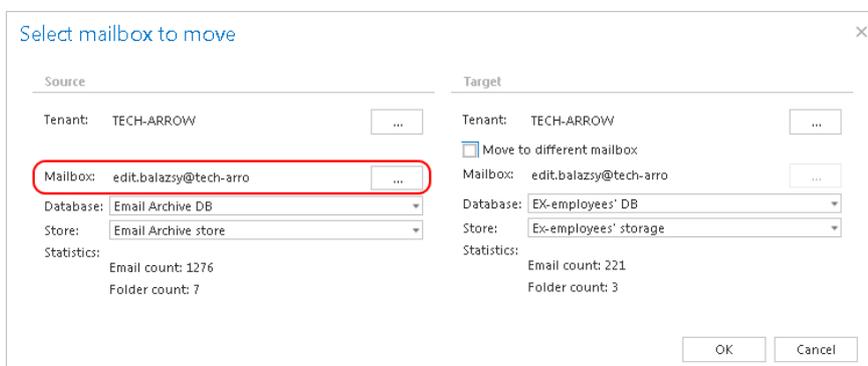


Mailbox move job configuration

There are multiple options how a mailbox move job can be created; you can add it as a new job from the Email archive's **Jobs** page or you can create a mailbox mover job directly from the address book by selecting the "Move mailbox" option from the desired mailbox's context menu. On the screenshot below it is possible to see how a mailbox move job is created for mailbox "edit.balazsy@tech-arrow.com" directly from the address book.



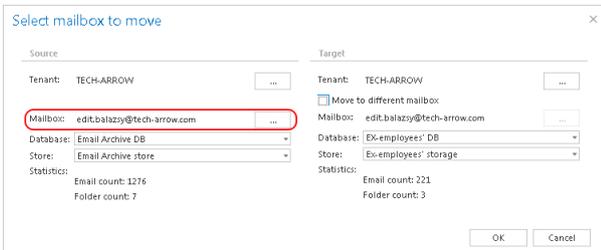
By clicking on the "Move mailbox" option in the mailbox's context menu, the **Select mailbox to move** dialog will automatically open. The desired source mailbox will be already preselected in this dialog. The new mailbox mover job will be created with the name of the selected mailbox. By default, the job will be able to run on any available node.



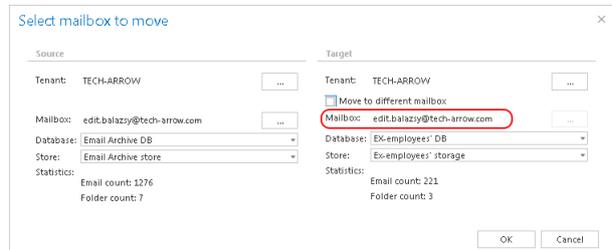
Note: The same dialog can be opened on the job’s configuration page, with clicking on “add” under **Mailboxes to move** section.

In the **Select mailbox to move** dialog the administrator may set the following:

- A) The source mailbox containing the archived data to be moved: if the job has been created from the address book, the source mailbox will be preselected; if the job has been created from the jobs page, the source mailbox has to be configured manually.
- B) The target mailbox; in special cases the archived data of the source mailbox may be moved to a target mailbox archive. To achieve this, check the “Move to different mailbox” option on the target side and specify a new target mailbox. If you would not like to move the source mailbox archive data to a target mailbox archive, select the source mailbox on the target side, too (by default it is configured like this).



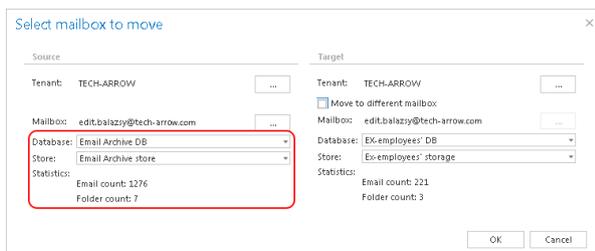
Screenshot A



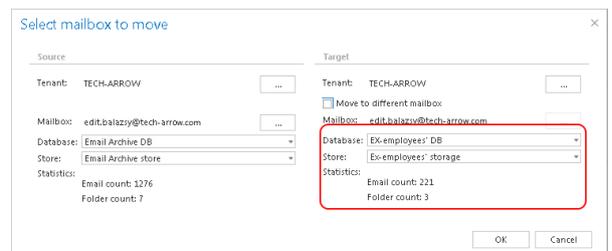
Screenshot B: Source mailbox archive selected on the target side

- C) The source database and storage: by default the already associated database and storage of the source mailbox are set here. The source mailbox statistics (email count, folder count) can be seen in the source column.

- D) The target database and storage: the user may select here the target destinations, where the archived data of the source mailbox should be moved. On Screenshot D we have selected Ex-employees’ DB and Ex-employees’ storage. The target mailbox statistics (email count, folder count) can be seen in the target column as well.

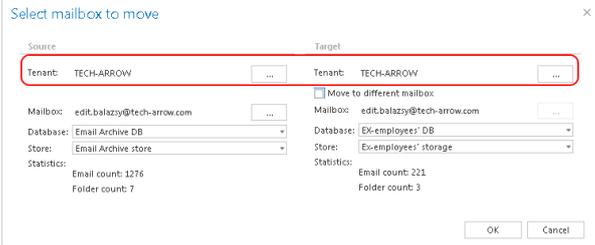


Screenshot C: Associated DB and store



Screenshot D: Target DB and store

E) An across tenant move is also supported:



You have some configuration options - based on them the behavior of the Mailbox move job will change.

If you:

- **Select DIFFERENT databases but the same store**, then the records will be moved (copied and then deleted) from the source database into the new target one, but the binary will be kept in the same store
- **Select same databases but DIFFERENT store**, then the records in the database will be updated only with the new storeID. The source storage data will be copied into the new storage and the old files will be removed from the source store if the source store supports deletion. Deletion is actually supported in Disk store and HybridStore. If the store does not support deletion, then the binary will be kept in the source store
- **Select DIFFERENT database and DIFFERENT store**, then the combination of the above will happen, so the database records and binaries will be moved.
- **Move into different mailbox**, then the original mailbox record will also be deleted from the database if all entries were successfully moved.

When configuring a Mailbox move job the administrator is also required to set the running time of the job, notification settings and the resource settings on the job's configuration page:

✓ **Scheduling settings:** the administrator may select a scheduler from the dropdown list, which will determine when the moving process will run. For this plugin type it is recommended to set one time scheduler, or to start the job manually. For more information about how to set up schedulers please refer to section [Schedules](#).





- ✓ **Notification settings:** if you want to use notification emails to be informed about potential failures of the mailbox move process, then select a) in which cases such notifications need to be sent, b) who will be the recipient of such emails. It is recommended to set here **Errors or warning occur** option (or to check the job events on the **System logs** page).

Notification settings

Send when:	Errors or warnings occur
Recipient list:	x.y@tech-arrow.com

- ✓ **Resource settings.** Set the value, which will determine how many items will be processed simultaneously by the mailbox move job.

Option “consolidate” on the job’s configuration page: Consolidation option is the fastest way of correcting your mistake if you have archived the same mailbox into multiple databases. By clicking the consolidate button, the system will find all mailboxes, which are in two or more databases, and will list them on the **Mailbox selection** page. The target database/target store are the already assigned ones based on the **View address book**. So, once you have the list, you just select one or more mailboxes and click **OK**.

Mailbox selection

<input type="checkbox"/>	Email Address	Source Database Id	Target Database Id	Target Store Id	Message
<input checked="" type="checkbox"/>	edit.balazsy@tech-arrow.com	EX-employees' DB	Email Archive DB	Email Archive store	

OK Cancel

If this dialog is empty, it means that all your metadata are in one database only, there is nothing to correct.

How to check if the mailbox move was finished successfully? The user may check on the **System logs** page if the mailbox move job successfully moved the selected mailbox archive to the desired database/storage. To check this, navigate to the email archive jobs’ page on the ribbon (**Email Archive** tab → **Archive** → **Jobs**). Open the context menu of the mailbox move job and click on “Show last logs”. This will redirect the user to the **System logs** page, where the last run of the selected job will be preselected, and the correspondent job events can be viewed.



Mailbox move job description

All the numbers and descriptions in the job's progress have a particular meaning. In this section, we are going to explain the numbers and descriptions of a **Mailbox move job**.

Description	Explanation
x mailboxes processed	x mailboxes were finished by the job
(y failed)	y mailboxes failed (out of the x mailboxes)
x emails moved	x emails were moved
(x recoveries failed)	x emails failed to move
(x filtered out)	x emails were skipped because of filter or because they were already moved
(x folders skipped)	x folders were skipped from the processing because of folder exclude settings

Shortcut synchronization job

The shortcut synchronization is a process of keeping live emails in sync with the archive.

When an item is archived, the item location is stored in the archive. The user can later delete, move or copy the archived item in the mailbox – but the archive does not follow these changes.

The main function of shortcut synchronization is to update the location of the item in the archive based on the current location of the item in the live mailbox. Secondary functions of the shortcut synchronization are:

- Detection of foreign shortcuts and restoration of such items
- Shortcut cleanup – removal of expired shortcuts
- Inactive folders – marking the missing folders as inactive (displayed with a grey color in contentWEB)



To start the shortcut synchronization, the prerequisites are the following:

- **Configured Email Archive** (based on the Email Archive settings described [here](#))
- **The mailbox must be assigned to a store and database**
Details: If the mailbox is not assigned to a database, the following error message will be logged:
x mailboxes synchronized (1 failed), 0 shortcuts updated (xx folders skipped, xx unchanged)
The **System logs** will contain the following error: *Unable to open database as it is not configured!*
- **Configured Shortcut synchronization job**

Note: If the shortcut synchronization needs to restore a shortcut, the globally defined restore method will be used (which is either an in-place restore or restoring using a new item). These settings are defined in the [Email Archive System settings](#) described earlier.

Shortcut synchronization job configuration

Create a new job instance and open its configuration page. In this use case we will create a configuration job with name “My sync job” that will synchronize Jack Bolton’s archive. We know that some shortcuts in this user’s mailbox have been moved to another mailbox folder. The job will update the location of these items in the archive, based on the location of the shortcuts in the mailbox. In this example the job will run only once.

The configuration of this job consists of the following sections:



contentACCESS Central Administration Tenant: TECH-ARROW

System | File Archive | Email Archive | SharePoint Archive | GDPR | Teams Archive | Custom plugins

Save | Discard changes | Databases | Storages | System settings | Provisioning settings | Retentions | Shortcut configuration | Schedules | User experience | View address book | Jobs | Remote agents | PST import | Legacy data configuration

Edit | Settings | Archive | Remote agents | Miscellaneous

Shortcut synch

Email Archive > Archive > Jobs > Shortcut synch

start immediately | refresh | disable auto refresh | deactivate job | logs | edit

Status: Idle
Progress:

Scheduling settings

Scheduled in: Manual

Notification settings

Send when: Never
Recipient list: john.doe@example.com, peter.white@example.com

Processing settings

Use MAPI to communicate with Exchange Server (Supported only for versions up to Exchange 2013)

Allow to update folder path based on shortcut location

Allow to clean up orphaned shortcuts

Allow to restore foreign shortcuts

Clean up empty folders

Allow to update folder permissions

Allow to update items

Allow item maintenance

Allow to mark deleted emails as inactive

Move unknown shortcuts to folder: UnknownShortcuts

Address book objects to process

select

Name	Type
TADC01	Server

Include folders

Folder filtering type: Entire mailbox

Exclude folders

+ new | import

Pattern

No data to display

Resource settings

Worker thread count: 2

[Online help](#)

- **Scheduling setting:** Defines the time slots of the job run. Our synchronization job will run only once, so we have configured a one time running scheduler for that. For more information about schedulers refer to section [Schedules](#).
- **Notification settings:** In case that you want to get notification emails if any errors or warnings occurred, you can set it here.
- **Processing settings:** The processing settings specify the functions that should be executed inside one job. Performing multiple functions inside one job is optimizing the Exchange access: the mailbox is read only once, but multiple functions are performed on the same set of data.

Important: Processing of **In-Place archive mailboxes** is allowed by default.

- It is possible to use MAPI instead of EWS.



- The “Allow to update folder path based on shortcut location” checkbox turns on/off the folder path synchronization.
- The “Allow to clean up orphaned shortcuts” checkbox turns on/off the function that deletes shortcuts, which are pointing to emails that were deleted (purged) by the [Delete job](#).
- The “Allow to restore foreign shortcuts” checkbox turns on/off the automatic restore of shortcuts not belonging to the mailbox.
- The “Clean up empty folders” function deletes the empty archive folders in contentWEB.
- The “Allow to update folder permissions” checkbox turns on/off the folder permissions updating.
- The “Allow to update items” function allows the job to detect shortcuts (normal, HTML or keep original) that have been changed and synchronize these changes to the archive.
- The “Allow item maintenance” checkbox turns on/off the function that processes emails and shortcuts that were archived by contentACCESS version older than 3.3 and updates their categories and reply/forward status (without this, they wouldn’t reflect the changes in categories and status).
- The “Allow to mark deleted emails as inactive” function allows the job to compare the shortcuts with the database. If a shortcut is present, but the status in the database is "inactive", the document will be set to "active". If a shortcut is not present in the folder, but the database has it, the document will be set to "inactive". The inactive documents are displayed in [contentWEB](#) the same way as inactive File archive documents.
- The “Move unknown shortcuts to folder” option allows the job to move unknown shortcuts (shortcuts that are not found in contentACCESS and are not purged by the Delete job) to a specified folder in the mailbox. The name of the folder can be set here.

In this use case we set the folder update allowance option only like shown on the picture above.

- **Address book objects to process:** Allows to set the whole Exchange server, Exchange groups or mailboxes to be involved in the job. Click on “select” and search for server, group or mailbox in the pop-up dialog:



Mailbox selection

refresh

<input checked="" type="checkbox"/>	Name	Type
<input type="checkbox"/>	jack	
<input checked="" type="checkbox"/>	jack.bolton	Mailbox

Beginns with[(Name), 'jack'] [Clear](#)

OK Cancel

Important: If an on-premise Exchange group is used in a job configuration, the job configuration needs to be updated after the group is moved to the cloud, since the group identifier changes and the job is still using the old identifier.

Steps to take:

- open job's configuration page
- remove the group from the list of **Address book objects to process**
- select the group and re-add it to the list
- save the job configuration

- **Include folders:** Set the folders (in our use case the entire mailbox) that the job needs to process.
- ✓ **Exclude folders:** Exclude the folders that should not be touched by the synchronization job. The list of folders can be imported from files, too (more information about this option [here](#)). Only folders allowed by the include/exclude filters are processed.

Note: it is recommended to process the entire mailbox to receive the best coverage.

In this case we would not like to exclude any folder from the process, so we can skip these settings.

- ✓ **Resource settings:** The selected mailboxes are processed on multiple threads defined here. Each thread is processing one folder from any mailbox at any time.



Save your settings and wait until the scheduler starts the job (or start it manually from the header bar).

Feature limitations - Multiple copies of the same shortcut

If the user has multiple copies of the same shortcut in the mailbox, the shortcut synchronization will not be able to determine the correct location. In such cases, the last writer will win (the folder which was processed as the last will win).

Email shortcut synchronization job description

All the numbers and descriptions in the job's progress have a particular meaning. In this section, we are going to explain the numbers and descriptions of an **Email shortcut synchronization job**.

Description	Explanation
x mailboxes synchronized	x mailboxes were finished by the job
(y failed)	y mailboxes failed (out of the x mailboxes)
x emails updated	x shortcuts were updated (location updated, properties updated, etc.)
(x failed)	x shortcuts failed to synchronize
(x unchanged)	x shortcuts were skipped because the shortcut is already of the correct type
(x restored)	x foreign shortcuts were restored (because of the settings)
(x shortcuts purged)	x shortcuts were removed because of expiration (settings)
(x marked as inactive)	x shortcuts were marked as inactive because the mailbox no longer contains them
(x marked as active)	x shortcuts were marked as active because the mailbox still contains them (or they were recovered back into mailbox)
(x folders skipped)	x folders were skipped from the processing because of folder exclude settings



(x removed)	x shortcuts were removed because the archive is damaged (special settings)
(x damaged found)	x shortcuts were detected as damaged (special settings)
(x unknown shortcuts moved)	x shortcuts were moved to the "unknown folder" (special settings)

Shortcut repair job

There are situations when mails are archived with a shortcut type which turns out to be incorrect. This is usually because of incorrect planning or bad decisions.

If there are shortcuts already created and they need to be replaced, the Shortcut repair job type can easily solve this problem, while keeping the database and storage size under control.

The shortcut repair job is a mailbox crawler – it scans the live mailboxes and locates contentACCESS shortcuts. It is able to locate all types of shortcuts: Keep original, HTML and Normal shortcuts as well.

The whole mailbox is scanned, but the administrator can define which folders should be included and excluded.

Note: You can't use "%INBOX%" in the Include folders section and use the language independent default folders.

Important: The **Shortcut repair job** will **NOT** take the shortcut settings from **Archive settings override**.

Shortcut repair job configuration

On the job's configuration page the user is required to configure the following settings:

✓ Report mode settings

If the **Use report mode** checkbox is checked, the job will run in report mode. After the job finishes its run in this mode, the user will be able to download a .csv report file here in this section. The file will contain a



list of emails that belong to the entities selected in section **Address book objects to process** of the job and some information to them, including whether they will be processed or not.

Report mode settings

Use report mode:

Generated report file: File name: JobReport_7779b902-c4eb-49f0-b7de-6eed8313a926.csv
 Size: 1.3 KB
 Date: 4/4/2019 3:01:51 PM

Download report

A	B	C	D	E
Subject	SentDate	Sender	Status	Filter
Microsoft logo	4/3/2019 13:50		will be processed	no filter
Indexing 10	8/28/2018 14:48		will be processed	no filter
Indexing 09	8/28/2018 14:47		will be processed	no filter
Indexing 08	8/28/2018 14:47		will be processed	no filter
Indexing 07	8/28/2018 14:46		will be processed	no filter
Indexing 06	8/28/2018 14:38		will be processed	no filter
Indexing 05	8/28/2018 14:38		will be processed	no filter
Indexing 04	8/28/2018 14:38		will be processed	no filter
Indexing 03	8/28/2018 14:38		will be processed	no filter
Indexing 02	8/28/2018 14:37		will be processed	no filter
Indexing 01	8/28/2018 14:35		will be processed	no filter

Screenshot: Report file preview

✓ **Scheduling settings**

In this step the running time(s) of the job must be selected. It is possible either to select a scheduler from the list or to create a new scheduler via create new option.

Scheduling settings

Scheduled in:

✓ **Notification settings**

The user may select here, when to send notification emails from the job regarding the successfulness of the process. It is possible to set here if you need a notification email always/never, or you need it only in case



when an error/warning occurred during the process. Into the **Recipient list** textbox insert the email address(es) of the person(s), whom such notifications will be sent to. Notification emails may be useful if the **System logs** feature is not used to detect possible failures of job running.

Notification settings

Send when:	Never
Recipient list:	john.doe@example.com,peter.white@example.com,

✓ Processing settings

From the **Repair** dropdown list, select what will be repaired by the job. There are 3 options:

- Mailboxes
- In-Place Archives
- Mailboxes and In-Place Archives

There is also the possibility to use MAPI to communicate with the Exchange server by checking the checkbox in this section. This checkbox is available only in case **Mailboxes** are selected in the **Repair** dropdown list.

Processing settings

Repair:	In-Place Archives	
Processing settings:	<div style="border: 1px solid #ccc; padding: 5px;"> <div style="background-color: #f0f0f0; padding: 2px;">In-Place Archives</div> <div style="padding: 2px;">Mailboxes</div> <div style="background-color: #0070c0; color: white; padding: 2px;">In-Place Archives</div> <div style="padding: 2px;">Mailboxes and In-Place Archive</div> </div>	(Supported only for versions up to Exchange 2013)

✓ Repair options

Repair options

Repair shortcuts

i If you specify a filter, it will be applied on the shortcuts, not on the original emails.

Use shortcut for shortcuts, where filter is not set

[\[Change\]](#)

Update reply/forward status icon

Allow to re-archive items (if the items were archived by a different archive server)



Repair shortcuts - the option can be used to completely regenerate the shortcuts with new settings. Set the shortcut type to be applied. In this function it is possible to apply a new type of shortcut for existing shortcuts.

Click on the **Change** button and set the filtering according to your needs and/or regulations. To learn more about how to work with filtering settings, please, check [this](#) section of our documentation.

Filter settings

+ add custom property

visual text

AND	Sent date	Older than	10M		
	Importance	Equals	High		
	Body	Contains	Microsoft		
	Is from In-Place Archi	=	Yes		

+add group +add condition

+add new group

OK Cancel



Update reply/forward status icon – the option should be used if upgrading from older contentACCESS versions to version 3.1. In the 3.1 version the reply/forward status of the mail is reflected into the shortcut icon – there is a different shortcut icon for replied and forwarded mails. If the customer wants to update the existing shortcuts, use this function. The job will search for all Normal and HTML shortcuts which have the incorrect icon and will update them. Please note that this function only makes sense for shortcuts where the message class was changed (i.e. the shortcuts are having a different icon).

Allow to re-archive items – this option should be used if a mailbox was archived with “Keep original” on **one system** and that mailbox was moved to **another domain archived with a different system**. Since the mailbox is on a new Exchange server together with the shortcuts, the new system is skipping the emails archived by old system to prevent compatibility problems. To allow archiving the items again, but on the new system, this option must be checked.

✓ **Address book objects to process**

Here you can select the mailboxes, groups or the entire Exchange server, which will be processed by the job. Click on the  **select** option and check the groups or servers in the **Mailbox selection** window, then click on **OK**:

Note: If the **In-Place Archives** option is selected in the **Repair** dropdown list in **Processing settings**, this warning will pop up for the **Address book objects**. In this case, only servers, groups and In-Place Archive mailboxes can be selected after clicking on the **Select** option.

Address book objects to process

 Only mailboxes having In-Place Archive will be processed.

Mailbox selection ✕

 refresh

<input type="checkbox"/>		Name	Type
<input type="checkbox"/>		Office365	Server ← select the entire server
<input type="checkbox"/>		techarrow_all	Group
<input type="checkbox"/>		techarrow_sales	Group
<input type="checkbox"/>		Test01	Group ↖
<input type="checkbox"/>		build_notification	Group
<input type="checkbox"/>		elm_team	Group ← ... or select group(s)
<input type="checkbox"/>		emailarchive	Group ↘
<input type="checkbox"/>		Administrators notification	Group
<input type="checkbox"/>		TenantAdmins_2092c	Group
<input type="checkbox"/>		HelpdeskAdmins_3ffa9	Group
<input type="checkbox"/>		RIM-MailboxAdmins87a5acd646e1460	Group
<input type="checkbox"/>		Compliance Management	Group
<input type="checkbox"/>		Hygiene Management	Group
<input type="checkbox"/>		Discovery Management	Group
<input type="checkbox"/>		Records Management	Group

Page 1 of 4 (52 items) ⏪ 1 2 3 4 ⏩

Important: If an on-premise Exchange group is used in a job configuration, the job configuration needs to be updated after the group is moved to the cloud, since the group identifier changes and the job is still using the old identifier.

Steps to take:

- open job's configuration page
- remove the group from the list of **Address book objects to process**
- select the group and re-add it to the list
- save the job configuration

✓ **Include folders**



The job is able to process any folders of the mailbox; the entire mailbox, one single folder, multiple folders, recursive folder structures etc. Before you enter the folder name(s) to be crawled, it is necessary to select the folder filtering type.

Include folders

Folder filtering type:

✓ **Exclude folders**

With this function you may set, which folders/subfolders should not be repaired. The folders that should not be repaired may be

- a) Added via the “+ new” button – The settings are the **same as for the Email archive job**.
- b) Imported from a file via the **import** button - For more information refer chapter [Importing contentACCESS configurations from files](#) of this guide.

Exclude folders

a) + new b) ↶ import

✓ **Resource settings**

Set the value, which will determine how many items will be processed simultaneously by the recovery job. The recommended value is “2”.

Resource settings

Worker thread count:

The job will scan the mailbox and repair based on the following logic:

Located shortcut	After repair
Keep original	Not modified
Normal shortcut	HTML



HTML	HTML
Journal shortcut	Not found

Note: The shortcuts are completely re-created with the actual settings.

Email shortcut repair job description

All the numbers and descriptions in the job's progress have a particular meaning. In this section, we are going to explain the numbers and descriptions of an **Email shortcut repair job**.

Description	Explanation
x mailboxes repaired	x mailboxes were finished by the job
(y failed)	y mailboxes failed (out of the x mailboxes)
x emails updated	x shortcuts were updated/repared
(x failed)	x shortcuts failed to repair
(x unchanged)	x shortcuts were skipped because the shortcut is already of the correct type
(x folders skipped)	x folders were skipped from the processing because of folder exclude settings

Public folder archiving

Definition of terms:

Public folder – one folder in the public folder hierarchy

Public folder hierarchy – the tree of all public folders in the organization

Public folder database – special Exchange database (2007, 2010) holding public folders

Public folder mailbox – special Exchange mailbox (2013, 2016) holding public folders

Archive public folder mailbox – contentACCESS representation of public folder (virtual mailbox)

contentACCESS allows to archive public folders in an organization. Individual public folders or folder hierarchies can be archived just as any other mailbox items, and they can be replaced by shortcuts as well.



Archiving the public folders with contentACCESS offers many advantages. You can archive using shortcuts and save storage space, still ensuring quick access to the desired items directly from your mailbox. The items can be restored from shortcuts and they can also be recovered if they have been deleted. You can browse for your public folder items in the archive using contentWEB. User-access to the archived content is comfortable and extremely fast.

contentACCESS is supporting a wide range of Exchange Servers, starting from Exchange 2007 SP1 up to Exchange 2019. Public folders can be hosted on as many servers as desired. Even if the public folders are hosted by multiple servers, contentACCESS treats them as one entity (i.e. one mailbox).

Note: If you have a mixed Exchange environment (e.g. both Exchange 2010 and Exchange 2016) and want to archive public folders, set the highest Exchange server version containing the public folders on the [Email Archive System settings](#) page, in section **EWS settings**. On the same page, in section **General settings**, the **Public folder access** must be set to an email address from the **highest Exchange server containing public folders**.

The default contentACCESS setting is not to archive public folders, because not every organization has public folder on the Exchange server. Public folder archiving must be set individually in **Email Archive → Settings → System settings**, under section **General settings**.

contentACCESS Central Administration Tenant: TECH-ARROW

System File Archive Email Archive SharePoint Archive GDPR Teams Archive Custom plugins

Save Discard changes Databases Storages System settings Provisioning settings Retentions Shortcut configuration Schedules User experience View address book Jobs Remote agents PST import Legacy data configuration

Edit Settings Archive Remote agents Miscellaneous

System settings

Email Archive > Settings > System settings

Database settings

Database connection: PROD-FULTEXTDEMOCA-SQLDB

Exchange connection settings

Exchange server type: Exchange Online (O365)
 Region: Global
 Exchange server interface version: Exchange 2016 or higher

EWS Url: https://outlook.office365.com/EWS/Exchange.asmx
 Use impersonation:
 EWS authentication mode: Basic

PowerShell Url: https://ps.outlook.com/PowerShell
 PowerShell auth: Basic
 Max connection count: 2
 Ignore SSL errors:
 Keep connection alive:

Use explicit credentials:
 User name: companyadmin@tech-arrow.com
administrator@domain.com or domainadministrator
 Password:

General settings

Use forest wide queries:
 Allow to re-link mailboxes:
 Allow to archive public folders:
 Public folder access: mne@tech.internal
 Retention reference date: Sent date
 Allow to archive one-off emails:

[Online help](#)

Allow to archive public folders: If you want to archive public folders, this option must be selected, otherwise the provisioning job will ignore them and they won't be archived. If public folder archiving is turned on and later off, the existing archived public folder mailbox is not removed (nor disabled). It will be simply not archived further, but the existing data will remain in the archive.

Note: Restore and recover will also not work if public folders are turned off.

Public folder access: The "Public folder access" is an email address. It is recommended to set this value to the SMTP (Simple Mail Transfer Protocol) address of the superuser. If this value is changed, it is necessary to run the email provisioning job.



Important: For **Mixed Exchange environment** - If you move the user to a **newer Exchange Server**, the **public folder will be moved to the new Exchange Server** as well! Therefore, it is recommended not to move the user if the public folders should be archived on the old Exchange Server. If the user needs to be moved, we recommend to change the public folder email address to a different mailbox, which still resides on the **old Exchange Server**.

The public folders are synchronized to the contentACCESS address book by the email archive provisioning job. If public folder archiving is **turned off in the System settings**, the public folders are completely ignored:

- If there is no archived public folder mailbox yet, it will not be created
- If there is already an archived public folder mailbox, it is not actualized

If public folder archiving is **turned on**, the provisioning will do the following after all mailboxes are processed:

- Search for public folder mailboxes (Exchange 2013-2019) using PowerShell
- Search for public folder databases (Exchange 2007-2010) using PowerShell
- If there is no public folder found at all, the process is cancelled
- If there are more public folders found, it always picks the newest ones (if there is Exchange 2013/2016/2019 public folder mailbox found, that will be used)
- If there is no “archive public folder mailbox” yet, it is created
- If there is already an “archived public folder mailbox”, the email address is updated from the **System settings** (if the system settings were changed, this step actualizes the value)

As the last step, all contentACCESS users (belonging to the same domain) are granted the “User” role on the public folder mailbox (the users will be able to select the “Public folders” in contentWEB).

The provisioned public folders have a separate section in the contentACCESS Address book.

Public folders					
Name	Access email	Archive database	Store	Active	
✓ Public Folders	*** vwe@tech.internal	TECH	TECHStore	Yes	
<div style="border: 1px solid black; padding: 2px;"> Assign database and storage Deactivate Manage access Move mailbox </div>					
Exchange mailboxes					
Name	Mai	Create contentWEB access	Archive database	Store	Act



The context menu options allow to assign a database and storage to the public folders to be archived as for Exchange groups or mailboxes. It's also possible to activate/deactivate the public folders on the license server, to set contentWEB permissions to them (option "Manage access") or to move the content to a mailbox. The "Access email" column displays the value from the System settings page (section "General settings") and is actualized by the provisioning job if changed.

How to configure an archive job to archive public folders?

To archive public folders, you will need to create a standard email archive job. Every job configuration option is the same as in the standard email archive job – you can decide about the shortcut type, time periods when the job will run, the retention time etc. The only difference is the configuration section "Address book objects". Here the public folder is selected.



contentACCESS Central Administration Tenant: TECH-ARROW

System | File Archive | **Email Archive** | SharePoint Archive | GDPR | Teams Archive | Custom plugins

Save | Discard changes | Databases | Storages | System settings | Provisioning settings | Retentions | Shortcut configuration | Schedules | User experience | View address book | Jobs | Remote agents | PST import | Legacy data configuration

Edit | Settings | Archive | Remote agents | Miscellaneous

Scheduling settings

Scheduled in:

Storage settings

Storage name:

Shortcutting

Shortcut types:

Apply to NOT ARCHIVED items
Use shortcut for items where filter is not set [\[Change\]](#)

Apply to ALREADY ARCHIVED items with keep original shortcutting method
Use shortcut for items where filter is not set [\[Change\]](#)

Retention settings

Retention:

Address book objects to process

select

Name

Public Folders ...

Include folders

Folder filtering type:

Exclude folders

[+ new](#) [↩ import](#)

Pattern

No data to display

Exclude addresses

[Online help](#)

When you click select, the **Mailbox selection** dialog opens – you need to select the “Public folders” item from the list. If the public folders haven’t been provisioned yet, then this item is not included in the list.

Mailbox selection ×

 refresh

<input type="checkbox"/>		Name	Type
		<input type="text"/>	<input type="text"/>
<input type="checkbox"/>		TECHEX2K10	Server
<input type="checkbox"/>		MIGRATION	Server
<input type="checkbox"/>		TECH only	Group
<input type="checkbox"/>		pfi2010	Mailbox
<input checked="" type="checkbox"/>		Public Folders	PublicFolder

Important: If an on-premise Exchange group is used in a job configuration, the job configuration needs to be updated after the group is moved to the cloud, since the group identifier changes and the job is still using the old identifier.

Steps to take:

- open job's configuration page
- remove the group from the list of **Address book objects to process**
- select the group and re-add it to the list
- save the job configuration

Further you can specify, which folders will be archived in the public folder hierarchy (sections "Include folders"/"Exclude folder"). In the "Include folders" it is necessary to specify the exact folder path that needs



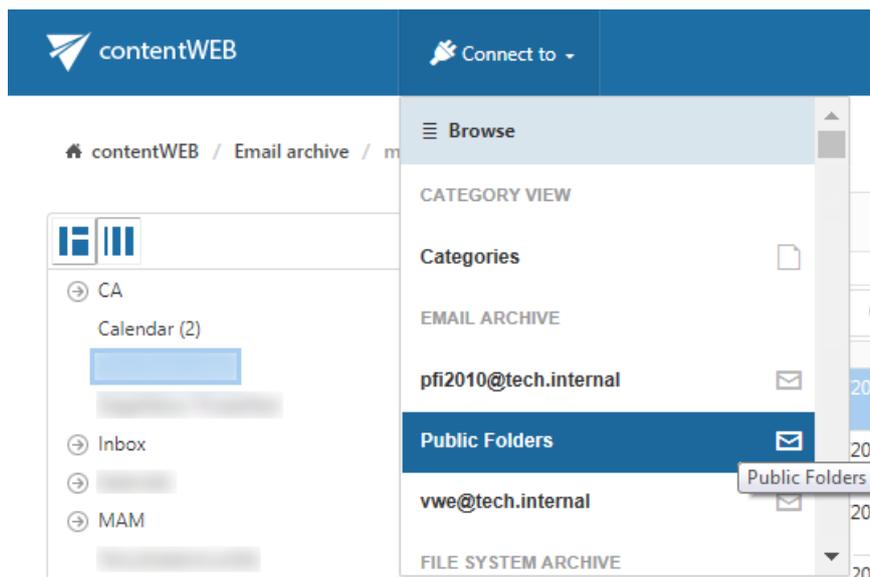
to be archived. Same rules apply as for mailboxes, with one exception: it is not possible to use the placeholders like %INBOX% and similar.

The public folders can be selected in other Email archive jobs – Email archive restore job, Email archive recovery job, Mailbox move job, Shortcut synchronization job – as well.

Public folders in the contentWEB archive

The archived public folder mailbox can be accessed from contentWEB just like a regular mailbox – the logged on user needs to have permission on the public folders – then the public folder permissions are evaluated on each folder and only the correct ones can be accessed.

The public folders are displayed like “Public Folders” in the connection list:



The contentWEB user has the possibility to manually recover the archived public folder items in contentWEB back into the original location. When folders are recovered, the top level folders must exist.

User permissions to public folders

During the run of the provisioning job, the users are automatically getting the permission to access the public folders:

Manage Access to Object

Object > Manage access

[+ new](#)

User name	Role name	Flags
vwe	*** Public folder admin	Manual
vettel	*** Normal user	Automatic (100)
vettel	*** Normal user	Automatic (100)
alonso	*** Normal user	Automatic (100)
vettel	*** Normal user	Automatic (100)
alonso	*** Normal user	Automatic (100)
button	*** Normal user	Automatic (100)
button	*** Normal user	Automatic (100)
alonso	*** Normal user	Automatic (100)
button	*** Normal user	Automatic (100)
vettel	*** Normal user	Automatic (100)
alonso	*** Normal user	Automatic (100)
button	*** Normal user	Automatic (100)

[Go back](#)

The assigned role is “Normal user”, which allows the user to see public folders as a separate entity in contentWEB:

The screenshot shows a file explorer window with a 'Connect to' dropdown at the top. Below it is a list of users and folders. The 'Public Folders' entry is highlighted, and a tooltip labeled 'Public Folders' is visible next to it. The list includes:

- messi@cg.local
- pf12010@tech.internal
- Public Folders**
- ronaldo@cg.local
- rosberg@cg.local
- schumacher@cg.local
- vladimir.werskov@tech-arrow.com
- vwe@tech.internal



The “Public Folders” are visible, but it does not mean that all data will be displayed to the user. Everything else depends on the folder permissions that the given user has – if the user can read the folder, the folder will be visible. Otherwise the folder will not be displayed at all.

Granting administrator access to all public folders

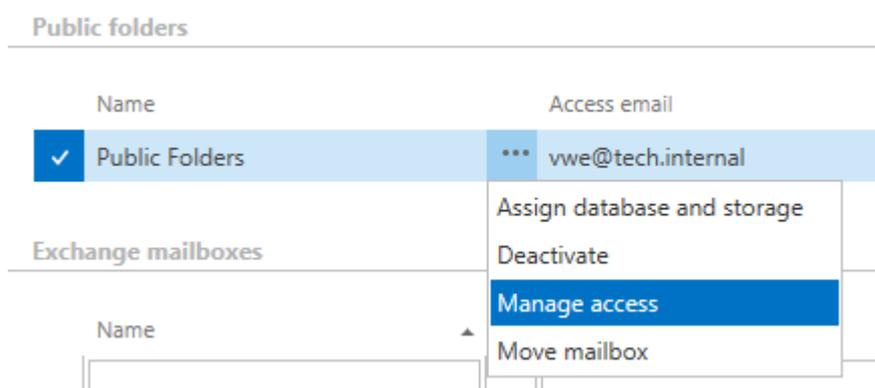
There are situations when you want to grant an administrator access to all public folders in the contentWEB archive. In this case, you need to create a new role, add the permission “**View all public folders**” to this role and then assign the role (on the public folder mailbox) to the future public folder administrator. To create such a user, follow these steps:

- Create the role on the “**Roles**” page and add the permission “View all public folders” to the role (option Specific allowed).

The screenshot shows a 'Role details' dialog box with a close button (X) in the top right corner. The 'Role display name' field contains 'Public folder admin'. Below this is a 'Permissions' section with a table of permissions. The 'View all public folders' permission is highlighted with a red arrow pointing to the 'All allowed' radio button.

Permission	Not allowed	All allowed	Specific allowed	Help
View mailboxes:	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	?
Export:	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	?
Manual recovery:	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	?
Preview:	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	?
View all public folders:	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	?

- Go to the contentACCESS address book (Email Archive → Archive → View address book), and choose **Manage access** from the public folder’s context menu:





- Grant the role to the user/administrator

Create new role association ✕

Tenant information

Role:

Invitation type:

Search for existing user*:

The user “**pfi**” was granted “Public folder admin” permissions on the “Public Folders” mailbox. This allows for this “**pfi**” user to see all public folders, regardless of the Exchange permissions.



Manage Access to Object

Object > Manage access

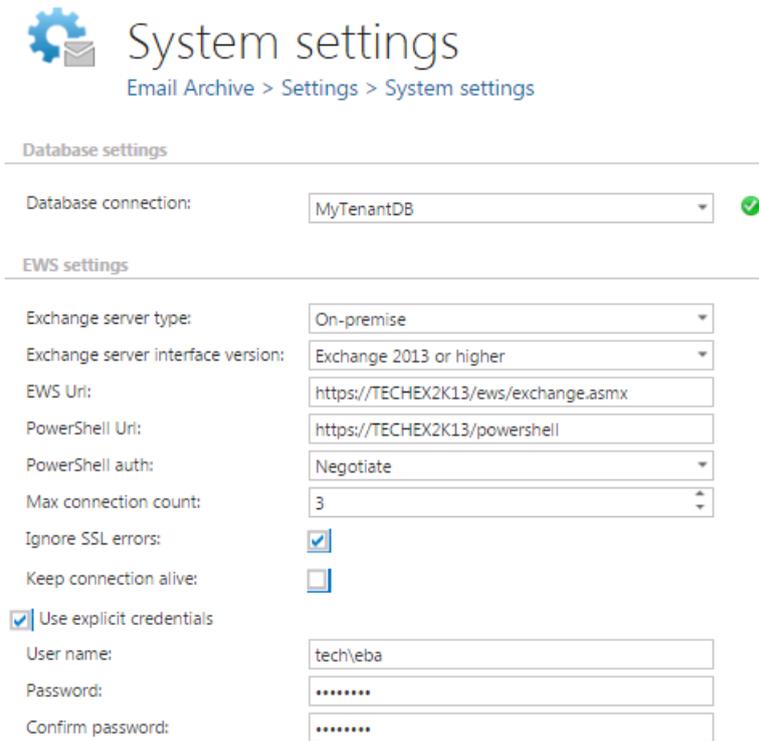
+ new

User name	Role name	Flags
vwe	*** Public folder admin	Manual
vettel	*** Normal user	Automatic (100)
vettel	*** Normal user	Automatic (100)
alonso	*** Normal user	Automatic (100)
vettel	*** Normal user	Automatic (100)
alonso	*** Normal user	Automatic (100)
button	*** Normal user	Automatic (100)
button	*** Normal user	Automatic (100)
alonso	*** Normal user	Automatic (100)
button	*** Normal user	Automatic (100)
vettel	*** Normal user	Automatic (100)
alonso	*** Normal user	Automatic (100)
button	*** Normal user	Automatic (100)
pfi	*** Public folder admin	Manual

Public Folder archiving in mixed Exchange environments

Many organizations use a mixed Exchange environment and have Public folders on an Exchange server, which also need to be archived. E.g. the standard mailboxes are hosted by Exchange server 2013 (in this use case “TECHEX2K13”), but Public folders are on Exchange 2010 (in this use case “TECHEX2K10”), and both need to be archived. In such case, the system must be configured accordingly:

- 1) On the **Email Archive → Settings → System settings** page, under **EWS settings**, set the Exchange version to the highest Exchange version that you use and specify an EWS user, who has the necessary rights on this Exchange server.



System settings
Email Archive > Settings > System settings

Database settings

Database connection: MyTenantDB

EWS settings

Exchange server type: On-premise

Exchange server interface version: Exchange 2013 or higher

EWS Uri: https://TECHEX2K13/ews/exchange.asmx

PowerShell Uri: https://TECHEX2K13/powershell

PowerShell auth: Negotiate

Max connection count: 3

Ignore SSL errors:

Keep connection alive:

Use explicit credentials

User name: tech\eba

Password:

Confirm password:

- 2) On the same **Email Archive System settings** page, in section **General settings**, allow to archive public folders and set the public folder owner's email address. This is the email address of a user, **who is hosted by the Exchange server containing public folders**.



General settings

Use forest wide queries:

Default restore method: In-place restore. Restore data into the shortcut.
 Create new item and replace the shortcut.

Allow to archive public folders:

Public folder access:

Important: If you move the user to a **newer Exchange Server**, the **public folder will be moved to the new Exchange Server** as well! Therefore, it is recommended not to move the user if the public folders should be archived on the old Exchange Server. If the user needs to be moved, we recommend to change the public folder email address to a different mailbox, which still resides on the **old Exchange Server**.

3) Set the email archive provisioning standardly and start the provisioning job - all the Exchange server mailboxes will be read and written to the contentACCESS Address book. First the higher versions are synchronized, then the lower versions follow.



Provisioning settings

Email Archive > Settings > Provisioning settings

start immediately
 refresh
 disable auto refresh
 deactivate job
 logs
 edit

Status: **Idle**
Progress:

(Click to maintain a full crawl for the next provisioning run.)

Scheduling settings

Scheduled in:

Notification settings

Send when:

Recipient list:

Exchange servers

Please choose servers or groups you decided to process by provisioning job. If a server is selected, all the groups in it will be processed.

Servers:

Name	Server DN
TECHEX2K10	*** /o=TECH-ARROW/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Configuration/cn=Servers/cn=TECHEX2K10
TECHEX2K13	*** /o=TECH-ARROW/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Configuration/cn=Servers/cn=TECHEX2K13

[Online help](#)

4) Go to the Address book. The Exchange server section features all synchronized servers.

5) By default, the system uses the default EWS URL previously set on the **System settings** page (**EWS settings** section) to connect with the respective Exchange mailboxes. Set the right EWS URL for all your Exchange servers using the "Change server settings" context menu option.



View address book

Email Archive > Archive > View address book

Mailboxes

Public folders

Groups

Servers

[import servers manually](#) + [add server manually](#)

Name	EWS version	Create contentWEB access	Associate with role	Server DN
TADC01	Exchange2010_SP2	Yes	Inherited	/o=First Organization/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Configuration/cn=Servers/cn=TADC01

Page 1 of 1 (1 items) 1

Automatically create contentWEB user
 Do not create contentWEB user
 Change server settings

Server configuration

EWS version:

Custom EWS Url:

6) Configure the archive job and archive both your standard mailboxes (from Exchange server 2013) and public folders (from Exchange server 2010).

SMTP archiving

To successfully archive emails via SMTP, the following must be completed first:

- configured contentACCESS and default shortcut type for Email archive
- configured at least one storage and retention
- if you want to archive to an existing mailbox, it must contain either some previously archived data, or its properties must be set in the address book
- configured [SMTP](#) during contentACCESS installation
- ports 25, 465 or 587 allowed in Firewall on the computer that hosts the SMTP server for incoming traffic
- MX record created (described below)



Creating MX record

The MX record defines the IP address/alias of the server registered for the given domain name. The MX stands for mail exchange and handles email communication. MX record indicates which computer is responsible for handling the mail for a particular domain.

You can have multiple MX records for a single domain name, ranked in preference order. If a host has three MX records, a mailer will try to deliver to all three before queuing the mail.

*An **MX** and **A** record example:*

Record FQDN	Record Type	Record Value	MX Pref.
mail.example.net	A	123.123.123.123	
example.net	MX	mail.example.net	10

An “A” record maps a domain name to the IP address (IPv4) of the computer hosting the domain.

MX and A record on azure.tech-arrow.com has the following configuration:

azure.tech-arrow.com	1800	A	40.113.116.9
azure.tech-arrow.com	1800	MX	10 azure.tech-arrow.com

After everything is set, go over to [SMTP Servers](#). On this page the list of all registered SMTP servers in contentACCESS can be found. It is also necessary to set here the domains that should/shouldn't be used in SMTP archiving. If a domain is not white-listed here, it can't be later used to create [SMTP Mappings](#) and therefore for SMTP archiving. It is possible to set automatic deletion of files (locally stored on SMTP) after clicking on **Edit** in the context menu of the servers on this page.

Delete settings

Deletion types:

- Delete files automatically after archive if they are older than days
- Delete files automatically if they are stored for more than days

On the [SMTP Mappings](#) page the user has to map email addresses. The SMTP will archive emails based on the created mappings. The **Email address** will process the incoming emails and archive them to the specified folder in the **Entity**. Only mailboxes with assigned **Archive database** and **Store** in the **Address book** can be used as **Entities**, however, dummy mailboxes can be used as **Email addresses**.

Note: To learn how to manually create mailbox(es) in the archive for SMTP archiving, please check [this](#) section.

SMTP Mapping ✕

SMTP mapping

Email address: @

Folder:

Model:

Entity:

Important: One **Email address** can be associated only with one **Entity**! However, one **Entity** can be associated with multiple **Email addresses**.

The archived emails won't be visible in the mailbox directly, but they can be viewed and worked with in contentWEB.



contentWEB Connect to - Administrator

contentWEB / Email archive / SNE@ta.internal Search (SNE@ta.internal) English

Deleted Items Inbox SMTPmapping

Subject	From	Date
Test email	test@contentaccesstestdomain.com	3/28/2018 11:43 AM
Test email	test@contentaccesstestdomain.com	3/28/2018 11:31 AM
Test email	test@contentaccesstestdomain.com	3/28/2018 11:17 AM

Test email

From test@contentaccesstestdomain.com
Date 3/28/2018 11:43:34 AM
To john.smith@microsoft.com
Cc test2@contentaccesstestdomain.com <test2@contentaccesstestdomain.com>
Expiration 3/28/2019

Message

Test message body

Online help



SharePoint archive plugin

Organizations use SharePoint to make information more accessible to end users and to enhance collaboration among work groups. The benefits that SharePoint delivers are undeniable: better and more efficient team collaboration, version control for documents edited by multiple team members and faster access to information through searches. SharePoint brings a new level of structure to high-volume, user-generated content.

When choosing the reliable software to archive these crucial data, the following questions must be answered:

- ***How does the archiving solution enable end-users to access SharePoint content?***

When the users go to SharePoint and want to get the desired documents, they don't want to search multiple repositories for data. Rather, the right solution will make access seamless. In contentACCESS the user may choose between more shortcut types: the item that has been already archived can be kept in the original SharePoint file container, but if it's no more in use, it can be also deleted from there. E.g. items younger than 2 years can be kept in SharePoint so they remain directly accessible, but items older than 2 years can be deleted and will be accessible using the archive interface only.

- ***How does the solution enable retention management?***

A unified content archive allows a company to quickly implement retention policies and to preserve all archived data that may be extremely important, e.g. in a legal action that the company is involved in. With contentACCESS SharePoint Archive you can define the required retention time for the archived items and you can also set different retention times for different set of data.

- ***Is the solution part of an integrated content archiving platform?***

An intelligent and efficient archiving solution unifies email, file and SharePoint archiving in one, ensuring unified access to any content.

- ***What scope of SharePoint content and metadata is captured?***

Some solutions capture only a portion of SharePoint content. contentACCESS from TECH-ARROW **captures not only document-type content, but also calendar items, tasks, custom lists, contacts, document libraries, picture libraries and their attachments.** All of this content and metadata are important to be accessed at any time.



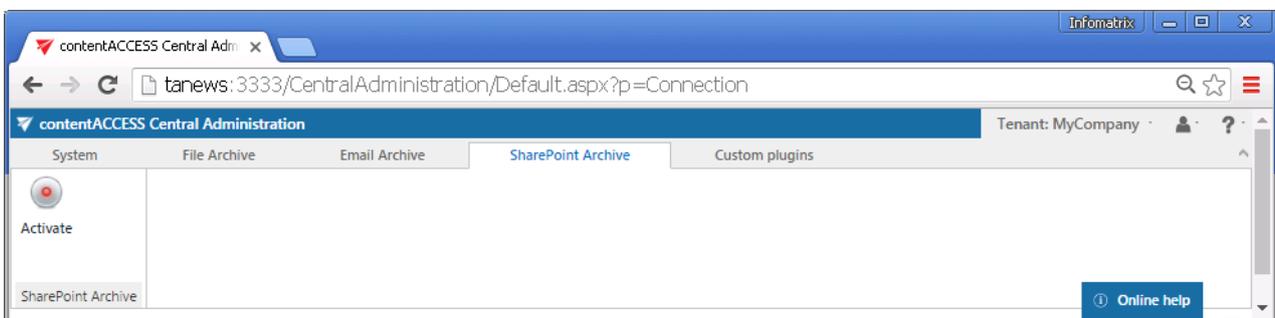
With contentACCESS you can automatize the archiving process. The periodic data processing is solved with automatically running jobs. The time periods, when such an archive job runs, are determined by schedulers.

contentACCESS SharePoint Archive guarantees an oversimple access to your crucial data. You can still reach your (already archived) files through the SharePoint user interface and browse for them in the contentWEB archive. Archived files that have been deleted from the original SharePoint location can be recovered, too. You can define multiple SharePoint sites to archive and set own retention categories and/or filtering options to them. Do you need to publish data into SharePoint from a third-party storage? SharePoint Publishing job solves this scenario as well.

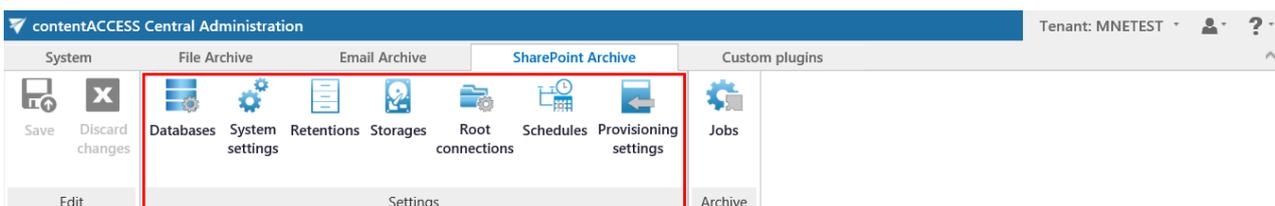
In the following subchapter we will learn about the necessary settings to be done before creating a SharePoint job.

SharePoint Archive settings

When the SharePoint setting are configured in the contentACCESS Central Administration for the very first time, SharePoint Archive must be activated:



All SharePoint settings that are necessary to set to create a SharePoint archive job can be found on the SharePoint **Settings** page (SharePoint Archive tab → **Settings** group).



The administrator configures here the:



▪ Databases

This is a list of MS SQL database connections configured for your tenant. These databases can be further selected on the archive job's configuration page. You can either configure an already existing database connection (option “**configure existing**”) or add a new database on the “**All databases**” page (**System** tab → **Tenants** group → **All databases**)

▪ System settings

The main system database for the SharePoint Archive is selected here. All the root connections (and its settings) are kept in this database.

Select the database connection to be applied from the dropdown list (deploy it by clicking “Deploy” in the warning message if needed) and save your settings.

▪ Retentions

Retentions define the time period, during which the data are stored in the archive storage; for more information about how to create retentions to be applied refer to chapter [Retentions](#) of this guide.

▪ Storages

The administrator must set here the SharePoint Archive storage for the binaries; for detailed information about how to create a new storage connection refer to chapter [Storages](#) of this guide.

▪ Root connections

In this section the administrator configures the connections to the SharePoint sites that will be archived. **The root connections define the start point of the SharePoint site to be archived.** Every item in the SharePoint hierarchy, that can be archived, can be defined as a root connection as well. These archivable SharePoint items and their sample URLs (to be defined in the root connection) are:

- a **site collection** – with URL like: <http://sharepointserver.com/sites/testcompany>
- a **subsite of the site collection** like <http://sharepointserver.com/sites/testcompany/hr>
- a **SharePoint library** (SharePoint document libraries, picture libraries, lists, tasks, contacts etc.) like <http://sharepointserver.com/sites/testcompany/hr/testlibraryA>
- a **SharePoint folder** like <http://sharepointserver.com/sites/testcompany/hr/testlibraryA/testfolderA>



The URL cannot be a parent URL or a sub URL of an existing connection. Example: If you've got a root connection with URL <http://sharepointserver.com/sites/testcompany/hr> then you're not allowed to add another root connection with URL <http://sharepointserver.com/sites/testcompany> or <http://sharepointserver.com/sites/testcompany/hr/division1>. This feature prevents the users from archiving the same content into two different databases/storages. If the user wants to add a root which already exists in the system database, he will be prompted about this.

When you're adding a new root connection, you need to specify the following parameters:

- **Url:** URL of the site collection, subsite, library or folder you want to archive
- **Authentication type:** From this dropdown list, you can select one of the three authentication types: **Basic**, **Integrated** and **Modern**.
- **Database connection:** The database where the archived data will be stored
- **Storage name:** The storage where the binaries will be stored

Basic authentication

With this authentication, you will need to enter your username and password that will be used to access the specified SharePoint site.

- **User name:** The name of the user who's got the rights to access the site collection, subsite, library or the folder
- **Password:** The password of the above specified user
- **Confirm password:** Re-enter the password

Integrated authentication

The user's current Windows identity will be sent to the SharePoint server and used for authentication.

Modern authentication

The required data for the modern authentication are the following:

Application ID: the ID of the registered Azure application

Tenant ID: the tenant/directory ID of the Azure tenant, can be acquired from the Azure app Overview page



Certificate file: .pfx file, which contains the private and public key of the certificate. Must be the same certificate as the .cer file that has been uploaded to Azure during [app registration](#). The app can be registered by using [this](#) PowerShell script too.

Certificate password: the password for the .pfx file.

Important: contentACCESS supports also **AAD groups** in Sharepoint archive. This support works only with **Modern** authentication.

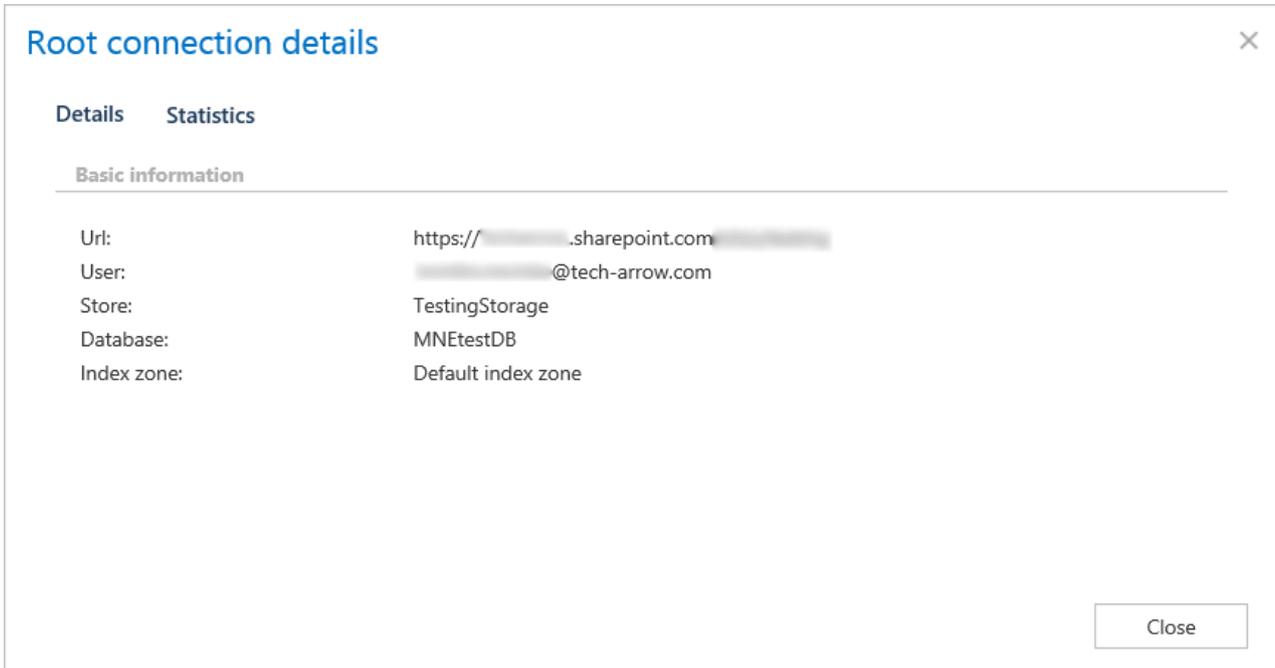
Site connection ✕

Url:	<input type="text" value="https://techarrow.sharepoint.com/sites/testing"/>		
Authentication type:	<input style="border: none; background-color: #f0f0f0; width: 100%;" type="text" value="Modern"/>		
Application ID:	<input type="text" value="2ff-..."/>		
Tenant ID:	<input type="text" value="4b0-..."/>		
Certificate file:	<input type="text" value="Please select a file to upload"/>	<input type="button" value="Browse..."/>	
Certificate info:	Common name: CN=TechArrow Expiration date: 5/1/2022 2:00:00 AM		
	<input type="button" value="Download certificate"/>		
Certificate password:	<input type="password"/>		
	<input type="button" value="Test"/>		
Database connection:	<input type="text" value="caDev_SpModernAuthenticator"/>	<input type="button" value="Change"/>	✔
Storage name:	<input type="text" value="Disk storage"/>	<input type="button" value="Change"/>	
Index zone:	<input type="text" value="Default index zone"/>		
<input type="button" value="OK"/>		<input type="button" value="Cancel"/>	

Note: It is recommended to add a site collection or subsite as a root connection, the libraries, folders etc. can be specified later as a relative URL on the respective archive jobs' configuration page.

To view the details and archive statistics of the selected root connection, click on **Details** in its context menu.

Details:



Root connection details [Close]

Details **Statistics**

Basic information

Url:	https://[redacted].sharepoint.com
User:	[redacted]@tech-arrow.com
Store:	TestingStorage
Database:	MNEtestDB
Index zone:	Default index zone

[Close]

URL – URL of the root connection

User – the username used when connecting to the SharePoint site

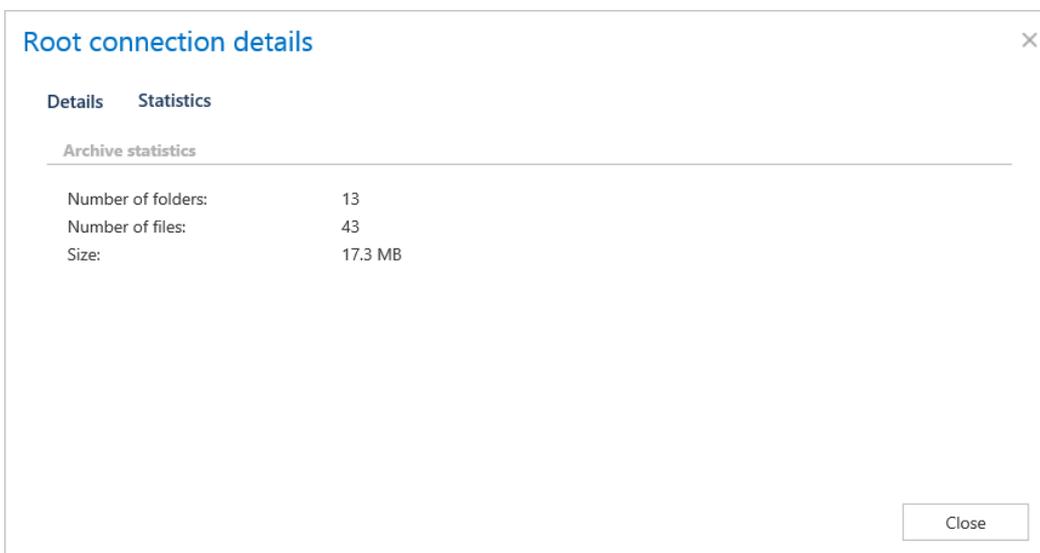
Store – store assigned to the connection

Database – database assigned to the connection

Index zone – index zone assigned to the connection

Statistics:

Statistics show archived folders count, document count and total size of the files that were archived.



Root connection details [Close]

Details **Statistics**

Archive statistics

Number of folders:	13
Number of files:	43
Size:	17.3 MB

[Close]



- **Schedules:** The schedules automatizing the archive process must be set here.

There are 4 available SharePoint job types in contentACCESS:

- ✓ SharePoint Archive job
- ✓ SharePoint recovery job
- ✓ SharePoint Publishing job
- ✓ SharePoint Provisioning job

- **Provisioning settings:** The job that creates and updates contentACCESS users and assigns contentACCESS roles to them based on information gathered from SharePoint.

Each job type, together with its configurations, will be detailed in the following chapters of the guide.

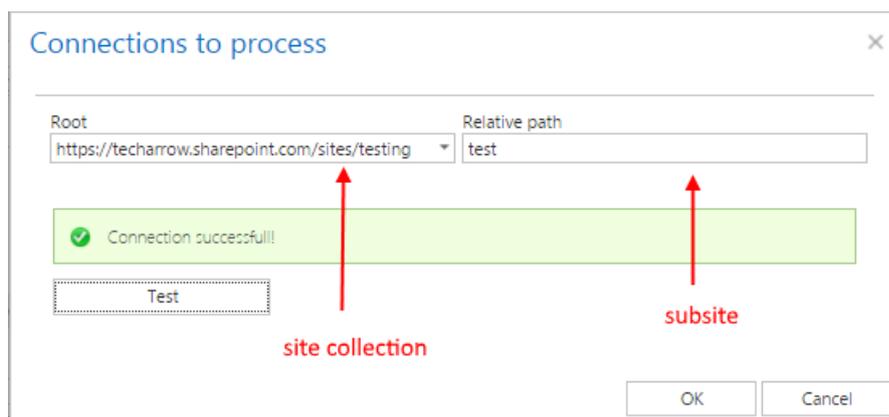
SharePoint Archive job configuration

After you have configured all necessary settings, you can create and configure a SharePoint Archive job. Click **+ new** on the **Jobs** page (**SharePoint Archive** tab → **Archive** group → **Jobs**), fill the required settings (Job type, Run on node, Display name) in the pop up window and click on **Add**.

To configure the job immediately, click **Yes** in the next pop up window, or configure it later on (using the **Configure** option in the job's context menu). On the job's configuration page set the:



- **Report mode settings** - if the checkbox is checked, the job will run in report mode and the user will be able to download a .csv report file here in this section after the job finishes the run
- **Scheduling settings** – time slots of the job running
- **Retention settings** – time period of keeping the archived item in the storage
- **Archive settings** – possible to skip template saving by checking the checkbox in this section
- **Shortcut settings** – the administrator can decide if the archived item will remain in the original location and will be directly accessible from there – option “Keep original item”, or that it will be deleted and will be accessible only from the archive interface – option “Delete original item”. With this option, only the items are deleted - folder, libraries etc. are kept untouched.
- **Connections to process** – Click on “+new” and specify the root connection and the relative URL in the pop-up window. A root can be a site collection, a subsite, a library or a folder already defined in the **Root connections** section. In this use case we will archive our items on subsite <https://techarrow.sharepoint.com/sites/testing/test>, where the root is a site collection.



- **Filtering settings** – Click on the **Change filter** button and set the filtering according to your needs and/or regulations. To learn more about how to work with filtering settings, please, check [this](#) section of our documentation.

Filter settings ✕

+ add custom property

visual
text

A N D ▼	Creation date ▼	> ▼	3M	📅	✕
	Size ▼	>= ▼	100	KB ▼	✕
+add group +add condition					

+add new group

OK
Cancel

Important!!!: When the user changes the file content of an already archived item, e.g. deletes a picture from the file, saves it to the original location (and thus the file size will be reduced e.g. from 110 to 85 kB) and file size filter is set on >100 kB, then SharePoint archive job will not archive the newly created item by the next processing. The newly created item will be saved in the original location. For this reason, it is recommended to always check the size filter settings first, if a file has not been archived by the archiving process.



- **Notification settings** - Select here, when you will need to get notification emails from the SharePoint archive job. Into the **Recipient list** textbox insert the email address(es) of the person(s), who will get such notifications. It is also possible to set that the emails will be sent only when the version count reaches a certain number.
- **Resource settings** – The number of worker threads responsible for the archiving processes can be set here; by default this value is set to 2.

The screenshot displays the 'contentACCESS Central Administration' interface. The top navigation bar includes tabs for System, File Archive, Email Archive, BackMailz, SharePoint Archive, and Custom plugins. The 'SharePoint Archive' tab is active, showing a 'Testing site archive' job configuration page. The breadcrumb trail is 'SharePoint Archive > Archive > Jobs > Testing site archive'. The job status is 'Idle' and it is in report mode. The interface is divided into several sections: 'Report mode settings' (including a report file download button), 'Scheduling settings' (set to Manual), 'Retention settings' (set to 0 0 and 0), 'Archive settings' (Skip template saving checked), 'Shortcut settings' (Keep original item), 'Connections to process' (listing a root path), 'Filtering settings' (Filter: AND, Uri:(Contains "testing")), 'Notification settings' (Send when: Never, Recipient list: john.doe@example.com,peter.white@example.com, Notify if version count reaches: 50), and 'Resource settings' (Worker thread count: 2). An 'Online help' button is located in the bottom right corner.

If the job is configured, save your changes and wait until it starts based on the defined schedule (or start it manually from the status bar).

SharePoint archive job description

All the numbers and descriptions in the job's progress have a particular meaning. In this section, we are going to explain the numbers and descriptions of a **SharePoint archive job**.

Description	Explanation
x folders processed	x folders have been processed (a site, document library, list or subfolder counts as a folder)
x documents processed	x documents have been published to the SharePoint site
x documents failed	x documents' publishing failed
x folders failed	x folders' processing from the source provider failed, see logs for further details

SharePoint archive retention changer job configuration

This job changes the retention time of selected items if it's allowed to change the retention on storage level. Storages that support this change are: Disk, Azure, Amazon S3.

Go to Jobs -> click on **+new** -> select **SharePoint archive retention changer**.

Add new job instance ✕

Available jobs:

Run on node:

Display name:

Description:



On the job's configuration page go through the following sections:

✓ Running mode settings (mandatory)

The job can be run in 3 modes:

- 1) **Immediate processing** -> collects the items and changes their retention.

Running mode settings

Run in mode:

- 2) **Create report** -> collects the items and provides a csv file with a list of items. The administrator can review and edit the list of affected documents.

Running mode settings

Run in mode:

Generated report file:
 File name: GeneratedRC_12_16_2019 7_42_18 PM.csv
 Size: 2.6 KB
 Date: 12/16/2019 7:42:18 PM

- 3) **Apply report** -> a csv file with a list of items to be processed must be uploaded. The administrator can delete items from the list before running the job (only items which are in the list will be processed). The job reads the list and changes the retention of the items that are on the list.

Running mode settings

Run in mode:

Reviewed report file: ...

File name: GeneratedRC_12_16_2019 7_42_18 PM.csv
 Size: 2.6 KB
 Date: 12/16/2019

✓ Retention settings (mandatory)

Select the new retention to be applied for the items.

Retention settings

Target retention:

✓ Scheduling settings (mandatory)

In this section the running times of the **retention changer job** must be selected. It is possible either to select a scheduler from the list or to create a new scheduler via the “**Create new ...**” option.

Scheduling settings

Scheduled in:

- Create new ...
- Manual
- TaskRunnerScheduler

✓ Connections to process (mandatory)

Click on **+new** and specify the root connection and the relative URL in the pop-up window. A root can be a site collection, a subsite, a library or a folder already defined in the **Root connections** section.

Connections to process ✕

Root: Relative path:

✓ Connection successful!



✓ Filtering settings (optional)

Click on the **Change filter** button and set the filtering according to your needs and/or regulations. To learn more about how to work with filtering settings, please, check [this](#) section of our documentation.

Filter settings

×

visual text

AND	Creation date	Older than	1Y	📅	✖
	Creation date	Younger than	2Y	📅	✖

[+add group](#) [+add condition](#)

[+add new group](#)

OK Cancel

✓ Notification settings (mandatory)

Select here, when you will need to get notification emails from the **Retention changer job**. It is possible to set here if you need a notification email always/never, or you need it only if an error/warning occurred



during the process – for example, if the retention change of one or more items failed, then you may get a notification email about this error. Into the **Recipient list** textbox insert the email addresses of the people whom you would like to send these emails to – if there are multiple recipients, the addresses must be separated by “,” or “;”.

Notification settings

Send when:	<input type="text" value="Errors or warnings occur"/>
Recipient list:	<input type="text" value="walter_white@tech-arrow.com"/>

✓ Resource settings (mandatory)

Set the value, which will determine how many items will be processed simultaneously by the **Retention changer job**. The recommended value is 2, as in our case.

Resource settings

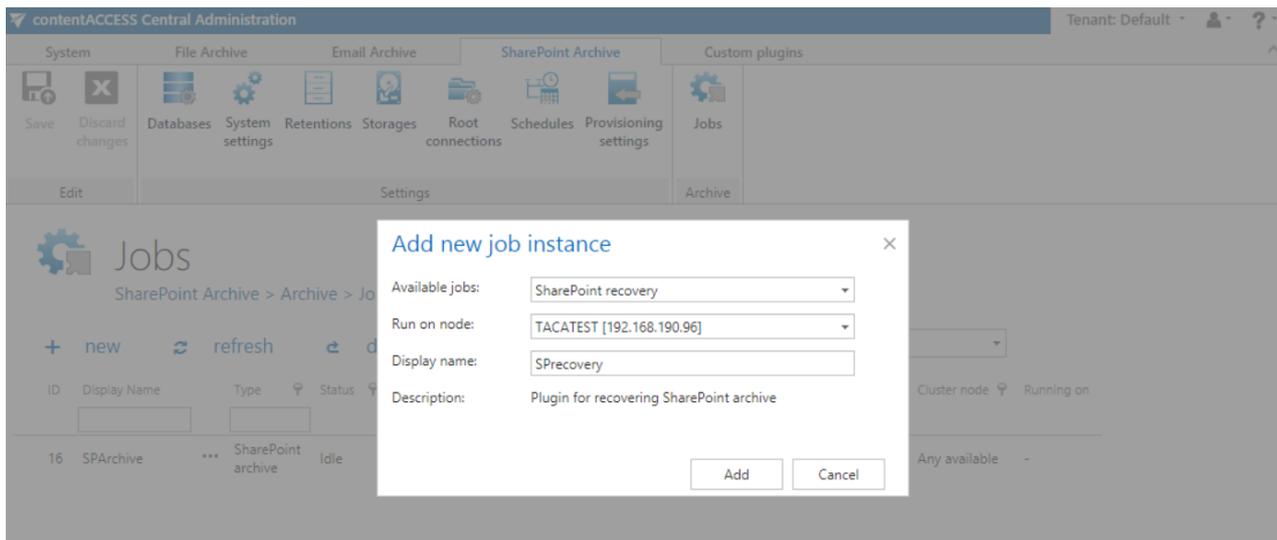
Worker thread count:	<input type="text" value="2"/>
----------------------	--------------------------------

At the end never forget to save your job configurations: click on **Save** in the left upper corner of UI.

SharePoint recovery job configuration

SharePoint recovery is used to recover already archived SharePoint items that have been deleted from the original SharePoint location. All items that can be archived by contentACCESS are also recoverable. contentACCESS is able to recover subsites, libraries and folders, so if they have been deleted, you don't have to create them manually again for recovery job to work. It is also able to recover complete sites with their settings if the connection set in the connections to process is a site.

To create a SharePoint recovery job, create a SharePoint recovery job instance first on the SharePoint archive's **Jobs** page:



Further configure this job as follows:

- **Scheduling settings:** set the time when the recovery job should run; this is usually a one-time action, so a one-time scheduler is set in this use case.
- **Recovery settings:** by checking this checkbox (recommended in case a complete site should be recovered to an empty site), the job will recover not only files and/or folders, but all settings related to the site selected in **Connections to process**.
- **Connections to process:** Set the path that should be recovered (root connection and relative path if any).
- **Resource settings:** the number of workers threads running in parallel.

Save your settings and wait until the scheduler starts the recovery process (or start it immediately using the status bar).



contentACCESS Central Administration Tenant: TECH-ARROW

System | File Archive | Email Archive | BackMailz | SharePoint Archive | Custom plugins

Save | Discard changes | Databases | System settings | Retentions | Storages | Root connections | Schedules | Provisioning settings | Jobs

Edit | Settings | Archive

SP recovery
SharePoint Archive > Recovery > Jobs > SP recovery

start immediately
 refresh
 disable auto refresh
 deactivate job
 logs
 edit

Status: **Idle**
Progress: 10 folders processed 41 items processed (40 skipped, 1 recovered) (completed 7 months ago (November 2017))

Scheduling settings

Scheduled in:

Recovery settings

Recover all site related settings:

Connections to process

+ new

Root	Relative path
https://techarrow.sharepoint.com/sites/testing	test/

Notification settings

Send when:

Recipient list:

Resource settings

Worker thread count:

[Online help](#)

SharePoint recovery job description

All the numbers and descriptions in the job’s progress have a particular meaning. In this section, we are going to explain the numbers and descriptions of a **SharePoint recovery job**.

Description	Explanation
x folders processed	x folders have been processed (a site, document library, list or subfolder counts as a folder)
x folders failed	x folders’ processing failed
x documents processed	x documents have been processed
x documents skipped	x documents have been skipped, because the original items exist on the SharePoint site
x documents failed	x documents’ processing failed
x documents recovered	x documents have been successfully recovered

Configuration of Delete job in SharePoint archive

This job type deletes data, which have been archived, from the archive.

Note: First, you need to mark files/emails for delete in contentWEB (read more in [this](#) section).

Go to Jobs -> Add new -> Delete from archive.

Add new job instance ✕

Available jobs:

Run on node:

Display name:

Description: Removes the documents from the archive, with expired retention time.

On the job's configuration page go through the following sections; most of them are mandatory, filtering settings are optional:

✓ Running mode settings

The job can be run in 3 modes:

- 1) Immediate deletion** -> collects the expired documents and deletes them.

Running mode settings

Run in mode:

- 2) Create report** -> collects the expired documents and provides a csv file with a list of documents.

The administrator can delete documents from the list.

Running mode settings

Run in mode:

Generated report file:

File name:	Generated_8_3_2017 7_27_25 PM.csv
Size:	120 B
Date:	8/3/2017 7:27:25 PM



- 3) **Apply report** -> a csv file with a list of documents to be deleted must be uploaded. The administrator can delete documents from the list before running the job (only documents which are in the list will be processed). The job reads the list and if the documents are expired, deletes them.

Running mode settings

Run in mode:	Apply report
Reviewed report file:	Please upload a csv file ...
File name:	Generated_8_3_2017 7_27_25 PM.csv
Size:	120 B
Date:	8/3/2017
Get uploaded file	

✓ Scheduling settings

In this step the running times of the delete job must be selected. It is possible either to select a scheduler from the list or to create a new scheduler via the “**Create new ...**” option.

Scheduling settings

Scheduled in:	Manual
	Create new ...
	Manual
	TaskRunnerScheduler

✓ Connections to process

In this section the user is required to select the root connection(s) where the data are located. A root can be a site collection, a subsite, a library or folder already defined in the **Root connections** section.

Click on “**+new**” to specify the connection from where the items should be deleted. In the “Connections to process” dialog unroll the list of already created roots and select the one that should be applied. This dropdown lists the roots that are already configured (in SharePoint Archive settings: *SharePoint Archive* → *Settings* → *Root connections*). Enter the **Relative path** if necessary, test the path via the “Test” button and click “OK”.



Connections to process ✕

Root	Relative path
<input type="text" value="https://techarrow.sharepoint.com/sites/testing"/>	<input type="text"/>

✔ Connection successful!

Test

✓ **Processing settings**

In this section, you may check the **Delete even if not marked for delete** checkbox. If you do so, the **Delete job** will delete the expired item without them needing to be marked for delete.

Processing settings

Delete even if not marked for delete:

✓ **Filtering settings**

Click on the **Change filter** button and set the filtering according to your needs and/or regulations. To learn more about how to work with filtering settings, please, check [this](#) section of our documentation.

Filter settings ✕

visual
text

A N D ▼	Creation date ▼	> ▼	1Y	✕
	Extension ▼	Equals ▼	.png	✕

+add group +add condition

+add new group

OK
Cancel

✓ Notification settings

Select here, when you will need to get notification emails from the Delete job. It is possible to set here if you need a notification email always/never, or you need it only if an error/warning occurred during the process – for example, if the deletion of one or more items failed, then you may get a notification email about this error. Into the **Recipient list** textbox insert the email addresses of the people whom you would like to send these emails to – if there are multiple recipients, the addresses must be separated by “,” or “;”.



Notification settings

Send when:	Errors or warnings occur
Recipient list:	walter_white@tech-arrow.com

✓ Resource settings

Set the value, which will determine how many items will be processed simultaneously by the delete job. The recommended value is 2, as in our case.

Resource settings

Worker thread count:	2
----------------------	---

At the end never forget to save your job configurations: click on **Save** in the left upper corner of UI.

When does the document expire?

Retention repository ✕

Retention name:	<input type="text" value="1 year"/>
Description:	<input type="text" value="1 year"/>
Calculated from:	<input type="text" value="Reference date"/>
Protected retention time in months:	<input type="text" value="12"/>
<input checked="" type="checkbox"/> Has unprotected retention time	
Unprotected retention time in months:	<input type="text" value="12"/>

- 1) **If the protected retention has expired** (archive date / reference date + protected retention is in the past) and the document is not under legalhold and the document is marked for deletion
- 2) **If the unprotected retention is defined and has expired** (archive date / reference date + unprotected retention is in the past)



SharePoint delete job description

All the numbers and descriptions in the job's progress have a particular meaning. In this section, we are going to explain the numbers and descriptions of a **SharePoint delete job**.

Description	Explanation
x connections scanned	x configured sites have been scanned for deletable documents in the archive
x failed	x configured sites' processing failed, see logs for further details
x documents purged	x documents have been purged, or if the job ran in report mode x documents have been added to the report
x skipped	x documents' deletion skipped, or in case of report mode x documents has not been added to the report because of the filtering settings
x failed	x documents' deletion failed



SharePoint archive Provisioning settings

The provisioning job

- Creates and updates contentACCESS users and assigns contentACCESS roles to them based on information gathered from SharePoint

Note: The contentACCESS technical user account performing the provisioning job reads the permissions set on the archived SharePoint objects. Therefore it needs to read the SharePoint users, groups and group membership information. To achieve this, please add the contentACCESS technical user account to the list of Site Collection Administrators.

In contentACCESS, a provisioning job is created automatically when activating SharePoint archive for the first time.

The process is similar for on-premise SharePoint and SharePoint online. The differences are as follows:

On-premises SharePoint

- Scans SharePoint groups and users, then they are snapshotted in the SharePoint archive database
- Picks users with Windows login and creates these users in contentACCESS (see more in [SharePoint Archive settings](#), section System settings) together with Windows login
- Grants permissions to access the given SharePoint connection (archive only)

The on-premises SharePoint is working with the Active Directory and using its users and groups to grant them access to sites, folders and items.

SharePoint defines SharePoint groups, which is a collection of AD users, AD groups and other users (Azure, etc.).

The provisioning job also collects information about AD groups and their members. This is important when permissions are evaluated, because they are configured through AD groups.

Snapshot means that a copy of the user/group is created in the archive, which remains even after the user or group is deleted from SharePoint. This allows to use the last known permissions for the user when working with the archive.

At the end of the provisioning job, the archive has collected the following information:

- Collected all AD groups which are somehow related to SharePoint



- Collected all AD users which are somehow related to SharePoint
- Collected AD group memberships
- Collected SharePoint groups for the given root site connection
- Collected members of the SharePoint groups

To access the folders and documents the user requires individual permissions, which are synchronized by the SharePoint archive job.

Note: The user will only see those folders and items to which it really has access.

SharePoint online

The users and SharePoint groups from Office 365 are also synchronized by the provisioning job.

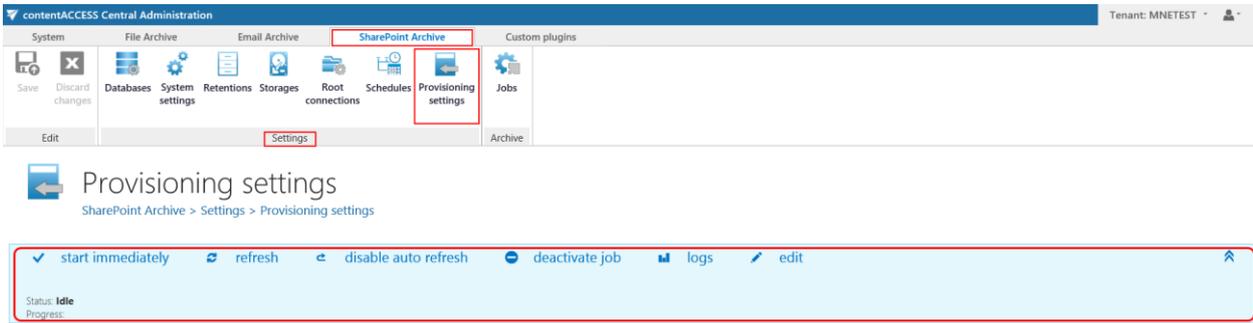
Office 365 users, together with Office 365 logins, are also created automatically by the provisioning job.

SharePoint Archive provisioning settings are available on the **Provisioning settings** page (**SharePoint Archive ⇒ Settings ⇒ Provisioning settings**):

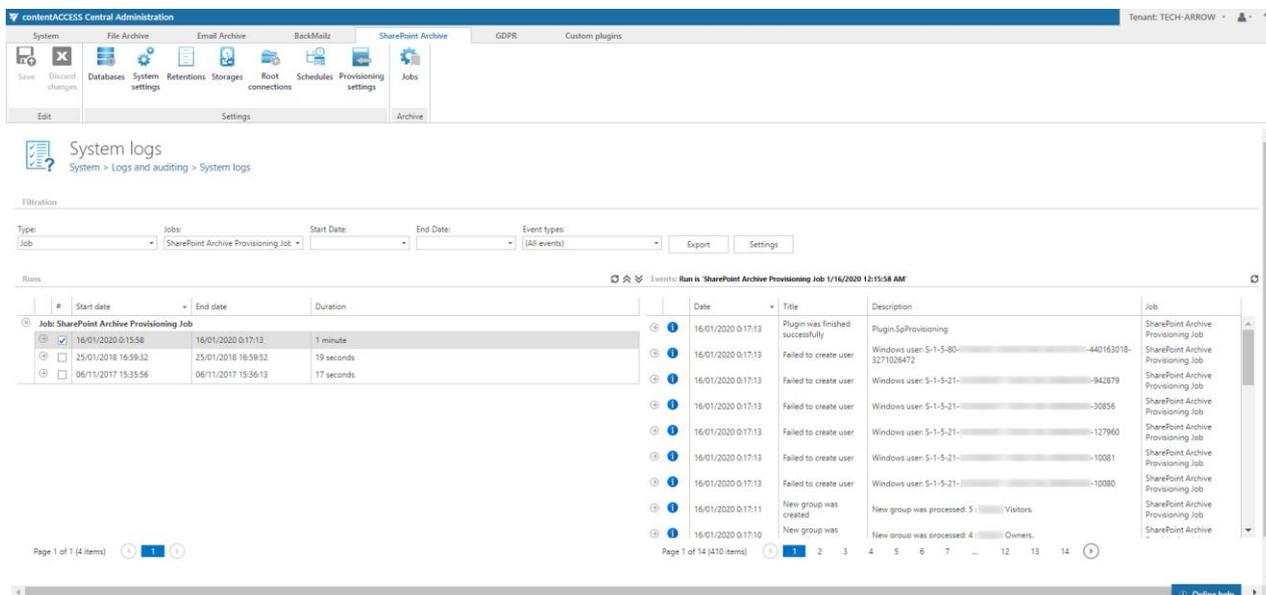
The screenshot shows the 'contentACCESS Central Administration' interface. The top navigation bar includes 'System', 'File Archive', 'Email Archive', 'SharePoint Archive', and 'Custom plugins'. The 'SharePoint Archive' section is highlighted with a red box, and the 'Provisioning settings' link is also highlighted. Below the navigation bar, the 'Provisioning settings' page is displayed. The page title is 'Provisioning settings' and the breadcrumb is 'SharePoint Archive > Settings > Provisioning settings'. The status is 'Idle'. The page contains three sections: a) Role to assign (Created user role: Standard user), b) Scheduling settings (Scheduled in: MANUAL), and c) Notification settings (Send when: Never, Recipient list: john.doe@example.com,peter.white@example.com). There is an 'Online help' button in the bottom right corner.



The **status bar** of the provisioning job offers the following options:



If a scheduler has not been selected, the provisioning job can be started/stopped manually with the **“start immediately/stop”** control button. To manually refresh the provisioning progress information, click on **“refresh”** button. To enable/disable auto refresh in every 5 seconds, click on **“enable auto refresh”/“disable auto refresh”** button. A deactivated job will not start automatically, nor can be started manually. The **“deactivate job”** button is used to select the node, where provisioning job will be run. The user may also rename the provisioning job here. To view further event details of provisioning job (and also to detect any potential failures/errors in the provisioning events), click on **“logs”** button. This will redirect you to the **System logs** page, where the last run of the provisioning job will be preselected and the last events will be shown in the events table.



Screenshot.1. System logs page with logs



The following configuration sections are available on the **Provisioning settings** page:

- a. **Role to assign:** This configuration section allows to assign default contentWEB user roles. It is recommended to specify here a default role with less contentWEB permissions. The roles to be assigned must be created on the [Roles](#) page.

Note: Roles containing Manage system and/or Manage tenant permissions are unavailable in the default roles' dropdown list.

- b. **Scheduling settings:** Select the running times of the provisioning job or create a new scheduler. For more information on how to configure scheduler settings please refer to section [Schedules](#).
- c. **Notification settings:** If the provisioning job could not run properly due to some reasons, contentACCESS can send a warning about the problem. The notification email message will be sent to the email address that is set here under **Recipient list** option. Here you can also choose when these email messages should be sent: only if errors occur, or when errors or warnings occur, or always, regardless of the faultless running of the provisioning job.

SharePoint provisioning job description

All the numbers and descriptions in the job's progress have a particular meaning. In this section, we are going to explain the numbers and descriptions of a **SharePoint provisioning job**.

Description	Explanation
x users processed	x users have been processed
x users added	x users have been added to the system
x users skipped	x users have been skipped
x users updated	x users have been updated in the system
x objects failed	x groups' processing failed
x contentWEB accesses granted	contentWEB access has been granted for x users
x contentWEB accesses revoked	contentWEB access has been revoked from x users

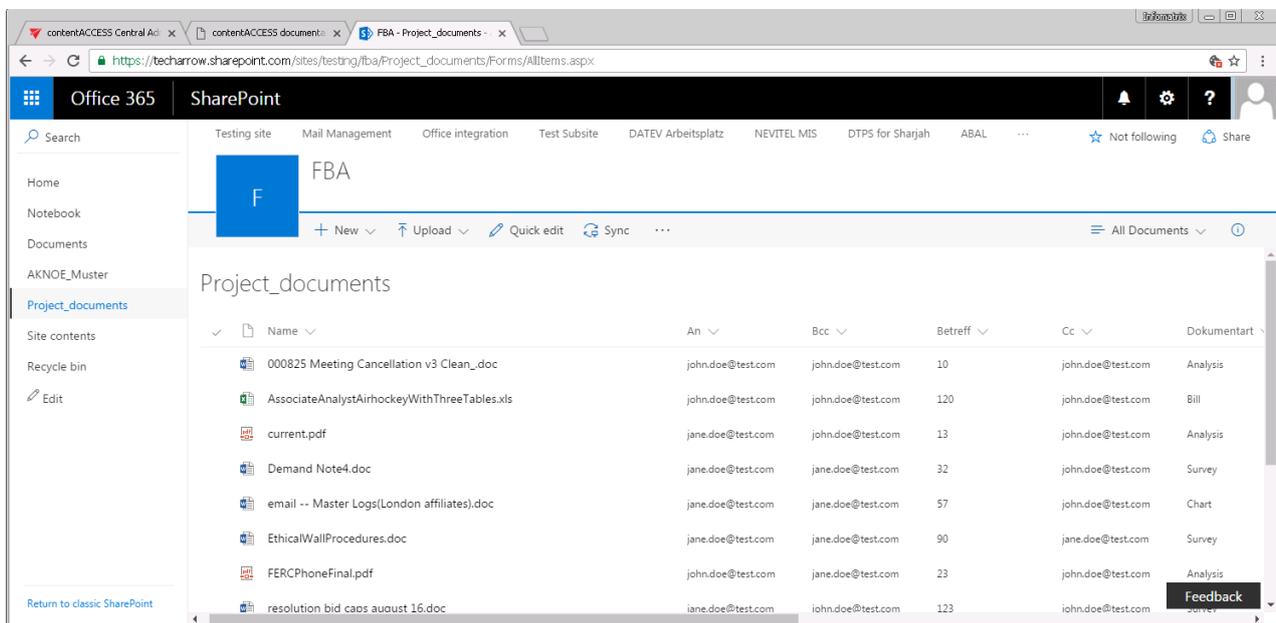
SharePoint publishing job

The purpose of this job is to publish data into SharePoint from a third party store.

Note: Currently the Kendox store type supports this. Read more in chapter [Storages](#).

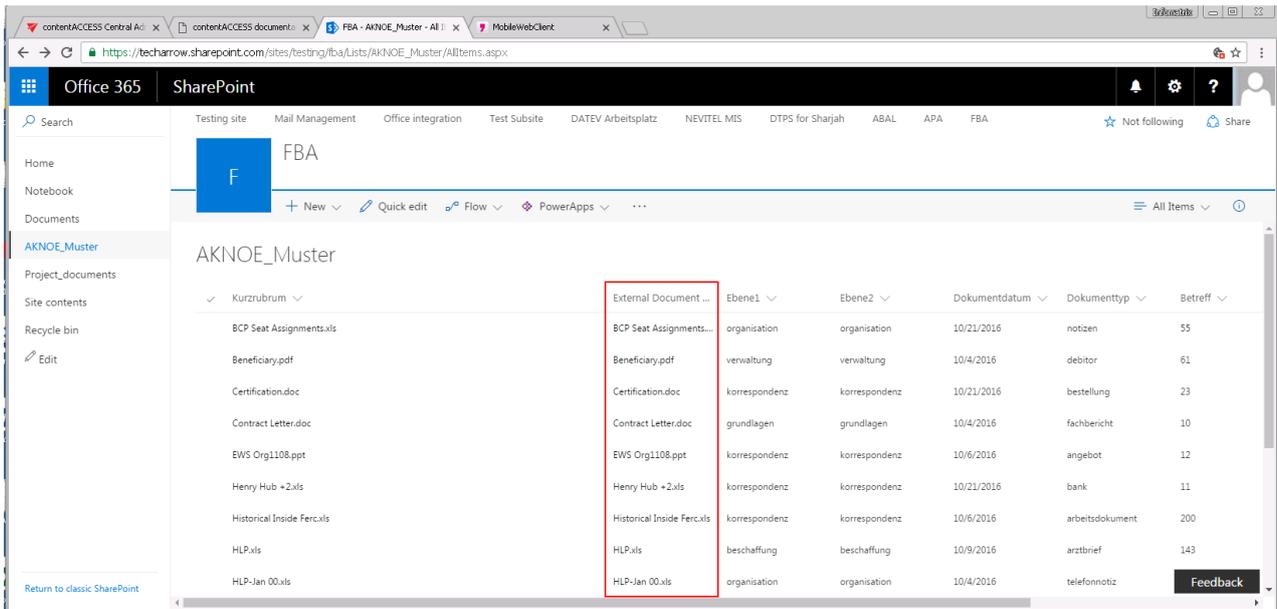
There are 2 publishing methods to be used:

- a) The job can **create a document library with real documents** or



Screenshot A: Project_documents library with real documents

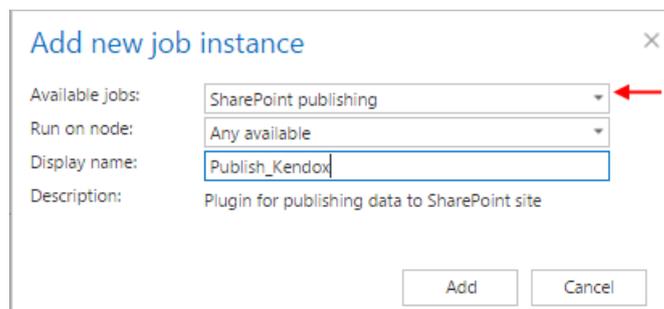
- b) It can create a **custom list** with “placeholder” items that have an **extra metadata field with an URL pointing to the document residing in the 3rd party document system** (column “External Document URL”). The custom list using the link option is like a shortcut, there’s no real binary data stored in SharePoint. Only the metadata of the original documents and the links to access them are available.



Screenshot B: AKNOE_Muster custom list with links

The document library/custom list names (“Project_documents” and “AKNOE_Muster” on the pictures above) are inherited from the source folder.

To create a new SharePoint Publishing job, click **+ new** on the **Jobs** page (**SharePoint Archive** tab → **Archive** group → **Jobs**) and select this job type in the **Add new job instance** dialog:



When a new job is created, the user is asked to configure the job immediately. On the SharePoint Publishing job’s configuration page the following must be set:

- **Scheduling settings:** Set the time when the job should run.
- **Document source:** Select the configured 3rd party storage from where you want to publish the documents into SharePoint. The storage must be first configured on the “Storages” page. (Read more in [SharePoint Archive settings.](#))
- **SharePoint configuration:** Set there the URL of the site collection or sub web where you want to create the document library/custom list based on the folder from the 3rd party storage. The URL



must be a site collection or a subweb, it cannot be an existing document library/list or a subfolder of a document library/list.

- **Publishing method:** The documents from the source storage can be either published as a
 - a) document – option “Create documents” or
 - b) as a link – option “Create link”.

If the “Create documents” option is selected, then the publishing job will create a document library based on the source folder with a content type created by the source folder’s content type. The documents will be uploaded to this document library.

If the “Create links” option is selected, then a custom list will be created with a content type based on the source folder’s content type and a new list item will be created for each document in the source folder. The new list item will have the original metadata and an additional column will be added to it with name “External Document URL”. This column will contain the link pointing to the actual document in the 3rd party system (refer to Screenshot B above).

- **Resource settings:** set here the number of workers threads running in parallel during the publishing process.

The screenshot shows the 'contentACCESS Central Administration' interface. The 'SharePoint Archive' tab is active, displaying various settings categories like Databases, System settings, Retentions, Storages, Root connections, Schedules, and Provisioning settings. Below this, the 'SharePoint publishing' configuration page is visible, showing the following settings:

- Scheduling settings:** Scheduled in: Manual start
- Document source:** Document source: Kendox
- Sharepoint configuration:**
 - Sharepoint site URL:
 - Username:
 - Password:
- Publishing method:**
 - Create documents
 - Create links
- Resource settings:** Worker thread count:

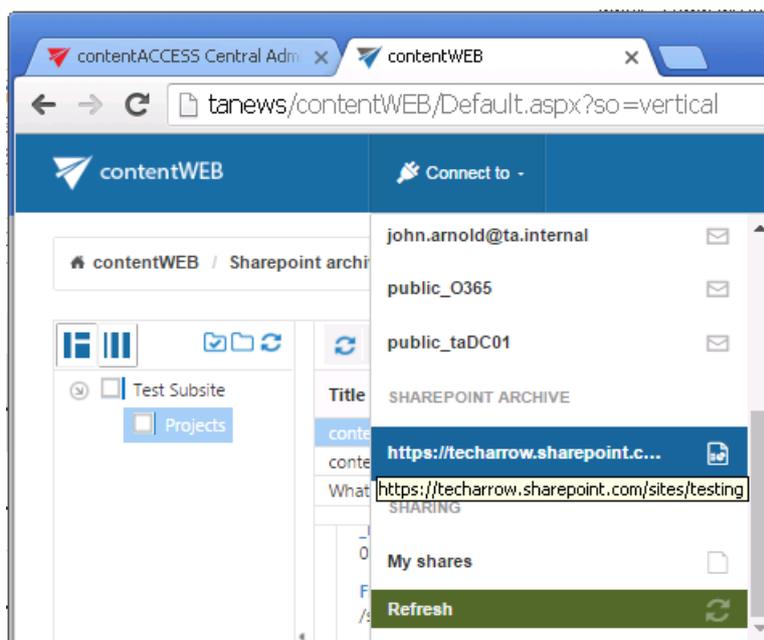
SharePoint publishing job description

All the numbers and descriptions in the job's progress have a particular meaning. In this section, we are going to explain the numbers and descriptions of a **SharePoint publishing job**.

Description	Explanation
x folders processed	x folders have been processed (a site, document library, list or subfolder counts as a folder)
x documents processed	x documents have been published to the SharePoint site
x documents failed	x documents' publishing failed
x folders failed	x folders' processing from the source provider failed, see logs for further details

SharePoint in the contentWEB archive

The archived SharePoint items can be easily accessed from contentWEB:



GDPR plugin

The **General Data Protection Regulation** (GDPR) is a regulation in EU law regarding data protection and privacy. It addresses the export of personal data outside the EU and aims to give control back to citizens and residents over their personal data.

The GDPR plugin of contentACCESS is used for making data GDPR compliant in a quick and easily understandable way. Data are indexed during every job run, so you will be able to easily search in them and view them in contentWEB and other end-user tools. If an item was changed or deleted, so will it be in the index and database during the next run of the job(s).

The whole configuration and usage will be described in the next sections.

GDPR Settings

In the following sections we will describe the settings that need to be configured if the user wants to use the [GDPR Processing](#) features.

GDPR Databases

The administrator must set here the database, where GDPR will store the metadata. For further information about how to add new databases and perform database settings, please refer to section [Databases](#).

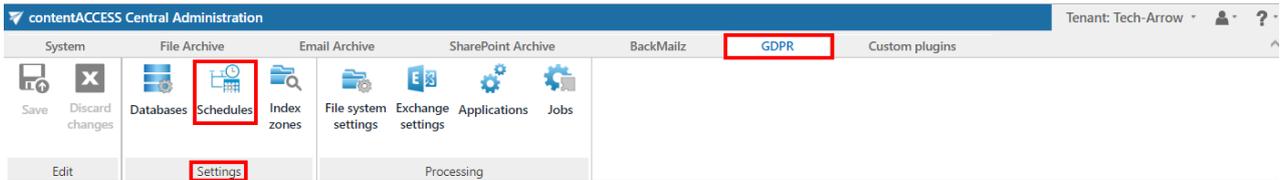


Connection name	Server	Type	Database	Schema	User	Is default
TechArrowDB	*** DEMO-CA\SQLEXPRESS	MSSQL	TechArrowDB	dbo	techarrow	Yes

The full list of all accessible databases configured for the current tenant can be found here.

GDPR Schedules

The already configured schedulers are listed on this page, in the scheduler's grid. By clicking on the **+ new** option, it is possible to create a new scheduler. For more information about how to set schedulers, please refer to the section [Schedules](#).



Schedules

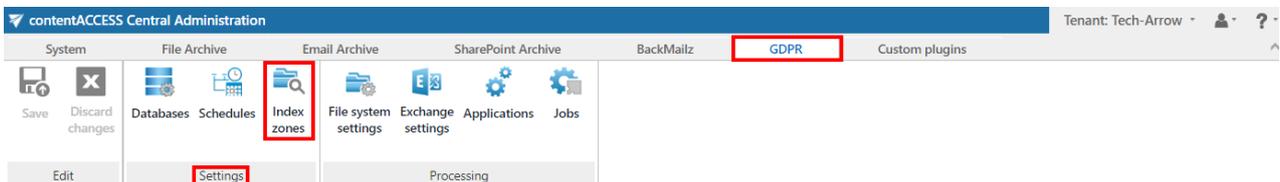
GDPR > Settings > Schedules

[+ new](#) [manage access](#)

Name	Type	Description
Belegarchiv	*** AlwaysRun	Always running in every X minutes
Daily at 1AM	*** WeekMapWithRepeat	Running based on the weekmap and continuously repeat in every X minutes
Every 1 hour	*** AlwaysRun	Always running in every X minutes
Every 2 minutes	*** AlwaysRun	Always running in every X minutes
G+P Kategorisierung	*** AlwaysRun	Always running in every X minutes
Janse-Holding	*** WeekMapWithRepeat	Running based on the weekmap and continuously repeat in every X minutes
Never	*** OneTime	Running on 1/1/2000 12:00:00 AM
TaskRunnerScheduler	*** AlwaysRun	Always running in every X minutes
WGV Journal	*** OneTime	Running on 1/1/2000 12:00:00 AM

GDPR Index zones

[Index](#) zones can be defined as a set of one or more Elasticsearch indexes, which are used for logical and physical separation of indexed documents. They were introduced to keep Elasticsearch indexes small, since smaller indexes are easier to move and distribute on multiple Elasticsearch servers.



Index zones

GDPR > Settings > Index zones

[+ new](#) [manage access](#)

Index zone name	Is default
Default index zone	*** Yes
Emails	*** No
Files	*** No
SharePoint	*** No
GDPR	*** No

Already configured Index zones are displayed on this page. By clicking on the **+ new** option, it is possible to configure a new one. Simply enter the name and click **Save**.

Index zone ✕

Index zone name:



GDPR Processing

File system settings, **Exchange settings** and **Applications** are used as data sources for the **GDPR jobs** (similar as root folders/connections and mailboxes are for File archive, Email archive and SharePoint archive jobs). In the following section we will explain how they are configured, what they are used for, and how they are working.

GDPR File system settings

Navigate to **GDPR** ⇒ **Processing** ⇒ **File system settings**:

The screenshot shows the contentACCESS Central Administration interface. The top navigation bar includes tabs for System, File Archive, Email Archive, SharePoint Archive, BackMailz, **GDPR**, and Custom plugins. Under the GDPR tab, there are sub-tabs for File system settings, Exchange settings, Applications, and Jobs. The File system settings sub-tab is selected, and the Processing button is highlighted. Below the navigation bar, the page title is "File system settings" with a breadcrumb trail: "GDPR > Processing > File system settings". The main content area is divided into sections: Database settings (with a dropdown for "TechArrowDB" and a "Change" button), Index zone settings (with a dropdown for "GDPR"), and File system locations (with a "+ new" button and a table listing existing locations). The table has columns for Path, User, Type, Version, and Agent, with one entry: "C:\Enron files", "*", "OnPrem", "None", and an empty Agent field.

The settings that will be used by the **GDPR File system job** have to be set here.

✓ Database settings:

Select an already configured connection from the dropdown list. Here the metadata will be stored. We have configured for GDPR plugin the database named “TechArrowDB”, so we set it here. (For further information on how to set database connections please refer to section [Databases.](#))

✓ Index zone:

Pick the Index zone that will be assigned to the **File system locations** by the **GDPR File system job** from the dropdown list. If you want to configure a new one, navigate to **GDPR** ⇒ **Settings** ⇒ **Index zones**.

✓ File system locations:

The File system locations that should be processed by the GDPR File system job have to be set here. To add a new location, click on + new and a pop-up window will appear. Enter the file path (location of the folder)



and the applicable user credentials. The **Type of connection** shows if the files to be processed are located on the server (on-premise) or on network shares (remote). **Version** can be either way Business or Private. The **Server** column will display the name of the server where the folder is located (if it is located on network shares). We also recommend to test the connection via the **Test connection** button.

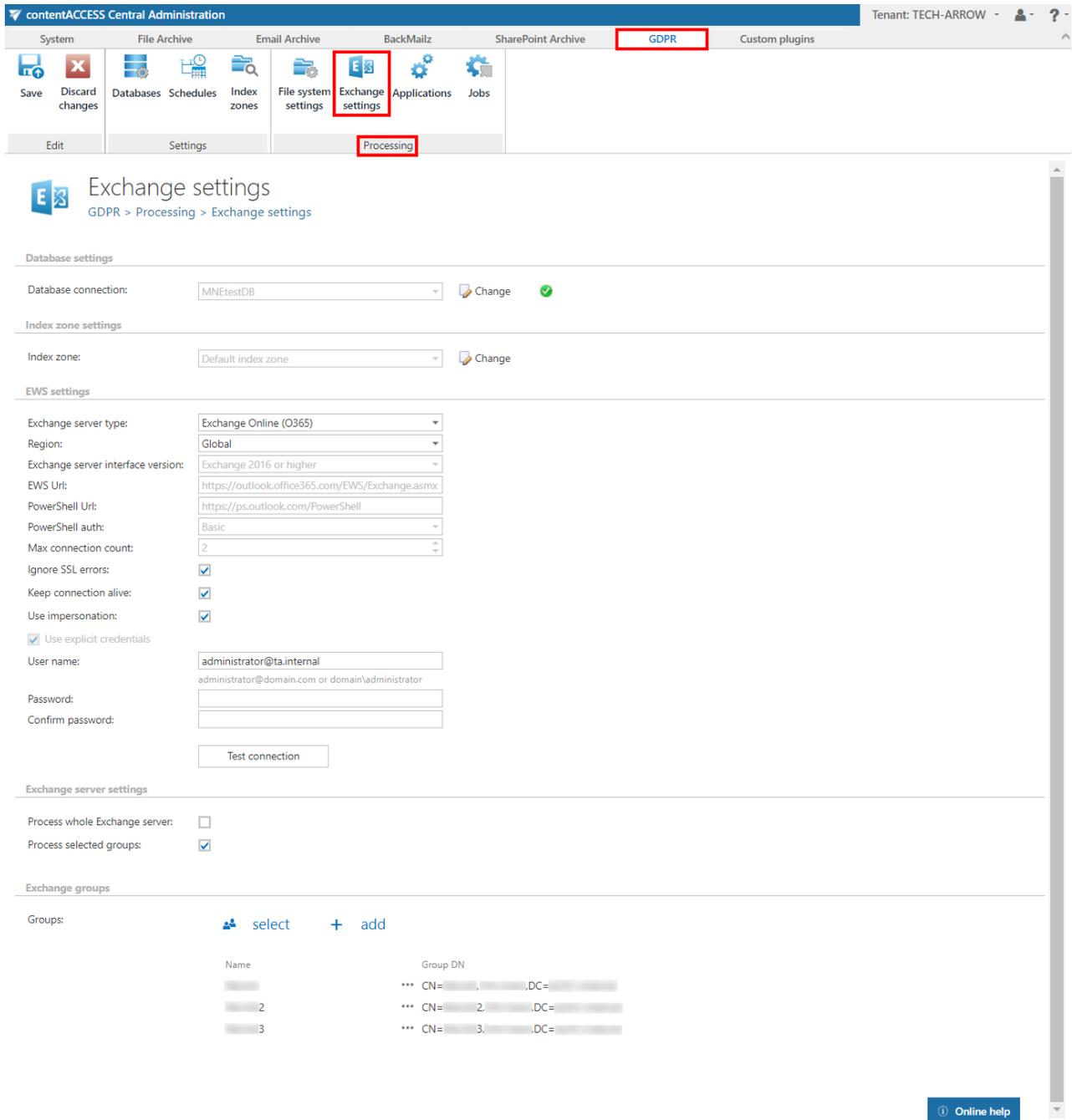
File Path ✕

Path:	<input type="text" value="C:\TestData2"/>
Use explicit credentials:	<input checked="" type="checkbox"/> Use explicit credentials
User name:	<input type="text" value="ta\administrator"/>
Password:	<input type="password" value="....."/>
Confirm Password:	<input type="password" value="....."/>
Type of connection:	<input type="text" value="On-premise file server"/>
Version:	<input type="text" value="-"/>
Server:	<input type="text"/>

✔ Connection successfull!

GDPR Exchange settings

Navigate to **GDPR** ⇒ **Processing** ⇒ **Exchange settings**:



The screenshot shows the 'contentACCESS Central Administration' interface. The top navigation bar includes 'System', 'File Archive', 'Email Archive', 'BackMailz', 'SharePoint Archive', 'GDPR', and 'Custom plugins'. The 'GDPR' tab is active, and the 'Exchange settings' link is highlighted. Below the navigation bar, the 'Exchange settings' page is displayed, showing the following sections:

- Database settings:** Database connection: MNEtestDB (Change button with green checkmark).
- Index zone settings:** Index zone: Default index zone (Change button).
- EWS settings:**
 - Exchange server type: Exchange Online (O365)
 - Region: Global
 - Exchange server interface version: Exchange 2016 or higher
 - EWS Uri: https://outlook.office365.com/EWS/Exchange.asmx
 - PowerShell Uri: https://ps.outlook.com/PowerShell
 - PowerShell auth: Basic
 - Max connection count: 2
 - Ignore SSL errors:
 - Keep connection alive:
 - Use impersonation:
 - Use explicit credentials
 - User name: administrator@ta.internal (administrator@domain.com or domain\administrator)
 - Password: [Empty field]
 - Confirm password: [Empty field]
 - Test connection button
- Exchange server settings:**
 - Process whole Exchange server:
 - Process selected groups:
- Exchange groups:**
 - Groups: select + add
 - Table with columns: Name, Group DN
 - Table content:

Name	Group DN
1	CN=1, .DC=
2	CN=2, .DC=
3	CN=3, .DC=

An 'Online help' button is located in the bottom right corner of the interface.

The settings that will be used by the GDPR Exchange job have to be set here.

✓ Database settings:

Select the GDPR database, that you have previously configured on **GDPR** ⇒ **Settings** ⇒ **Databases** page (in our case it is database "TechArrowDB"), from the dropdown list. This selected database will be used by the GDPR Exchange job. The job will store here the metadata during the synchronization process.



✓ Index zone settings:

Pick the Index zone that will be assigned to the **Exchange groups/servers** by the **GDPR Exchange job** from the dropdown list. If you want to configure a new one, navigate to **GDPR ⇒ Settings ⇒ Index zones**.

✓ EWS settings:

Under **Exchange server type** and **Exchange server interface version** select the type and version of the server, where your email provider is running.

Then enter the **EWS URL**, **PowerShell URL** and select the **PowerShell authentication** from the dropdown list. These data must be requested from the email provider you are using (the configuration properties are the same for On-premise and Hosted Exchange).

In case of the user having/using a [German cloud](#) (dedicated and isolated Microsoft Azure version for Germany), **Germany** must be selected in the **Region** dropdown list.

Under **Max. connection count** option, the user may define how many parallel connections will be maintained by the system when connecting to PowerShell.

If you do not have a valid certificate, you can check the **Ignore SSL errors** checkbox.

Keep connection alive: If this option is turned on, then the connection between contentACCESS and the Exchange server is cached, which increases the performance. If the Exchange is load balanced, some requests can land on another Exchange and therefore cause errors in contentACCESS. In these cases, unchecking the keep alive option will destroy the connection after each request and will rebuild it on the next request.

- If you are communicating with **one Exchange server**: **turn it on** to increase the performance
- If you have a **load balanced Exchange environment** and there are **communication problems** with the Exchange: it is recommended to **turn it off**

Further enter the applicable **User name** and **Password** to connect to the Exchange (use explicit credentials or log in under service-credentials).

Important!!! The user set under Exchange connections must have **impersonation rights** for the mailbox(es) that he/she would like to process.

We recommend to run a test connection via **Test** button.



✓ Exchange server settings:

Here the user may select if he would like to process the whole Exchange server or just selected groups.

✓ Exchange groups:

This section will appear only if the user checked the option **Process selected groups** in the previous section. The groups to be processed may be added by clicking on **select** and then picking some groups from the Exchange server, or by clicking on **add** and then writing the name of the group.

GDPR Applications

Navigate to **GDPR** ⇒ **Processing** ⇒ **Applications**:

The screenshot shows the 'contentACCESS Central Administration' interface. The top navigation bar includes 'System', 'File Archive', 'Email Archive', 'SharePoint Archive', 'BackMailz', 'GDPR', and 'Custom plugins'. The 'GDPR' tab is selected. Below the navigation bar, the 'Applications' icon is highlighted with a red box. The 'Processing' sub-tab is also highlighted with a red box. The main content area shows the 'Applications' settings page, which includes a breadcrumb trail 'GDPR > Processing > Applications'. The 'Database settings' section shows 'Database connection' set to 'TechArrowDB'. The 'Index zone settings' section shows 'Index zone' set to 'GDPR'. The 'Applications' section shows a table with one application named 'Nortwind'.

Application name	Database name	Database server
Nortwind	*** Northwind	.\sqlcxpress

The settings that will be used by the GDPR Application job have to be set here.

✓ Database settings:

Select an already configured connection from the dropdown list. Here the metadata will be stored. We have configured for GDPR plugin the database named “TechArrowDB”, so we set it here. (For further information on how to set database connections please refer to section [Databases](#).)

✓ Index zone:

Pick the Index zone that will be assigned to the **Applications** by the **GDPR Application job** from the dropdown list. If you want to configure a new one, navigate to **GDPR** ⇒ **Settings** ⇒ **Index zones**.

✓ Applications:

The applications to be processed by the GDPR Application job are added/edited here. To add a new application, click on **+ new**.

Applications

Application name	Database name	Database server
Nortwind	Northwind	.\sqlexpress

Write down the name of the application and click **Next**.

New application

Name of the application

Welcome to the New application wizard. As first step, please provide the name of the application you would like to get mapped by contentACCESS.

Application name:

Specify the database connection parameters. By default contentACCESS is connected to the database with the credentials of the user, under whom contentACCESS is running. If you want to use SQL credentials that differ from these credentials data, then check checkbox **Use explicit credentials** and enter the **User** and **Password** that you want to use for connecting to database. You can also run a test connection with the **Test** button in the left corner of the window.

New application

Database connection

Please provide the database connection parameters of your application.

Database server:

Database name:

Use explicit credentials:

Database user:

Database password:

Database schema:



Choose if the data should be loaded from a template (well-known application, predefined template) or from a database (defining the set of data from scratch). Click **Next**.

New application ×

Data mapping

To have an application mapped by contentACCESS, the set of tables, views and columns meant to be indexed has to be defined. contentACCESS is familiar with the structure of several well-known applications. Their data definition can be loaded from a predefined template, by choosing 'Load from template'. If you would like to define the set of data from scratch, choose 'Load from database'.

Load from template

Load from database

Select the tables and/or views from which you would like to acquire data and click on the **Add** button. If you want to add all items, click on **Add all**. The selected tables/views will be added to the lower table. To remove items from the list, select them and click on the **Remove selected** button under the lower table. Click **Next**.



Edit application ✕

Tables and views

Please select the tables and views from which you would like to acquire data.. You can provide a display name for each of them. This name will be shown for the GDPR users in contentWEB and other end-user tools.

Available tables and views:

<input type="checkbox"/>	Name	Type
<input type="checkbox"/>	Alphabetical list of products	View
<input type="checkbox"/>	Categories	Table
<input type="checkbox"/>	Category Sales for 1997	View
<input type="checkbox"/>	Current Product List	View
<input type="checkbox"/>	Customer and Suppliers by City	View
<input type="checkbox"/>	CustomerCustomerDemo	Table
<input type="checkbox"/>	CustomerDemographics	Table
<input type="checkbox"/>	EmployeeTerritories	Table

Selected tables and views:
It is possible to specify the display name by doubleclicking on the grid cell.

#	Name	Display name	Type
<input type="checkbox"/>	Contacts	Contacts	Table
<input type="checkbox"/>	Customers	Customers	Table
<input type="checkbox"/>	Employees	Employees	Table
<input type="checkbox"/>	Orders	Orders	Table
<input type="checkbox"/>	Suppliers	Suppliers	Table

Choose the columns from which you would like to acquire data (the columns of items in [contentWEB](#) and other end-user tools). It is also important to define the identifier in every table and view (for example, we chose ContactID for Contacts, as seen on screenshot below). The identifier serves for exact identification of a record in database. In the lower table specify the display name, Title, Identifier and Keyword fields. If the user tries to specify more than one column as the title, he will be warned about that. Click **Next**.



Edit application

Data mapping

Please choose the columns from which you would like to acquire data. You can provide a display name for each of them. This name will be shown for the GDPR users in contentWEB and other end-user tools. It is also important to define the identifier in every table and view. The identifier is built from one or more columns, and serves for exact identification of a record in a database.

Available columns:

<input type="checkbox"/>	Data source	Column	Type
<input type="checkbox"/>	Contacts	ContactTitle	Text
<input type="checkbox"/>	Contacts	ContactType	Text
<input type="checkbox"/>	Contacts	Extension	Text
<input type="checkbox"/>	Contacts	Fax	Text
<input type="checkbox"/>	Contacts	HomePage	Text
<input type="checkbox"/>	Contacts	Phone	Text
<input type="checkbox"/>	Contacts	PhotoPath	Text
<input type="checkbox"/>	Contacts	PostalCode	Text

It is possible to specify the display name, Identifier, Title and Keyword fields by doubleclicking on the grid cells.
 *Note : Only one column can be specified as a title column for a datasouce.

#	Data source	Column	Display name	Type	Identifier	Title	Keyword
<input type="checkbox"/>	Contacts	Address	Address	Text	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	Contacts	City	City	Text	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	Contacts	CompanyName	CompanyName	Text	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	Contacts	ContactID	ContactID	Integer	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	Contacts	ContactName	ContactName	Text	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Page 1 of 7 (35 items) ◀ 1 2 3 4 5 6 7 ▶

The contentWEB columns will then look like this (for example for our data source **Contacts**, because of the columns we chose in the screenshot above):

Title	Address	City	CompanyName	ContactID	ContactName
-------	---------	------	-------------	-----------	-------------

It is possible to save the configuration as a template for a later use by checking the **Save as template** checkbox. Click on **Save application** and you app will be ready for use in GDPR Application job!



Edit application ✕

Save template

Feel free to save the configured data mapping as a template for future use.

Save as template

Save application Cancel

GDPR Jobs

The job processes all the specified roots/groups that are present on the configuration page (one job can be used only for one configuration page – one job can't process for example both Exchange and Applications). The job crawls all the roots recursively, builds up the structure in the database and immediately indexes the data (Exchange – it indexes attachments as well). The job indexes all the data that are allowed by the filters. After the job has finished its run, the folder structure and the data will be visible in contentWEB and in the other client-side applications as well. If an item/folder is modified or deleted, at the next run of the job it will be modified or deleted from the database and index as well – this will help to keep your data GDPR compliant, as you can easily search, select and delete the data you have/want to get rid of (for example when a customer unsubscribes or when an employee leaves the company).

All GDPR jobs available for the current tenant are visible on **GDPR ⇒ Processing ⇒ Jobs**.

The screenshot shows the 'Jobs' page in the 'contentACCESS Central Administration' interface. The breadcrumb is 'GDPR > Processing > Jobs'. There are action buttons: '+ new', 'refresh', 'disable auto refresh', and 'manage access'. A dropdown menu shows 'Show all jobs'. Below is a table of jobs:

ID	Display Name	Type	Status	Last Start	Last Duration	Progress	Summary	Next Start	Is active	Cluster node	Running on
120	GDPR application	GDPR Application	Idle	5 days ago	52 seconds	0 %	5 entities processed 1092 items processed	Never	Yes	Any available	-
131	GDPR Email	GDPR Exchange	Idle	11 hours ago	5 hours	100 %	4 mailboxes synchronized. 16383 items newly indexed (83 folders skipped. 29320 skipped. 115 failed. 106 updated)	in 12 hours	Yes	Any available	-
132	GDPR file	GDPR File system	Idle	1 day ago	5 minutes	100 %	11 folders processed 2631 documents processed (2631 newly processed)	Never	Yes	Any available	-

GDPR File system job

This job processes the File system locations that are set in the [GDPR File system settings](#).

To create a new GDPR File system job, click on the **+ new**, pick the job type from the dropdown list and enter the display name. Click on **Add**.

Add new job instance ✕

Available jobs:

Run on node:

Display name:

Description: Plugin for File system GDPR

On the job's configuration page go through the following sections:

✓ Report mode settings:

If the **Use report mode** checkbox is checked, the job will run in report mode. After the job finishes its run in this mode, the user will be able to download a .csv report file here in this section. The file will contain a list of files that belong to the folder(s) that is (are) configured in **GDPR File system settings** and some information to them, including whether they will be processed or not.

Report mode settings

Use report mode:	<input checked="" type="checkbox"/>	
Generated report file:	File name:	JobReport_7779b902-c4eb-49f0-b7de-6eed8313a926.csv
	Size:	1.3 KB
	Date:	4/4/2019 3:01:51 PM
<input type="button" value="Download report"/>		

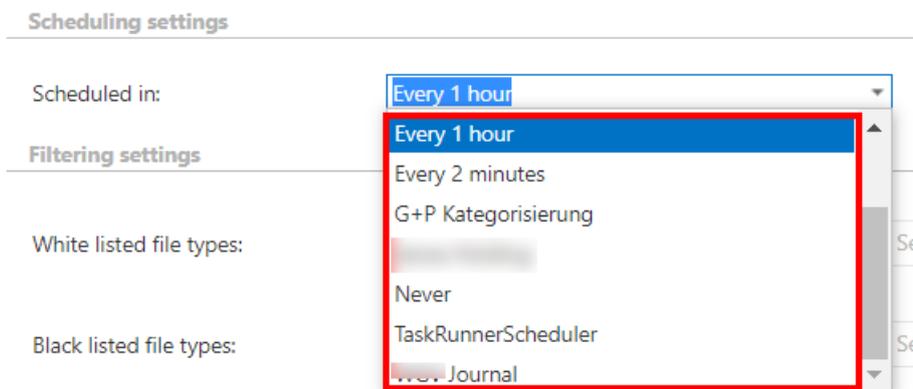


	A	B	C	D	E
1	FileName	ModificationDate	Path	Status	Filter
2	10-crucial-	5/19/2017 13:26	C:\TestReport\	will be processed	no filter
3	256x256_p	1/18/2017 14:50	C:\TestReport\	will be processed	no filter
4	9h6c0qj.jp	1/12/2017 10:36	C:\TestReport\	will be processed	no filter
5	ai-email.jp	2/22/2017 14:26	C:\TestReport\	will be processed	no filter
6	bdb3d704:	2/1/2017 11:13	C:\TestReport\	will be processed	no filter
7	cloud.mail	2/7/2017 13:40	C:\TestReport\	will be processed	no filter
8	office-101	3/17/2017 13:10	C:\TestReport\	will be processed	no filter
9	Outlook-E	5/29/2018 11:18	C:\TestReport\	will be processed	no filter
10	pros-and-c	5/29/2018 11:18	C:\TestReport\	will be processed	no filter
11	TestingRFA	5/31/2018 12:23	C:\TestReport\	will be processed	no filter
12	windows-1	5/29/2018 11:18	C:\TestReport\	will be processed	no filter

Screenshot: Report file preview

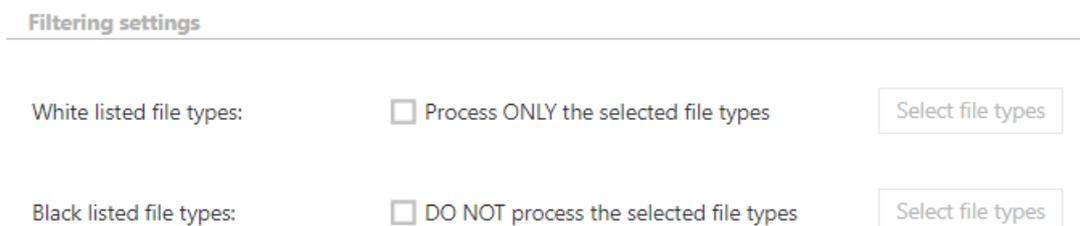
✓ **Scheduling settings:**

In this step the running time(s) of the job must be selected. It is possible either to select a scheduler from the list or to create a new scheduler via **create new...** option from the dropdown list. For the GDPR jobs it is recommended to set a schedule, which will start the job every week.

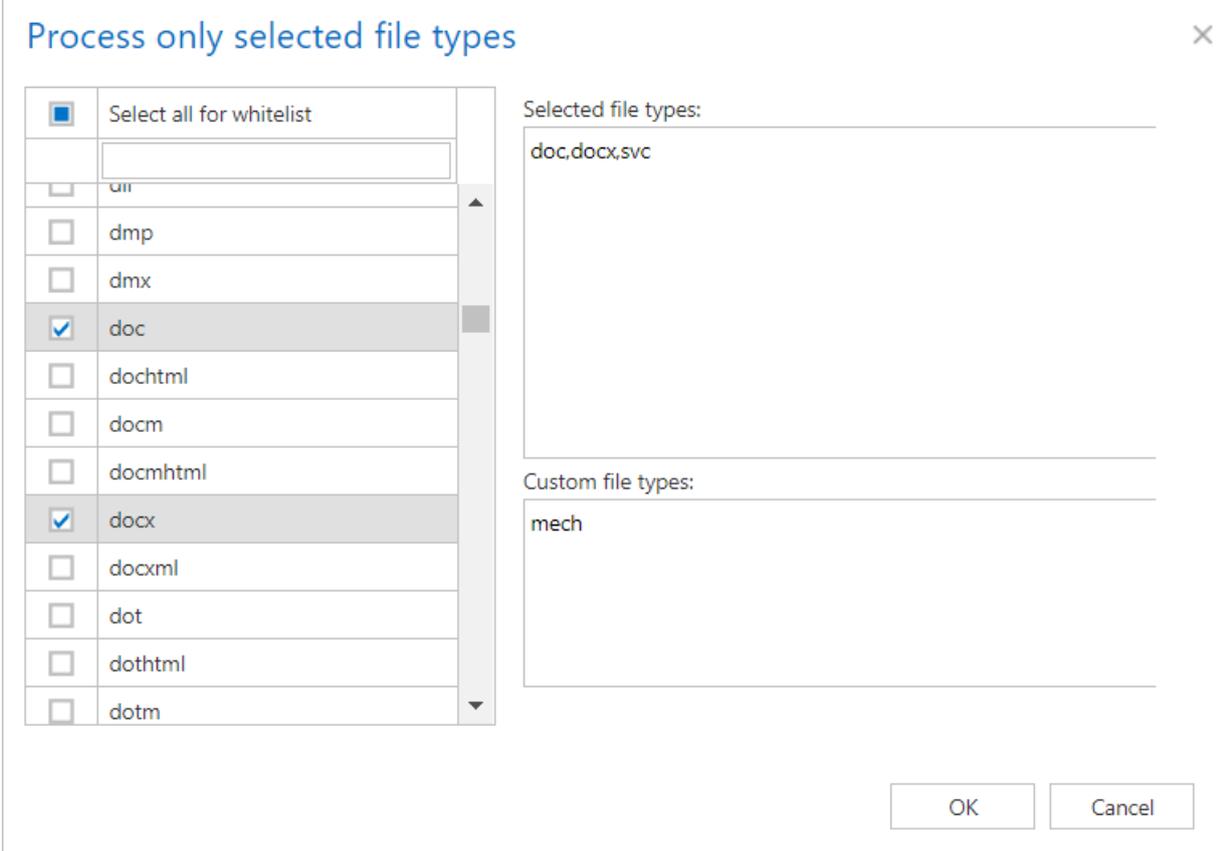


✓ **Filtering settings:**

In this section it is possible to select the file types from which the job should/shouldn't extract the content. It is also possible to specify custom file types.



White listed file types: If this option is checked and the file types are filled in, only content of those types will be extracted. Any other file type's content will not be extracted.



Process only selected file types ✕

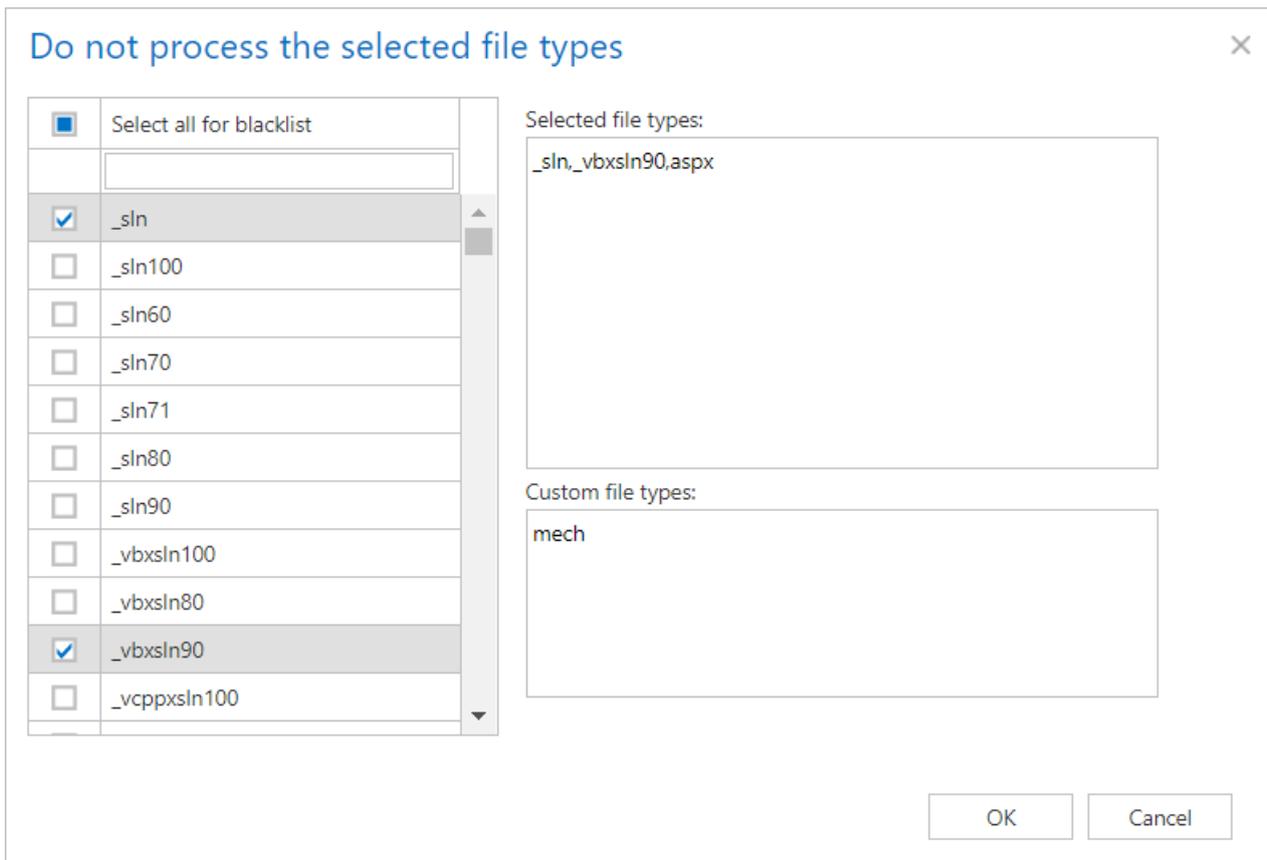
<input checked="" type="checkbox"/>	Select all for whitelist
<input type="checkbox"/>	uri
<input type="checkbox"/>	dmp
<input type="checkbox"/>	dmx
<input checked="" type="checkbox"/>	doc
<input type="checkbox"/>	dohtml
<input type="checkbox"/>	docm
<input type="checkbox"/>	docmhtml
<input checked="" type="checkbox"/>	docx
<input type="checkbox"/>	docxml
<input type="checkbox"/>	dot
<input type="checkbox"/>	dohtml
<input type="checkbox"/>	dotm

Selected file types:
doc,docx,svc

Custom file types:
mech

OK Cancel

Black listed file types: If this option is checked and the file types are filled in, content of those types will not be extracted. Any other file type's content will be extracted.



✓ **Filtering settings:**

Click on the **Change filter** button and set the filtering according to your needs and/or regulations. To learn more about how to work with filtering settings, please, check [this](#) section of our documentation.

Filter settings ✕

visual
text

A N D ▼	File name ▼	Equals ▼	Microsoft logo ✕
	Size ▼	<= ▼	2 MB ▼ ✕

+add group +add condition

+add new group

OK
Cancel

✓ Notification settings:

Select here the cases, in which you need to get notification emails from the GDPR File system job. It is possible to set here if you need such a notification email always/never, or if you need it only in case when an error/warning occurred during the job run. Into the **Recipient list** textbox insert the email address(es) of the person(s), who will get such notifications. **Notifications** should be used if the administrator does not use the **System logs** feature.



Notification settings

Send when:	Never
Recipient list:	john.doe@example.com,peter.white@example.com,

Job functionality

File deletion: After a file is deleted from one of the specified root folders and the job is ran, the file is deleted from the database and from the index as well.

Folder deletion: After a subfolder is deleted from one of the specified root folders and the job is ran, the folders and the files under that folder are deleted recursively from the database and from the index as well.

File move: After a file has been moved between different folders and the GDPR File system job has been ran again, the file will disappear from its original location and show up under the new location. These information will also be updated in the database and index.

Folder move: After a folder has been moved between different locations and the GDPR File system job has been ran again, the folder and the files will disappear from their original location and show up under the new location. These information will also be updated in the database and index.

Root folder deletion: After a root folder is deleted from the **File system settings** configuration, the next time the job is started, it will delete all the root folder related data from the database and from the index as well.

File modification: If a file has been modified since the last run of the job, then the job will update the file's content and properties in the database and index as well.

GDPR file system job description

All the numbers and descriptions in the job's progress have a particular meaning. In this section, we are going to explain the numbers and descriptions of a **GDPR file system job**.

Description	Explanation
x folders processed	x folders and subfolders have been processed
x folders failed	x folders' processing failed
x documents processed	x documents have been processed



x documents skipped	x documents have been skipped because they already exist in the index, or because of the filtering settings
x documents failed	x documents' indexing failed
x documents updated	x documents' data have been updated in the index
x newly processed	x documents have been newly indexed
x folders skipped	x folders have been skipped because of the filtering settings
x folders deleted	x folders have been deleted from the index because they don't exist in the source anymore
x documents deleted	x documents have been deleted from the index because they don't exist in the source anymore

GDPR Exchange job

This job processes the Exchange servers/groups that are set in the [GDPR Exchange settings](#).

To create a new GDPR Exchange job, click on the **+ new**, pick the job type from the dropdown list and enter the display name. Click on **Add**.

Add new job instance
×

Available jobs:

Run on node:

Display name:

Description: Plugin for accessing Exchange to ensure GDPR.



On the job's configuration page go through the following sections:

✓ Scheduling settings:

In this step the running time(s) of the job must be selected. It is possible either to select a scheduler from the list or to create a new scheduler via **create new...** option from the dropdown list. For the GDPR jobs it is recommended to set a schedule, which will start the job every week.

Scheduling settings

Scheduled in: Every 1 hour

Filtering settings

White listed file types: ... Sel

Black listed file types: ... Sel

✓ Filtering settings:

In this section it is possible to select the file types from which the job should/shouldn't extract the content. It is also possible to specify custom file types.

Filtering settings

White listed file types: Process ONLY the selected file types Select file types

Black listed file types: DO NOT process the selected file types Select file types

White listed file types: If this option is checked and the file types are filled in, only content of those types will be extracted. Any other file type's content will not be extracted.

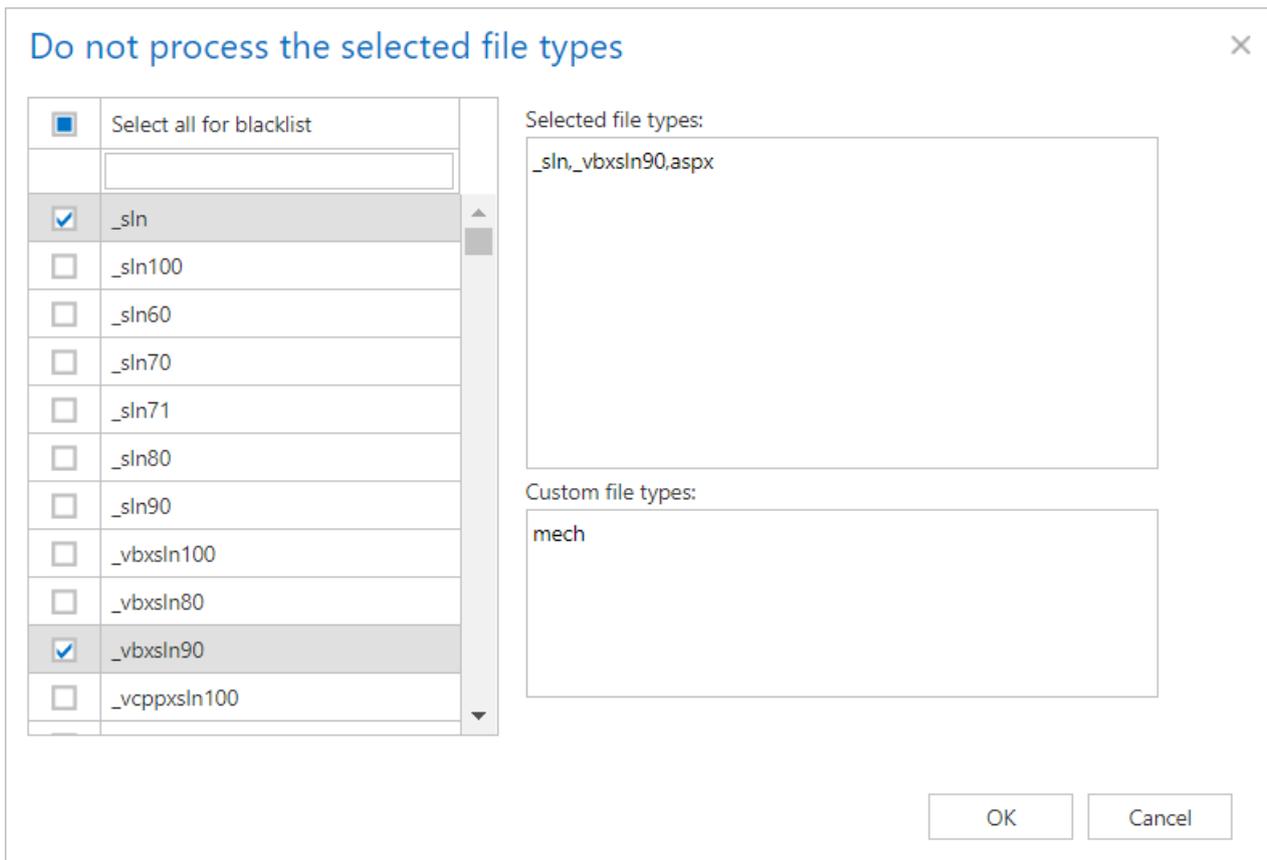
Process only selected file types ✕

<input checked="" type="checkbox"/>	Select all for whitelist
<input type="checkbox"/>	uri
<input type="checkbox"/>	dmp
<input type="checkbox"/>	dmx
<input checked="" type="checkbox"/>	doc
<input type="checkbox"/>	dohtml
<input type="checkbox"/>	docm
<input type="checkbox"/>	docmhtml
<input checked="" type="checkbox"/>	docx
<input type="checkbox"/>	docxml
<input type="checkbox"/>	dot
<input type="checkbox"/>	dohtml
<input type="checkbox"/>	dotm

Selected file types:
doc,docx,svc

Custom file types:
mech

Black listed file types: If this option is checked and the file types are filled in, content of those types will not be extracted. Any other file type's content will be extracted.



✓ **Filtering settings:**

Click on the **Change filter** button and set the filtering according to your needs and/or regulations. To learn more about how to work with filtering settings, please, check [this](#) section of our documentation.

Filter settings ✕

+ add custom property

visual
text

AND	Has attachment ▼	= ▼	No ▼	✕
	Body ▼	Contains ▼	Update	✕
	Subject ▼	Equals ▼	Microsoft	✕
+add group +add condition				
+add new group				

OK
Cancel

✓ Exclude folders:

The folders to be excluded may be selected manually or imported from a file. The file to be imported must contain the list of folders to be excluded. This excluding works the same as in [File archive](#) and [Email archive](#).



Exclude folder ✕

Exclude folder settings

Pattern:

Hint:

\Example	Exclude the folder Example on the root
Example	Exclude all folders with name Example
\Example\Example	Exclude subfolder 'Example' of the folder Example on the root
Example\Example	Exclude subfolder Example of folders with name Example
\Example*	Exclude subfolders of the folder Example on the root
Example*	Exclude all subfolders of folders with name Example
\Example**Example*	Exclude subfolder *Example* of the folder Example on the root
Example**Example*	Exclude subfolder *Example* of folders with name Example
\Ex*	Exclude all folders that start with Ex on the root
Ex*	Exclude all folders that start with Ex
\Ex**	Exclude all subfolders of folders that start with Ex on the root
Ex**	Exclude subfolders of all folders that start with Ex

Special characters *, +, ?, [, { }, [], (), ^, \$, ., # need to be escaped by backslash \

Example: Folder\Folder \John\ will exclude the path Folder\Folder (John). If the folder divider \ is followed by subfolders pattern * or with any escaped special character it must be escaped, too. E.g. the folder Test\#abc# is excluded with using a pattern Test\\#abc\#.

The entered pattern is case-insensitive

✓ **Notification settings:**

Select here the cases, in which you need to get notification emails from the GDPR Exchange job. It is possible to set here if you need such a notification email always/never, or if you need it only in case when an error/warning occurred during the job run. Into the **Recipient list** textbox insert the email address(es) of the person(s), who will get such notifications. **Notifications** should be used if the administrator does not use the **System logs** feature.



Notification settings

Send when:	<input type="text" value="Never"/>
Recipient list:	<input type="text" value="john.doe@example.com,peter.white@example.com"/>

✓ Resource settings:

Set the value, which will determine how many items will be processed simultaneously by the GDPR Exchange job. The recommended value is "2".

Resource settings

Worker thread count:	<input type="text" value="2"/>
----------------------	--------------------------------

Job functionality

Minified provisioning: Based on the selected groups that need to be processed every time when the job is started, a minified version of the provisioning is also started - it adds the mailboxes that can be found in the specified groups to the provisioning table (cannot be seen by the user) and later on the job is processing these mailboxes. If the selected groups are changed and in the current selection there are mailboxes which are no longer part of any groups, then all the data related to these mailboxes are deleted from the database and from the index as well, including emails, folders and the mailboxes themselves.

Item deletion: After an item is deleted from one of the mailboxes and the job is ran, the item is deleted from the database and from the index as well.

Folder deletion: After a subfolder is deleted from one of the specified mailboxes and the job is ran, the folders and items under that folder are deleted recursively from the database and from the index as well.

Item move: After an item has been moved between different folders and the GDPR Exchange job has been ran again, the item will disappear from its original location and show up under the new location. These information will also be updated in the database and index.

Folder move: After a folder has been moved between different locations and the indexing job has been ran again, the folder and the items will disappear from its original location and show up under the new location. These information will also be updated in the database and index.

Item updating: If an item has been updated in the mailbox since the last run of the job, then the job will update the email's content and properties in the database and index as well.



Exchange group/server deletion: After an exchange group/server is deleted from the **Exchange settings** configuration, the next time the job is started, it will delete all the related data from the database and from the index as well.

GDPR Exchange job description

All the numbers and descriptions in the job's progress have a particular meaning. In this section, we are going to explain the numbers and descriptions of a **GDPR Exchange job**.

Description	Explanation
x mailboxes synchronized	x mailboxes have been processed
x mailboxes failed	x mailboxes' processing failed
x items newly indexed	x items have been newly indexed
x folders skipped	x folders have been skipped because they are hidden or because of the filtering settings
x items skipped	x items have been skipped because they are already indexed or because of the filtering settings
x items failed	x items' indexing failed
x items removed	x items have been removed from the index because they don't exist in the source mailbox anymore
x items update	x items have been updated in the index

GDPR Application job

This job processes the Applications that are set in the [GDPR Applications](#).

To create a new GDPR Application job, click on the **+ new**, pick the job type from the dropdown list and enter the display name. Click on **Add**.

Add new job instance ✕

Available jobs:

Run on node:

Display name:

Description: Plugin for accessing applications to ensure GDPR.

On the job's configuration page go through the following sections:

✓ **Scheduling settings:**

In this step the running time(s) of the job must be selected. It is possible either to select a scheduler from the list or to create a new scheduler via **create new...** option from the dropdown list. For the GDPR jobs it is recommended to set a schedule, which will start the job every week.

Scheduling settings

Scheduled in:

Notification settings

Send when:

Recipient list:

Resource settings

Worker thread count:

Every 1 hour

Every 1 hour

Every 2 minutes

G+P Kategorisierung

Never

TaskRunnerScheduler

Journal

✓ **Notification settings:**

Select here the cases, in which you need to get notification emails from the GDPR Application job. It is possible to set here if you need such a notification email always/never, or if you need it only in case when an error/warning occurred during the job run. Into the **Recipient list** textbox insert the email address(es) of the person(s), who will get such notifications. **Notifications** should be used if the administrator does not use the **System logs** feature.



Notification settings

Send when:	<input type="text" value="Never"/>
Recipient list:	<input type="text" value="john.doe@example.com,peter.white@example.com"/>

✓ Resource settings:

Set the value, which will determine how many items will be processed simultaneously by the GDPR Application job. The recommended value is “2”.

Resource settings

Worker thread count:	<input type="text" value="2"/>
----------------------	--------------------------------

Job functionality

Information deletion: After an information is deleted from one of the specified tables or views of the specified application and the job is ran, the information is deleted from the database and from the index as well.

Table/view deletion: After a table/view is deleted from one of the specified applications and the job is ran, the information under that table/view are deleted recursively from the database and from the index as well.

Information move: After an information has been moved between different tables/views and the GDPR Application job has been ran again, the information will disappear from its original location and show up under the new location. It will also be updated in the database and index.

Table/view move: After a table/view has been moved in the specified application and the GDPR Application job has been ran again, the table/view will disappear from its original location and show up under the new location. These information will also be updated in the database and index.

Application deletion: After an application is deleted from the **Applications** configuration, the next time the job is started, it will delete all the related data from the database and from the index as well.

Item modification: If an item has been modified since the last run of the job, then the job will update the item’s content and properties in the database and index as well.

GDPR application job description

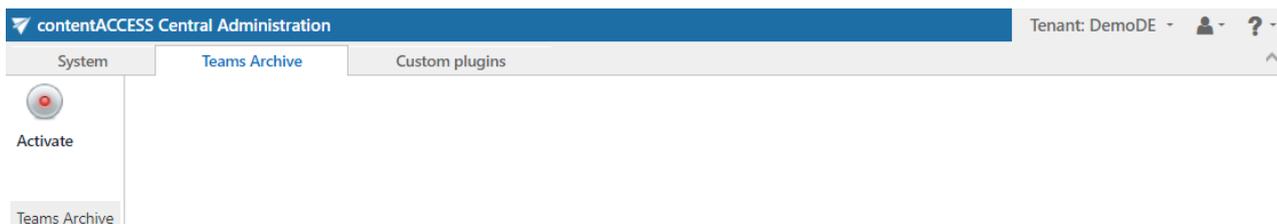
All the numbers and descriptions in the job's progress have a particular meaning. In this section, we are going to explain the numbers and descriptions of a **GDPR application job**.

Description	Explanation
x entities processed	x database connections have been processed
x entities failed	x database connections' processing failed
x items processed	x database entries' indexing succeeded
x items failed	x database entries' indexing failed

Teams archive

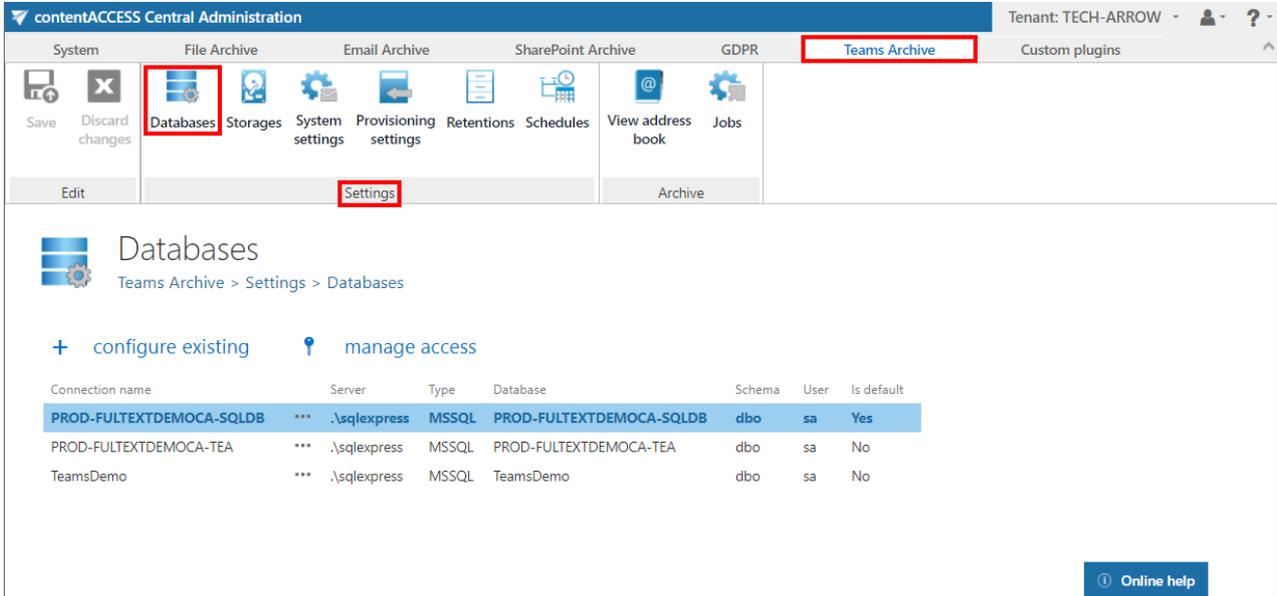
Teams archive plugin of contentACCESS is used for archiving private chat messages, messages of selected Teams and their channels (including message replies, reactions, files, all tabs, etc.), full SharePoint content and also permissions. The archived items can be later viewed in contentWEB.

When configuring Teams archive for the first time, the user needs to activate it. After successful activation, the **Settings** of the **Teams archive** get displayed.



Teams archive databases

Navigate to **Teams Archive** ⇒ **Settings** ⇒ **Databases**:



The screenshot shows the 'contentACCESS Central Administration' interface for a tenant named 'TECH-ARROW'. The ribbon includes 'System', 'File Archive', 'Email Archive', 'SharePoint Archive', 'GDPR', 'Teams Archive', and 'Custom plugins'. The 'Teams Archive' tab is active, and the 'Databases' button is highlighted. Below the ribbon, the 'Settings' button is also highlighted. The main content area displays the 'Databases' configuration page, showing a table of configured databases.

Connection name	Server	Type	Database	Schema	User	Is default
PROD-FULTEXTDEMOCA-SQLDB	***. \.sql\express	MSSQL	PROD-FULTEXTDEMOCA-SQLDB	dbo	sa	Yes
PROD-FULTEXTDEMOCA-TEA	***. \.sql\express	MSSQL	PROD-FULTEXTDEMOCA-TEA	dbo	sa	No
TeamsDemo	***. \.sql\express	MSSQL	TeamsDemo	dbo	sa	No

Here you can find the full list of all accessible databases, which are configured for the tenant. The destination for storing processed metadata can be set as **on premises** or **cloud** on the **Database settings** page. For further information on how to add new databases and perform database settings, please refer to section [Databases](#).

Teams archive System settings

General Teams archive system settings are available on the System settings page. To configure these settings, navigate to **Teams Archive** ⇒ **Settings** ⇒ **System settings** on the ribbon:

contentACCESS Central Administration Tenant: First

System | File Archive | Email Archive | SharePoint Archive | GDPR | **Teams Archive** | Custom plugins

Save | Discard changes | Databases | Storages | **System settings** | Provisioning settings | Retentions | Schedules | View address book | Jobs

Edit | **Settings** | Archive

System settings

Teams Archive > Settings > System settings

a) Database settings

Database connection: TeamsArchive

b) Client application settings

Application (client) ID: 72c73cf4-
 Directory (tenant) ID: 4b0eddf1-
 Client secret:
 Permission type: Application
 SharePoint access: Use explicit SharePoint app credentials
 SharePoint application ID: 2ff43d19-
 Certificate file: Please select a file to upload **Browse...**
 Certificate info: Common name: CN=TechArrow
 Expiration date: 5/1/2022 2:00:00 AM
 Download certificate
 Certificate password:
 Test

c) Retention settings

The retention of documents can be calculated either from the time of archiving or from a time defined by the file dates. Here you can define which date should be used as reference date for the retention calculation.

Retention reference date: Creation date

d) Private chat archiving

Allow private chat archiving:

Chat archive database: TeamsArchive

Chat archive storage: DiskStorage1

Chat archive index zone: Default index zone

Exchange server type: Exchange Online (O365)
 Region: Global
 Exchange server interface version: Exchange 2016 or higher

EWS Url: https://outlook.office365.com/EWS/Exchange.asmx
 Use impersonation:
 EWS authentication mode: Modern
 OAuth application ID: a6d8f2eb-
 OAuth tenant ID: 4b0eddf1-
 OAuth client secret:
 Use explicit credentials:
 User name: companyadmin@tech-arrow.com
 administrator@domain.com or domain\administrator
 Password:
 Test connection

[Online help](#)



a) Database settings

Select the Teams archive database, that you have previously configured on **Teams Archive** ⇒ **Settings** ⇒ **Databases** page (in our case it is database “MNEtestDB”), from the dropdown list. This selected database will be used by the provisioning job. The provisioning job will store here the metadata during the synchronization process.

b) Client application settings

In this part, the connection with the **Microsoft Teams application** is established. **Application ID** and **Directory ID** are automatically generated during the **App registration on Azure portal**, **Client secret** can be manually generated in section **Certificates & secrets** after the application is registered. Teams archive registration is described in [this](#) section.

Permission type has two options in the dropdown list:

- **Application** – this permission type allows you to connect to the Teams endpoint of the Graph API without providing the username and password. To grant this permission type, it is necessary to [contact Microsoft](#). **SharePoint account** is used to connect to the SharePoint – as the files of the Teams are stored in SharePoint.

The **application** registered on **Azure portal** is used to access the Teams infrastructure, like teams, channels etc. By default, this application cannot be used to read channel messages, as it requires the application to have special permissions approved by Microsoft. If the registered application does not have such permissions, you should enter the credentials (username and password) of a user who can access all the teams that are going to be archived.

- **Delegated** – If you do not have the application permission type, you can specify the user who is able to access all teams with this option. The superuser must also be the owner of all teams to be archived. You can use the Teams account to connect to the SharePoint as well, but you have the option to specify explicit credentials for SharePoint access if necessary. With this permission type, the private channels will be archived only if the specified user is a member of that channel.



SharePoint access

There are two options:

- **Use the Teams app credentials** – pick this option if the SharePoint related permissions and client certificate are added to the Teams app registered on Azure portal
- **Use explicit SharePoint app credentials** – pick this option if the SharePoint related permissions are registered in a separate app

SharePoint application ID: Application ID of the registered SharePoint app, this needs to be filled in in case **Use explicit SharePoint app credentials** is selected in the previous step

Certificate file: .pfx file, which contains the private and public key of the certificate. Must be the same certificate as the .cer file that has been uploaded to Azure during [app registration](#)

Certificate password: the password for the .pfx file

It is also possible and recommended to test the connection by clicking on the **Test** button.

c) Retention settings

The date, from which the retention of the items will be calculated, can be selected here. Choose the setting to be applied from the dropdown list.

Retention settings

The retention of documents can be calculated either from the time of archiving or from a time defined by the file dates. Here you can define which date should be used as reference date for the retention calculation.

Retention reference date:

Creation date

Creation date

Modification date

Most recent date

d) Private chat archiving

contentACCESS gives you the possibility to archive private **Teams** chat messages too. If you want to allow the system to do so, check the **Allow private chat archiving** checkbox and set the following:



Chat archive database: Select an already configured connection from the dropdown list. Here the metadata will be stored. For further information on how to set database connections, please refer to section [Databases](#).

Chat archive storage: Choose an already configured storage from the dropdown list. The processed binaries will be stored here. For more information on how to set storages check section [Storages](#) above.

Chat archiv index zone: Set the **Index zone** that will be assigned to the items by the archiving job.

Under **Exchange server type** and **Exchange server interface version** select the type and version of the server, where your email provider is running. This is used to access all chat data.

In case of the user having/using a [German cloud](#) (dedicated and isolated Microsoft Azure version for Germany), **Germany** must be selected in the **Region** dropdown list.

In case that the predefined settings for **O365** don't match your expectation and/or needs, it is possible to select the **Custom** option from the **Region** dropdown list and specify your own values.

Choose whether you want to **Use impersonation** or not. By default, this checkbox is turned off. If it is turned on, the **Teams chat archive** will use **Impersonation** instead of **Delegation** (more information in [this](#) section).

Impersonation allows the superuser account to impersonate any other user's account and access their data.

Note: Only accounts with the **ApplicationImpersonation** role can use impersonation. For more information about how to configure impersonation for your account, please check [this](#) page.

If the O365 user has "desktopless" license, his account **can't be used** for impersonation. The problem is that EWS access is disabled for such user (he is unable to connect to EWS).

Select one **EWS authentication mode** from the dropdown list. There are 2 options: **Basic** and **Modern**. **Basic** authentication is older and less secure method. **Modern** authentication is more secure and complex and requires the app (Teams archive in this case) to be registered on **Azure portal**. How to register it and gain the necessary **IDs** and **client secret** is described in [this](#) section.



Further enter the applicable **Username** and **Password** to connect to the Exchange (use explicit credentials or log in under service-credentials). We recommend running a test connection via the **Test connection** button.

Do not forget to **Save** your settings.

Teams archive Provisioning settings

The provisioning job

- Synchronizes **users of the Teams** and **AAD groups** specified on the **Provisioning settings** page to the **Teams archive Address book**
- Verifies the user's Teams memberships and records these memberships to contentACCESS
- If contentWEB user creation is turned on in the Address book for an object (Teams/Team groups/Teams' users/AAD group), it creates a contentWEB user for the object users with an **Office 365** authentication type
- Based on the roles assigned in the Address book, it gives permissions on the specific Teams and private chats

In contentACCESS, a provisioning job is created automatically when **Teams Archive** is activated for the first time.

Teams Archive provisioning settings are available on the **Provisioning settings** page (**Teams Archive -> Settings -> Provisioning settings**):

contentACCESS Central Administration Tenant: First

System | File Archive | Email Archive | SharePoint Archive | GDPR | **Teams Archive** | Custom plugins

Save | Discard changes | Databases | Storages | System settings | **Provisioning settings** | Retentions | Schedules | View address book | Jobs

Edit | **Settings** | Archive

Provisioning settings
Teams Archive > Settings > Provisioning settings

start immediately
 refresh
 disable auto refresh
 deactivate job
 logs
 edit

Status: **Idle**
Progress: 1 team processed (1 updated), 2 groups processed (2 updated), 17 users processed (17 updated), 0 contentACCESS users created (completed 19 hours ago)

a) Report mode settings

Use report mode:

b) Scheduling settings

Scheduled in:

c) Teams to process

Process teams:

Display name	
ScrumTeam	...

d) AAD groups

Name	
aan_test	...
ScrumTeam	...

e) Notification settings

Send when:

Recipient list:

f) Role settings

Selected role:

[Online help](#)

a) Report mode settings

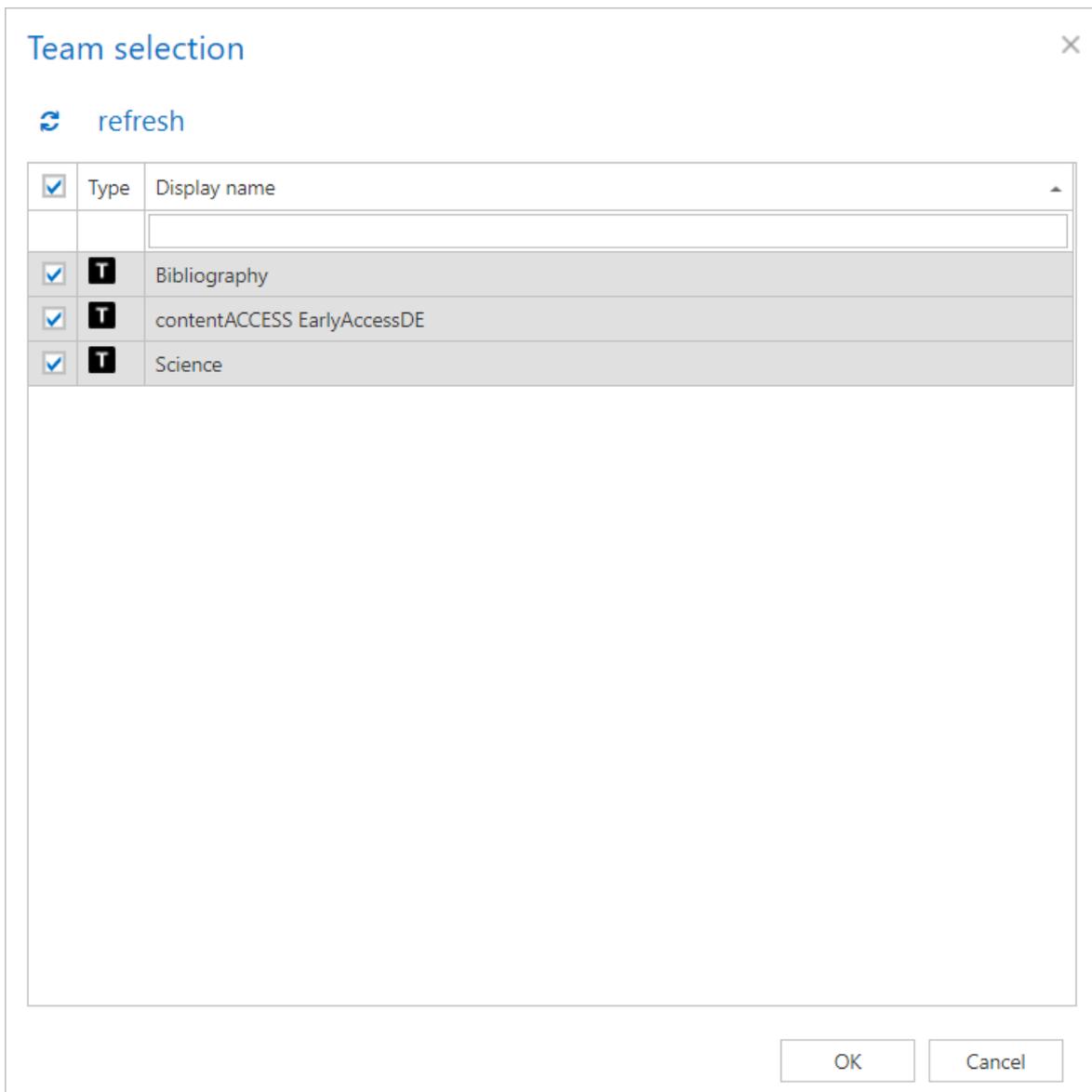
If the **Use report mode** checkbox is checked, the job will run in report mode. After the job finishes its run in this mode, the user will be able to download a .csv report file here in this section. The file will contain a list of teams selected in section **Teams to process** of the job and some information to them, including whether and how will they be processed.

b) Scheduling settings

Select the running times of the provisioning job or create a new scheduler. For more information on how to configure scheduler settings please refer to section [Schedules](#) described above.

c) Teams to process

In this section, the user can choose if he wants to process all accessible **Teams** and **Team groups** or select only some of them manually. If he decides to select them manually, the  **select** option will appear. After clicking on it, the **Team selection window** will open. Here it is possible to select the **Teams** or **Team groups** to be processed. After the selection is made, click **OK**.



<input checked="" type="checkbox"/>	Type	Display name
<input checked="" type="checkbox"/>	T	Bibliography
<input checked="" type="checkbox"/>	T	contentACCESS EarlyAccessDE
<input checked="" type="checkbox"/>	T	Science



There is also the option to set up **Automated Team provisioning**. After selecting this option from the **Process teams** dropdown list, click on **+ new**. The **Team selection** window will open. Here you will be able to specify a list of filters for a group, based on which teams do you want to be processed. Every filter is associated with one group. All teams matching the specified filter will be added into the group.

The screenshot shows a dialog box titled "Team selection" with a close button (X) in the top right corner. It contains the following elements:

- Group:** A dropdown menu that is currently empty.
- Filter:** A text input field.
- Processing strategy:** Two radio button options: "Only add" and "Synchronize".
- Buttons:** "Create group" (top right), "Change filter" (middle right), "OK" (bottom left), and "Cancel" (bottom right).

Before specifying a filter, you will first need to select a **Group** from the dropdown list. If you have no groups created, it is possible to create one directly from here by clicking on the **Create group** button (more info about group creation can be found in [this](#) section).

This screenshot is identical to the previous one, but the "Group:" dropdown menu now displays the text "Testing". A red arrow points to the dropdown arrow on the right side of the menu.

To specify a filter, click on the **Change filter** button. Specify your desired filtering options in the **Filter settings** window. **Team name** and **Description** are what you specify when creating a team, **Members** value must be specified as UPN (user principal name) – e-mail address used for logging in to Office 365. **Team name** can be also specified in **case sensitive** (CS) way.



Note: If the description is not filled in for a team during team creation, the team's name will be used as description by the filtering. So, if a team is named „Team A“ (no description) and in filtering you set the **Description** to **starts with „Team“**, this team will be processed, because the text „Team A“ is returned as description value.

Filter settings ✕

visual
text

AND	Description ▼	Equals ▼	This is a testing team. ✕
	Members ▼	Any ▼ Contains ▼	@tech-arrow.com ✕
	Team name ▼	CS Equals ▼	TA Testing ✕

+add group
+add condition

+add new group

OK
Cancel

Select one of **Processing strategy** options:

- **Only add** - new teams matching the filtering settings will be added, but the old team members that do not match the filtering settings will **not** be removed from the group



- **Synchronize** - only the teams that match the filtering settings can be group members, teams that do not matching the filtering settings will be removed from the group

Team selection ✕

Group: Create group

Filter: **(Team name Contains "test" AND Members [Any]Contains "tech")** Change filter

Processing strategy: Only add Synchronize

OK Cancel

Click **OK**. The group settings (database, store, index zone, creation of contentWEB access) will be applied to the teams that are members of the group. If the team has already associated database, store or index zone, it won't be overwritten by the provisioning job.

d) AAD groups

In this section, it is possible to select AAD groups that you would like to add to the **Address book** and later use for private chat archiving. To manually select from the available groups, click on the  **select** button. The **Select AAD Group(s)** window will open. Here it is possible to select the **AAD groups** to be processed. After the selection is made, click **OK**.

Select AAD Group(s) ✕

 refresh

Drag a column header here to group by that column

<input checked="" type="checkbox"/>	Name
<input type="checkbox"/>	
<input checked="" type="checkbox"/>	aan_test
<input type="checkbox"/>	AbalGroup
<input type="checkbox"/>	accounting
<input type="checkbox"/>	Accounting_de
<input type="checkbox"/>	
<input type="checkbox"/>	Admin notifications
<input type="checkbox"/>	AdminAgents
<input type="checkbox"/>	Administrators notification
<input type="checkbox"/>	Admins@tech-arrow
<input type="checkbox"/>	
<input type="checkbox"/>	Adobe
<input type="checkbox"/>	Adobe TA
<input type="checkbox"/>	@tech-arrow.com
<input type="checkbox"/>	AKA TEST GROUP
<input type="checkbox"/>	Test TEAM

Page 1 of 14 (207 items) ◀ 1 2 3 4 5 6 7 ... 12 13 14 ▶

If you want to add a group that is not in the list of available groups, click on the **+ add** button. The **Add AAD group** window will open. Here you can specify the group's name and then click on **OK** to add it to the **AAD groups** list in **Provisioning settings**.



Add AAD Group

Name:

OK Cancel

e) Notification settings

If the provisioning job could not run properly due to some reasons, contentACCESS can send a warning about the problem. The notification email message will be sent to the email address that is set here under **Recipient list** option. Here you can also choose, when these email messages should be sent: only if errors occur, or when errors or warnings occur, or always, regardless of the faultless running of the provisioning job.

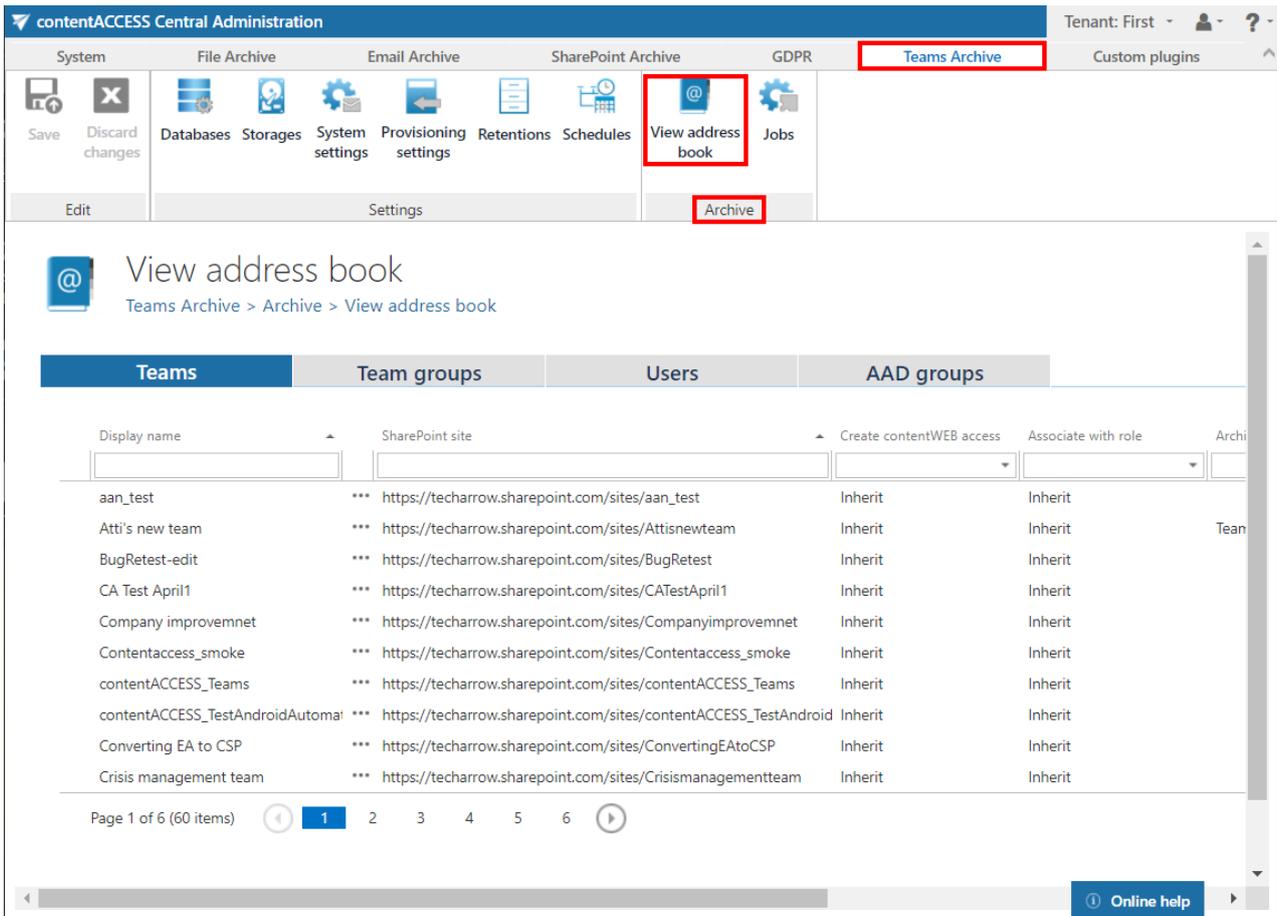
f) Role settings

Here it is possible to select the role that will be assigned by the **Provisioning job**.

Save the settings and start the **Provisioning job**.

Teams archive Address book

Navigate to **Teams Archive** ⇒ **Archive** ⇒ **View Address Book** to open the **View address book** page:



The screenshot shows the 'contentACCESS Central Administration' interface. The 'Teams Archive' tab is selected in the top navigation bar. Below it, the 'View address book' page is displayed. The page has a breadcrumb trail: 'Teams Archive > Archive > View address book'. There are four tabs: 'Teams' (selected), 'Team groups', 'Users', and 'AAD groups'. Below the tabs is a table with columns: 'Display name', 'SharePoint site', 'Create contentWEB access', 'Associate with role', and 'Archi'. The table lists several teams, including 'aan_test', 'Atti's new team', 'BugRetest-edit', 'CA Test April1', 'Company improvemnet', 'Contentaccess_smoke', 'contentACCESS_Teams', 'contentACCESS_TestAndroidAutoma', 'Converting EA to CSP', and 'Crisis management team'. The 'Display name' column is currently empty. At the bottom of the page, there is a pagination control showing 'Page 1 of 6 (60 items)' and a blue 'Online help' button.

The address book contains a read-only list of objects that are provisioned in the address book. To simplify their management, contentACCESS provides the option to group teams into **Team groups**. This is especially useful and recommended to do in case that same archiving policies need to be applied on multiple teams (same database, store, index zone, contentACCESS user creation policy, etc.).

The objects can be added to the address book:

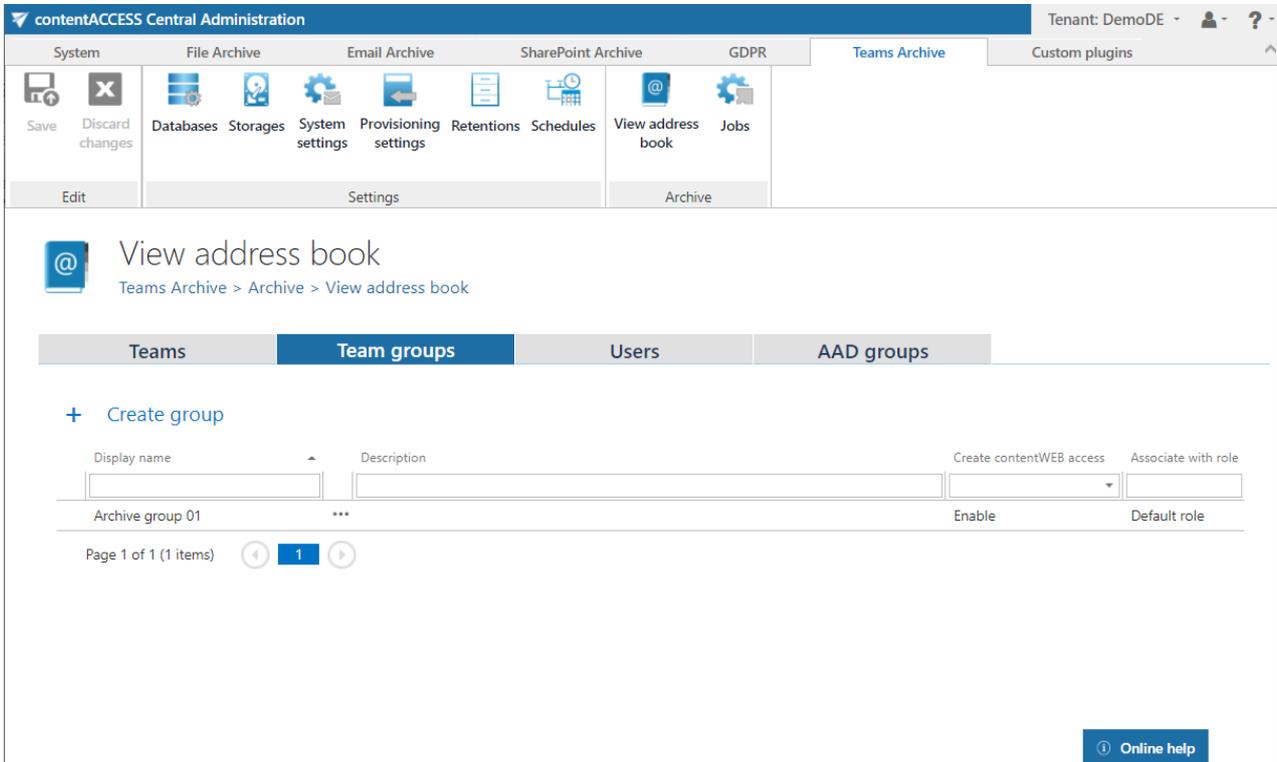
- by the provisioning job (Teams, users, AAD groups)
- created manually from the address book (Team groups)

A team group can be created by two ways:

- from the **Team groups** tab



Click on **+ Create group**. A pop-up window will open. Here you need to name your group and can write also a description. After clicking on **Create**, your group will be added to the list of groups in the tab.



- from the **Teams** tab

Select your desired team and click on **Show details** in its context menu.



contentACCESS Central Administration

Tenant: First

System | File Archive | Email Archive | SharePoint Archive | GDPR | Teams Archive | Custom plugins

Save | Discard changes | Databases | Storages | System settings | Provisioning settings | Retentions | Schedules | View address book | Jobs

Edit | Settings | Archive

View address book

Teams Archive > Archive > View address book

Teams | Team groups | Users | AAD groups

Display name	SharePoint site	Create contentWEB access	Associate with role	Arch
aan_test	*** https://techarrow.sharepoint.com/sites/aan_test	Inherit	Inherit	
Atti's new team	*** https://techarrow.sharepoint.com/sites/Attisnewteam	Inherit	Inherit	Team
BugRetest-edit	gRetest	Inherit	Inherit	
CA Test April1	TestApril1	Inherit	Inherit	
Company improvemnet	mpanyimprovemnet	Inherit	Inherit	
Contentaccess_smoke	ntentaccess_smoke	Inherit	Inherit	
contentACCESS_Teams	ntentACCESS_Teams	Inherit	Inherit	
contentACCESS_TestAndroidAutomat	ntentACCESS_TestAndroid	Inherit	Inherit	
Converting EA to CSP	https://techarrow.sharepoint.com/sites/convertingEAtoCSP	Inherit	Inherit	
Crisis management team	*** https://techarrow.sharepoint.com/sites/Crisismanagementteam	Inherit	Inherit	

Page 1 of 6 (60 items)

Online help

Switch to the **Groups of the team** tab and click on **Manage group membership**.

Team details

Team details | Team members | **Groups of the team** | Statistics

Enter text to search...

Display Name
Testing

Page 1 of 1 (1 items)

Manage group membership

Close



Teams	Team groups	Users	AAD groups						
Display name	SharePoint site	Create contentWEB access	Associate with role	Archive database	Store	Index zone	Active	Deleted	Deleted on
Bibliography	https://caearlyaccessde.sharepoint.com/sites/Bibliography	Enable	Default role	DemoDE	Default	Default index zone	True	False	-
contentACCESS EarlyAccessDE	https://caearlyaccessde.sharepoint.com/sites/contentACCESSEarlyAccessDE	Inherit	Inherit	DemoDE	Default	Default index zone	True	False	-
Science	https://caearlyaccessde.sharepoint.com/sites/Science	Enable	Default role	DemoDE	Default	Default index zone	True	False	-

The **Create contentWEB access** column indicates if there is a command for the **Provisioning job** to create contentWEB users for the selected object. If the **create contentWEB access** value displays **Inherit** on the **Users** tab, it means that the teams of the user and groups of the teams will be checked. The **Inherit** value on the **Teams** level means that the value set for the group of the team will be used (if the team is in more groups, the user will be created if at least one of the groups has contentWEB user creation enabled). Once a contentWEB access is granted (provisioning job must be run), every user of the provisioned object will be able to access the archived content of the objects he has the necessary permissions for.

Teams	Team groups	Users	AAD groups						
Display name	SharePoint site	Create contentWEB access	Associate with role	Archive database	Store	Index zone	Active	Deleted	Deleted on
Bibliography	https://caearlyaccessde.sharepoint.com/sites/Bibliography	Enable	Default role	DemoDE	Default	Default index zone	True	False	-
contentACCESS EarlyAccessDE	https://caearlyaccessde.sharepoint.com/sites/contentACCESSEarlyAccessDE	Inherit	Inherit	DemoDE	Default	Default index zone	True	False	-
Science	https://caearlyaccessde.sharepoint.com/sites/Science	Enable	Default role	DemoDE	Default	Default index zone	True	False	-

The **Associate with role** column displays the role assigned/to be assigned for the object by the next running Teams provisioning job. By default, the objects inherit the default role specified in the Teams archive Provisioning settings, but the administrator can decide to assign custom roles for the objects.

Teams	Team groups	Users	AAD groups						
Display name	SharePoint site	Create contentWEB access	Associate with role	Archive database	Store	Index zone	Active	Deleted	Deleted on
Bibliography	https://caearlyaccessde.sharepoint.com/sites/Bibliography	Enable	Default role	DemoDE	Default	Default index zone	True	False	-
contentACCESS EarlyAccessDE	https://caearlyaccessde.sharepoint.com/sites/contentACCESSEarlyAccessDE	Inherit	Inherit	DemoDE	Default	Default index zone	True	False	-
Science	https://caearlyaccessde.sharepoint.com/sites/Science	Enable	Default role	DemoDE	Default	Default index zone	True	False	-

The Teams archive database, storage and index zone assigned to the objects are displayed in the **Archive database**, **Store** and **Index zone** columns. Database and storage is assigned automatically by the first running archive job, or manually using the object’s context menu (this option is used when the selected



team to archive does not have associated database and storage). If a Team does not have an index zone assigned, the next running **indexing job** will assign the index zone set in its configuration.

Teams	Team groups	Users	AAD groups		Archive database	Store	Index zone	Active	Deleted	Deleted on
Bibliography	*** https://caearlyaccessde.sharepoint.com/sites/Bibliography	Enable	Default role		DemoDE	Default	Default index zone	True	False	-
contentACCESS EarlyAccessDE	*** https://caearlyaccessde.sharepoint.com/sites/contentACCESSEarlyAccessDE	Inherit	Inherit		DemoDE	Default	Default index zone	True	False	-
Science	*** https://caearlyaccessde.sharepoint.com/sites/Science	Enable	Default role		DemoDE	Default	Default index zone	True	False	-

Column **“Active”** shows, if the respective object is active in contentACCESS. With this feature it is possible to deactivate no longer used objects, keeping the licenses under control. Deactivated objects are not touched by the Teams archive job, nor are they counted to the licensed objects. To set an object to active/inactive, the telemetry job must be run, too. It is running automatically every day or can be started manually on the Licensing page (**System tab => Services group => Licensing**, option **“update telemetry”**).

Teams	Team groups	Users	AAD groups		Archive database	Store	Index zone	Active	Deleted	Deleted on
Bibliography	*** https://caearlyaccessde.sharepoint.com/sites/Bibliography	Enable	Default role		DemoDE	Default	Default index zone	True	False	-
contentACCESS EarlyAccessDE	*** https://caearlyaccessde.sharepoint.com/sites/contentACCESSEarlyAccessDE	Inherit	Inherit		DemoDE	Default	Default index zone	True	False	-
Science	*** https://caearlyaccessde.sharepoint.com/sites/Science	Enable	Default role		DemoDE	Default	Default index zone	True	False	-

Column **Deleted** shows if the selected Team was deleted from Teams.

Teams	Team groups	Users	AAD groups		Archive database	Store	Index zone	Active	Deleted	Deleted on
Bibliography	*** https://caearlyaccessde.sharepoint.com/sites/Bibliography	Enable	Default role		DemoDE	Default	Default index zone	True	False	-
contentACCESS EarlyAccessDE	*** https://caearlyaccessde.sharepoint.com/sites/contentACCESSEarlyAccessDE	Inherit	Inherit		DemoDE	Default	Default index zone	True	False	-
Science	*** https://caearlyaccessde.sharepoint.com/sites/Science	Enable	Default role		DemoDE	Default	Default index zone	True	False	-

If the selected Team was deleted, column **Deleted on** will show when it was deleted.

Teams	Team groups	Users	AAD groups		Archive database	Store	Index zone	Active	Deleted	Deleted on
Bibliography	*** https://caearlyaccessde.sharepoint.com/sites/Bibliography	Enable	Default role		DemoDE	Default	Default index zone	True	False	-
contentACCESS EarlyAccessDE	*** https://caearlyaccessde.sharepoint.com/sites/contentACCESSEarlyAccessDE	Inherit	Inherit		DemoDE	Default	Default index zone	True	False	-
Science	*** https://caearlyaccessde.sharepoint.com/sites/Science	Enable	Default role		DemoDE	Default	Default index zone	True	False	-



Column **Description** shows the description that was written for the selected group.

Teams | **Team groups** | Users | AAD groups

+ Create group

Display name	Description	Create contentWEB access	Associate with role
Archive group 01		Enable	Default role

Page 1 of 1 (1 items) ◀ 1 ▶ 📘 Online help

In the column **User principal name**, the email that the user is using to log into Teams is displayed.

Teams | Team groups | **Users** | AAD groups

Display name	User principal name	Associated user	AAD user type	Create contentWEB access	License status	Associate with role
	@tech-arrow.com		Member	Inherit	Allowed	Inherit
✓	@tech-arrow.com		Member	Inherit	Allowed	Inherit
	@tech-arrow.com		Member	Inherit	Allowed	Inherit
	@tech-arrow.com		Member	Inherit	Allowed	Inherit
	@tech-arrow.com		Member	Inherit	Allowed	Inherit
	@tech-arrow.com		Member	Inherit	Allowed	Inherit
	@tech-arrow.com		Member	Inherit	Allowed	Inherit
Microsoft Test	mstest@tech-arrow.com		Member	Inherit	Allowed	Inherit
	@tech-arrow.com		Member	Inherit	Allowed	Inherit

Page 1 of 2 (11 items) ◀ 1 2 ▶ 📘 Online help

The **AAD user type** column shows the user type of the selected user in **Azure Active directory**. There are 2 options: Member and Guest.

Teams | Team groups | **Users** | AAD groups

Display name	User principal name	Associated user	AAD user type	Create contentWEB access	License status	Associate with role
	@tech-arrow.com		Member	Inherit	Allowed	Inherit
✓	@tech-arrow.com		Member	Inherit	Allowed	Inherit
	@tech-arrow.com		Member	Inherit	Allowed	Inherit
	@tech-arrow.com		Member	Inherit	Allowed	Inherit
	@tech-arrow.com		Member	Inherit	Allowed	Inherit
	@tech-arrow.com		Member	Inherit	Allowed	Inherit
	@tech-arrow.com		Member	Inherit	Allowed	Inherit
	@tech-arrow.com		Member	Inherit	Allowed	Inherit
Microsoft Test	mstest@tech-arrow.com		Member	Inherit	Allowed	Inherit
	@tech-arrow.com		Member	Inherit	Allowed	Inherit

Page 1 of 2 (11 items) ◀ 1 2 ▶ 📘 Online help



The **License status** column shows if a license is assigned to the user (and therefore if the user can be archived).

Teams	Team groups	Users	AAD groups			
Display name	User principal name	Associated user	AAD user type	Create contentWEB access	License status	Associate with role
	*** @tech-arrow.com		Member	Inherit	Allowed	Inherit
<input checked="" type="checkbox"/>	*** @tech-arrow.com		Member	Inherit	Allowed	Inherit
	*** @tech-arrow.com		Member	Inherit	Allowed	Inherit
	*** @tech-arrow.com		Member	Inherit	Allowed	Inherit
	*** @tech-arrow.com		Member	Inherit	Allowed	Inherit
	*** @tech-arrow.com		Member	Inherit	Allowed	Inherit
	*** @tech-arrow.com		Member	Inherit	Allowed	Inherit
Microsoft Test	*** mstest@tech-arrow.com		Member	Inherit	Allowed	Inherit
	*** @tech-arrow.com		Member	Inherit	Allowed	Inherit

Page 1 of 2 (11 items) 1 2 Online help

The **SID** column shows the security identifier of an AAD group.

Teams	Team groups	Users	AAD groups			
Name	SID	Create contentWEB access	Associate with role	Deleted	Deleted on	
aan_test	*** S-1-12-1-4057088150-1214818095-78384...	Not set	Not set	No	-	
<input checked="" type="checkbox"/> ScrumTeam	*** S-1-12-1-2313000782-1220119370-26330...	Enable	Default role	No	-	

Page 1 of 1 (2 items) 1

Using the Team’s/group’s/user’s context menu, the administrator with the necessary permissions can:

- View object details
- Assign database, storage and index zone for Exchange groups and mailboxes
- Automatically create contentWEB user also with custom permissions
- Manage access for second users to the selected **Teams** and **Users**
- Activate/Deactivate – users can be deactivated only directly from the **Users** tab, otherwise just teams are deactivated
- [Remove](#) team/group/user/AAD group



Teams	Team groups	Users	AAD groups
Display name	SharePoint site	Create contentWEB access	
aan_test	*** https://techarrow.sharepoint.com/sites/aan_test		Inherit
Atti's new team	*** https://techarrow.sharepoint.com/sites/Attisnewteam		Inherit
BugRetest-edit	Show details	gRetest	Inherit
CA Test April1	Assign database, storage and index zone	TestApril1	Inherit
Company improvemnet	Automatically create contentWEB user	mpanyimprovemnet	Inherit
Contentaccess_smoke	Manage access	ntentaccess_smoke	Inherit
contentACCESS_Teams	Deactivate	ntentACCESS_Teams	Inherit
contentACCESS_TestAndroidAutoma	Remove team	https://techarrow.sharepoint.com/sites/contentACCESS_TestAndroidAutomation	Inherit
Converting EA to CSP	*** https://techarrow.sharepoint.com/sites/ConvertingEAtoCSP		Inherit
Crisis management team	*** https://techarrow.sharepoint.com/sites/Crisismanagementteam		Inherit

Page 1 of 6 (60 items) 1 2 3 4 5 6

After clicking on **Show details**, a pop-up window opens. Here it is possible to view the following details:

Teams

Team details

On this tab, it is possible to view the basic information about a team – like name, storage, index zone etc.

Team details ✕

Team details | Team members | Groups of the team | Statistics

Basic information

Team name: LBA CoffeeBar
 Team identifier: ce43d4d1-
 SharePoint site: https://techarrow.sharepoint.com/sites/LBACoffeeBar
 Archive database:
 Storage:
 Index zone:
 Active: True
 Deleted: No

Close



Team members

Here you can see what members belong to the currently selected team.

Team details ✕

Team details

Team members

Groups of the team

Statistics

Display name	User principal name	AAD user type
[blurred]	[blurred]@tech-arrow.com	Member

Page 1 of 1 (8 items)

⏪
1
⏩

Groups of the team

On the **Groups of the team** tab, it is possible to **Manage group membership** and create new groups as mentioned above in this section.

Team details ✕

Team details

Team members

Groups of the team

Statistics

Display Name

Testing

Page 1 of 1 (1 items)

⏪
1
⏩



Statistics

On this tab, you can view the Archive statistics and Index statistics of the currently selected team.

Team details ×

- Team details
- Team members
- Groups of the team
- Statistics**

Archive statistics

Channel count:	0
Item count:	0
Size:	0

Index statistics

Post count:	0
Reply count:	0
File count:	0

Close

Team groups

Group details

Here you can view the name and description of the currently selected group.



Group details
✕

Group details

Group members

Basic information

Group name:	MNEtest
Description:	Testing teams group

Close

Group members

On this tab, you can see the members of the currently selected group and their SharePoint URL. It is also possible to create a new group from here by clicking on the **Manage group membership** button.

Group details
✕

Group details

Group members

Display name	SharePoint URL
Football	https://techarrow.sharepoint.com/sites/Football

Page 1 of 1 (1 items)

⏪
1
⏩

Manage group members

Close

contentACCESS Manual | Version 5.1 | ALL RIGHTS RESERVED

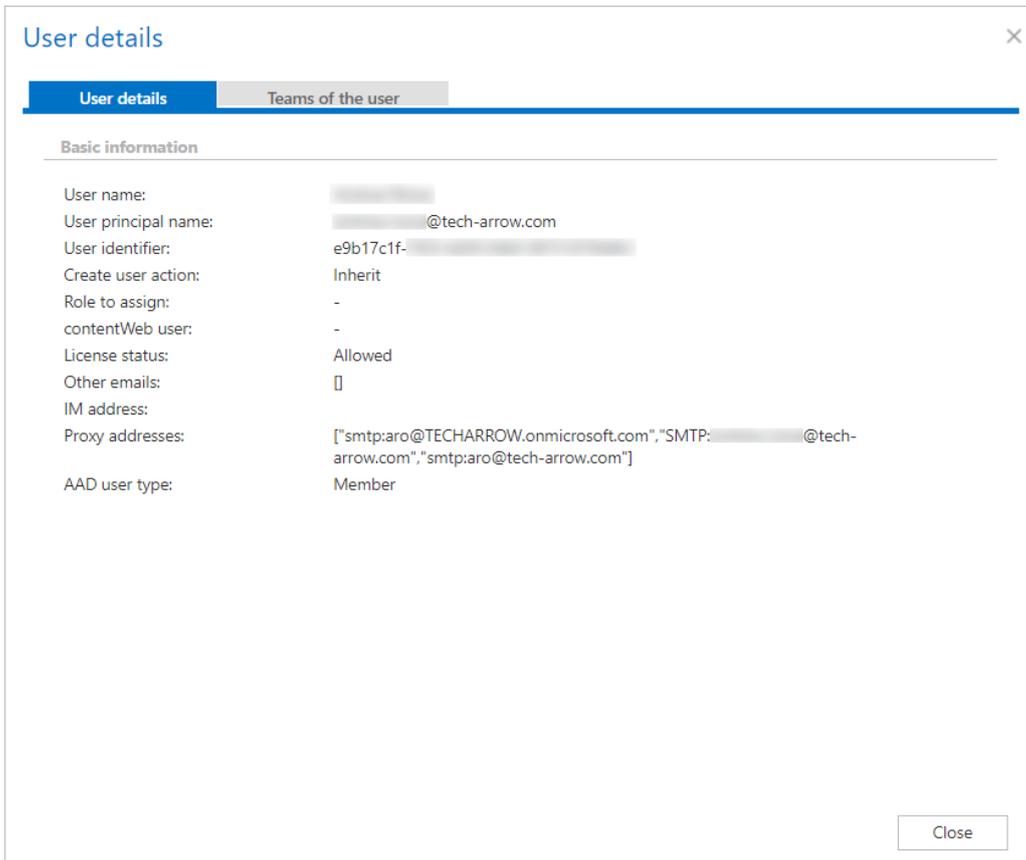
TECH-ARROW, a. s. | Kazanská 5B, 821 06 Bratislava, Slovakia, EU | E-mail: sales@tech-arrow.com | www.tech-arrow.com

758/872

Users

User details

On this tab, it is possible to view the basic information about a user – like name, principal name, license status, AAD user type etc.



User details [Close]

User details | Teams of the user

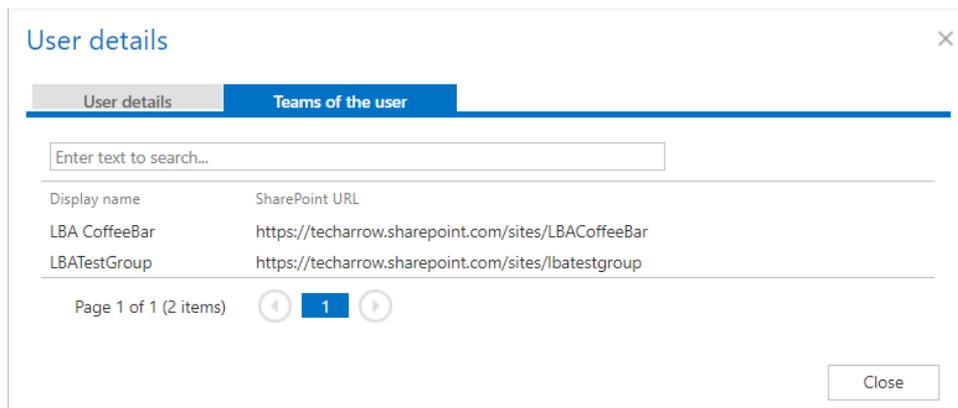
Basic information

User name:	[Redacted]
User principal name:	[Redacted]@tech-arrow.com
User identifier:	e9b17c1f-[Redacted]
Create user action:	Inherit
Role to assign:	-
contentWeb user:	-
License status:	Allowed
Other emails:	[]
IM address:	
Proxy addresses:	["smtp:aro@TECHARROW.onmicrosoft.com","SMTP:[Redacted]@tech-arrow.com","smtp:aro@tech-arrow.com"]
AAD user type:	Member

[Close]

Teams of the user

On this tab, you can see a list of the teams the currently selected user is a member of and their SharePoint URL.



User details [Close]

User details | **Teams of the user**

Enter text to search...

Display name	SharePoint URL
LBA CoffeeBar	https://techarrow.sharepoint.com/sites/LBACoffeeBar
LBA Test Group	https://techarrow.sharepoint.com/sites/lbatestgroup

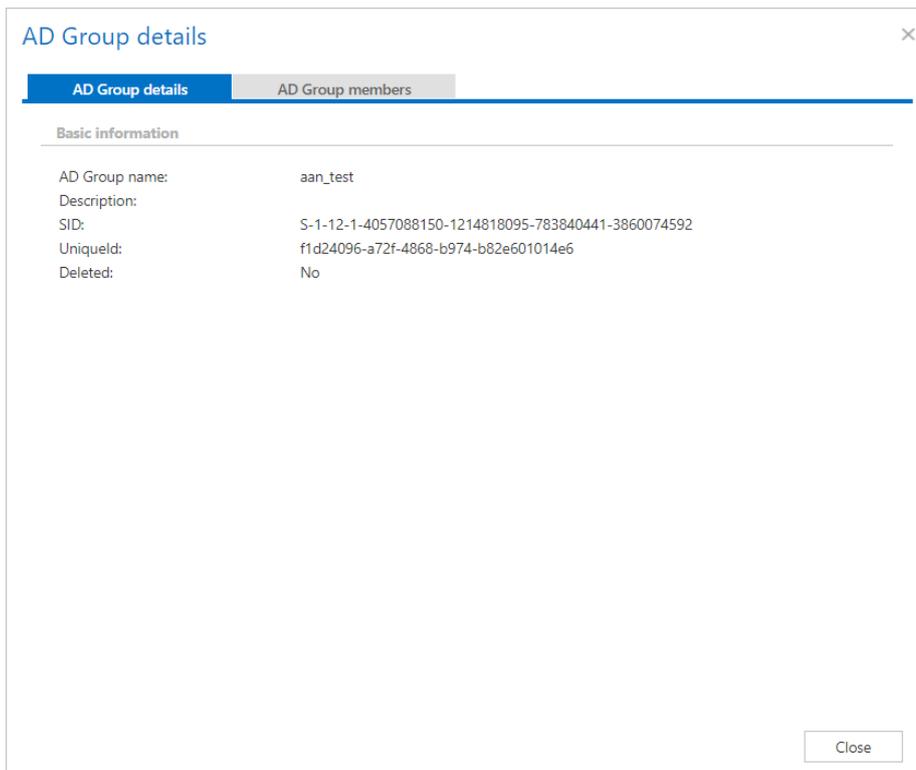
Page 1 of 1 (2 items) [Previous] 1 [Next]

[Close]

AAD groups

AD Group details

On this tab, it is possible to view the basic information about an AD group – name, description, SID, UniqueId and whether the group is deleted or no.



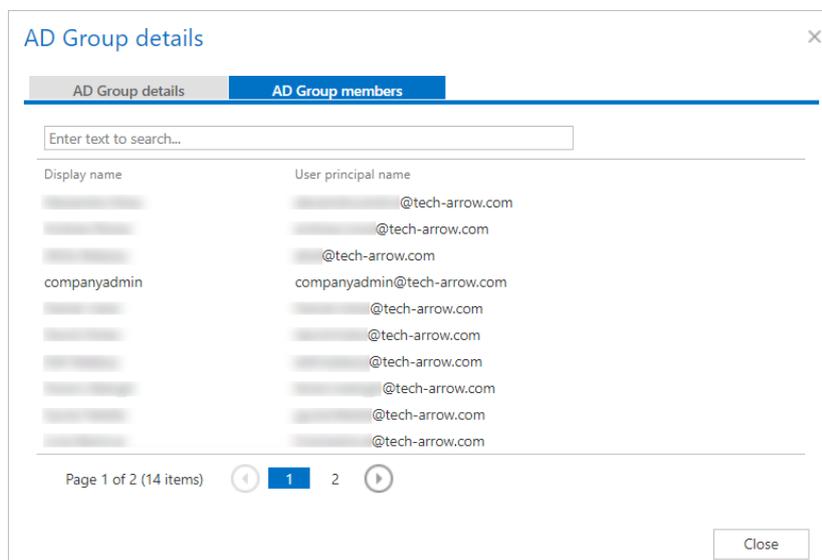
The screenshot shows a window titled "AD Group details" with two tabs: "AD Group details" (selected) and "AD Group members". Under the "Basic information" section, the following details are listed:

AD Group name:	aan_test
Description:	
SID:	S-1-12-1-4057088150-1214818095-783840441-3860074592
UniqueId:	f1d24096-a72f-4868-b974-b82e601014e6
Deleted:	No

A "Close" button is located at the bottom right of the window.

AD Group members

Here you can view all members of the selected AD group.



The screenshot shows the "AD Group details" window with the "AD Group members" tab selected. At the top, there is a search bar with the placeholder text "Enter text to search...". Below the search bar is a table listing the members of the group:

Display name	User principal name
[Redacted]	[Redacted]@tech-arrow.com
[Redacted]	[Redacted]@tech-arrow.com
[Redacted]	[Redacted]@tech-arrow.com
companyadmin	companyadmin@tech-arrow.com
[Redacted]	[Redacted]@tech-arrow.com

At the bottom of the list, there is a pagination control showing "Page 1 of 2 (14 items)" and navigation arrows. A "Close" button is located at the bottom right of the window.

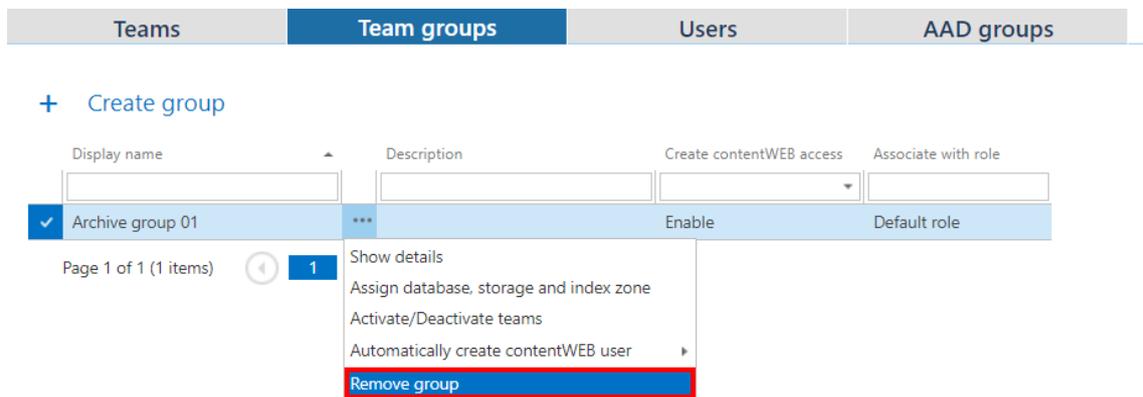
Removing objects from Teams archive Address book

It is possible to remove teams, groups, users and AAD groups **without any archived data** from the **Address book**.

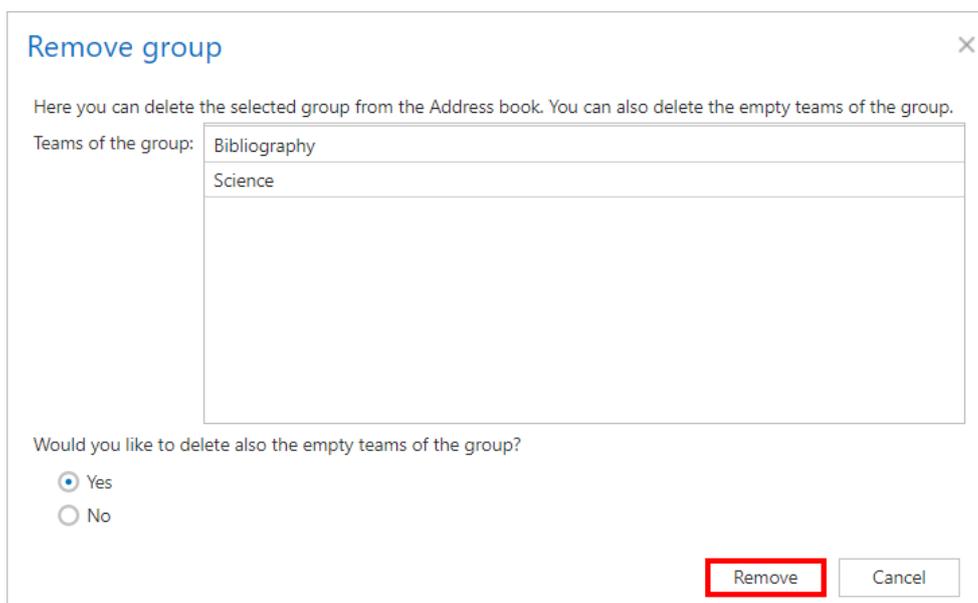
Removing a Group

If you would like to remove a group with all members (teams), the group will be removed only if all teams in it were removed (all teams are empty in the archive). You can remove the group also without removing the teams. In this case, all teams - the archived and not archived ones are remaining in the Address book, but the group will disappear.

To remove a group from the **Address book**, click on **Remove group** from its context menu.



In the next window, you can select if you want to remove also empty teams (and their users) from the Address book. Click **Remove**.

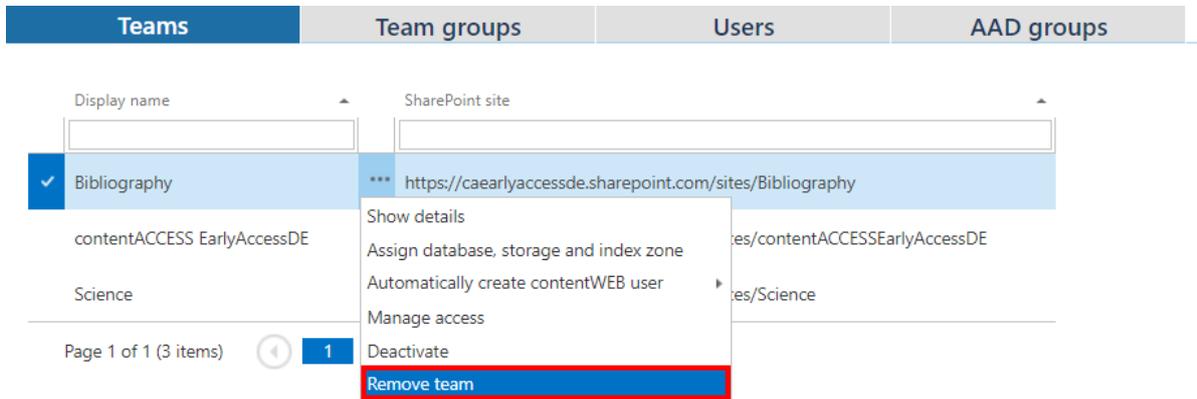




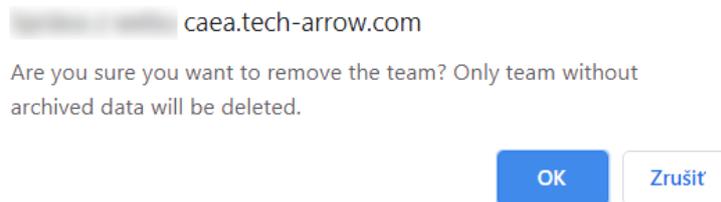
Removing a Team

If you would like to remove a team, it is possible to do so only if the team is empty in the archive.

To remove a team from the **Address book**, click on **Remove team** from its context menu.

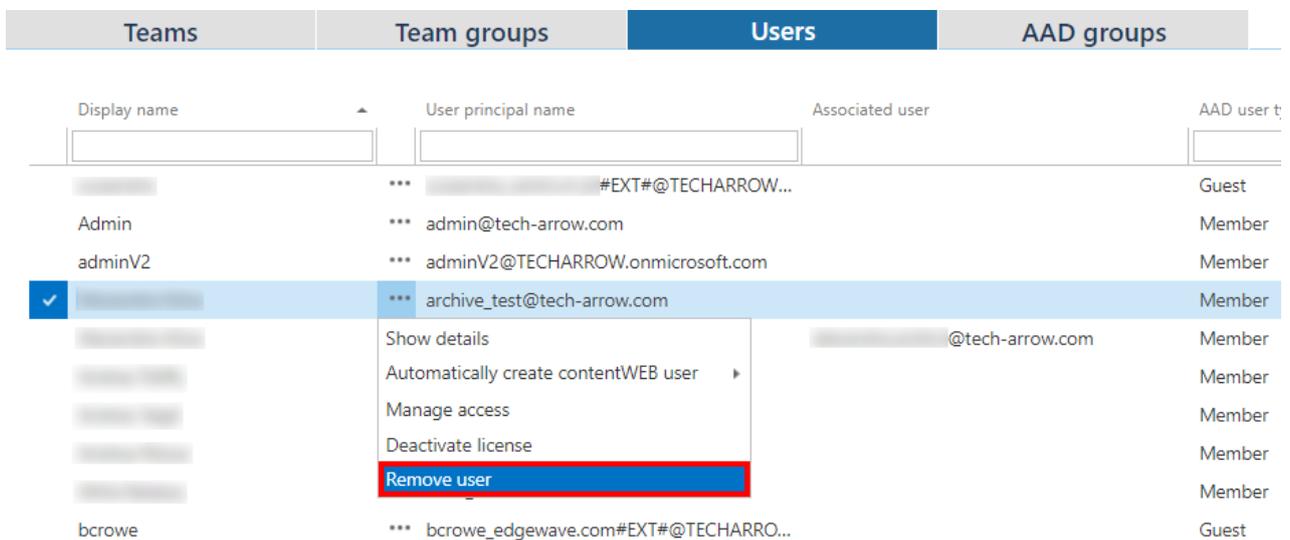


A warning window will pop up. You will be asked if you are sure about removing the team and warned that only teams without archived data can be removed. Click **OK**.



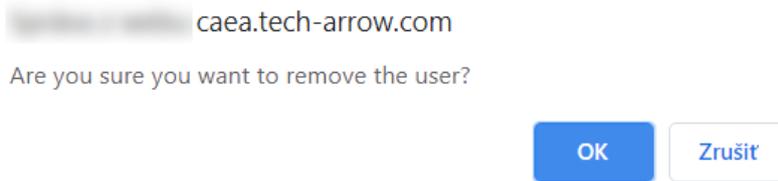
Removing a User

To remove a user from the **Address book**, click on **Remove user** from its context menu.



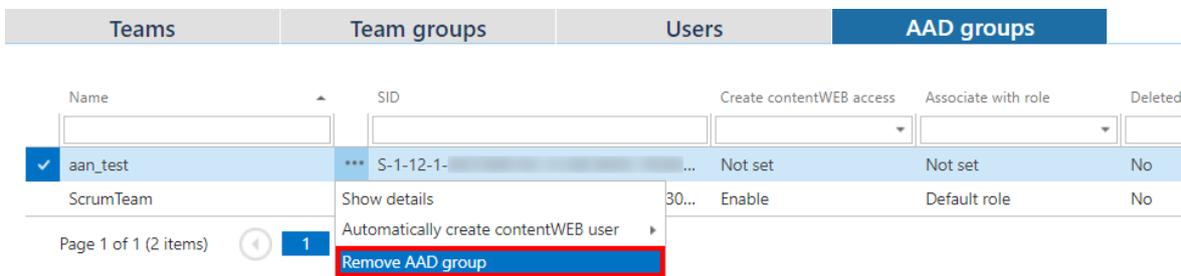


Confirm your choice in the pop-up window.

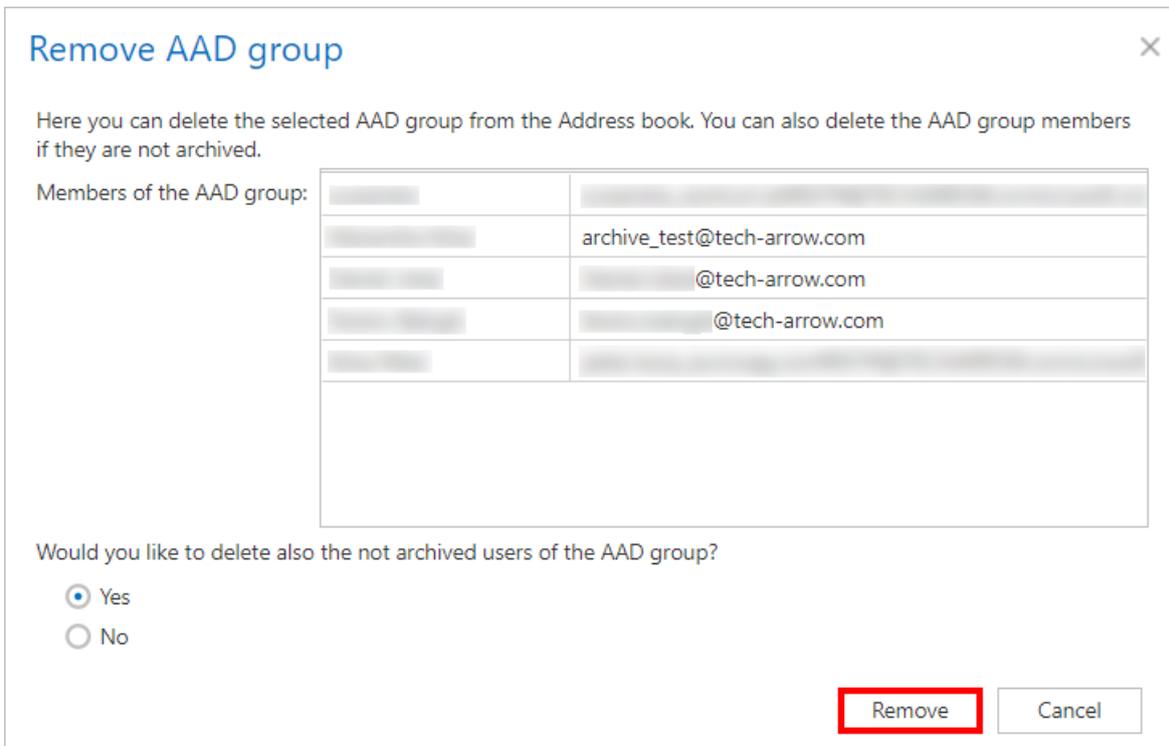


Removing an AAD group

If you would like to remove an AAD group from the **Address book**, click on **Remove AAD group** from its context menu.



In the next window, you can select if you want to remove also not archived AAD users from the Address book. Click **Remove**.





Teams archive Licensing

The licensing of **Teams archive** is based on the users who are members of a team. If a new user is added to any team (the user was not licensed yet), the system will check whether there are enough licenses and if yes, will assign one to the user. **A team will be archived only if all its members are licensed.** The archive job will check the team license status before starting the archiving process and will write a monitoring warning in case a team is not licensed, and the archiving can't be done.

Note: Private chats archiving can be done only when it is allowed in [System settings](#) and only for licensed users.

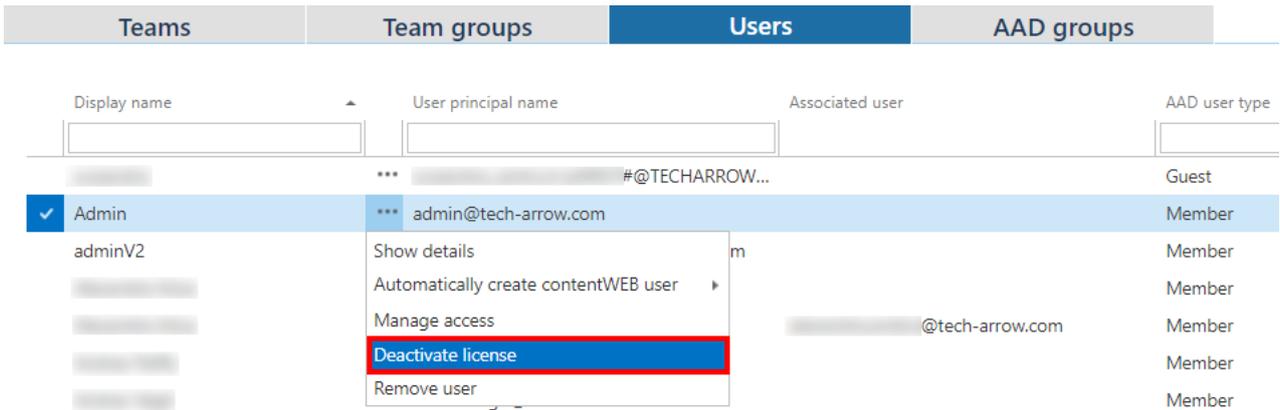
Archiving process

1. Provisioning adds all members of the teams (selected in provisioning job) into the database
2. Each user license state is **unassigned** at this moment
3. Archive job will pick up the team(s) and will read the team members. For each member that does not have a license assigned, it will check if the given tenant has free licenses
 - If **YES** - a new license is assigned to a user
 - If **NO** - the user is left unlicensed
4. Once all users are checked, the archive job will verify if all team members are licensed
 - If **YES**, the team(s) will be archived
 - If **NO**, the team(s) will not be archived -> a monitoring warning will be written

Revoking user license

When removing a member from a team (in teams app), the contentACCESS Teams archive license is not revoked automatically from the user, it must be revoked manually in **Central Administration**. To revoke a license from a user:

- Go to **Teams archive** -> **Archive** -> **View address book** -> **Users** tab
- Click on the user -> select **Deactivate license** from his context menu
- If the user is a part of multiple teams, the system will give a warning that the following teams will not be archived if the user license is revoked. Click **OK**.
- User will be marked as unlicensed.



Telemetry

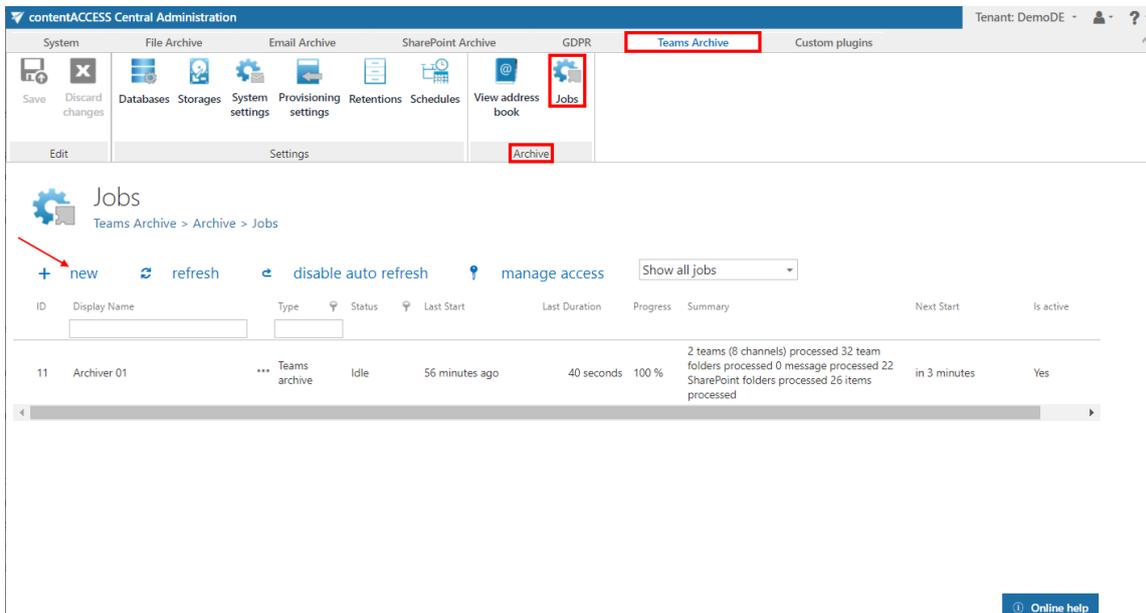
Telemetry counts the licensed users, number of teams, number of chat items/users, chat size and storage used by **Teams archive**. This information will be sent to license server.

Teams archive Jobs

Archiving is managed by jobs that are configured on the job’s configuration page. Here you can define the exact configurations (i.e. database, schedulers, storage, address book objects to process etc.) of a job. In the following sections, we will describe the configuration of jobs available for **Teams archive**.

Teams archive job

To configure a new Teams archive job, navigate to **Teams Archive -> Archive -> Jobs**. Here, click on **+new**.





In the **Add new job instance** dialog select **Teams archive** from the **Available jobs** dropdown list, the node where the job will run (option **Run on node**) and fill a **Display name** into the **Add new job instance** pop-up window. Then click on **Add**.

If you want to configure the job immediately, then click **OK** in the pop-up window and the job configuration page opens immediately. If not, the configuration page is accessible any time using the **Configure** option in the given job's context menu.

On the job's configuration page go through the following sections:

✓ Report mode settings

If the **Use report mode** checkbox is checked, the job will run in report mode. After the job finishes its run in this mode, the user will be able to download a .csv report file here in this section. The file will contain a list of items that belong to the objects selected in section **Address book objects to process** of the job and some information to them, including whether they will be processed or not.

Report mode settings

Use report mode:	<input checked="" type="checkbox"/>
Generated report file:	File name: JobReport_2ed3dc5c-9fb2-426a-9748-46d993fd3f3cf.csv Size: 59.9 KB Date: 5/29/2020 5:23:09 PM
<input type="button" value="Download report"/>	



✓ Scheduling settings

In this step, the running time(s) of the Teams archive job must be selected. It is possible either to select a scheduler from the list or to create a new scheduler via **create new ...** option from the dropdown list. For more information about how to set schedulers refer to the section [Schedules](#) above.

Scheduling settings

Scheduled in:

✓ Address book objects to process

Here the administrator may select the Teams and groups, which will be processed by the archive job. Click on the  **select** option and check the desired Teams or groups in the **Team selection** window, then click on **OK**.

Team selection ✕

 refresh

<input type="checkbox"/>	Type	Display name	Entry Type
<input checked="" type="checkbox"/>		Archive group 01	Group
<input type="checkbox"/>		Bibliography	Team
<input type="checkbox"/>		contentACCESS EarlyAccessDE	Team
<input type="checkbox"/>		Science	Team



✓ Database settings

Select an already configured connection from the dropdown list. Here the metadata will be stored. We have configured for our archived Teams the database named “DemoDE”, so we set it here. For further information on how to set database connections please refer to section [Databases](#).

Database settings

Database connection:

✓ Storage settings

Choose an already configured storage from the dropdown list. The processed binaries will be stored here. On the screenshot below we selected our already configured disk type store: “Default”. For more information on how to set storages check section [Storages](#) above.

Storage settings

Storage name:

✓ Retention settings

Choose an already configured retention time from the dropdown list. The archived objects will be stored during this time in the storage, and it will be impossible to delete them from there. It is highly recommended to select a retention time that is required by the law of your country. For more information about how to set retentions check section [Retentions](#) above.

Retention settings

Retention:

✓ Notification settings

Select here, when you will need to get notification emails from the Teams archive job. It is possible to set here if you need such a notification email always/never, or you need it only in case that an error/warning occurred during the archiving process – for example, if the archiving of one or more items failed, then you may get a notification email about this error. Into the **Recipient list** textbox insert the email address(es) of the person(s), who will get such notifications. Notifications should be used if the administrator does not use the **System logs** feature.

Notification settings

Send when:

Recipient list:



✓ Resource settings

Set the value, which will determine how many items will be processed simultaneously by the Teams archive job. The recommended value is “2”.

Resource settings

Worker thread count:

Save your changes and start the job manually or wait until the scheduler starts the job automatically.

Teams chat archive job

To configure a new Teams chat archive job, navigate to **Teams Archive** -> **Archive** -> **Jobs**. Here, click on **+new**.

The screenshot shows the contentACCESS Central Administration interface. The top navigation bar includes 'System', 'File Archive', 'Email Archive', 'SharePoint Archive', 'GDPR', 'Teams Archive', and 'Custom plugins'. The 'Teams Archive' section is expanded, showing 'Jobs' and 'Archive' sub-sections. The 'Jobs' page is displayed, showing a table of jobs. A red arrow points to the '+new' button in the top left of the Jobs section.

ID	Display Name	Type	Status	Last Start	Last Duration	Progress	Summary	Next Start	Is active
11	Archiver 01	Teams archive	Idle	56 minutes ago	40 seconds	100 %	2 teams (8 channels) processed 32 team folders processed 0 message processed 22 SharePoint folders processed 26 items processed	in 3 minutes	Yes

In the **Add new job instance** dialog select **Teams chat archive** from the **Available jobs** dropdown list, the node where the job will run (option **Run on node**) and fill a **Display name** into the **Add new job instance** pop-up window. Then click on **Add**.



Add new job instance ✕

Available jobs:

Run on node:

Display name:

Description: Plugin for Teams archiving.

If you want to configure the job immediately, then click **OK** in the pop-up window and the job configuration page opens immediately. If not, the configuration page is accessible any time using the **Configure** option in the given job's context menu.

tacatest.ta.internal

Would you like to configure this instance now?

On the job's configuration page go through the following sections:

✓ Report mode settings

If the **Use report mode** checkbox is checked, the job will run in report mode. After the job finishes its run in this mode, the user will be able to download a .csv report file here in this section. The file will contain a list of items that belong to the objects selected in section **Address book objects to process** of the job and some information to them, including whether they will be processed or not.

Report mode settings

Use report mode:	<input checked="" type="checkbox"/>						
Generated report file:	<table style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 15%;">File name:</td> <td>JobReport_2ed3dc5c-9fb2-426a-9748-46d993fd3fcf.csv</td> </tr> <tr> <td>Size:</td> <td>59.9 KB</td> </tr> <tr> <td>Date:</td> <td>5/29/2020 5:23:09 PM</td> </tr> </table>	File name:	JobReport_2ed3dc5c-9fb2-426a-9748-46d993fd3fcf.csv	Size:	59.9 KB	Date:	5/29/2020 5:23:09 PM
File name:	JobReport_2ed3dc5c-9fb2-426a-9748-46d993fd3fcf.csv						
Size:	59.9 KB						
Date:	5/29/2020 5:23:09 PM						
<input type="button" value="Download report"/>							



✓ **Scheduling settings**

In this step, the running time(s) of the Teams chat archive job must be selected. It is possible either to select a scheduler from the list or to create a new scheduler via **create new ...** option from the dropdown list. For more information about how to set schedulers refer to the section [Schedules](#) above.

Scheduling settings

Scheduled in:

✓ **Address book objects to process**

Here the administrator may select the AAD users or groups that will be processed by the archive job. Click on the **select** option and check the desired users and groups in the **Team selection** window, then click on **OK**.

Team selection ✕

refresh

<input type="checkbox"/>	Type	Display name	Entry Type
<input checked="" type="checkbox"/>		aan_test	Group
<input type="checkbox"/>		ScrumTeam	Group
<input type="checkbox"/>		[redacted]#EXT#@TECHARROW.onmicro	User
<input type="checkbox"/>		Admin [admin@tech-arrow.com]	User
<input type="checkbox"/>		adminV2 [adminV2@TECHARROW.onmicrosoft.com]	User
<input checked="" type="checkbox"/>		[redacted]@tech-arrow.com]	User
<input type="checkbox"/>		[redacted] [archive_test@tech-arrow.com]	User
<input type="checkbox"/>		[redacted] [redacted]@tech-arrow.com]	User
<input type="checkbox"/>		[redacted] [redacted]@tech-arrow.com]	User
<input type="checkbox"/>		[redacted] [redacted]@tech-arrow.com]	User
<input checked="" type="checkbox"/>		[redacted] [abal@tech-arrow.com]	User
<input type="checkbox"/>		[redacted] [redacted]@cloudgate365.de]	User
<input checked="" type="checkbox"/>		[redacted] [redacted]@tech-arrow.com]	User
<input type="checkbox"/>		companyadmin [companyadmin@tech-arrow.com]	User
<input type="checkbox"/>		[redacted] [redacted]@tech-arrow.com]	User

Page 1 of 4 (49 items) ⏪ 1 2 3 4 ⏩



✓ Retention settings

Choose an already configured retention time from the dropdown list. The archived objects will be stored during this time in the storage, and it will be impossible to delete them from there. It is highly recommended to select a retention time that is required by the law of your country. For more information about how to set retentions check section [Retentions](#) above.

Retention settings

Retention:

✓ Notification settings

Select here, when you will need to get notification emails from the Teams chat archive job. It is possible to set here if you need such a notification email always/never, or you need it only in case that an error/warning occurred during the archiving process – for example, if the archiving of one or more items failed, then you may get a notification email about this error. Into the **Recipient list** textbox insert the email address(es) of the person(s), who will get such notifications. Notifications should be used if the administrator does not use the **System logs** feature.

Notification settings

Send when:

Recipient list:

✓ Resource settings

Set the value, which will determine how many items will be processed simultaneously by the Teams chat archive job. The recommended value is “2”.

Resource settings

Worker thread count:

Save your changes and start the job manually or wait until the scheduler starts the job automatically.

Custom plugins

Many companies require to archive, access and collaborate on documents residing in their own data management systems (e.g. on the Exchange servers, SharePoint sites, Datengut storages etc.). This requires to have a custom solution that connects the respective data management system(s) with the central archive. contentACCESS uses its custom plugins to manage these scenarios in an organization.

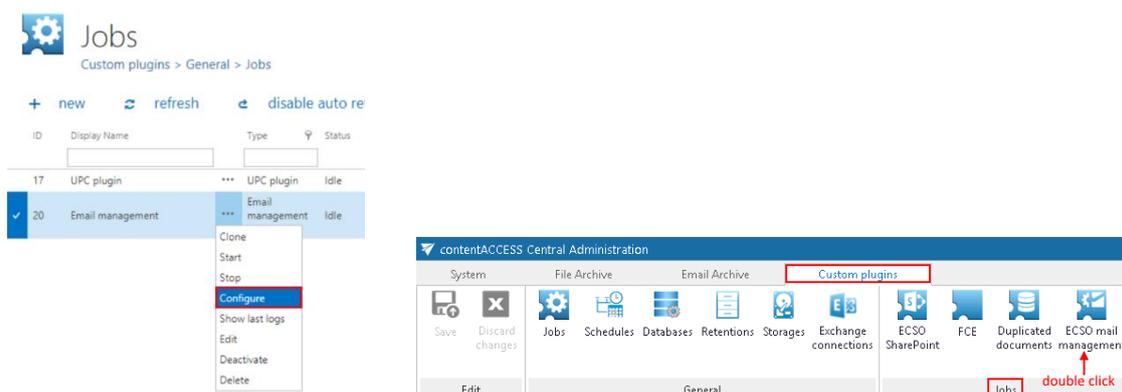
contentACCESS custom plugins enable to categorize, replicate, archive, protect, access, search for your data, or to connect them to your MS Outlook (using [officeGATE](#)) and collaborate on them from your mailbox directly. With custom plugins you can categorize the desired data into certain SharePoint libraries, share links to files residing in different DMSs directly from the mailbox, replicate the storages to protect your data etc.

The following chapters of this guide will introduce the configuration steps of the most used contentACCESS Custom plugins.

Email management job configuration

This plugin is used to scan the mailboxes and process & archive the email messages and its contents into a specific storage.

After you have successfully created a new job for Email management plugin (for more information how to create a new job please refer to section [Creating new jobs in contentACCESS](#)), you can start to configure it. Navigate to the **Custom plugins** → **General** → click on **Jobs** button and choose the job from the list. Click on ellipsis (...) and choose **Configure** option from the context menu as on Screenshot A (or double click on it in the grid). It is also possible to open the job for further configuration with a double click on the corresponding job icon in the **Jobs** ribbon group (Screenshot B).





Screenshot A

Screenshot B

The job's configuration page will open. The following sections must be configured here:

- **EWS Settings**

As first step it is necessary to select the previously configured Exchange connection from the dropdown list. Using these connection settings, the user will be allowed to operate over the mailboxes (check section **Mailbox settings** below). For further information on how to perform **EWS** (Exchange Web Services) settings please refer to section "[Exchange connections](#)".

Exchange connection settings

Exchange connection name: 

Note: The user set in the "[Exchange connections](#)" must have full access permission to all mailboxes.

- ✓ **Database settings:**

Select a connection, where the metadata will be stored, from the dropdown list. (For further information on how to set database connectors please refer to section [How to create/configure databases – All databases](#)).

Database settings

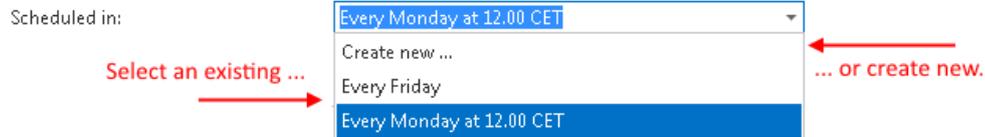
Database connection:  

- ✓ **Scheduling settings:**

In this step the running times of the Email management plugin instance must be selected. It is possible either to select a scheduler from the list or to create a new scheduler via create new option. (For more information about how to set schedulers refer to the section [Schedules](#) above.)



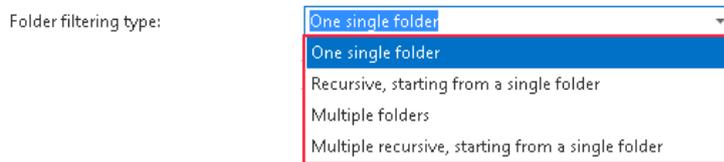
Scheduling settings



✓ **Include folders:**

Email management plugin is crawling in one single or in multiple mailbox folders and also in recursive folder structures. Before you enter the folders to be crawled, it is necessary to select the folder filtering type.

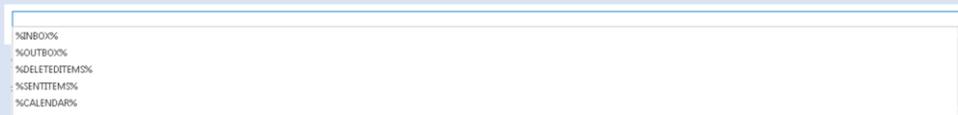
Folder selection



If you set **One single folder** type, then only one predefined folder will be processed (e.g. if you set %INBOX%\Subfolder1, then only Subfolder1 will be processed). If you set **Recursive, starting from a single folder** filtering type, then all folders starting from this folder will be processed (e.g. if you set %INBOX%\Subfolder1, then starting from Subfolder1, every subfolders will be processed in the structure).

The same rule applies to the **Multiple folders** and to **Multiple recursive, starting from a single folder** types, too, but in this case we can work with more folders simultaneously (e.g.: %INBOX%, %OUTBOX%\Folder name 5...or...%TASKS%, %CALENDARS%\Folder name 6).

Note: It is possible to either select an item type from the dropdown list or to enter the item type to the textbox manually. If crawling more item types/folders always put item types between percent signs and also separate them with a comma.



✓ **Storage settings:**

Choose an already configured storage from the dropdown list. The processed emails will be stored here. (For more information on how to set storages check section “[Storage](#)” above.)

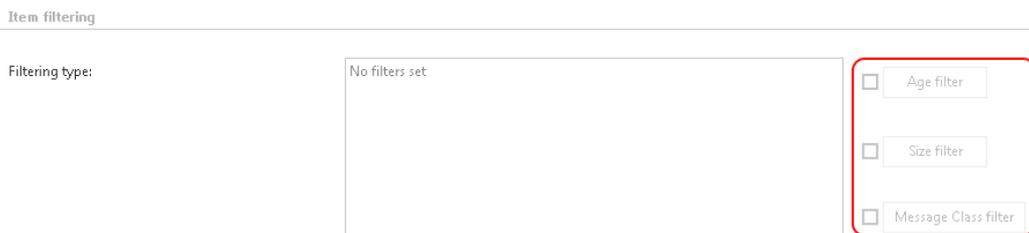


Storage settings

Storage name:

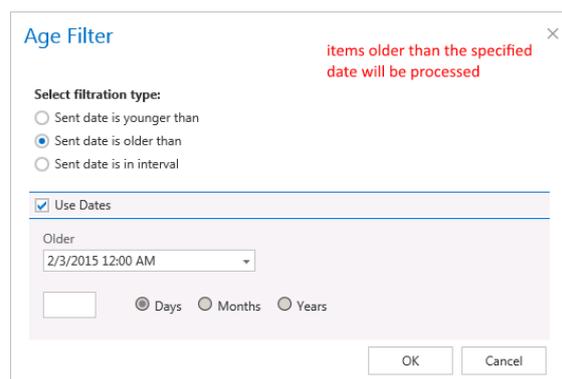
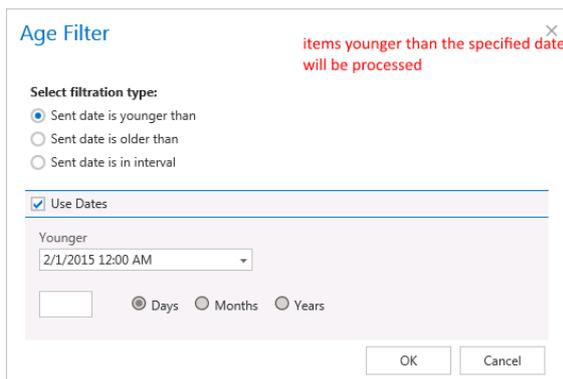
✓ **Item filtering:**

This configuration allows you to filter among your mailbox-items by 3 types of criteria: by age, size or message class. It is also possible to use more filters simultaneously. To activate any of these filters, check the corresponding checkbox first, then click on the button to open the filter dialog:



- **Age filter:** If you select an option from the “Select filtration type” list and check the **Use Dates** checkbox and specify a date, then the age filter will filter out all items, which have the sent date younger/older than this specific date. It is also possible to specify certain time interval with the **Use Dates** function. In this case the items falling under this sent date interval will be filtered out. This age filtering type should be used if you would like to process emails with a specific sent date.

Examples of **using dates:**





Examples of **filtering using days/months/years**: If the **Use dates** checkbox is not selected, then the date selection option becomes inactive. In this case it is allowed to filter between items that are **Younger/Older than** a certain number of days/month/years. Enter the number into the checkbox next to the **Days/Months/Years** radio button (screenshot A). It is also allowed to filter items which belong to a certain period of time, e.g. between items from months 1 to 3 (screenshot B). This age filtering type should be used if you would like to process items, which are older/younger than a certain number of days/months/years (e.g. items older than 1 year). If the Age filter has been set, click **OK**.

Screenshot A: processing items younger than 90 days

Screenshot B: processing items in age 1-3 months

- **Size filter**: This filter can be very useful, because it allows to find the biggest emails for further processing. If these large emails (and large attachments) are permanently processed, the Exchange server will be relieved from redundant megabytes that cause its slowness in many cases.

For filtering emails according to this criteria, activate **Size filter** button by checking the checkbox next to it, then click on the active button.

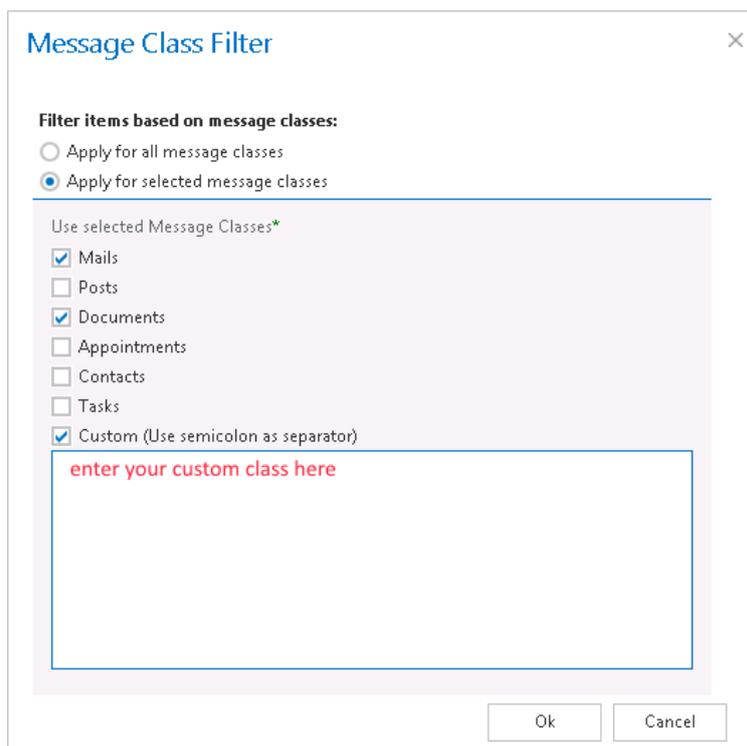
In the **Size filter** dialog choose from the filtering types (**Bigger then**, **Smaller then**, or **Between values**), enter the size (in kilobytes) and click **OK**.

- **Message class filter**: This filter was improved to select certain message classes to be processed. Using this filter, the user will be allowed to filter out different document types, such as mails, documents, contacts

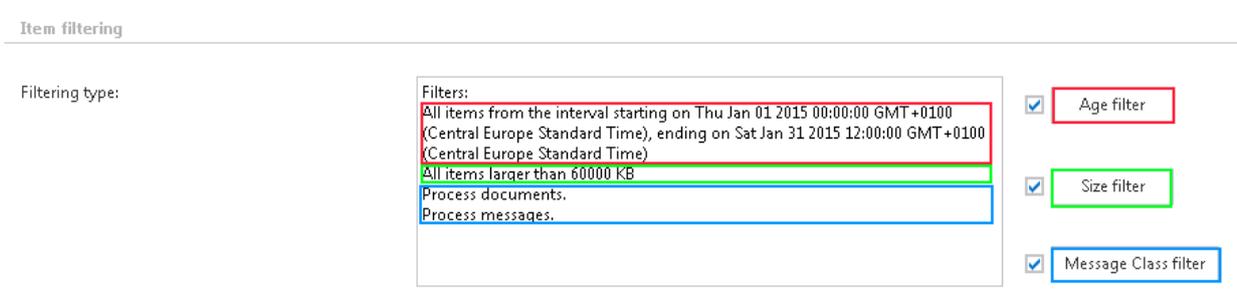


etc. For filtering emails according to this criteria, activate **Message class filter** button by checking the checkbox next to it, then click on the active button.

In the **Message class filter** dialog it is possible to choose if the filter will be applied for all message classes (choose radio button **Apply for all message classes**) or only for some selected classes (**Apply for selected message classes**). It is also allowed to add **Custom message classes** to the list of the already existing ones. After all necessary custom classes have been checked, click on **OK**.



After all settings have been done, a summary of filtering settings will be displayed under section **Item filtering** as it is shown on the screenshot below:





✓ Processing settings

The user can choose from 3 main ways of storing emails and attachments. It is possible either to archive the entire email message (in .msg format) with the attachment together (**Simple archive**), or just the attachment (**Archive attachment**). It is also possible to archive the entire email and copy it to the Public folder (**Archive and copy to Public folder**). This function helps to share the document with other users. Everyone with a user account and password on the Exchange server can access the Public Folder.

Processing settings

Processing type:

Custom categories to process

Split attachments

Create tag view

Public Folder user email:

Public Folder base folder:

Insert Public Folder data into the below displayed textboxes to establish the connection between the Public Folder and the archive management system:

Processing settings

Processing type:

Custom categories to process

Split attachments

Create tag view

Public Folder user email:

Public Folder base folder:

Custom categories to process function enables to restrict searching in the mailbox to the categories that are selected here. E. g. if Red Category is set, this means that only emails labeled with Red Category will be processed.

Split attachments: by checking this checkbox, the email message in .msg format and the corresponding attachments will be stored separately from each other. Both will be stored in the selected storage, but separately from each other. This helps to save storage space. Let's assume that emails of more users (for example 5 users) will be stored in the same storage. **Split attachments** function will recognize duplicate attachments and they will be stored only once (not 5x). However, email bodies will be stored 5 times, as emails in different mailboxes have different metadata.

Note: By splitting the attachments, it is possible to spare more storage space for the company documents. It is obligatory that the selected storage supports single instancing.



Create tag view: contentWEB and officeGATE are both associated with contentACCESS. Thus emails and attachments processed in contentACCESS can be easily found in contentWEB and officeGATE, too. By creating tag view, the items falling under more custom categories will be gathered together under a main folder, which is set here in the **Create tag view** textbox. This main folder will be displayed under this “tag view root name” both in contentWEB and officeGATE systems. Subfolders under this main folder will gather together all items falling under a certain custom category.

✓ Mailbox settings

A new mailbox that needs to be processed can be added here. Click on **+ new** and fill in the **Name** and **Email** into the popup window. Also check **Is Active** checkbox, otherwise the added mailbox will not be crawled (crawling of the mailbox will be in sleeping mode). Click on **OK**:

The 'Edit mailbox' dialog box contains the following fields and controls:

- Name:** Text input field containing 'XY'.
- Email:** Text input field containing 'X.Y@tech-arrow.com'.
- Is Active:** A checked checkbox.
- Buttons:** 'OK' and 'Cancel' buttons at the bottom right.

contentACCESS allows you to crawl more mailboxes at the same time. To select mailboxes to be crawled, navigate to **select** option and enter mailboxes into the **Mailbox selection** dialog box. With checking the checkbox next to **Name** you can select/deselect all mailboxes for further processing:

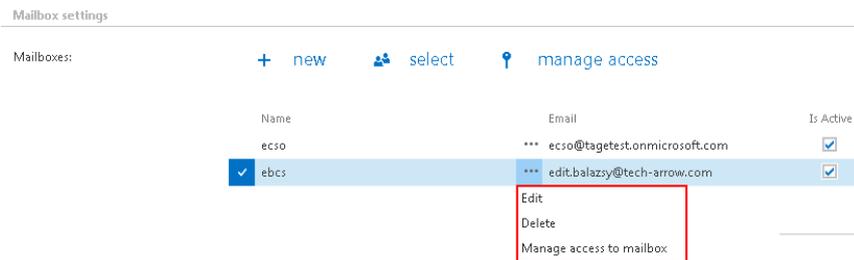
The 'Mailbox selection' dialog box features a table of mailboxes with a 'Name' column and a 'Type' column. A red arrow points to a checkbox in the 'Name' column, with a red text label 'select/deselect all mailboxes from the list' above it. The table lists the following mailboxes:

Name	Type
Office365	Server
techarrow_all	Group
techarrow_sales	Group
Test01	Group
build_notification	Group
elm_team	Group
emailarchive	Group
Administrators notification	Group
TenantAdmins_2092c	Group
HelpdeskAdmins_3ffa9	Group
RIM-MailboxAdmins:87a5acd646e1460	Group
Compliance Management	Group
Hygiene Management	Group
Discovery Management	Group
Records Management	Group

At the bottom of the dialog, there is a pagination control showing 'Page 1 of 4 (52 items)' and a set of navigation buttons (1, 2, 3, 4) with 'OK' and 'Cancel' buttons at the bottom right.



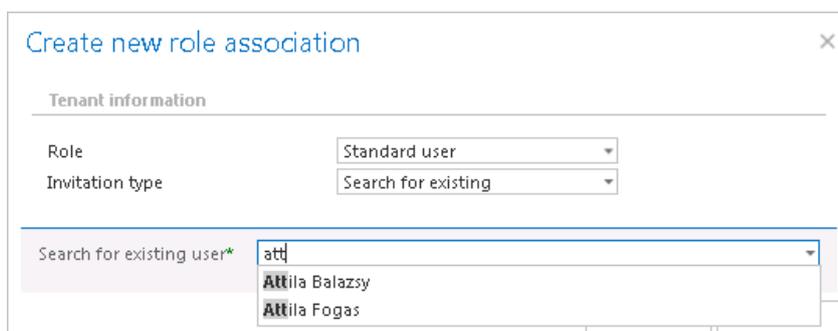
Under Mailbox settings you can also edit/delete or manage access to the selected mailbox(es). Click with left mouse on the ... (ellipsis) and choose an option from the dropdown list.



It is also possible to grant access to this mailbox for other users of contentWEB, officeGATE, or those who log in the mailbox through an online web application from mobile devices. By granting access to these users, they will have an access to the archived messages of the selected mailbox(es). Click on **Manage access to mailbox** in the context menu. Then click on **+ new** and fill the **Create new role association** dialogue box.

There are multiple options how to grant access to a mailbox for a user in the **Create new role association** window. You can **Create new** user, you can **Search for existing** worker from the company or you can also **Send an invitation** to somebody who is not a contentACCESS user yet.

In any case, the "Standard user" role type must be selected from the dropdown list (a standard user has only the right to check the mailbox). On the below displayed screenshot we give access rights to the mailbox for an already existing contentACCESS user.



✓ Resource settings

Under resource settings you can define the number of items that will be simultaneously crawled. It is not recommended to set here a value higher than the duplex number of cores of the processor, as it may extremely slow down the whole processing.



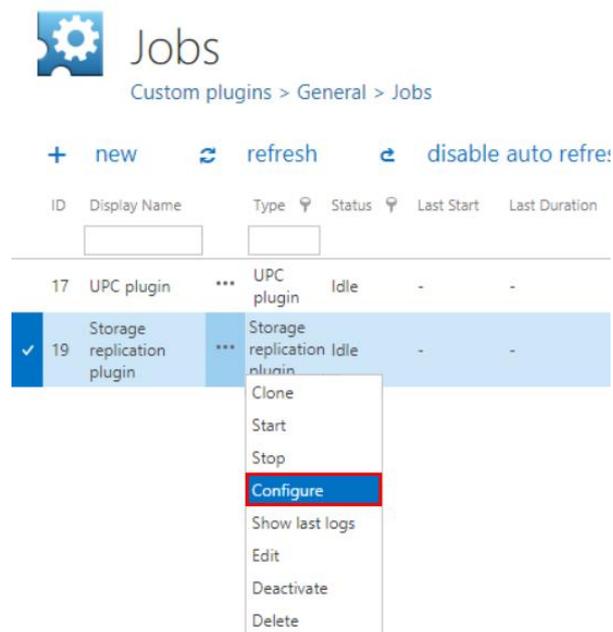


Never forget to save your job configurations at the end: click on **Save** in the upper left corner of the Central Administration ribbon.

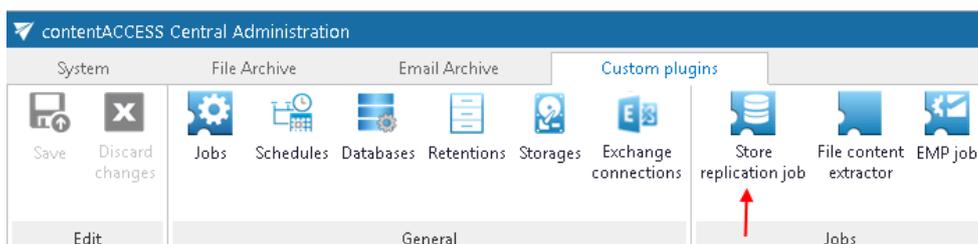
Storage replication plugin

A storage replication service is a managed service in which stored or archived data are duplicated in real time. A storage replication service provides an extra measure of protection that can be invaluable if the main storage backup system fails. Immediate access to the replicated data minimizes downtime and its associated costs. The service, if properly implemented, can streamline disaster recovery processes by generating duplicate copies of all backed-up files on a continuous basis. It can also speed up and simplify recovery from a disaster such as a fire, flood, hurricane or a virus.

After you have successfully created a new job for Store replication plugin (for more information on how to create a new job please refer to section [Creating new jobs in contentACCESS](#)), you can start to configure the storage replication job. Navigate to the **Custom plugins** → **General** → **Jobs**, choose the job from the list. Click on ellipses (...) and choose **Configure** option from the context menu.



The same job configurations can be done with a simple click on the icon of the job in **Custom plugins** → **Jobs** group in the ribbon:





- ✓ **Database settings:** Select an existing connection from the dropdown list or create a new one, where the job will save the metadata. (For further information on how to set database connections please refer to section [Databases.](#))

Database settings

Database connection:

A database of the Store replication job will contain the mapping data between the source storage and the target storage items. This means that after a failover of the main (source) storage this database will remember the mapping data between the source item and the target item, and a successful recovery from the backup (target) storage will be ensured.

- ✓ **Scheduling settings:** The storage replication job will run in times, which are set in the selected scheduler. On the screenshot below we have selected the “Always” scheduler, which will run the job without interruption. For more information on how to configure scheduler settings please refer to section [Schedules](#) described above.

Scheduling settings

Scheduled in:

- ✓ **Storage settings:** Within these settings it is necessary to set the source folder and the target folder(s). The source folder will be the primary folder. In case of any technical troubles, the required documents will be recovered from the secondary (target) folder with the assistance of data mapping saved in contentACCESS.

Storage settings

Source storage name:

Target storage name:

- ✓ **Resource settings:** Under resource settings it can be defined how many items/source folders will be simultaneously crawled. It is not recommended to set here a value higher than the duplex number of cores of the processor, as it will extremely slow down the whole processing.

Resource settings

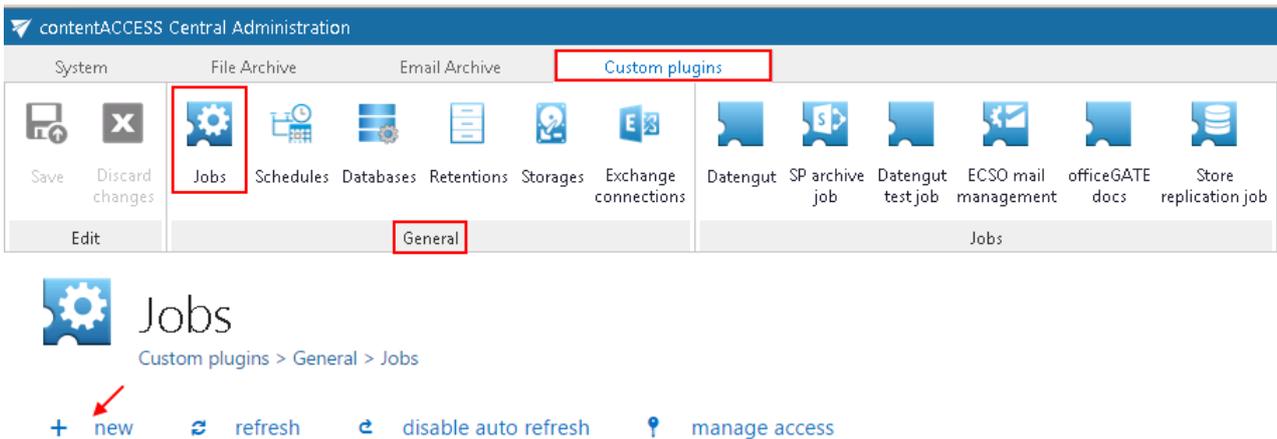
Worker thread count:

Sharing plugin

The Sharing job is used to collect files (e.g. big files that cannot be sent as email attachments) and enable them to be shared with other users. The job only collects these documents. The sharing process is done by [officeGATE](#), TECH-ARROW's genuine MS Outlook add-in. This section provides the user with the information about how to set up a Sharing job in contentACCESS. After the job is well configured, the plugin appears in the officeGATE's navigation pane in MS Outlook.

Sharing job configuration

Navigate to **Custom plugins** → **General** → **Jobs** on the Central Administration web interface to open the **Jobs** page. Click on **+ new** on this page.



contentACCESS Central Administration

System File Archive Email Archive **Custom plugins**

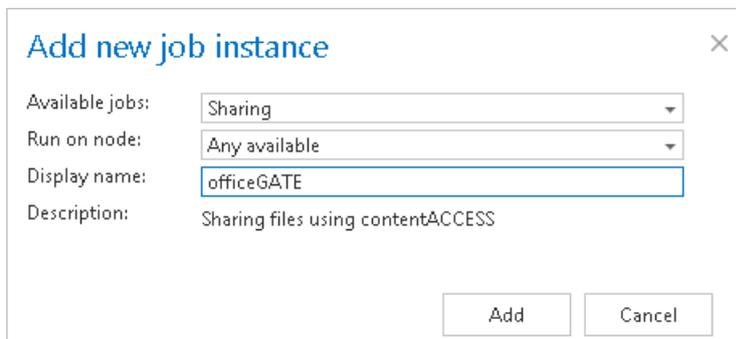
Save Discard changes **Jobs** Schedules Databases Retentions Storages Exchange connections Datengut SP archive job Datengut test job ECSO mail management officeGATE docs Store replication job

Edit **General** Jobs

Jobs
Custom plugins > General > Jobs

+ new refresh disable auto refresh manage access

In the “Add new job instance” window select “Sharing” from the list of Available jobs, name it and add it to the jobs’ list.



Add new job instance [X]

Available jobs:

Run on node:

Display name:

Description: Sharing files using contentACCESS

Add Cancel

contentACCESS will prompt you to configure the job instance now.



On the job's configuration page configure a database and a storage for the Sharing job and save your settings.

contentACCESS Central Administration

System File Archive Email Archive Custom plugins

Save Discard changes Jobs Schedules Databases Retentions Storages Exchange connections Datengut SP archive job Datengut test job ECSO mail management officeGATE docs Store replication job

Edit General Jobs

officeGATE
Custom plugins > Jobs > officeGATE

start immediately refresh disable auto refresh deactivate job logs

Status: **Idle**
Progress:

Storage settings

Storage name: File archive store Change

Database settings

Database connection: File Archive DB

Now the user can use the sharing function in officeGATE directly from his MS Outlook.

Datengut plugin

This custom plugin enables to connect the Datengut Document Management System with officeGATE. Based on the exact configurations of a Datengut job, the officeGATE user is allowed to

- Collaborate on the Datengut files using officeGATE
- Collaborate on the Datengut files using officeGATE + Synchronize email categories in multiple mailboxes if the same email is assigned to one Datengut project using officeGATE

If the Datengut job is already created (for more information about creating jobs refer to [Creating new jobs in contentACCESS](#)), open its page to configure it.



✓ **Login provider configuration settings**

Select the Datengut login provider that you have already configured in section **System** → **Security** → **Login providers** (refer to chapter [contentACCESS users in third-party systems](#) to learn how to create it).

✓ **Access management**

If you want to grant access to Datengut for more contentACCESS users, click on “Edit user permissions” button and configure a new user.

If you wish to synchronize email categories in multiple mailboxes, check the “Enable mailbox synchronization” checkbox. If you would not like to synchronize emails, left it unchecked and save your configurations above.

If email synchronization is enabled, the Datengut job updates the Email synchronizer job’s queue with the information about if the given category should be added/deleted to the given email. The user drag&drops (assigns) an email to a Datengut project in officeGATE and the Datengut job periodically updates the necessary data in the queue.

To enable email synchronization, the following extra settings need to be configured:

- **Database connection** - select a database where the Datengut job will write the metadata
- **Plugin job** - select the Email synchronizer job that is already configured (more information [here](#))
- **Username, Password:** specify the user credentials to be used to connect with the Datengut system
- **Scheduled in:** set the scheduler which will trigger the job in the given time periods
- **Notification settings:** if you need to get emails about any possible warning or errors, configure it with the recipient list here



Enable email synchronization

start immediately
 refresh
 enable auto refresh
 deactivate job
 logs
 edit

Database settings

Database connection: TESTDB

Plugin configuration

Plugin job: Email synchronizer plugin

User credentials

Username: username

Password: *****

Scheduling settings

Scheduled in: Today at 12 AM

Notification settings

Send when: Never

Recipient list: john.doe@example.com,peter.white@example.com

Email synchronizer plugin

Email Synchronizer plugin's function is to synchronize properties of the same email in multiple mailboxes. Currently the following actions are available:

- Add category: adds one or more categories to an email,
- Remove category: removes one or more categories from an email.

The email synchronizer job has a queue that the job checks periodically for new actions to be executed on emails. This queue is filled up by other plugins.

This chapter describes how an Email synchronizer job is configured.

Setting up an Email synchronizer job

After an Email synchronizer job is created on page **Custom plugins** → **General** → **Jobs**, you may start to configure it. For more information on how to create jobs refer to section [Creating new jobs in contentACCESS](#) of this guide.

On the configuration page of the given job the user is required to specify the following settings:

✓ **Exchange connection settings**

First the connection with the Exchange server must be established. Before processing, the job builds a list of all mailboxes and mailbox groups found on the specified Exchange server. Only the queue items in a mailbox handled by the Exchange server will be processed.



The process of setting an Exchange connection is described in section [Exchange connections](#) of this guide. Further select this Exchange connection on the synchronizer job's configuration page.

✓ **Database settings**

Set a database where the job will write the necessary data. For more information on how to create databases refer to section [Databases](#).

✓ **Scheduling settings**

By using schedulers, the administrator may automatize the running times of the given job. The mailboxes are periodically synchronized with the categories written into the queue in time intervals that are set here. For more information on how to set schedulers refer to section [Schedules](#) above.

✓ **Processing configurations**

There are 2 available methods of speeding up the synchronization process:

- **Use email archive database to enhance performance:** After processing emails with EntryId, the plugin continues with processing emails that have InternetMessageId only. Using this option, the process can be sped up if contentACCESS is used for email archiving. The plugin first searches for the queue item's EntryId in the archive. If it finds it, the queue item is added to the list of queue items with EntryId.
- **Search only for one email with MessageID in mailbox:** In case that the same email message exists in the mailbox multiple times, only the first email will be processed (marked with the given category) and all other emails in the given mailbox will be ignored. The first email will be marked in the recipient mailboxes, too (if exists).

✓ **Notification settings**

By using this option, the administrator may set when the notification emails need to be sent (always, only when errors occur, when both errors and warnings occur, or never) by the job. The recipient list of such emails is set in this section as well.

✓ **Resource settings**

The number of threads running in parallel is set here. The value is set to "2" by default.



contentACCESS Central Administration

System | File Archive | Email Archive | **Custom plugins**

Save | Discard changes | Jobs | Schedules | Databases | Retentions | Storages | Exchange connections | Perceptive | Datengut test job | officeGATE | SP archive job | Store replication inh | Datengut | ECSO mail management | **Email synchronizer plugin**

Edit | General | **Jobs**

Email synchronizer plugin

Custom plugins > Jobs > Email synchronizer plugin

start immediately
 refresh
 disable auto refresh
 deactivate job
 logs
 edit

Status: **Idle**
Progress:

Exchange connection settings

Exchange connection name: O365 connection

Database settings

Database connection: Email Archive DB ✓

Scheduling settings

Scheduled in: Daily at 5 PM

Processing configuration

Use email archive database to enhance performance
 Search only for the first email with MessageId in mailbox

Notification settings

Send when: Never
Recipient list: john.doe@example.com,peter.white@example.com

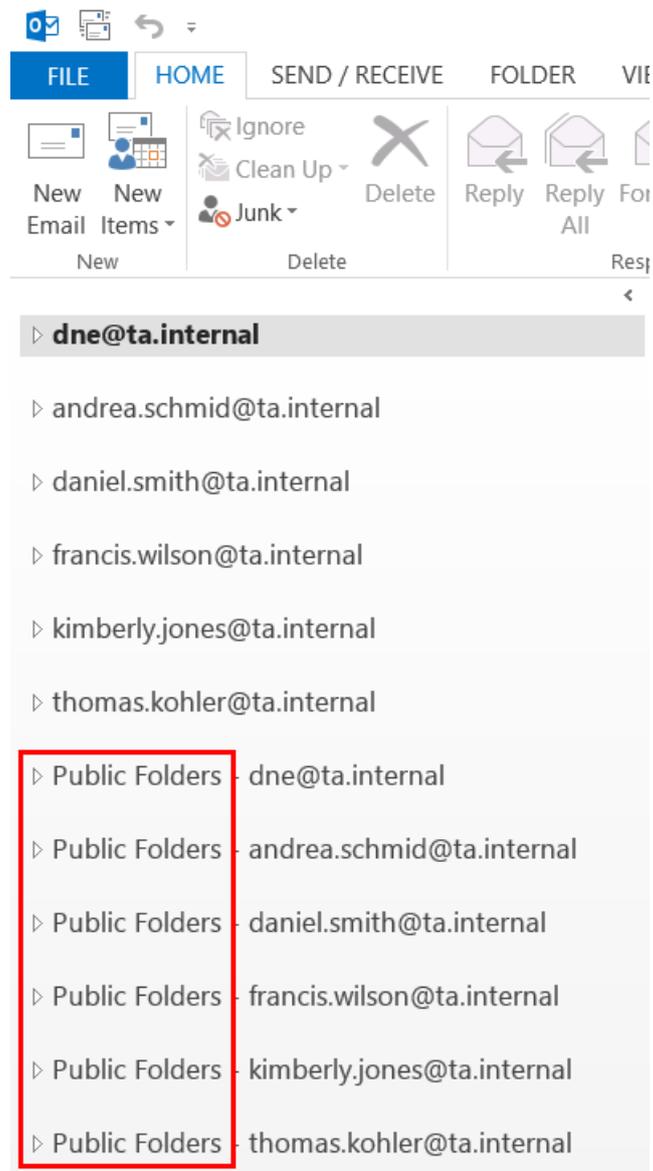
Resource settings

Worker thread count: 2

Categorize to Public folders plugin

This contentACCESS custom plugin is used for creating exactly one copy of tagged mails in public folders. The users are tagging mails Outlook with categories. Each category is associated with exactly one public folder. The tagged mails are then copied to the respective public folder and are further processed.

The folder name is used as the name for the Outlook category. The public folders are organized in hierarchy, but the folder names are unique across the organization.



Plugin requirements

- mapping table: **category name to public folder** path

This mapping must be maintained by the administrator: when new categories are created, the mapping must be updated. The changes in the mapping table are immediately reflected in the job (plugin).

- already set Exchange server connections, where the mailbox to be crawled is located (read more in [Exchange connections](#))



Configuring the Categorize to Public folders job

Go to **Custom plugins** -> **Jobs**, click **+New** and select **Categorize to Public folders**.

Add new job instance [X]

Available jobs: **Categorize to Public Folders** ▼

Run on node: Any available ▼

Display name: Categorize to Public folders

Description: Plugin for copying categorized mails to public folders. The plugin scans mailboxes and creates a copy of categorized mails in the corresponding public folder.

Add Cancel

On the configuration page of the given job the user is required to specify the following settings:

✓ Exchange connection settings

First the connection with the Exchange server must be established. Before processing, the job builds a list of all mailboxes and mailbox groups found on the specified Exchange server. Only those queue items will be processed which mailbox is handled by the Exchange server.

The process how an Exchange connection can be set is described in section [Exchange connections](#) of this guide. Further select this Exchange connection on the synchronizer job's configuration page.

✓ Database settings

Set a database where the job will write the necessary data. For more information how to create databases refer to section [Databases](#).

✓ Scheduling settings

In this step the running time(s) of the job must be selected. It is possible either to select a scheduler from the list or to create a new scheduler via **create new** ... option from the dropdown list. Using schedulers the administrator may automatize the running times of the given job. The mailboxes are periodically synchronized with the categories written into the queue in time intervals which is set here. For more information how to set schedulers refer to section [Schedules](#) above.



✓ **Processing settings**

The email of the public folder user must be entered here.

✓ **Category mapping**

A category name to a public folder must be mapped. The full folder path must be entered here. When new categories are added, the administrator must update this mapping.

✓ **Mailbox settings**

Mailboxes to be processed by the job must be selected here.

✓ **Include folders**

The job is crawling the entire mailbox or recursive folder structures from the mailbox for further processing. Before you enter the folder name(s) to be crawled, it is necessary to select the folder filtering type.

Include folders

Folder filtering type:

- One single folder
- Entire mailbox
- One single folder
- Recursive, starting from a single folder
- Multiple folders
- Multiple recursive, starting from a single folder

✓ **Resource settings**

Set the values, which will determine how many items will be processed simultaneously by the job. The recommended value is "2".



contentACCESS Central Administration Tenant: TECH-ARROW

System | File Archive | Email Archive | BackMailz | SharePoint Archive | Custom plugins

Save | Discard changes | Jobs | Schedules | Databases | Retentions | Storages | Exchange connections | Email sync MNE | Categorize to Public folders | Sharing plugin | Saperion | Lobo MNE | Email manage MNE | Storage replic MNE | Datengut MNE

Categorize to Public folders
 Custom plugins > Jobs > Categorize to Public folders

start immediately
 refresh
 disable auto refresh
 deactivate job
 logs
 edit

Status: **Idle**
 Progress:

Exchange connection settings

Exchange connection name:

Database settings

Database connection: ✔

Scheduling settings

Scheduled in:

Processing settings

Public Folder user email:

Public Folder base folder:

Allow duplicate checking:

Category mapping

+ new ↶ import

Category Name	Folder Path	
Testing emails	Testing\Testing mails	***

Mailbox settings

Mailboxes: + new 👤 select 🔑 manage access

Name	Email	Is Active
Daniel Smith	*** daniel.smith@ta.internal	<input checked="" type="checkbox"/>

Include folders

Folder filtering type:

Resource settings

Worker thread count:

Subworker thread count:

[Online help](#)

Crawling the mailbox content

The mailboxes are crawled using EWS. Only minimal information is retrieved, which helps to speed up the process of deciding if the message needs to be processed or not.

The processed messages are tracked in the contentACCESS database. The processed category is also tracked for each message. The modification date of the message is also stored, which helps to identify if the message was modified. Not modified messages can be skipped from processing.



When is an email/message processed?

The message is only processed if it has at least one category, which is in the category mapping. Private messages (messages with non-zero Sensitivity) are skipped from processing.

The message categories are processed sequentially. For each category the mapping is searched. If there is no hit, the given category is ignored and no record is created. If there is a hit, the message is copied to the defined public folder.

Special cases

- 1) The message was not yet processed

In this case the message ENTRYID is not found in the contentACCESS database and therefore is sent for processing. All categories of the message are processed.

- 2) The message was already processed
- 3) Category was changed on the processed message
- 4) Category mapping was changed

In this cases the messages/emails may not be processed again.

LoboDMS plugin

The LoboDMS plugin's function is to collect emails. It is not connected with the contentACCESS LoboDMS storage. The plugin uses a separated storage type in LoboDMS instead, where the emails are stored.

The plugin scans the configured mailboxes for what is defined in the **Processing pattern** and then according to the configuration decides whether the email should be sent to LoboDMS and have a category applied. The category signalizes the user that this email was already processed and will be found in LoboDMS.



Configuring the LoboDMS plugin

Go to **Custom plugins** -> **Jobs**, click **+New**. In the popup window select the **Lobo DMS plugin** and provide a display name.

The plugin configuration page has several sections, some of them are optional, some are required to fill in. The next sections are provided:

✓ LoboDMS job processing configuration

LoboDMS job processing configuration

Processing pattern:*	<input type="text" value="LoboDMS Accept"/>
Categories to skip:	<input type="text" value="LoboDMS Skip"/>
Category to apply:*	<input type="text" value="SentToLoboDMS"/>
Message format:*	<input type="text" value="EML"/>
Repository:*	<input type="text" value="lobo-dms@loboDemo"/>
Document type:*	<input type="text" value="lobo:email_inbox"/>
Enable bookmarks:	<input type="checkbox"/>

- **Processing pattern** – Regular expressions which will be tested against the email subject. If the email subject matches the expression, then the email will be transmitted into LoboDMS.
- **Categories to skip** – It is a comma separated list of categories. The plugin will skip any email having a category from this list, even if the processing pattern matches.
- **Category to apply** – The category that will be applied to the mails which were processed and sent to LoboDMS should be provided here.
- **Message format** – The format of the message in which the email will be sent to LoboDMS.
- **Repository** – The repository ID which is defined in LoboDMS.
- **Document type** – The type defined in LoboDMS, where the emails are stored.



- **Enable bookmarks** – The plugin processes folders. Items are sorted according to the modification date. If bookmarking is enabled, then plugin saves the last processed item modification date and in the next run it will process items from exchange which are younger than the bookmarked. If it is turned off, then it will request all items from exchange and will skip items which were already processed.

✓ **LoboDMS authentication**

The plugin uses the server and credentials specified here for communication with the given LoboDMS instance.

LoboDMS authentication

LoboDMS server:	<input type="text" value="http"/> <input type="text" value="://"/> <input type="text" value="cloudapp.net"/> : <input type="text" value="9000"/>
Username:	<input type="text"/>
Password:	<input type="password"/>
	<input type="button" value="Test"/>

✓ **Database settings**

The plugin requires a database, where some data will be stored during the run and configuration.

Database settings

Database connection:	<input type="text" value="TenantDBAho"/> <input type="button" value="✓"/>
----------------------	---

✓ **Exchange connection settings**

Exchange connection which the plugin will use to connect with exchange. New connection can be added in Exchange connections tab.

Exchange connection settings

Exchange connection name:	<input type="text" value="O365"/>
---------------------------	-----------------------------------



✓ Mailbox settings

According to the exchange settings, here you can select mailboxes and groups, which will be processed by the plugin.

Mailbox settings

Mailboxes: + new 👥 select 🔑 manage access

	Name	Email	Is Active
👥	AHOgroup	*** tech.internal/Users/AHOgroup	<input checked="" type="checkbox"/>
👤	Adam [REDACTED]	*** aho1@tech.internal	<input checked="" type="checkbox"/>
👤	Adam [REDACTED]	*** aho2@tech.internal	<input checked="" type="checkbox"/>

✓ Notification settings

Select here, when you will need to get notification emails from the plugin. It is possible to set here, if you need a notification email always/never, or, you need it only if an error/warning occurred during the process – for example, if the processing of one or more items failed, then you may get a notification email about this error. Into the **Recipient list** textbox insert the email addresses of the people whom you would like to send these emails to – if there are multiple recipients, the addresses must be separated by “,” or “;”.

Notification settings

Send when:

Recipient list:

✓ Resource settings

Set the value, which will determine how many threads will process the selected mailboxes simultaneously. The recommended value is 2, as in our case.

Resource settings

Worker thread count:

At the end never forget to save your job configurations: click on **Save** in the left upper corner of UI.

ThreatTest

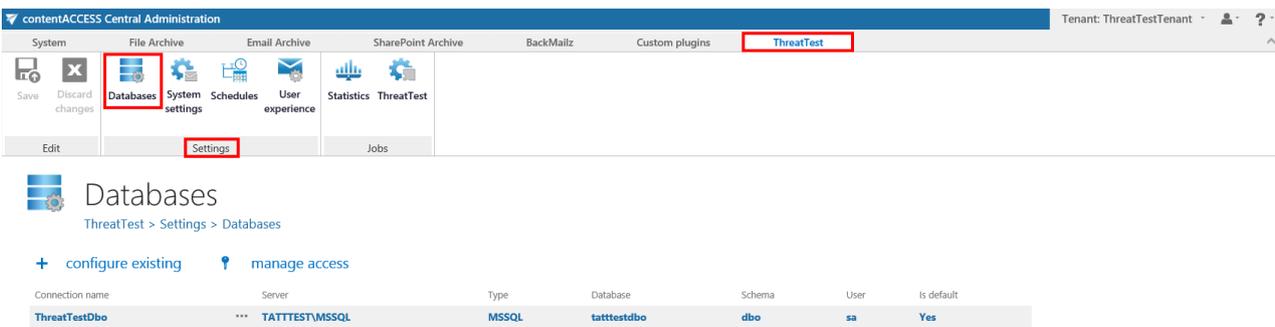
ThreatTest is a mail add-in application, which can help you quickly report and execute actions on suspicious emails. It's an automated, advanced anti-phishing service that empowers users to stop email-borne threats by seamlessly reporting suspicious emails for threat investigation in real-time with the click of a button. ThreatTest is configured by the administrator in contentACCESS.

ThreatTest configuration

In the following sections, we will show you the contentACCESS configuration part.

ThreatTest Databases

Navigate to **ThreatTest** ⇒ **Settings** ⇒ **Databases**:



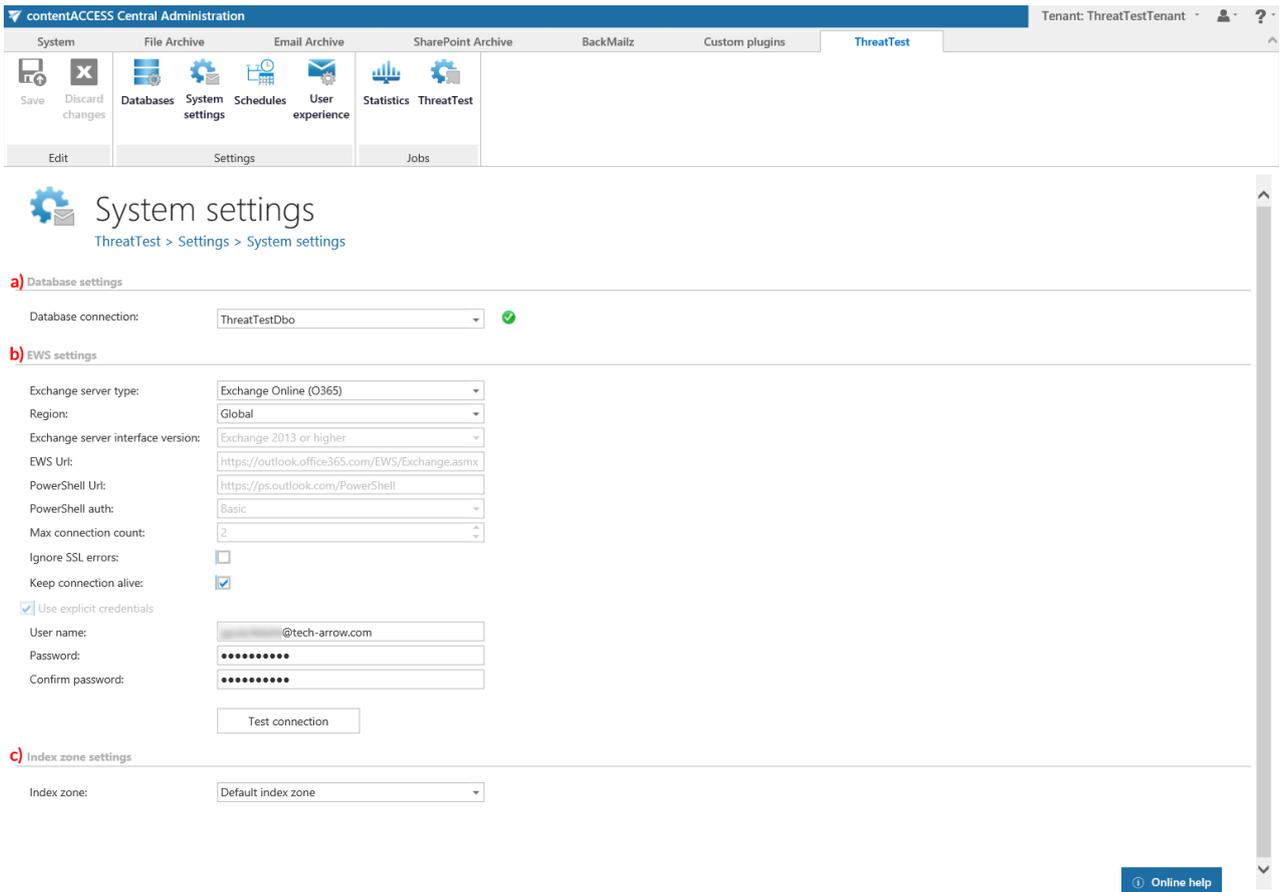
The screenshot shows the contentACCESS Central Administration interface. The top navigation bar includes tabs for System, File Archive, Email Archive, SharePoint Archive, BackMailz, Custom plugins, and ThreatTest. The ThreatTest tab is active, and the Databases sub-tab is selected. Below the navigation bar, there are buttons for Save, Discard changes, Databases, System settings, Schedules, User experience, Statistics, and ThreatTest. The Databases section is expanded, showing a table of configured databases.

Connection name	Server	Type	Database	Schema	User	Is default
ThreatTestDb0	TATTTEST\MSSQL	MSSQL	tatttestdbo	dbo	sa	Yes

Here you can find the full list of all accessible databases configured for the tenant. Database settings enable to choose the destination on premise or cloud, where the processed metadata will be stored. For further information about how to add new databases and perform database settings, please refer to section [Databases](#).

ThreatTest System settings

General ThreatTest System settings are available on the System settings page. To configure these settings, navigate to **ThreatTest** ⇒ **Settings** ⇒ **System settings** on the ribbon:



a) Database settings

Database connection: ThreatTestDbo ✓

b) EWS settings

Exchange server type: Exchange Online (O365)
 Region: Global
 Exchange server interface version: Exchange 2013 or higher
 EWS Url: https://outlook.office365.com/EWS/Exchange.asmx
 PowerShell Url: https://ps.outlook.com/PowerShell
 PowerShell auth: Basic
 Max connection count: 2
 Ignore SSL errors:
 Keep connection alive:
 Use explicit credentials
 User name: @tech-arrow.com
 Password: ●●●●●●●●
 Confirm password: ●●●●●●●●

Test connection

c) Index zone settings

Index zone: Default index zone

Online help

a) Database settings

Select the ThreatTest database, that you have already configured on **ThreatTest** ⇒ **Settings** ⇒ **Databases** page (in our case it is database “ThreatTestDbo”), from the dropdown list. This selected database will be used by the ThreatTest job and all metadata during the synchronization process will also be stored here.

b) EWS settings

Under **Exchange server type** and **Exchange server interface version** select the type and version of the server where your email provider is running. Then enter the **EWS URL**, **PowerShell URL** and the **PowerShell authentication**. These data must be requested from the email provider that you use (the configuration properties are the same for On-premise and Hosted Exchange).

Note: In case of the user having/using a **German cloud** (dedicated and isolated Microsoft Azure version for Germany), **Germany** must be selected in the **Region** dropdown list.



EWS settings

Exchange server type:	Exchange Online (O365) ▼
Region:	Germany ▼
Exchange server interface version:	Exchange 2013 or higher ▼
EWS Url:	https://outlook.office.de/EWS/Exchange.asmx
PowerShell Url:	https://outlook.office.de/PowerShell
PowerShell auth:	Basic ▼
Max connection count:	2 ▲▼

Under **Max. connection count** option the user may define how many parallel connections will be maintained by the system when connecting to PowerShell.

If you do not have a valid certificate, you can check the **Ignore SSL errors** checkbox.

Keep connection alive: If this option is turned on, then the connection between contentACCESS and the Exchange server is cached, which increases the performance. If the Exchange is load balanced, some requests can land on another Exchange, which causes errors in contentACCESS. In these cases unchecking the **Keep connection alive** option will destroy the connection after each request and will rebuild it on the next request.

- If you are communicating with **one Exchange server: turn it on** to increase the performance
- If you have a **load balanced Exchange environment** and there are **communication problems** with the Exchange: it is recommended to **turn it off**

Further enter the applicable **User name** and **Password** to connect to the Exchange (use explicit credentials or log in under service-credentials). The user entered here must have the necessary rights to all mailboxes that he wants to activate ThreatTest for. The necessary rights are the following:

- Full-access to all mailboxes
- View only organization management
- Org Custom Apps (this is required for add-in installation)

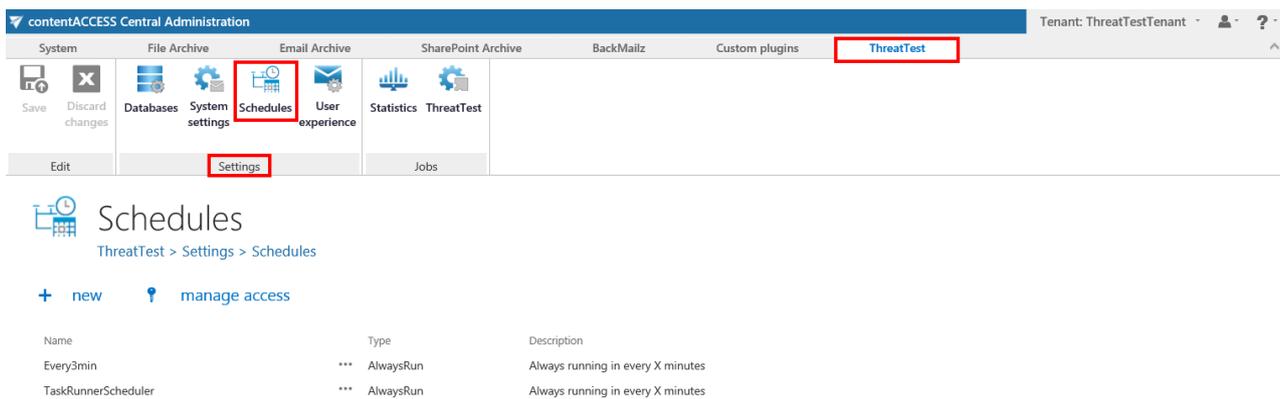
We recommend to run a test connection via **Test** button.

c) Index zone settings

Select here a previously configured [Index zone](#) that will be assigned to all items processed by the [ThreatTest job](#).

ThreatTest Schedules

Navigate to **ThreatTest** ⇒ **Settings** ⇒ **Schedules**:



The screenshot shows the 'contentACCESS Central Administration' interface. The top navigation bar includes 'System', 'File Archive', 'Email Archive', 'SharePoint Archive', 'BackMailz', 'Custom plugins', and 'ThreatTest'. The 'ThreatTest' tab is selected. Below the navigation bar, there are several icons for 'Save', 'Discard changes', 'Databases', 'System settings', 'Schedules', 'User experience', 'Statistics', and 'ThreatTest'. The 'Schedules' icon is highlighted with a red box. Below the navigation bar, there are 'Edit' and 'Settings' buttons, with 'Settings' also highlighted with a red box. The main content area shows the 'Schedules' page for 'ThreatTest > Settings > Schedules'. It includes a '+ new' button and a 'manage access' link. Below these are two scheduler entries in a table:

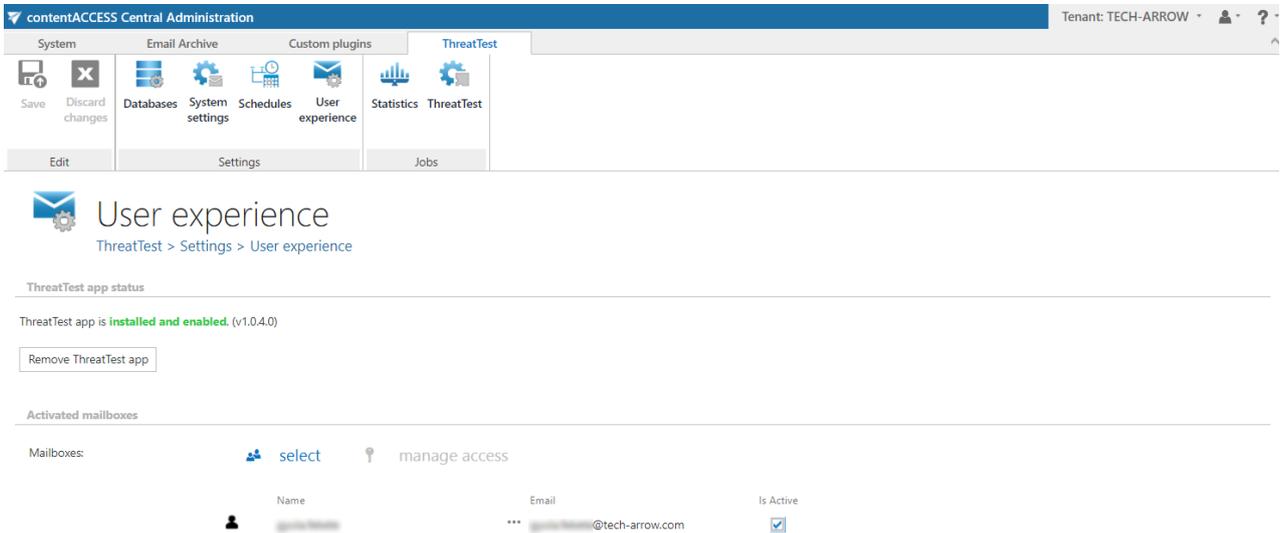
Name	Type	Description
Every3min	*** AlwaysRun	Always running in every X minutes
TaskRunnerScheduler	*** AlwaysRun	Always running in every X minutes

The already configured schedulers are listed on this page, in the scheduler's grid. By clicking on the **+ new** option, it is possible to create a new scheduler. For ThreatTest, we recommend to set up a scheduler that will run every 1 minute. This option will cause the lowest delay in the process. (For more information about how to set schedulers, please refer to the section [Schedules](#)).

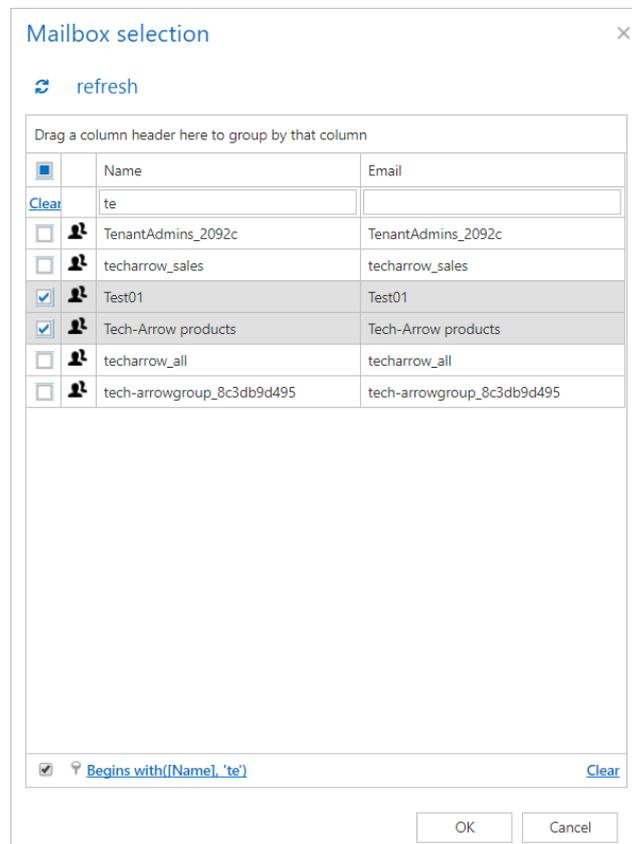


ThreatTest User experience

On this page it is possible to install and enable the ThreatTest app for the users.



To enable the app for new users, click on the **select** and select the desired mailbox(es) (similar to mailbox selection in [Email archive](#)).





At the next run of the Notification job, the users that were added here will get a notification email and they can start using the ThreatTest app/add-in!

It is also possible to assign a contentACCESS role to a user from here. Select him/her and click on [manage access](#). This will redirect you to the [Manage Access to Object](#) page. Here, click on **+ new** and select the role and invitation type. Roles define the permissions that a certain contentACCESS user has in the entire system (read more [here](#)). Invitation informs the user about a role being created for him/being invited to contentACCESS (read more [here](#) – part **Creating/inviting contentACCESS users**).

Create new role association ✕

Tenant information

Role	Standard user
Invitation type	Invitation

E-mail address*	test@tech-arrow.com
Additional message	Hello, please accept my invitation.



ThreatTest Statistics

The statistics of the reported email can be seen on this page. The page is divided into 3 sections: **30 days**, **Overtime** and **Recently reported emails**.

contentACCESS Central Administration
Tenant: TECH-ARROW

System
Custom plugins
ThreatTest

Save
Discard changes
Databases
System settings
Schedules
User experience
Statistics
ThreatTest

Statistics

ThreatTest > Jobs > Statistics

30 Days Summary

24 total submissions
11 malicious message detected
3 unique users
16 mins average response time

Overtime

Domains: (All domains) Quick Date Filtering: Please select Start Date: 1/16/2018 End Date: 2/15/2018 Run

Number of submissions by category

Top users by number of submissions

Unique users

Top domains by number of submissions

Recently reported emails

Date	EmailAddress	Subject	Status	Status date
2/8/2018 10:31:48 AM	@tech-arrow.com	test	UNPROCESSED	2/8/2018 10:47:22 AM
2/6/2018 3:11:41 PM	@tech-arrow.com	TECH-ARROW	UNPROCESSED	2/6/2018 3:27:26 PM
2/6/2018 2:50:02 PM	@tech-arrow.com	Virus test	VIRUS	2/6/2018 2:51:19 PM
2/6/2018 1:30:31 PM	@tech-arrow.com	ThreatTest Final Response for @tech-arrow.com	UNPROCESSED	2/6/2018 1:46:15 PM
2/6/2018 1:13:53 PM	@tech-arrow.com	virus test	VIRUS	2/6/2018 1:14:43 PM
2/6/2018 1:06:40 PM	@tech-arrow.com	Testing email attachment	UNPROCESSED	2/6/2018 1:58:27 PM
2/6/2018 1:06:25 PM	@tech-arrow.com	Claim your prize	SPAM	2/6/2018 1:07:29 PM
2/6/2018 11:11:20 AM	@tech-arrow.com	Test email	SAFE	2/6/2018 11:20:08 AM
1/25/2018 1:49:20 PM	@tech-arrow.com		THREAT	1/25/2018 1:50:25 PM
1/25/2018 1:12:39 PM	@tech-arrow.com		THREAT	1/25/2018 2:38:15 PM
1/22/2018 3:50:18 PM	@tech-arrow.com	ThreatTest Confirmation of Receipt for @tech-arrow.com	FAILURE	1/22/2018 4:42:01 PM
1/22/2018 2:00:25 PM	@tech-arrow.com	TT Test 3	FAILURE	1/22/2018 2:52:03 PM
1/22/2018 2:00:17 PM	@tech-arrow.com	TT Test 2	VIRUS	1/22/2018 2:01:54 PM
1/22/2018 2:00:10 PM	@tech-arrow.com	TT Test 1	FAILURE	1/22/2018 2:52:02 PM
1/22/2018 1:25:27 PM	@tech-arrow.com	Web API test 1	FAILURE	1/22/2018 1:15:01 PM

Open Archive Portal for more details...

[Online help](#)



30 days

This section shows the summary statistics about emails that were reported in the last 30 days.

Overtime

In this section the statistics about all emails are displayed. The user can filter them by domain, age (max 90 days), start or end date. There are 4 graphs, each displaying the statistics based on a different factor: **Number of submissions by category, Top users by number of submissions, Unique users and Top domains by number of submissions.**

Recently reported emails

Here the recently processed emails are shown. The columns in the grid are as follows:

Date: The day, when the email was reported by the user.

Email address: Email address of the user that reported the email.

Subject: subject of the reported email.

Status: Status assigned to the reported email by ThreatTest.

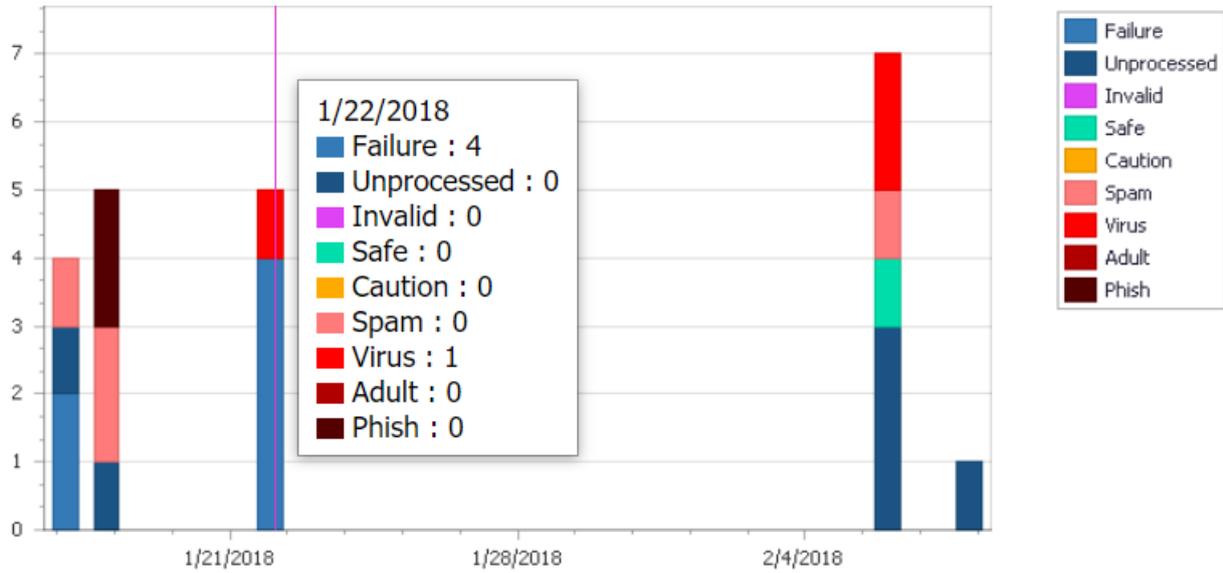
Status date: The day, when the status was assigned to the reported email.

Note: The filter, which is set in the **Overtime** section, also filters emails in this section.

When you put your cursor on a graph, the details will be displayed.



Number of submissions by category

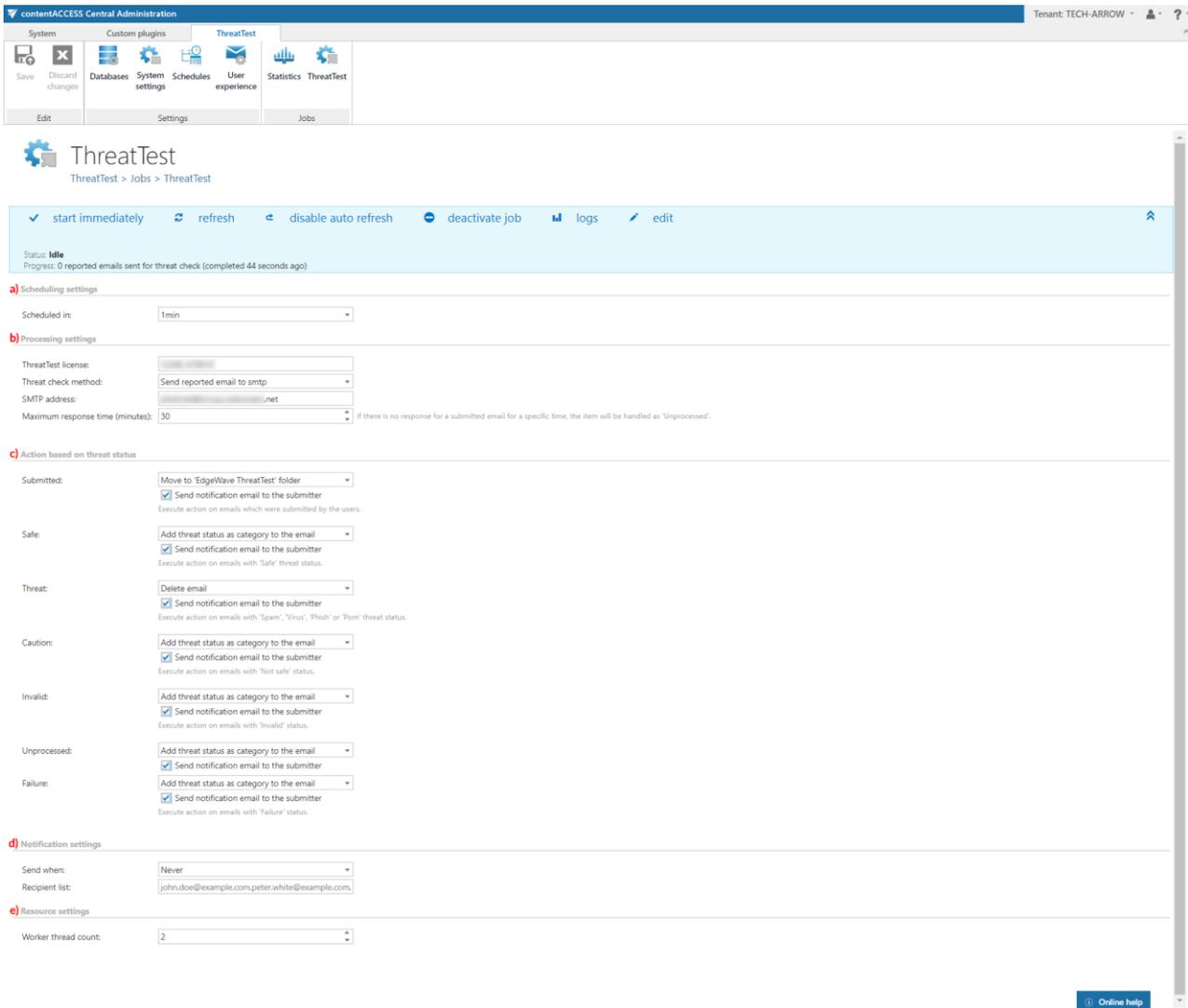


On the bottom of this page, there is the **Open Archive portal for more details...** button. This will redirect the user to [contentWEB](#), where he will be able to view the reported emails.

ThreatTest Job

Navigate to **ThreatTest** ⇒ **Jobs** ⇒ **ThreatTest**:

The job's page is divided into following sections:



a) Scheduling settings

In this step the running time(s) of the ThreatTest job must be selected. It is possible either to select a scheduler from the list or to create a new scheduler via **create new...** option from the dropdown list. For the ThreatTest job it is recommended to set a schedule, which will start the job every 1 minute. This option will cause the lowest delay in the process.

Scheduling settings

Scheduled in:

Every3min

Create new ...

Every3min

TaskRunnerScheduler



b) Processing settings

Here, the ThreatTest license must be entered. From the **Threat check method** dropdown list, choose one of the following methods (this will happen to the emails reported by users):

Processing settings

ThreatTest license:	<input type="text"/>
Threat check method:	<input type="text" value="Send reported email to smtp"/>
SMTP address:	<ul style="list-style-type: none">Internal (for testing)Send reported email to smtpPost reported email to service

If you select **Send reported email to smtp**, you need to specify the SMTP address that will process the emails. If you select **Post reported email to service**, you need to specify the Service URL address.

c) Action based on threat status

In this section, the actions to be executed on emails (depending on status assigned by ThreatTest) have to be selected. The following statuses are possible: **Submitted, Safe, Threat, Caution, Invalid, Unprocessed** and **Failure**.



Action based on threat status

Submitted:	<div style="border: 1px solid #ccc; padding: 2px; margin-bottom: 5px;">Move to 'EdgeWave ThreatTest' folder ▾</div> <input checked="" type="checkbox"/> Send notification email to the submitter <small>Execute action on emails which were submitted by the users.</small>
Safe:	<div style="border: 1px solid #ccc; padding: 2px; margin-bottom: 5px;">Add threat status as category to the email ▾</div> <input checked="" type="checkbox"/> Send notification email to the submitter <small>Execute action on emails with 'Safe' threat status.</small>
Threat:	<div style="border: 1px solid #ccc; padding: 2px; margin-bottom: 5px;">Delete email ▾</div> <input checked="" type="checkbox"/> Send notification email to the submitter <small>Execute action on emails with 'Spam', 'Virus', 'Phish' or 'Porn' threat status.</small>
Caution:	<div style="border: 1px solid #ccc; padding: 2px; margin-bottom: 5px;">Add threat status as category to the email ▾</div> <input checked="" type="checkbox"/> Send notification email to the submitter <small>Execute action on emails with 'Not safe' status.</small>
Invalid:	<div style="border: 1px solid #ccc; padding: 2px; margin-bottom: 5px;">Add threat status as category to the email ▾</div> <input checked="" type="checkbox"/> Send notification email to the submitter <small>Execute action on emails with 'Invalid' status.</small>
Unprocessed:	<div style="border: 1px solid #ccc; padding: 2px; margin-bottom: 5px;">Add threat status as category to the email ▾</div> <input checked="" type="checkbox"/> Send notification email to the submitter
Failure:	<div style="border: 1px solid #ccc; padding: 2px; margin-bottom: 5px;">Add threat status as category to the email ▾</div> <input checked="" type="checkbox"/> Send notification email to the submitter <small>Execute action on emails with 'Failure' status.</small>

The following actions can be selected for the statuses (not all statuses have all options available):

No action: No action will be executed on the email.

Add 'Submitted' category to the email: This action is available only for the **Submitted** status and it will add the **Submitted** category to the email.

Add threat status as category to the email: This action will add the assigned threat status as category to the email.

Move to 'EdgeWave ThreatTest' folder: This action will move the email to the **EdgeWave ThreatTest** folder in the mailbox.

Move to custom folder: This action will move the email to the folder that you specify here.

Delete email: This action will delete the email.

Resubmit email: This action is available only for the **Unprocessed** status and it will automatically resubmit the email (the resubmission count has to be set here).



If the submitters want to receive notification emails, check the checkbox **Send notification email to the submitter** (you can check this for each status separately).

Reply Reply All Forward IM



Tue 06-Feb-18 12:21 PM

Edgewave Hybrid Threat Detection Team <noreply@edgewave.com>

ThreatTest Final Response for [redacted]@tech-arrow.com

To

contentACCESS

ThreatTest

+ Get more apps

✓ **Yay! You're All Set.**



The EdgeWave Hybrid Threat Detection Center didn't find any malicious content in your email.

Please go to the EdgeWave ThreatTest folder to get your email. By highlighting and right-clicking the email, you can move it back into your inbox. *Note that the EdgeWave ThreatTest folder may have other suspicious emails you've submitted that are still being analyzed.* Be sure to check the subject line before moving the email back to the inbox.

For more details on our terms of use, please click [here](#).

Here's the summary info.

Recipient	Submitted	Subject
[redacted]@tech-arrow.com	Tuesday, February 6, 2018 11:11 AM UTC	Test email

Screenshot: Notification email, when the reported email has been marked as **Safe**

d) Notification settings

Select here the cases, in which you need to get notification emails from the ThreatTest job. It is possible to set here if you need such a notification email always/never, or if you need it only in case when an error/warning occurred during the job run. Into the **Recipient list** textbox insert the email address(es) of the person(s), who will get such notifications. **Notifications** should be used if the administrator does not use the **System logs** feature.

Notification settings

Send when:

Recipient list:



e) Resource settings

Set the value, which will determine how many items will be processed simultaneously by the ThreatTest job. The recommended value is "2".

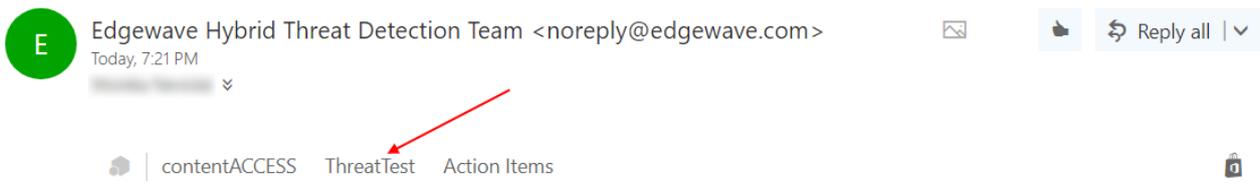
Resource settings

Worker thread count:

Using ThreatTest app

After receiving an activation email, it is necessary to activate the app first. That can be done by selecting the activation email, clicking on the **ThreatTest** button and then on the **Activate application** button.

ThreatTest Activation



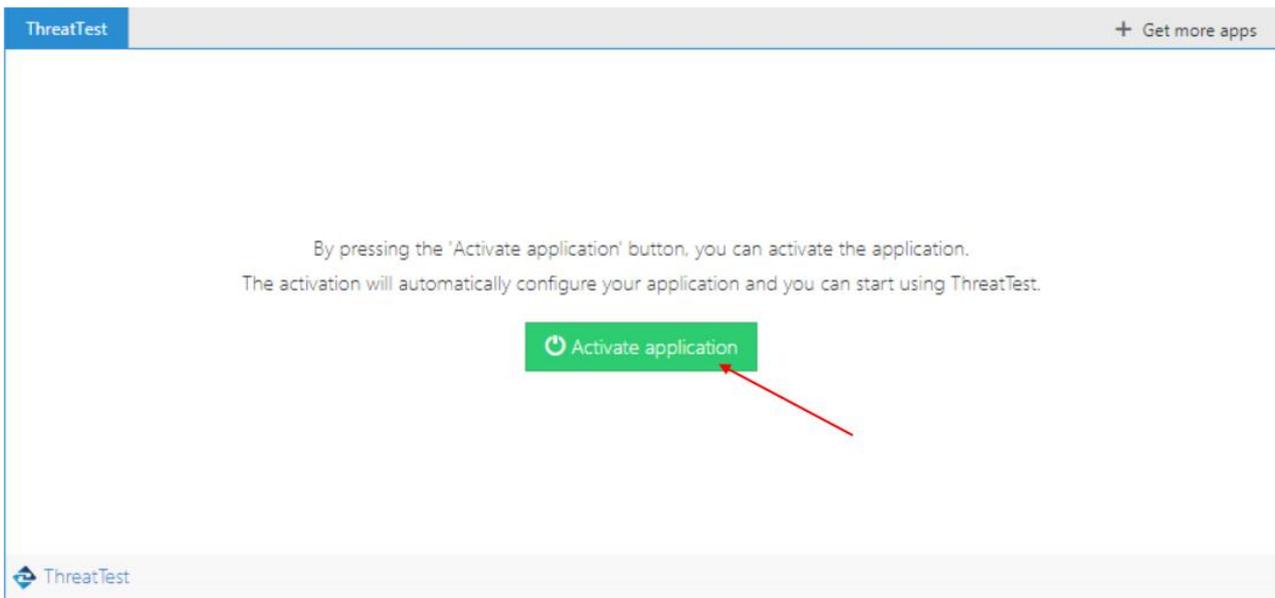
IT'S TIME TO ACTIVATE!

Thank you for registering for EdgeWave ThreatTest!

Now, to activate ThreatTest, all you need to do is click the ThreatTest button on the top ribbon bar on Outlook. It could take a little while to activate. If you don't see it after activation, try restarting your Outlook and it should be there. If you have any technical questions, please contact your IT administrator.

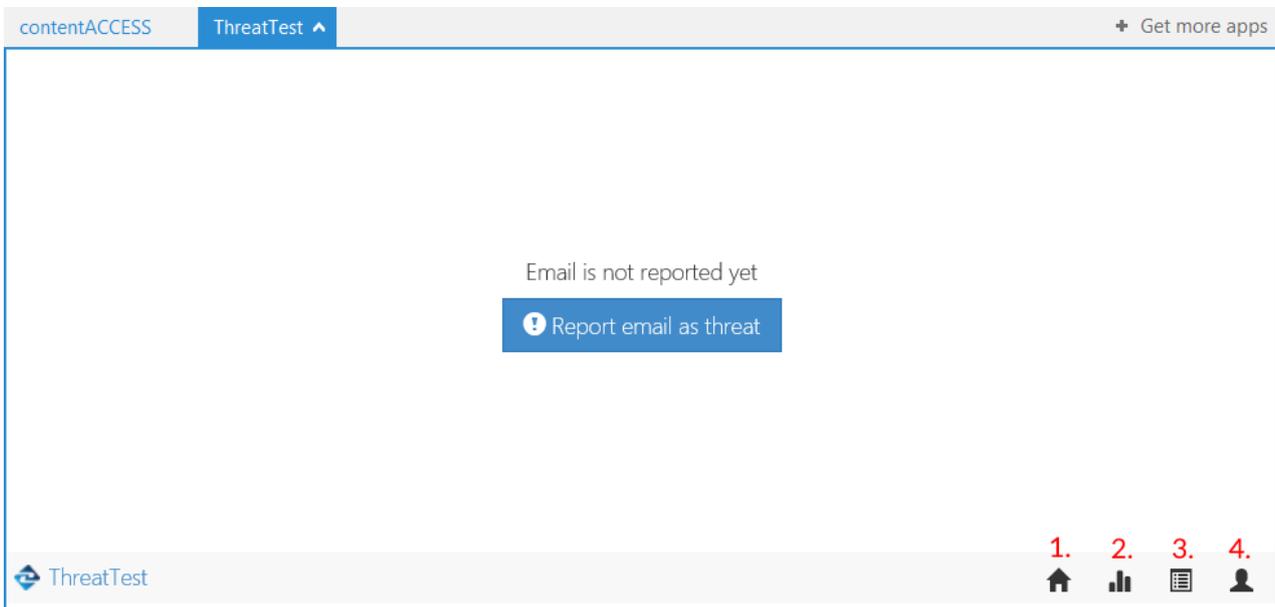
Happy clicking!

BTW...we'd love to hear from you. Please share your thoughts with us at share@threattest.edgewave.com.



Note: The app may not be visible right away, it may take up to an hour.

The buttons of the app are as follows:



1) Home button

This button will redirect you to the home screen (as seen on screenshot above), where the current status of the email can be seen. The actions, which will be executed on the emails based on the threat status, are set in the ThreatTest job. The following statuses are possible:



Failure – When Edgewave ThreatTestLab returns a Failure threat status for the email, contentACCESS can't forward it to Edgewave ThreatTestLab or when contentACCESS didn't get a result from ThreatTestLab in a specific time (configurable on ThreatTest plugin settings)

Not reported yet – the email was not yet reported using the ThreatTest app (as on screen above)

Submitted – The mail was already submitted, but not processed yet

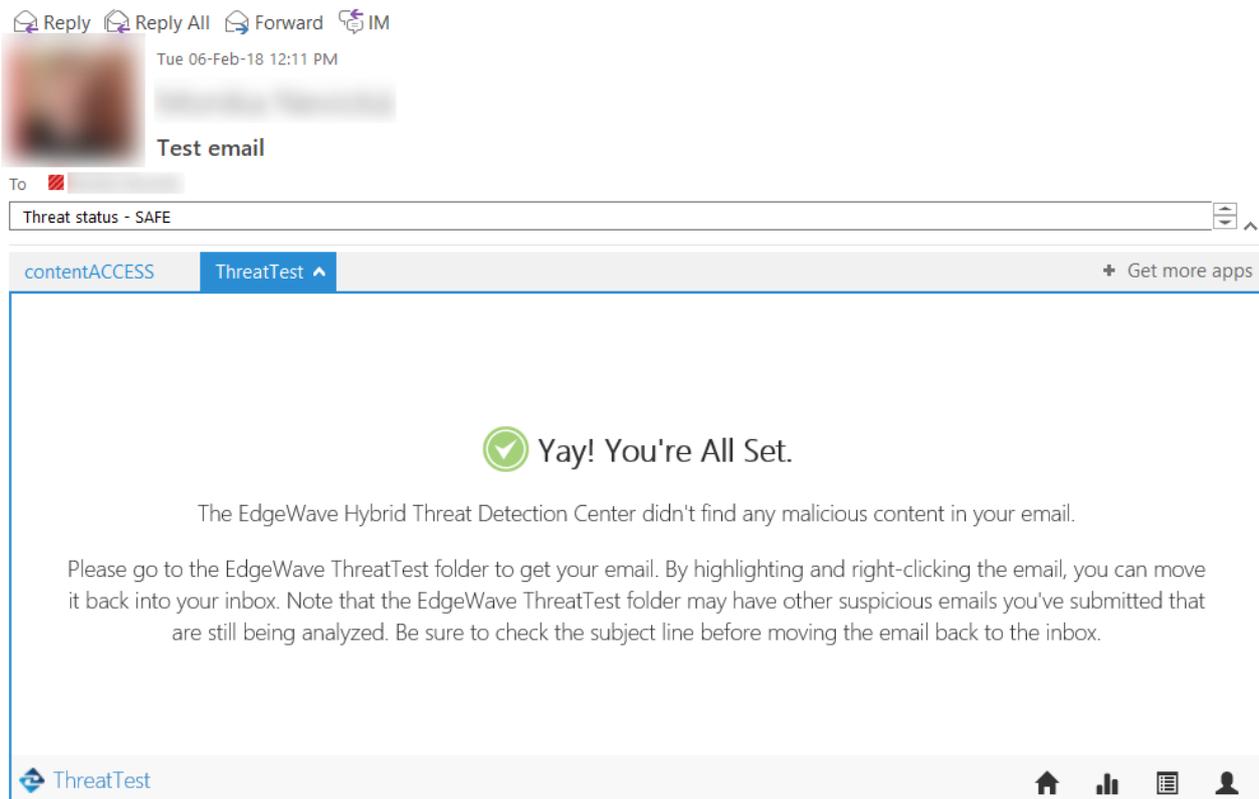
Safe – The mail was marked as safe by the Edgewave ThreatTestLab

Threat – The Edgewave ThreatTestLab found a malicious content in the email

Caution – The mail may contain some unsafe and harmful content, but doesn't have to be a threat

Invalid – When the email, which was reported, was a **forwarded** email and **not the original**

Unprocessed – The mail was marked as unprocessed by the Edgewave ThreatTestLab, but can be resubmitted again (even automatically, if configured in [ThreatTest job](#))



Screenshot: Email marked as safe; threat status category added



Reply Reply All Forward IM

Tue 06-Feb-18 1:40 PM

Testing email attachment

To [redacted]

Message 5 steps_122585617.jpg (434 KB)

contentACCESS
ThreatTest ^
+ Get more apps

You've Submitted.

Thank you for submitting your suspicious email.
 The EdgeWave Hybrid Threat Detection Center is processing it now and will get back to you shortly.
 While it's being analyzed, the email will be removed from your inbox and placed into the EdgeWave ThreatTest folder.

Submitted on 2/6/2018 2:06:39 PM. Waiting for result...

Status will be updated automatically

ThreatTest

🏠 📊 📄 👤

Screenshot: The email was submitted

2) Statistics

By clicking on this button, the statistics about your reported emails will appear. A graph can be seen on the **My statistics** tab. If you put your cursor on a part of the graph, a more detailed description will appear.

contentACCESS
ThreatTest ^
+ Get more apps

My Statistics
Reported emails

Pending
 Safe
 Threat
 Caution
 Failure

Your threat accuracy rate is 50%

ThreatTest

🏠 📊 📄 👤



A list of the reported emails and the count of all statuses can be seen on the **Reported emails** tab. The list has 4 columns (parameters):

Status: status assigned by the ThreatTestLab

Subject: subject of the reported email

Sender: sender of the reported email

Received: the day, when the reported email was received

Status	Subject	Sender	Received
▲ Virus	Virus test	[redacted]@tech-arrow.com>	2/6/2018 1:45:29 PM
▲ Unprocessed	Testing email attachment	[redacted]@tech-arrow.com>	2/6/2018 1:39:55 PM
▲ Spam	Claim your prize	[redacted]@tech-arrow.com>	2/6/2018 1:28:42 PM
✓ Safe	Test email	[redacted]@tech-arrow.com>	2/6/2018 12:10:51 PM

3) Show logs

By clicking on this button, the last logs of the application will open.

```

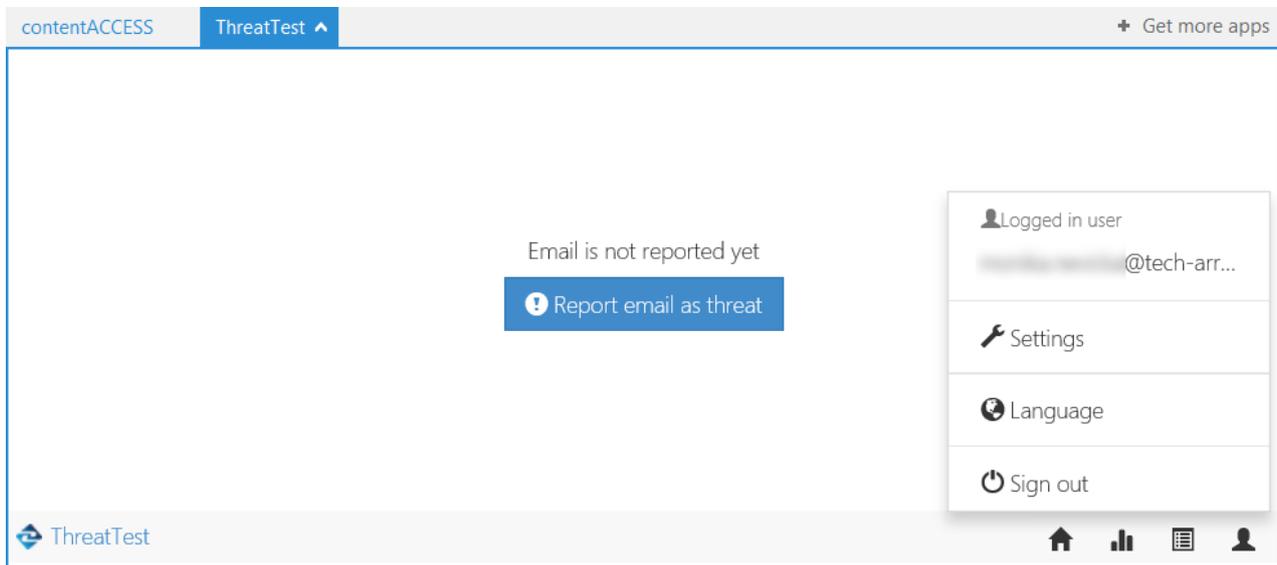
Logs from Tue Feb 06 2018 16:21:29 GMT+0100 (Central Europe Standard Time)

ThreatTest >> appContext.load >> AppContext load start.
ThreatTest >> configurationProvider.load >> Loaded settings from mailbox:
{"serverName":"[redacted]","currentLanguage":"en","modelId":"Merged[9]Custom[0]"}
ThreatTest >> MailboxItemContext.getItemBody >> Body from item: <html><head>

<meta http-equiv="Content-Style-Type" content="text/css">
<meta http-equiv="Expires" content="0">
<meta name="copyright" content="Copyright 2017, EdgeWave, Inc.">
<title>You've Submitted.</title>
<style type="text/css">
  body {
    background: #FFFFFF;
  }
    
```

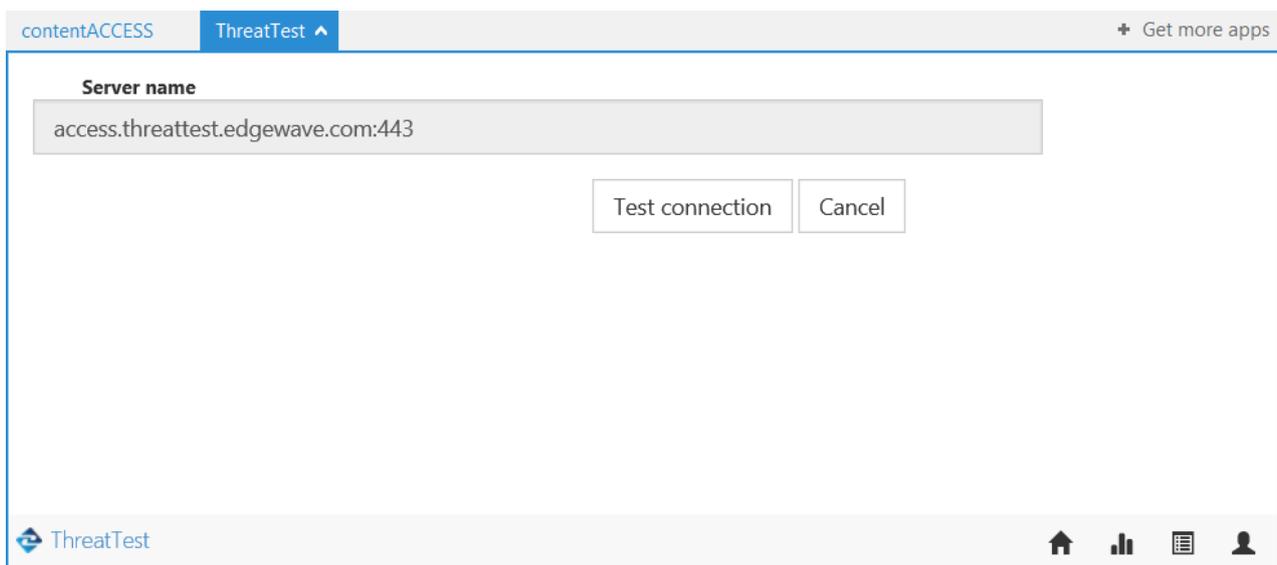
4) Menu

By clicking on this button, the following menu appears:



Logged in user: shows the user (mailbox) that is currently using the ThreatTest app

Settings: it is possible to view and test the connection to the server here (the connection that was set in the ThreatTest job, part Processing settings)



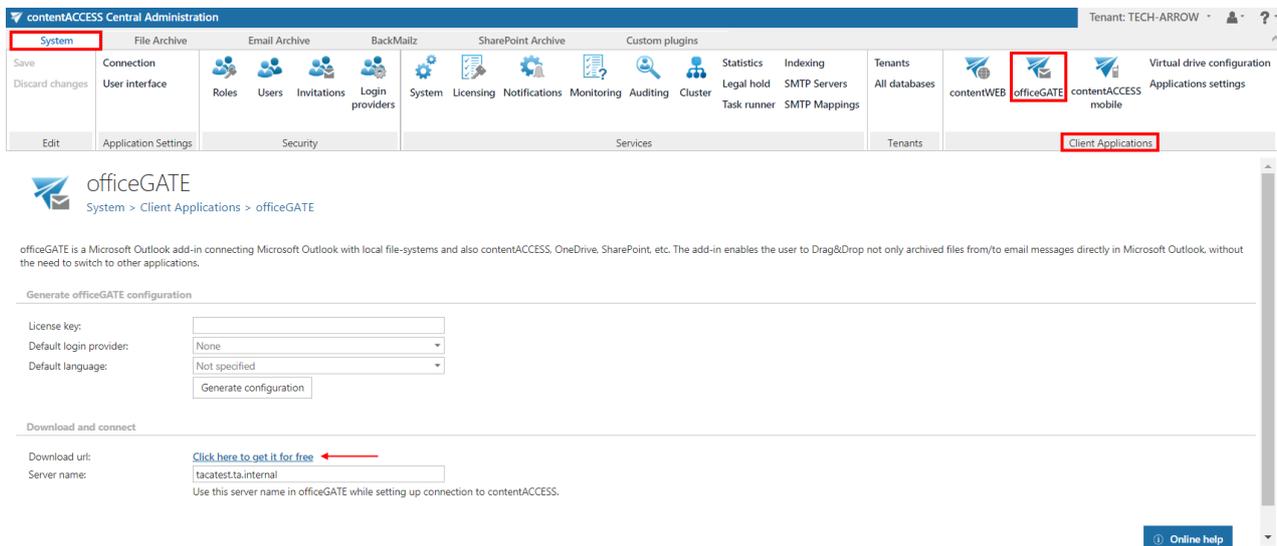
Language: the user can change the application language here (for now only English is available)

Sign out: signs out the currently logged in user (the user that is using the ThreatTest app)

officeGATE

officeGATE is an MS Outlook add-in connecting the email client with the local file-system and with SharePoint Online, contentACCESS, OneDrive, Dropbox, fileNshare and many other providers. With officeGATE it is not needed to switch to other applications when the user would like to access his files. It can be done directly from Outlook. The user can also easily access the archived documents in contentACCESS directly from here.

officeGATE can be downloaded for free from the respective page of contentACCESS Central Administration. Navigate to **System** → **Client applications** → **officeGATE** button on the ribbon and download a free version of officeGATE from the link.



The screenshot shows the contentACCESS Central Administration interface. The 'System' tab is selected in the ribbon, and the 'Client Applications' section is highlighted. The 'officeGATE' button is visible in the ribbon. Below the ribbon, the 'officeGATE' page is displayed, showing the 'Generate officeGATE configuration' section with fields for 'License key', 'Default login provider', and 'Default language'. A 'Generate configuration' button is present. The 'Download and connect' section shows a 'Download url' field with a link to 'Click here to get it for free' and a 'Server name' field with the value 'tacatest.ta.internal'. An 'Online help' button is located at the bottom right.

Installing officeGATE with Group policy (GPO)

officeGATE can be globally installed using Group policy. This simplifies the installation process of the product in a distributed company environment. Group policy installation of officeGATE is applied on 2 levels:

- 1. First the officeGATE XML files are distributed** to each user in the domain. This XML file contains the global configurations of officeGATE listed below.

This XML file containing global officeGATE settings is generated on the **officeGATE** page of Central Administration. The following global settings are specified:



License key – enter here the officeGATE license key

Default login provider – select the desired login method that should be applied when establishing connection between officeGATE and contentACCESS

Default language – select here the default language of the application. If a language is not specified here, then the language of MS Outlook will be automatically used.

Click **Generate configuration** and save the distributable XML file.

officeGATE
System > Client Applications > officeGATE

Generate officeGATE configuration

License key:

Default login provider:

Default language:

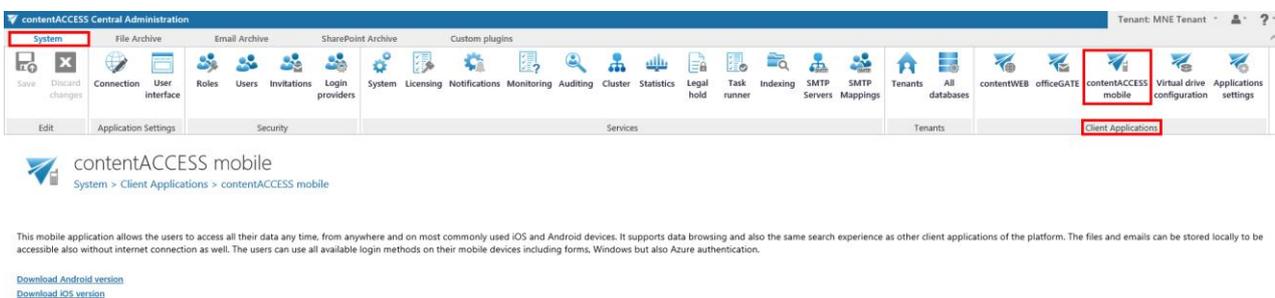
2. Further the **officeGATE setups are distributed** for each domain user and the product is automatically installed.

For more information about the XML distribution and installation using Group policy check [this](#) guide.

contentACCESS Mobile

contentACCESS Mobile is a native mobile device application over which the user can easily access his archived documents from contentACCESS. Offline access is also ensured for read-only use.

The contentACCESS mobile application can be downloaded on a mobile device (either Android or iOS) from contentACCESS Central Administration (**System** tab → **Client applications** → **contentACCESS Mobile**). You can also search for contentACCESS Mobile in Play store or Apple store to install the app on your mobile device.



Once the user has successfully downloaded the application on the mobile device and opens the application, he will be asked to type in the server name (connection URL) and his login credentials.

Note: For more information about contentACCESS Mobile, please check [this](#) documentation.



Virtual drive configurations

What is a virtual drive? It is a virtual file system that presents/virtualizes any data (files and folders of an actual disk) to the end-user. Virtual drive is a non-existing drive that does not physically exist in the computer, but it contains the exact structure of the items that have been processed by contentACCESS.

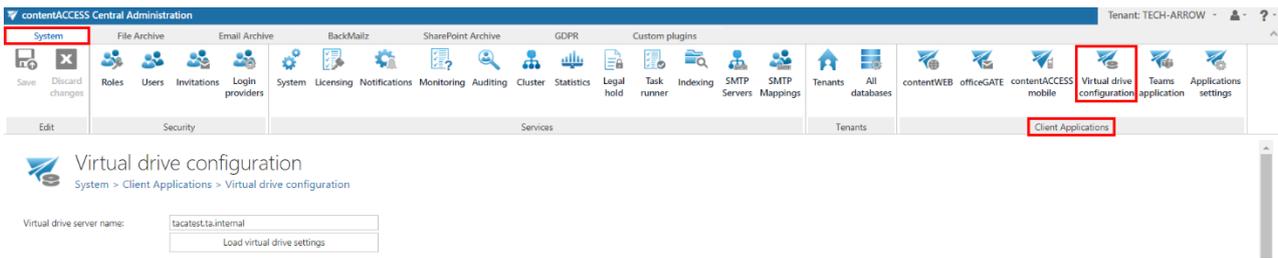
The contentACCESS Virtual Drive was developed by TECH-ARROW and serves as a key access point between the end user and the contentACCESS File Archive. Virtual Drive is a must-to application for user who has **File system Archive** and would like to use shortcutting. The user can view his archived files from here and if he has write access on the file(s), he can make changes to the file(s) – by simply opening, editing and saving with the associated application. The **Virtual drive** will detect the change and create a new version from the file(s) after a short delay (about 30 seconds).

By default, only the active items can be viewed on the virtual drive (active items = items in the archive, which have an original file or shortcut in the file system, too). To enable inactive view, the **Show inactive items** checkbox must be selected on the Virtual drive configuration page. This drive can be also shared with other users, so they can easily browse for their associated archived files in case of need. The original folder/ item permissions are also applied for the files/ folders in virtual drive. A user can access only the items on which he has access permissions in the original file system.

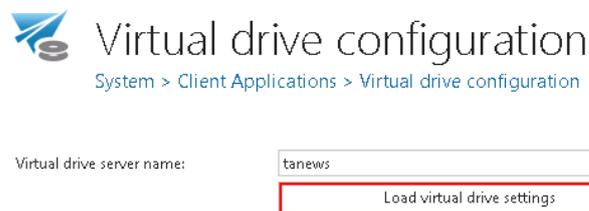
Note: If the shortcut pointing to the archive file is opened and edited through the Virtual drive, it must be saved back to the original file location. For more information refer to section [Editing of already archived files, file versions in File system archive](#).

After the Virtual drive was installed (link to the Virtual drive setup is accessible in the Tools of the contentACCESS setup package), it is necessary to configure its settings on the Virtual drive configuration page.

In contentACCESS Central Administration navigate to **System** tab → **Client Applications** → **Virtual drive configuration** control to open this page:



Enter the server name - where virtual drive (henceforth “VD”) is installed – into the **Virtual drive server name** textbox. To load the actual settings of VD, click **Load virtual drive settings** button.



contentACCESS server connection

It is possible to connect the Virtual drive to contentACCESS through **net.pipe** connection, through the **contentACCESS proxy** with a secure (**HTTPS**) or insecure (**HTTP**) connection, or **directly**, over HTTP connection.

The **net.pipe** communication is the fastest way of the communication between the Virtual drive and contentACCESS as it is using shared memory for the communication. The disadvantage is that this type is possible only if the Virtual drive and contentACCESS server are both installed on the same machine. In such cases this is the recommended communication type.

The connection through the **proxy** is recommended, if the virtual drive is installed somewhere in the cloud or on a server that differs from the contentACCESS server. It is recommended to use a direct connection (without using the proxy), if the virtual drive and contentACCESS are installed on the same server.



Virtual drive configuration

System > Client Applications > Virtual drive configuration

Virtual drive server name:

contentACCESS server connection

contentACCESS server name: :// :

Use windows authentication (using 'NT AUTHORITY\SYSTEM')

contentACCESS user:

contentACCESS password:

Model types to show:

Virtual drive settings

Root mount point:

Share for:

Show inactive items:

Download locally:

Folder refresh interval (s):

Download cache:

Permanent cache:

Cache size limit (MB):

Cache recalculation interval (ms):

Timeout:

Read-only mode:

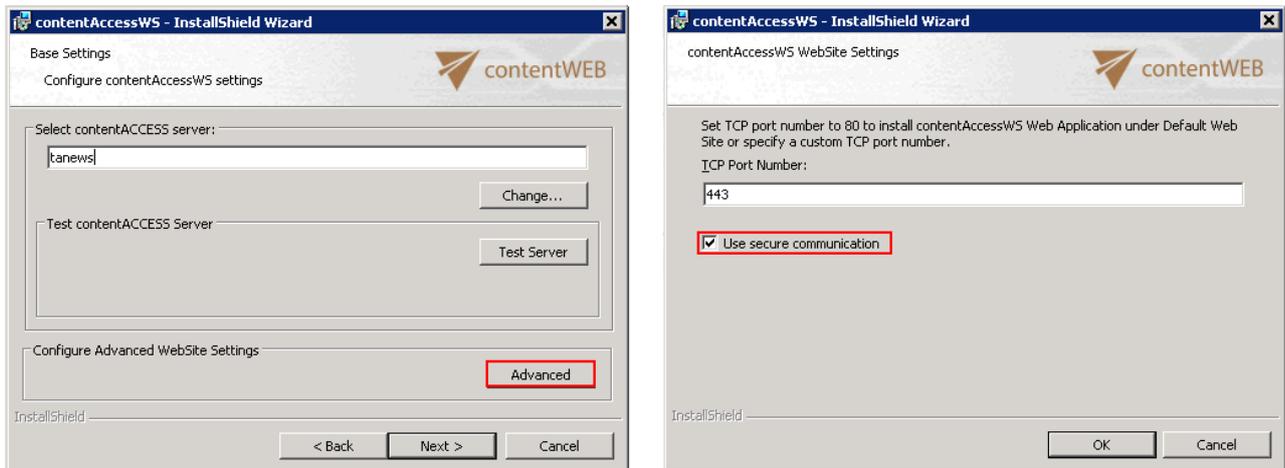
Debug:

Virtual drive management

Virtual drive status: Started

➤ Virtual drive configurations, if secure communication should be used (over the proxy):

The proxy must be installed over HTTPS connection (HTTPS connection must be selected during the installation process of the proxy);



In Central Administration, on the **Virtual drive configuration** page: The connection of the Virtual drive to contentACCESS must be established over a HTTPS connection; port 443 must be entered into the connection URL.

contentACCESS server connection

contentACCESS server name: :

➤ **Virtual drive configurations, if the virtual drive will connect to the contentACCESS server directly:**

In Central Administration, on the **Virtual drive configuration** page: If having a direct connection, select HTTP connection when specifying the contentACCESS server name URL. The virtual drive and contentACCESS are installed on the same server, so the "localhost" URL can be configured. Enter 8736 for the port number.

contentACCESS server connection

contentACCESS server name: :

➤ **Virtual drive configurations using net.pipe for communication, if Virtual drive and contentACCESS are installed on the same machine:**

contentACCESS server connection

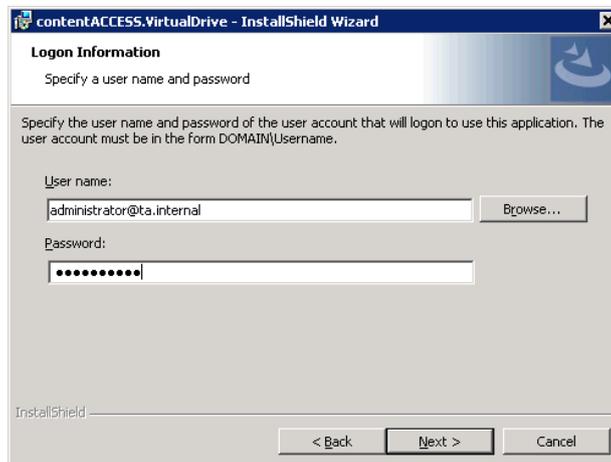
contentACCESS server name: :

In the next steps it is required to specify the user, over which VD will connect to contentACCESS.

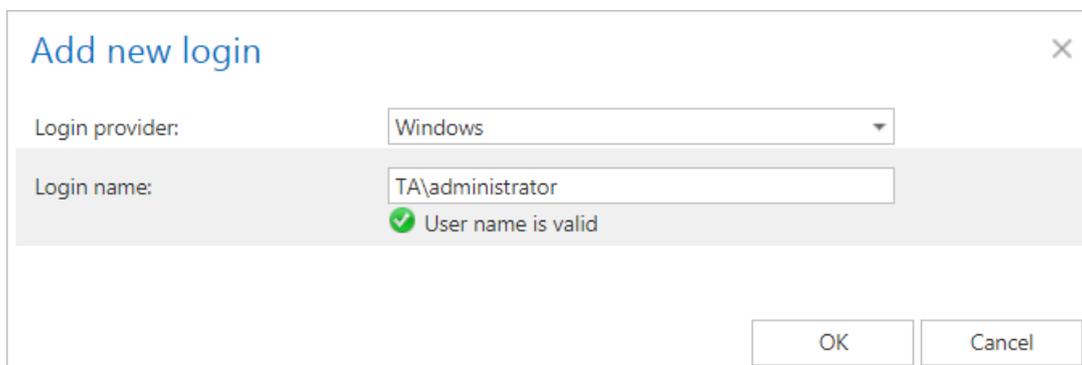
To establish the connection with the contentACCESS server, the system user, or a Windows user can be used. The Virtual drive will connect to contentACCESS over these credentials. By default, the contentACCESS system user is used to this connection. If you do not want to change these connection settings, leave the

“Use Windows authentication checkbox” unchecked. To enable the connection with Windows account the following steps must be performed:

- When installing the Virtual drive, the Windows user credentials should be specified. This VD service (GATE.contentAccess.VirtualDrive.Service) user will be taken to log in to contentACCESS.



- In contentACCESS, the corresponding Windows user login needs to be created (under System → Security → Users...double click on the user...add Windows user login in the User logins section...fill required fields in the **Add new login** dialog).



- On the configuration page of virtual drive, the “Use Windows authentication” checkbox must be selected:

Use windows authentication (using the service user 'TA\Administrator')

contentACCESS user:

contentACCESS password:

The main advantage of a Windows user is: if the system user credentials are changed by the user and he forgot to change it in the Virtual drive settings, Virtual drive will be disabled to connect to contentACCESS. If a Windows user is used, such problems can be avoided.

To finalize the VD configuration continue with configuring the following settings. Some of them are set by default, these can be left as they are:



Virtual drive settings

Root mount point:	<input type="text" value="G:"/>
Share for:	<input type="text" value="Domain Users"/>
Show inactive items:	<input type="checkbox"/>
Download locally:	<input checked="" type="checkbox"/>
Folder refresh interval (s):	<input type="text" value="10"/>
Download cache:	<input type="text" value="C:\Windows\TEMP\contentACCESS.VirtualDrive"/>
Permanent cache:	<input type="text" value="C:\Windows\TEMP\contentACCESS.VirtualDrive.Writ"/>
Cache size limit (MB):	<input type="text" value="1"/>
Cache recalculation interval (ms):	<input type="text" value="10000"/>
Timeout:	<input type="text" value="0"/>
Read-only mode:	<input type="checkbox"/>
Debug:	<input type="checkbox"/>

Virtual drive management

Virtual drive status:	Started
	<input type="button" value="Start virtual drive"/> <input type="button" value="Stop virtual drive"/>

Root mount point: Here you can choose an available disk for the Virtual drive. By default it is disk "G", but it is possible to change it.

Share for: The Virtual drive will be shared for this Active directory group only. It is recommended to specify a domain group that contains all the users who should have access to the Virtual drive. Usually, it is "Domain Users" or "Everyone".

Show inactive items: the user may set here whether he wants to see the inactive items (items in the archive, which do not have an original or shortcut in the file system) in the virtual drive, or not. In default view only the active items are shown.

Download locally: contentACCESS data can be stored a) as files in the cache, or b) as content in the memory. If you check option "Download locally", then files will be stored in the cache.

Folder refresh interval(s): The virtual drive folder will be refreshed in time intervals that are set here. During these intervals the newly archived files will become visible in the virtual drive folder.

Download cache: Virtual drive will save temporary files to this folder.

Permanent cache: Virtual drive will save all changes to this folder. When users are editing files, all changes are stored here until they are committed to the archive. This folder must have plenty of free space.

Note: The **Permanent cache** is used to hold the changes until the file is closed or after x seconds of inactivity. After the version is created in the archive, the file is removed from the **Permanent cache**.

It is also recommended to set different folders for the **Download cache** and the **Permanent cache** (can be on the same disk, but different folder).



Cache size limit (MB): When opening the archived data, the processed data are cached to unburden Virtual drive from unnecessary operations and to shorten access time to this data. This function helps to unburden the VD server. Here we can define the maximum size of data, which will be downloaded and stored by the Virtual drive. In our case we set this limit to 1 MB.

Cache recalculation interval (ms): The time set here will define the intervals when the cache will be “cleaned”. At the intervals that are set here, the cache will check if the cache size limit has not been exceeded.

Timeout: The duration of running of all operations can be determined here. After this time period, the operation will be interrupted. Value “0” means that the operation will be waiting infinitely.

Read-only mode: If virtual drive is in read-only mode, the files can't be edited and no new versions are created from them. After this setting is changed and saved, the **Virtual drive** needs to be restarted.

Debug: If you check this textbox, then all errors and warnings that have been noticed will be written into the .log file or into the debug view. It is recommended to turn on this function only if the user notices some problems with running of virtual drive, otherwise these notifications might slow down the operations.

Virtual drive status: This will show the current state of the virtual drive. With the buttons below you can start/stop the virtual drive. To connect to the G drive and start the virtual drive, click on **Start virtual drive**.

Do not forget to save the configuration.

Teams application

contentACCESS Teams application allows the contentACCESS users to search in their archive directly from MS Teams and share the result(s) with a team or with a chat partner without the need to switch to other applications.

The Teams application can be downloaded from contentACCESS Central Administration (**System** tab → **Client applications** → **Teams application**).



contentACCESS Central Administration Tenant: EA_Test

System | File Archive | Email Archive | SharePoint Archive | GDPR | Teams Archive | Custom plugins

Save | Roles | Users | Invitations | Login providers | System | Licensing | Notifications | Cluster | Statistics | Legal hold | Task runner | Indexing | SMTP Servers | SMTP Mappings | Sharing job | Sharing settings | System logs | Configuration auditing | Archive auditing | Tenants | All databases | contentWEB | officeGATE | contentACCESS mobile | Virtual drive configuration | **Client Applications** | Applications settings

Teams application
System > Client Applications > Teams application

contentACCESS Teams application will allow contentACCESS users to search in their archive using Teams and share the result with a team or with a chat partner without the need to switch to other applications. To be able to use the application you need fill out the form below and then register your tenant.

Client application settings

Application (client) ID:

Directory (tenant) ID:

Client secret:

Permission type:

SharePoint access:

SharePoint application ID:

Certificate file:

Certificate info:
Common name: CN:TechArrow
Expiration date: 5/1/2022 2:00:00 AM

Certificate password:

Register your tenant for contentACCESS Teams application

Registration status: Registered with 72c702e- application ID.

Download and install contentACCESS Teams application

Installation package:

Installation steps:

1. Download the application installation package using the button above.
2. In Teams, click on the 'Apps' button which is located bottom left in Teams window.
3. Click on 'Upload a custom app' (last item in the list).
4. Here you should select to install the application for your company.
5. Browse to the downloaded application installation package zip file and select it.
6. This will add the application to the company's application catalog, the catalog will be opened by default.
7. Click on the application in the catalog and install it for yourself by clicking on the 'Add' button.
8. Start typing '@contentACCESS' in any chat and have the benefit of accessing your archive directly inside Teams.

After the above steps are done, your co-workers can install the application in the following way:

1. In Teams, click on the 'Apps' button which is located bottom left in Teams window.
2. Click on 'Built for YOUR COMPANY NAME' - this opens the company's application catalog.
3. Click on the application in the catalog and install it for yourself by clicking on the 'Add' button.

You can find the user manual for the application here: [Teams application user manual](#)

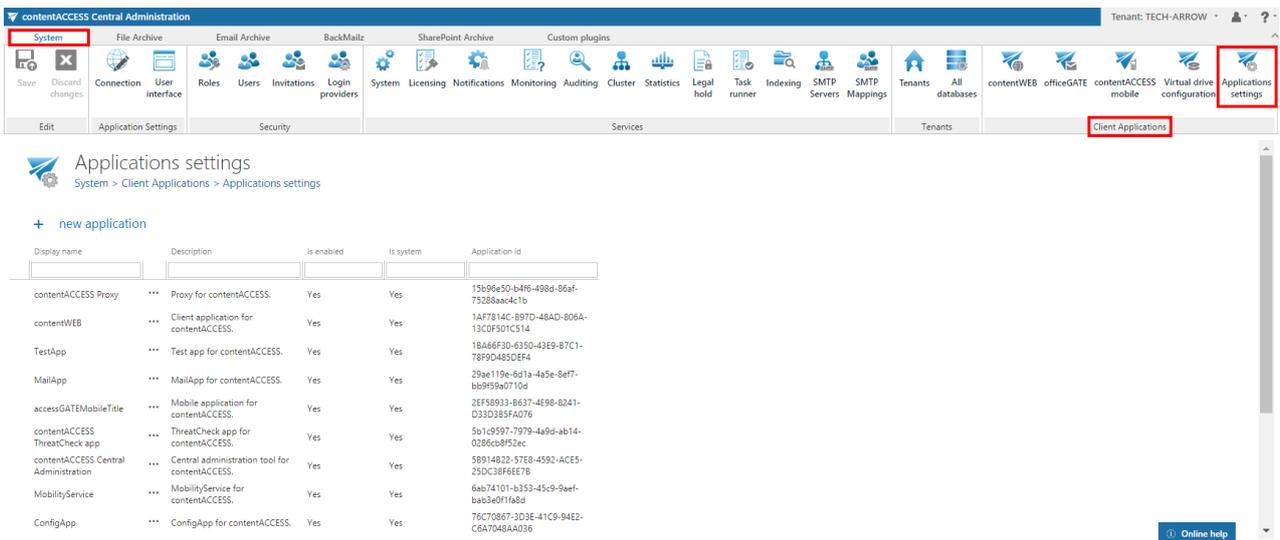
[Online help](#)

More information about the download and installation process can be found in [this](#) guide.



Application settings

The list of the contentACCESS client applications is available for the system and/or tenant administrator on the **Application settings** page (**System** tab → **Client applications** group → **Application settings** button).



The settings of the client applications listed on this page can be managed using the given application's context menu options:

Applications settings

System > Client Applications > Applications settings

+ new application

Display Name	Description	Is Enabled	Is System	App Id
Content Web	Client application for contentACCESS.	No	Yes	1AF7814C-B97D-48AD-806A-13C0F501C514
accessGateMobile	Mobile application for contentACCESS.	Yes	Yes	2EF58933-B637-4E98-8241-D33D3B5FA076
Central Administration	Central administration tool for contentACCESS.	Yes	Yes	5B914B22-57E8-4592-ACE5-25DC38F6EE7B
OfficeGate	OfficeGate for contentACCESS.	Yes	Yes	A0AD6FDC-4F18-463F-AB18-155F4BD0346D
contentAccess ShareApp	ShareApp ShareApp for contentACCESS.	Yes	Yes	B987D616-5E5C-4C25-B878-EF8F66828389
Central Login	Central login page for contentACCESS.	Yes	Yes	bb484a32-5bc6-4b83-8589-d951c5aa2c5c

The context menu options allow to:

- **Delete** the application – applications with “Is system” flag cannot be deleted.



It is also possible to add new applications using the “+ new application” button on the same page. By clicking the option, the “Add new application” dialog opens. Fill the fields, generate application credentials and add it to the list.

Add new application ×

Application

Display name:*

Application url:

Redirect url:

Name:*

Description:*

Enabled:

Application credentials

Application id: e8b97dc8-758d-4995-b566-c3e5154171aa

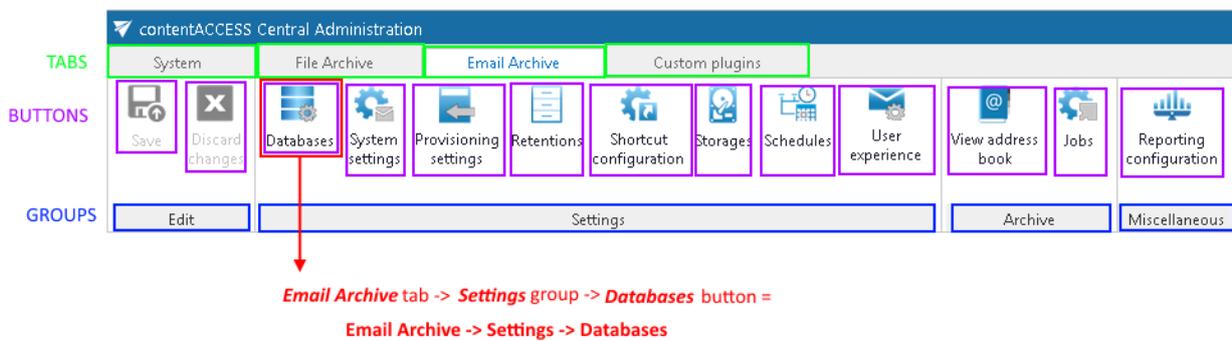
Application secret:

Terms of use

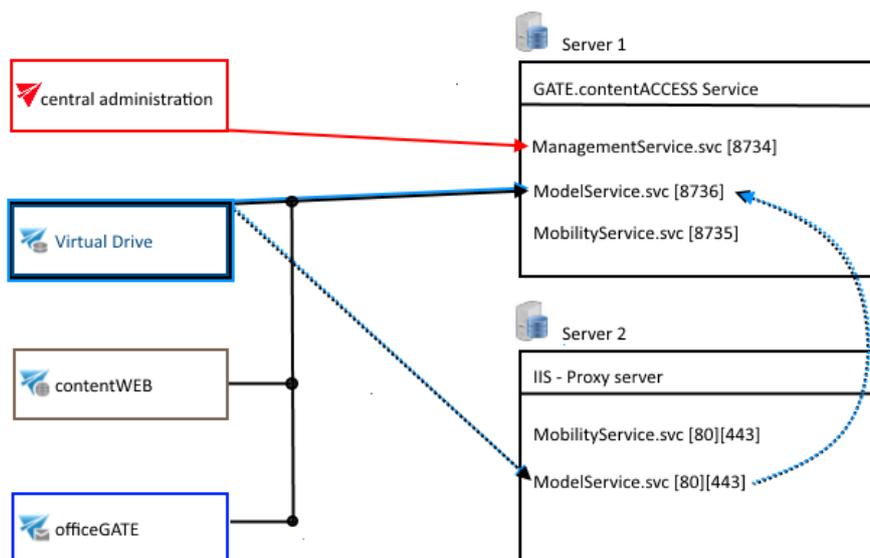
Definition of terms:

TAB, GROUP, BUTTON

contentACCESS Central Administration user interface is divided into tabs, groups and buttons. Each tab contains several groups, which also contain several buttons. When the reader of the manual encounters a path containing 3 levels, e.g. **Email Archive** → **Settings** → **Databases**, then this path will navigate the user through the following levels: **TAB** → **GROUP** → **BUTTON**.



Schema of services used by the products of TECH-ARROW





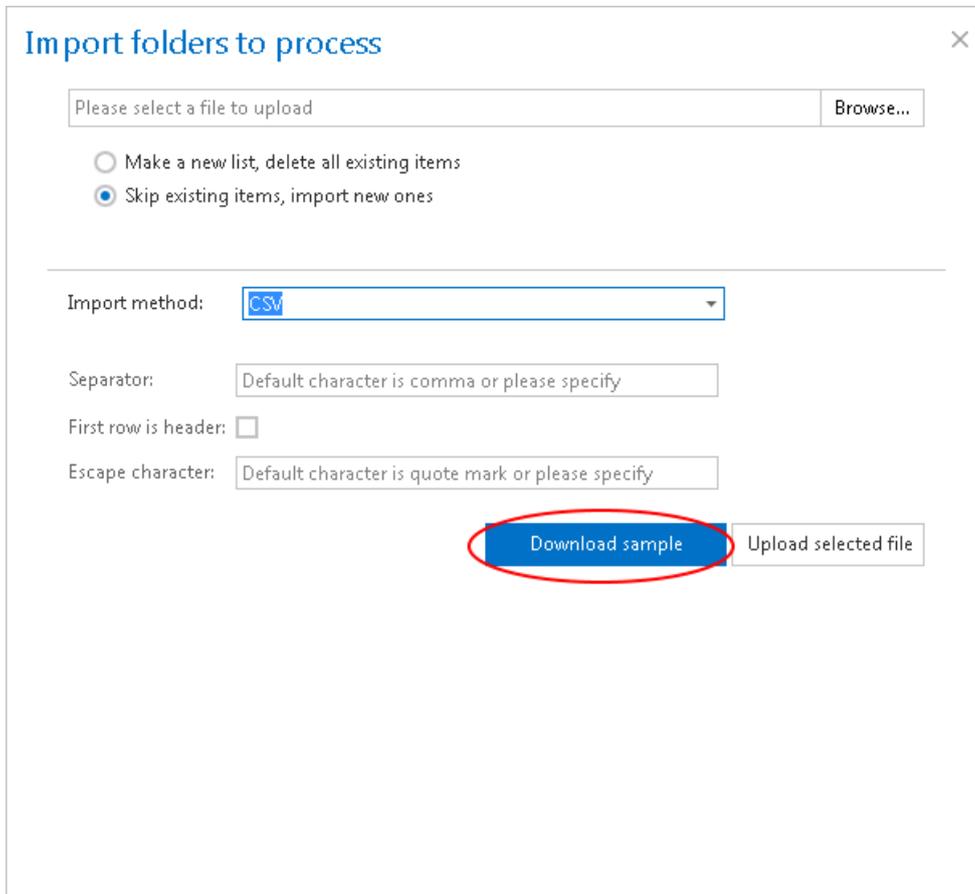
FAQ

If you have any problems with configuring the system, the following chapters may help you to solve the problems:

- [Download sample for the file to be imported does not work](#)
- [Archiving is not working, if MAPI is set to communicate with the Exchange server](#)
- [Virtual drive is still appearing after the uninstall](#)
- [Outlook forms problems](#)
- [Unable to open shortcuts of archived file on the server side](#)
- [Samples are not shown using "Show sample" option in the Import dialog](#)
- [Do I need to create separate tenants for file archiving and email archiving](#)
- [What is the recommended database size for email, file and SharePoint archiving](#)
- [The TEMP folder is running out of space when archiving big files](#)
- [The attachment could not be opened](#)
- [After updating Exchange 2013, the EWS connection might not work in contentACCESS](#)
- [If Windows authentication is not working in contentACCESS and an alias was created for contentACCESS](#)
- [contentACCESS Outlook add-in certificate issue](#)
- [PowerShell scripts for setting up Email archive](#)
- [Solution for Outlook security patches](#)
- [Solution for Outlook security patches through GPO](#)
- [Solution for indexing PDF files](#)
- [O365 SuperUser mailbox configuration](#)
- [Office365 journaling](#)
- [Organizational forms](#)
- [Multifactor authentication](#)
- [Region setting](#)
- [contentACCESS Mail app installation issue](#)
- [Azure app registration](#)

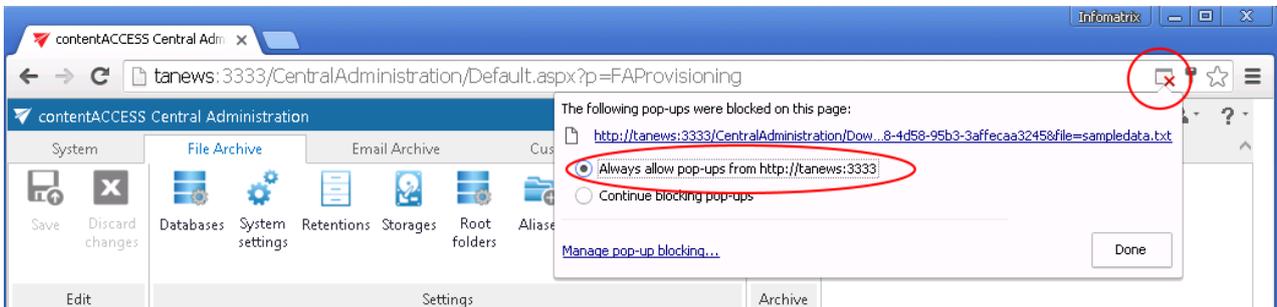
Download sample for the file to be imported does not work PROBLEM

The sample file for the file to be imported into contentACCESS cannot be downloaded:



SOLUTION

Pop-ups must be allowed in your browser.





Archiving is not working if MAPI is set to communicate with the Exchange server

PROBLEM

When using option “Use MAPI to communicate with Exchange Server”, the archiving does not work. Errors like this are present in the logs:

“Exception 80040111 (null) Failed to connect to admin mailbox. >> Exception 80040111 Failed to open default message store. 80040111 MAPI_E_LOGON_FAILED.”

SOLUTION

What should you do:

- log on to Windows with the service account (superuser)
- start Outlook with the service account
- check CGMAPIConnector service identity – it must be the service account
- start CGMAPIConnector – is it starting without error?

Try to run the job again. The profile with the following template should be created: `_<SERVERNAME>`. This corresponds to the name of the Exchange Server as seen in the address book.

If the profile is not created automatically, it means that contentACCESS is not able to log on with the superuser at all. In this case, it is necessary to create the profile manually:

- find your mailbox in address book
- find the Exchange server to which the mailbox belongs (Example: “TECHEX2K10”)
- log on with superuser to Windows and create a new Outlook profile
- name the profile: `_TECHEX2K10`
- configure the profile with the superuser as the primary mailbox
- turn off cached mode
- start Outlook with the profile
- close Outlook

If it works, restart the CGMAPIConnector service and start the job again.

Now it should reuse the existing profile. The profile is not deleted by contentACCESS. You need to repeat these steps for each Exchange Server in your address book.



Virtual drive is still appearing after the uninstall

PROBLEM

Virtual drive is still appearing even though it has been uninstalled.

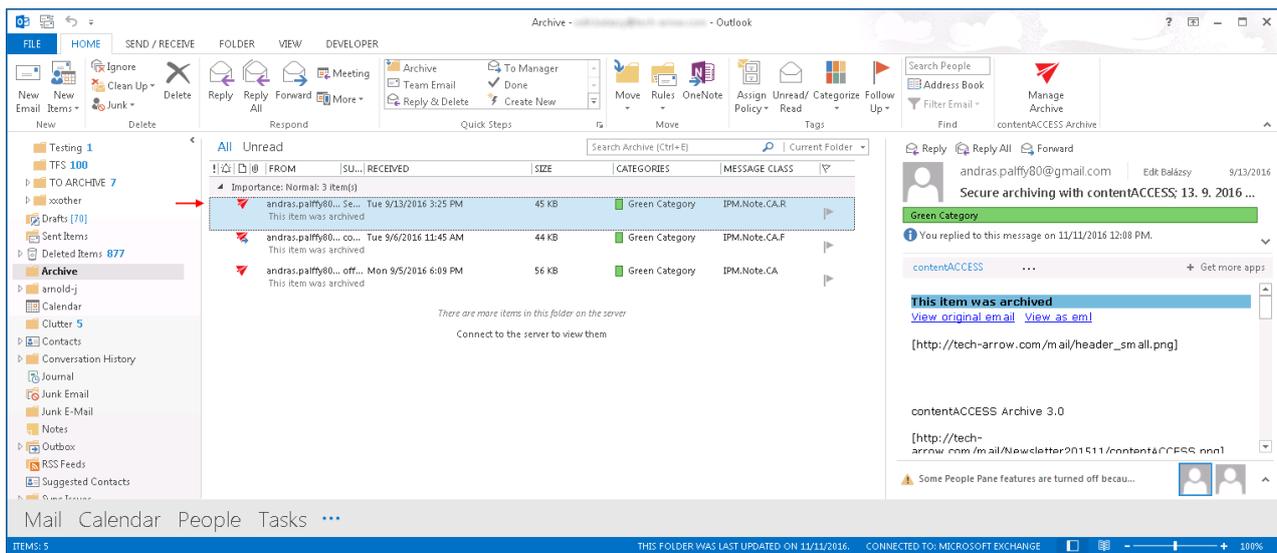
SOLUTION

Windows system needs to be restarted.

Outlook forms problems

PROBLEM 1:

Incorrect icons are appearing on the archived email messages in MS Outlook. E.g. if the message is replied, the standard icon (✉) is displayed (the right should be this: 📧)



SOLUTION 1:

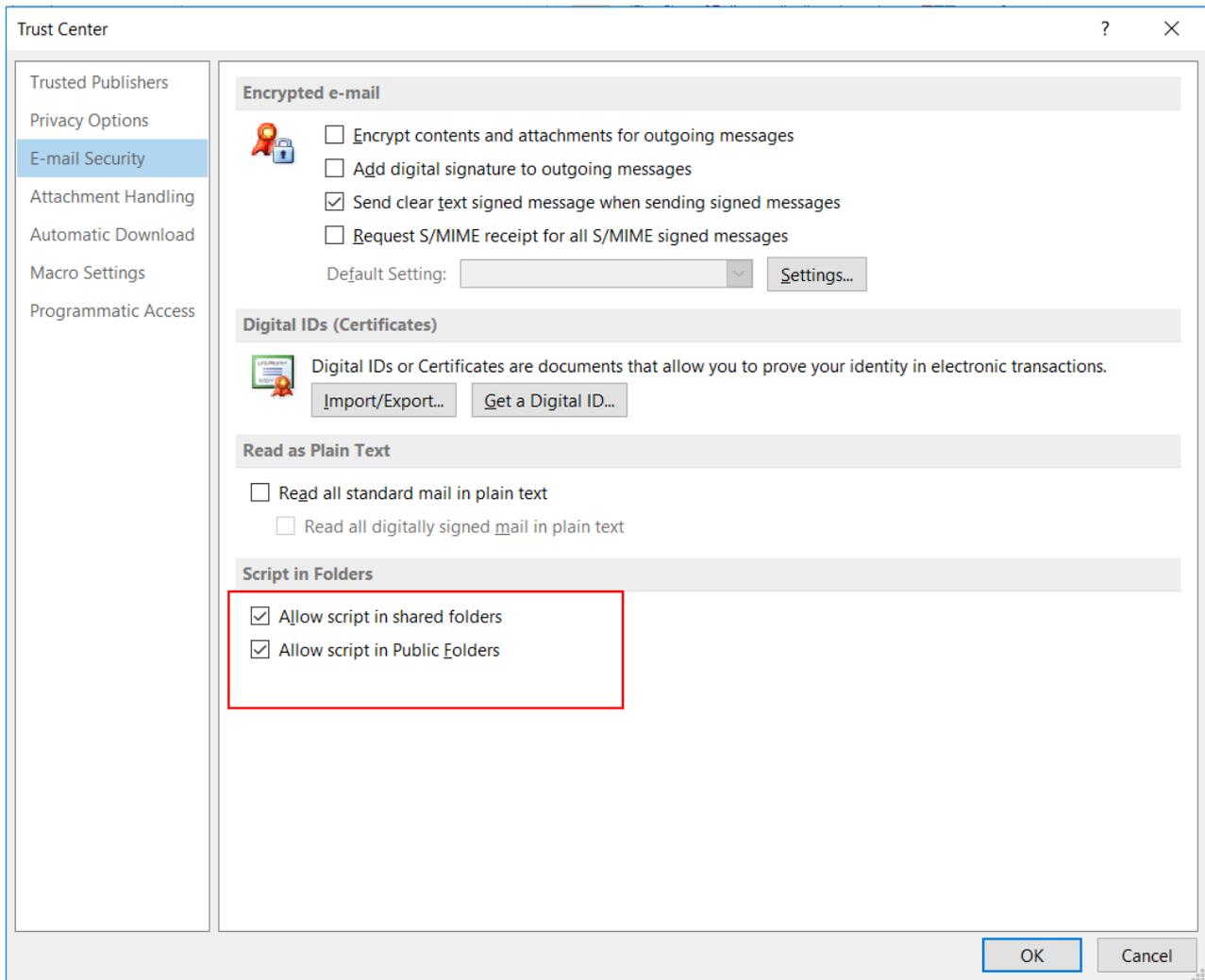
Clean up the Outlook cache. (For more info about how to clean the cache refer to this link: <http://www.slipstick.com/developer/custom-form/clean-outlooks-forms-cache.>)

PROBLEM 2:

Outlook forms are not working with shared folders and/or public folders.

SOLUTION 2:

If the Outlook forms are not working with shared folders and/or Public Folders, allow these scripts in the **Trust center** of MS Outlook. These settings are available in File → Options → Trust center → Trust center settings → Email security: options “Allow script in shared folders”; “Allow script in Public Folders”.

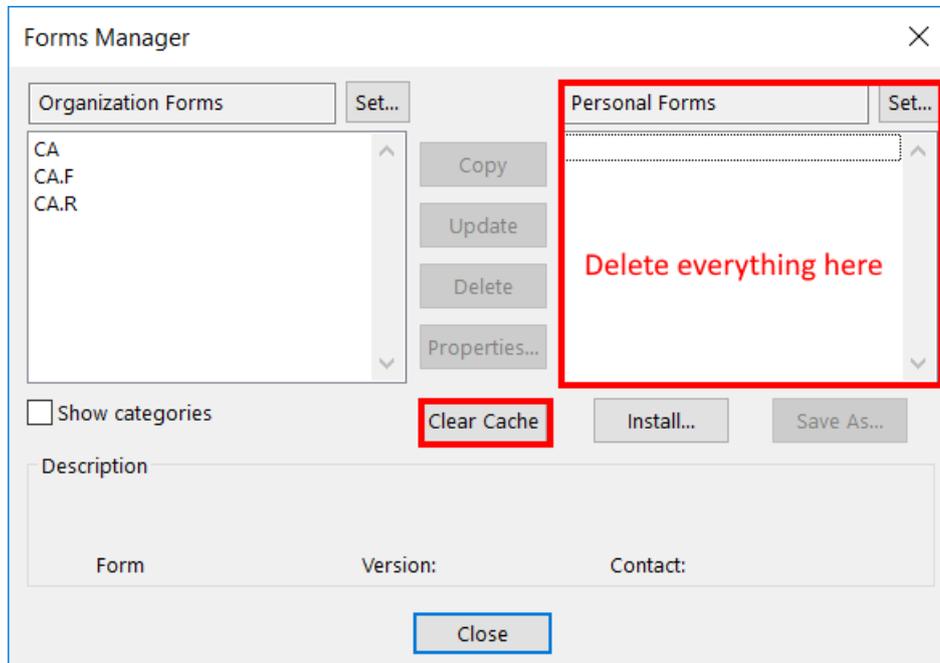


PROBLEM 2B:

Outlook forms are under both **Personal forms** and **Organization forms**. Personal forms could contain older version of Outlook forms and this could interfere with the newer forms under Organization forms.

SOLUTION 2B:

Delete the forms that are under **Personal forms** and clear the cache.



PROBLEM 3:

If Microsoft Outlook was installed on a Windows terminal server, then the VBScript support is not installed by default.

SOLUTION 3:

Please follow the steps described in the [Microsoft Knowledge Base article](#) to solve the problem.

PROBLEM 4:

After installing the security updates for Outlook, emails that were archived by third-party application are showing an unwanted behavior. All programs and applications using custom Outlook forms are affected.

SOLUTION 4:

Check out our FAQ sections, where two possible solutions are explained:



- [Solution for Outlook security patches](#)
- [Solution for Outlook security patches through GPO](#)

Unable to open shortcuts of archived files on the server side

PROBLEM:

It is not possible to open Shares with Alias names on the server.

SOLUTION:

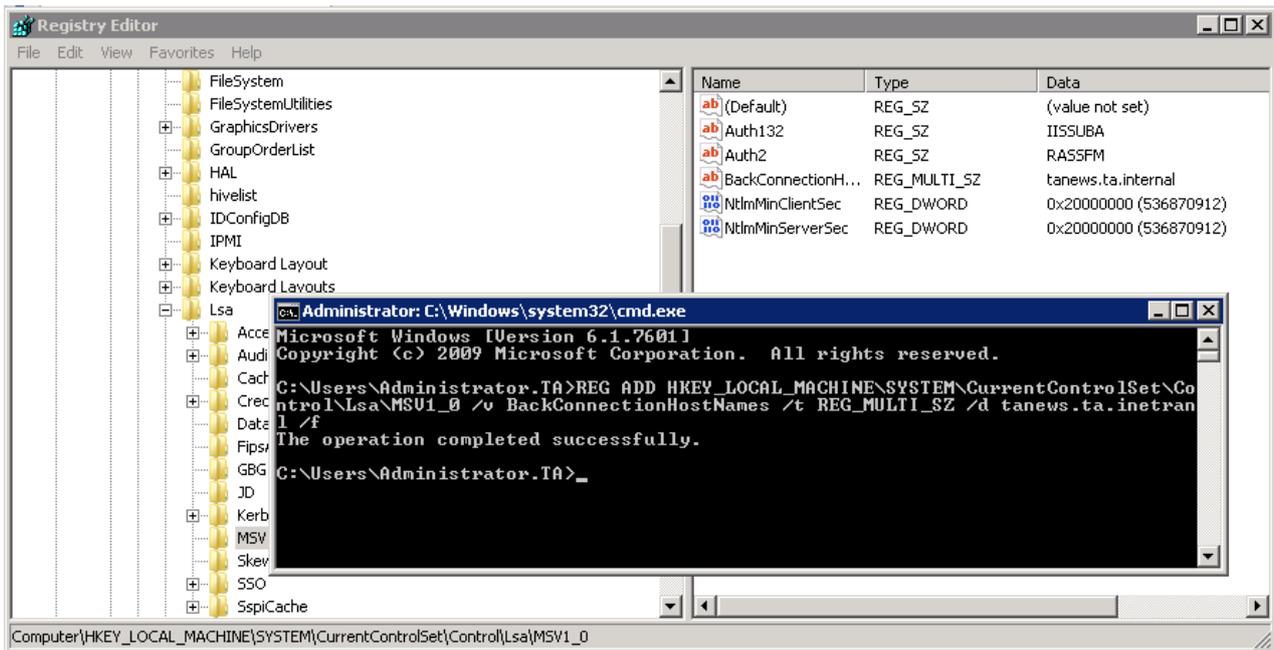
We needed to set at least the Registry key. Steps to follow:

- open cmd prompt as administrator
- type here

```
REG ADD HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\MSV1_0 /v  
BackConnectionHostNames /t REG_MULTI_SZ /d [MycontentACCESSServerName.domain.com] /f
```

and click Enter

- the Registry key will be written to the Registry editor
- restart your system



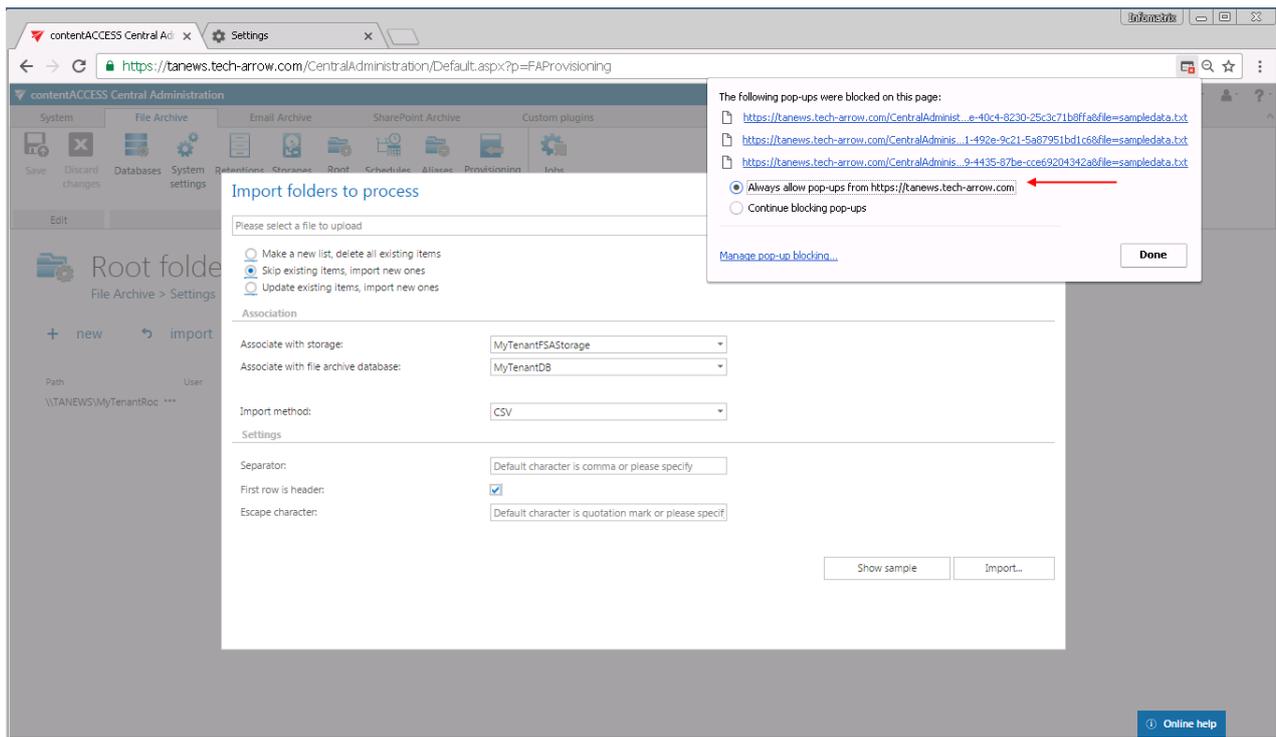
Samples are not shown using "Show sample" option in the import dialog

PROBLEM:

"Show sample" is not working in the **Import** dialog

SOLUTION:

Verify in your browser if the pop-ups are blocked...if blocked → allow pop-ups:



Do I need to create separate tenants for File archiving and Email archiving?

PROBLEM: Do I need a separate tenant for file archiving and a separate tenant for email archiving?

SOLUTION: It is not a must to create separate tenants for email and file archiving. You can just simply create separate databases – one for file archiving and second for email archiving. The recommended database count depends on the archivable mailbox count (in case of email archiving) / archivable root count (in case of file archiving). For more information about the database-size recommendations refer to section **“What is the recommended database size for email, file and SharePoint archiving.”**

What is the recommended database size for Email, File and SharePoint archiving

The recommended database size for email, file and SharePoint archiving depends on the size of the organization. Up to 1000 mailboxes (email archiving), 1 (max. 2) root folders with up to 60 million files (file archiving), 1 (max. 2) root connections with up to 60 million items (SharePoint archiving) the organization is considered as small-and medium sized company. If the numbers are over these limits, the company is



large sized. If emails, files and SharePoint contents are all archived within your organization, the structure and size of the databases to be created should be as follows:

- 1) Regardless of the size of your company, first create a database for the system (known as "contentACCESSDB").
- 2) Considering the size of your company, create the following archive databases:
 - a) **Medium and small customers: <1000 mailboxes (email archive) and/or <60 million files (file archive, SharePoint archive)**
 - Create a separate database for **email archiving** (EA system + email contents)
 - Create a separate database for **file archiving** (FS system + file contents)
 - Create a separate database for **SharePoint archiving** (SP system + SP contents).
 - b) **Medium and large customers: >1000 mailboxes (email archive) and/or >60 million files (file archive, SharePoint archive)**
 - Create a database for the **email archive system** (MailArchive)
 - Split mailboxes to groups (per 1000 or 2000 mailboxes per group) and **create separate databases for each group** (MailArchive01, MailArchive02). These databases will be then assigned to groups (you can do it in address book or within the archive jobs) and the archived emails will be put into these databases.
 - Create a database for the **file archive system** (FileArchive).
 - Create file archive databases (FileArchive01, FileArchive02) and **split the root folders to these individual databases (1 root folder per 1 database recommended)**. The databases are assigned to root folders in the **Root folders** settings (**File Archive** tab → **Settings** group → **Root folders** option on the Central Administration ribbon). The archived root contents will be put into these databases.
 - Create a database for the **SharePoint archive system** (SPArchive).
 - Create SharePoint archive databases (SPArchive01, SPSArchive02) and **split the root connections to these individual databases (1 root connection per 1 database recommended)**. The databases are assigned to root connections in the **Root connections** settings (**SharePoint Archive** tab → **Settings** group → **Root connections** option on the Central Administration ribbon). The archived root contents will be put into these databases.



The TEMP folder is running out of space when archiving big files

PROBLEM:

When archiving big files, the TEMP folder on the C disk (partition) could run out of space.

SOLUTION:

The only way to solve this issue is to change the Windows temp folder to a different disk (partition) with more storage space.

How can you do that:

- 1) Create a new TEMP folder on the disk (partition) where you want to have it.
- 2) Open the Control panel > System and Security > System > Advanced system settings.
- 3) In the **System Properties** window click on the **Advanced** tab and open the **Environment Variables** window.
- 4) Change the TEMP and TMP Variable values to the new folder that was created in the first point.
- 5) Restart your system.

This video can help you with setting the new temp folder:

<https://www.youtube.com/n264xQC6h3Q>

The attachment could not be opened

PROBLEM:

Encountering the following errors:

- The attachment could not be opened
- The remote server returned an error: (507) insufficient storage

SOLUTION:

The reason is probably the size of the attachment. EWS is limiting access to large attachments, but this limit can be extended.

In order to change the limit, edit the EWS configuration file on all CAS servers:



To change the maximum message size for Exchange Web Services clients, you need to change the value of `maxAllowedContentLength` and all instances of `maxReceivedMessageSize="67108864"` in `%ExchangeInstallPath%ClientAccess\exchweb\ews\web.config`

Also the update to Exchange 2013 SP1 should resolve the problem.

After updating Exchange 2013, the EWS connection might not work in contentACCESS

PROBLEM:

After updating Exchange 2013 to CU15 (maybe older CU as well), the EWS connection might not work in contentACCESS.

SOLUTION:

After updating the Exchange Server, please test again the EWS connection on each Email archive. If you receive the error: **(413) Request Entity Too Large**, then it is necessary to update the EWS configuration on each CAS server:

1. Back up file

C:\Program Files\Microsoft\Exchange Server\V15\FrontEnd\HttpProxy\ews\web.config

2. Replace the "uploadReadAheadSize" 0 value with 1048576 (bytes)

```
<serverRuntime uploadReadAheadSize="1048576" />
```

If Windows authentication is not working in contentACCESS and an alias was created for contentACCESS

PROBLEM:

On the inPoint /contentACCESS File server Shares with Alias name can't be opened.

SOLUTION:

Update the registry key below on the server running IIS to fix the issue.

1. In Registry Editor, locate and then click on the following registry key:

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\MSV1_0](#)



- .NET 4.8
- Visual Studio 2010 Tools for Office Runtime 10.0.60724 (can be downloaded [here](#))

[This](#) thread will also help you with solving the issue.

PowerShell scripts for setting up Email archive

This section with PowerShell scripts will help you with setting up your Email archive and checking and granting necessary permissions for the superuser.

Permissions for Email archive

The **Email archive** is using one account (called “**superuser**” in this section) to connect to the Exchange resources.

The Email archive is accessing Exchange resources through remote PowerShell. It is necessary to enable remote PowerShell on the target Exchange server or Office 365.

There are multiple authentication possibilities when connecting to remote PowerShell:

- Kerberos
- Negotiate
- Digest
- Basic

Note: The selected authentication method needs to be enabled on the Exchange Server.

The example below shows how to allow **Basic** authentication:

```
# Check if Basic Authentication is already allowed
Get-PowerShellVirtualDirectory | fl *auth*
```

```
# Allow Basic Authentication - replace the name of the virtual directory
Set-PowerShellVirtualDirectory -Identity "PowerShell (Default Web Site)" -BasicAuthentication $true
```



Connecting to remote PowerShell

This section will help you with testing the connection to the remote PowerShell. You can use this connection to set up the permissions for the Email archive as well.

The following script prompts for credentials and connects to remote PowerShell. **Do not forget to replace the <server name> with the full qualified name of the Exchange Server** (or ps.outlook.com for Office 365):

```
$ExServerPSURL = "https://<server name>/PowerShell"
$UserCredential = Get-Credential
$Session = New-PSSession -ConfigurationName Microsoft.Exchange -ConnectionUri $ExServerPSURL -Credential
$UserCredential -Authentication Basic -AllowRedirection
Import-PSSession $Session
```

If the connection was **successful**, it will be possible to execute commands. If the connection was **not successful**, try using other authentication method like Kerberos and check whether the credentials are correct. If the connection is **no longer needed**, it is highly recommended to close the session:

```
Remove-PSSession $Session
```

For more information about how to connect to Exchange using remote PowerShell, please check [this](#) page.

Access to resources

The email archive requires access to the following resources:

- Exchange groups and mailboxes
- Public folders (optional)
- Mailbox permissions
- Organization applications

The superuser account requires an active mailbox on the Exchange Server/Office 365 and the permissions included in the following role groups:

- View only organization management
- Public folder management
- Org Marketplace apps



These built-in role groups are allowing access to the complete address book information of Exchange and allowing to install/uninstall **Mail apps** for the whole organization.

Recommended permissions

For a smoother and more transparent configuration process, we recommend creating a new role group especially for contentACCESS, which will include all the necessary roles. The role group is merely a collection of the necessary permissions. If an account is assigned to this role group, the account automatically receives all permissions necessary for the Email archive.

The following script can be used to create the role group and add members to it:

```
New-RoleGroup -Name "contentACCESS Management" -Roles "View-Only Recipients", "View-Only Configuration", "Public Folders", "Org Custom Apps", "Org Marketplace Apps" -Members superuser
```

On-premise Exchange Server

For on-premise Exchange Servers, the superuser requires additional access to the following resources:

- ActiveDirectory users and groups

The connection to the ActiveDirectory is configured in **System** → **Services** → **System**, scroll down to section **Active Directory integration settings**. It is possible to use the same superuser account or use a different account.

Active Directory integration settings

LDAP Server name:	<input type="text" value="LDAP://192. . . 91"/>
	<small>Enter the LDAP server name or IP address if you are out of the domain. This value is used for user name resolving.</small>
Authentication type:	<input type="text" value="None"/>
<input checked="" type="checkbox"/> Use explicit credentials	
User name:	<input type="text"/>
Password:	<input type="password" value="....."/>
Confirm password:	<input type="password" value="....."/>

✔ Connection successful!



This account will connect to the configured domain controller or global catalog to access domain groups and users. The account requires read permission on groups and users. The account should be a member of Domain Administrators. If this is not possible, it is necessary to set up a Security group with the read permissions over the ActiveDirectory objects and add the account to this group.

Office 365 and Hybrid Exchange

These two do not have any special requirements.

Access to mailboxes

The Email archive requires access to mailboxes and optionally public folders.

contentACCESS can archive mailboxes using 2 different methods, both requiring different permissions:

- Delegation
- Impersonation

Delegation

When delegation is used, the superuser account requires full access permission to the archived mailboxes. The Exchange throttling is calculated for the superuser account and this might cause archive performance problems on Office 365.

The full access permission can be granted on individual mailboxes or on Mailbox databases. If permission is granted on individual mailboxes, the newly created mailboxes will not be accessible by the superuser. Therefore, the recommended approach is to set the permissions on mailbox database level (the process needs to be repeated for newly created mailbox databases).

On-premises Exchange Server

The following script grants access to all mailboxes in all mailbox databases:

```
#On-Prem Exchange:
```



```
#Set the permission for the superuser on all mailbox databases:
```

```
Get-MailboxDatabase | Add-ADPermission -User <superuser> -AccessRights 'ExtendedRight' -ExtendedRights 'Receive-As', 'ms-Exch-Store-Admin' -InheritanceType 'All'
```

The following script grants access to one specific mailbox:

```
#Set the permission for the superuser on one mailbox:
```

```
Add-MailboxPermission -Identity mailbox@domain.com -User <superuser> -AccessRights FullAccess -InheritanceType All -Automapping $false
```

Office 365

The following script grants access to all mailboxes currently available:

```
#0365:
```

```
#Set the permission for the superuser on all mailboxes:
```

```
Get-Mailbox | Add-MailboxPermission -User superuser -AccessRights fullaccess -InheritanceType all
```

The following script grants access to one specific mailbox:

```
#Set the permission for the superuser on one mailbox:
```

```
Add-MailboxPermission -Identity mailbox@domain.com -User superuser -AccessRights FullAccess -InheritanceType All -Automapping $false
```

Impersonation

Impersonation has multiple benefits:

- if a new user is added to Exchange, the superuser automatically has permissions to it
- it is easy to set up

Impersonation has big impact on Office 365 archiving. It allows to archive more emails/mailboxes, since the throttling is not calculated for one account, but for each archived mailbox individually. Therefore, if multiple mailboxes are archived, the throughput will be higher.

When impersonation is used, the superuser account requires one additional role: **ApplicationImpersonation**. With this role, the superuser account is able to access all the mailboxes in the organization. The Exchange throttling is calculated for each accessed mailbox individually. This method is recommended when archiving Office 365.



The following script grants ApplicationImpersonation role for the superuser:

```
New-ManagementRoleAssignment -name:contentACCESSImpersonation -Role:ApplicationImpersonation -User:superuser
```

Note: If the O365 user has “desktopless” license, his account **can’t be used** for impersonation. The problem is that EWS access is disabled for such user (he is unable to connect to EWS).

Solution for Outlook security patches

Important information

The security updates for Outlook released on September 12, 2017 are affecting the contentACCESS email archive. The users are no longer able to open the original archived messages from shortcuts, only the shortcut itself. This is caused by the Microsoft’s decision to disable Outlook form scripting by default.

After installing the security updates for Outlook, emails that were archived by third-party application are showing an unwanted behavior. All programs and applications using custom Outlook forms are affected.

List of security updates for Outlook

The following security updates are causing the issue:

Security Update for Microsoft Office Outlook 2007 (KB4011110)

<https://www.microsoft.com/en-us/download/details.aspx?id=55957>

Security Update for Microsoft Outlook 2010 (KB4011089) 64-Bit Edition

<https://www.microsoft.com/en-us/download/details.aspx?id=55924>

Security Update for Microsoft Outlook 2010 (KB4011089) 32-Bit Edition

<https://www.microsoft.com/en-us/download/details.aspx?id=55881>



Security Update for Microsoft Outlook 2013 (KB4011090) 64-Bit Edition

<https://www.microsoft.com/en-us/download/details.aspx?id=55930>

Security Update for Microsoft Outlook 2013 (KB4011090) 32-Bit Edition

<https://www.microsoft.com/en-us/download/details.aspx?id=55894>

Security Update for Microsoft Outlook 2016 (KB4011091) 64-Bit Edition

<https://www.microsoft.com/en-us/download/details.aspx?id=55941>

Security Update for Microsoft Outlook 2016 (KB4011091) 32-Bit Edition

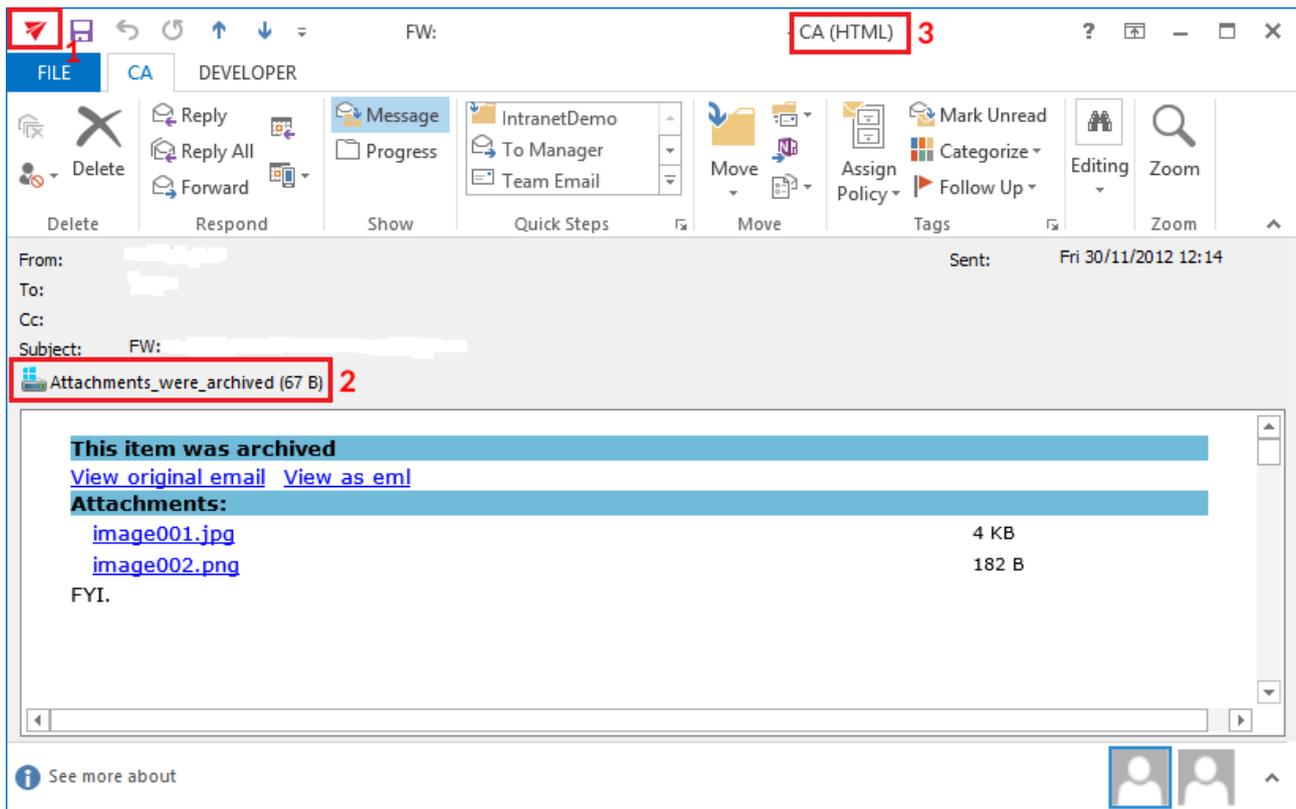
<https://www.microsoft.com/en-us/download/details.aspx?id=55934>

What is affected

Email archive

The security patches are preventing archived emails from opening. When the user double clicks on an archived email (shortcut), instead of the original item only the shortcut is opened. The attachments are only accessible if the shortcut was configured to contain the links.

The following figure is showing an example of an opened shortcut:



Screenshot: The shortcut with attachments is opened

The following signs can be observed:

- 1) The icon of the email is different
- 2) If the mail had attachments, there is a "Attachments_were_archived" text displayed
- 3) The title of the window contains "CA" instead of "Message"

How to fix the problem

The Outlook form scripting is disabled by default, but it can be enabled using registry keys as described here:

<https://support.office.com/en-us/article/Custom-form-script-is-now-disabled-by-default-bd8ea308-733f-4728-bfcc-d7cce0120e94>



We have prepared registry files, which can be applied on the affected client computers. There is a separate registry file based on Outlook version and the Windows version. Download and extract the ZIP file from here:

<http://www.tech-arrow.com/download/CustomFormFix.zip>

Choose the right *.reg file depending on your Outlook and Windows versions and apply it on the client computer (by executing the *.reg file).

Note: Registry key for MS Outlook 2016 works also with MS Outlook 2019.

Fix for Outlook 2007

Outlook and Windows version	Path in the ZIP file
Outlook 2007 on Windows 32-bit	Outlook 2007\Forms-2007-samebit.reg
Outlook 2007 on Windows 64-bit	Outlook 2007\Forms-2007-64win.reg

Fix for Outlook 2010

Outlook and Windows version	Path in the ZIP file
Outlook 2010 32-Bit Edition on Windows 32-bit	Outlook 2010\Forms-2010-samebit.reg
Outlook 2010 32-Bit Edition on Windows 64-bit	Outlook 2010\Forms-2010-64win.reg
Outlook 2010 64-Bit Edition on Windows 64-bit	Outlook 2010\Forms-2010-samebit.reg

Fix for Outlook 2013

Outlook and Windows version	Path in the ZIP file
Outlook 2013 32-Bit Edition on Windows 32-bit	Outlook 2013\Forms-2013-samebit.reg
Outlook 2013 32-Bit Edition on Windows 64-bit	Outlook 2013\Forms-2013-64win.reg
Outlook 2013 64-Bit Edition on Windows 64-bit	Outlook 2013\Forms-2013-samebit.reg



Fix for Outlook 2016

Outlook and Windows version	Path in the ZIP file
Outlook 2016 32-Bit Edition on Windows 32-bit	Outlook 2016\Forms-2016-samebit.reg
Outlook 2016 32-Bit Edition on Windows 64-bit	Outlook 2016\Forms-2016-64win.reg
Outlook 2016 64-Bit Edition on Windows 64-bit	Outlook 2016\Forms-2016-samebit.reg

Support

If you need any help with solving your problem with custom Outlook forms, just contact us at support@tech-arrow.com.

Solution for Outlook security patches through GPO

Important information

The security updates for Outlook released on September 12, 2017 are affecting the contentACCESS email archive. The users are no longer able to open the original archived messages from shortcuts, only the shortcut itself. This is caused by the Microsoft's decision to disable Outlook form scripting by default.

After installing the security updates for Outlook, emails that were archived by third-party application are showing an unwanted behavior. All programs and applications using custom Outlook forms are affected. More information can be found [here](#).

The Outlook form scripting is disabled by default, but it can be enabled using registry keys as described in the section mentioned above. This section describes the solution for the Outlook security patches through **Group policy (GPO)**.

The GPO solution

This solution consists of three steps:

1) Preparing the Distribution point

2) Creating the group policy object and assign it to the affected machines

3) Checking the changes

Preparing the Distribution point

To use the GPO for the solution, a distribution point has to be created on the publishing server:

- Log on to the server computer (Domain controller) as an administrator.
- Create a shared network folder that will contain the **CustomFormFix** folder that you want to distribute. Extract the [CustomFormFix.zip](#) to this folder.

Note: Registry key for MS Outlook 2016 works also with MS Outlook 2019.

- Set permissions on the shared folder to allow access to the distribution point (everyone should have at least read access).
- In this demo case the distribution group path is \\SharedFolder.

Note: Do not use special characters in setup names or be careful with long UNC paths.

Creating the group policy object and assigning it to the affected machines

To apply the solution, a new group policy object should be created and the [CustomFormsFix.ps1](#)

PowerShell script should be set in the GPO:

- Start the group policy management on the domain controller.
- Create a new group policy object in your domain.
- Link the newly created GPO object to your domain.

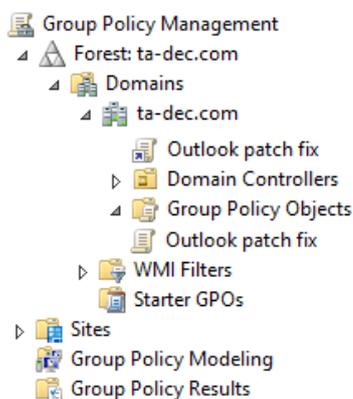


Figure 1: The created GPO object "Outlook patch fix" is linked to the ta-dec.com domain

- Set the Security filtering for the required computers (in our case we chose the Domain computers group).
- Right click and choose Edit on the new GPO.
- Choose the Computer configuration -> Windows Settings -> Scripts -> Startup option.
- In the Startup properties windows choose the PowerShell Scripts tab.

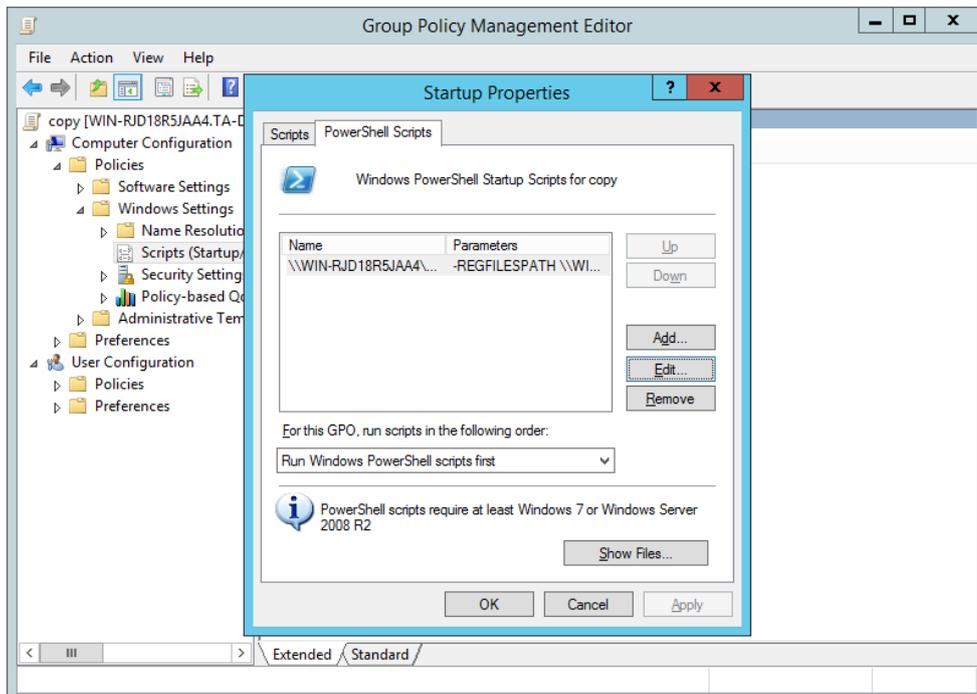


Figure 2: The GPO for Computer Startup configuration window

- Click on the Add button and create a new configuration. The script name in our case is: **\\ShareFolder\CustomFormFix\CustomFormFix.ps1** (the shared path of the extracted PowerShell script) and the Script Parameters is **-REGFILESPATH \\ShareFolder\CustomFormFix** (the -REGFILESPATH parameter plus the shared path of the earlier created CustomFormFix folder).

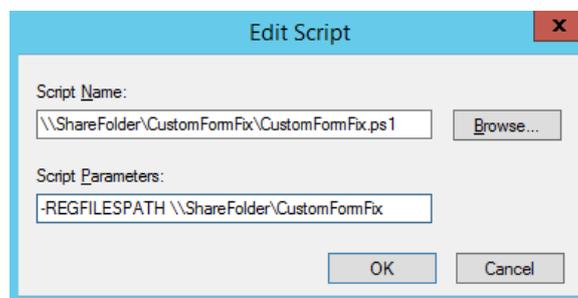


Figure 3: The configuration for the GPO

Checking the changes

To check if our configuration and GPO deployment was successful, it's necessary to restart the client machine, which was set in the **Security filtering**:

- Open the Registry Editor (regedit.exe)
- Find the path
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\
and open the Outlook KEY, which is created by your office version, for example:
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\15.0\Outlook
- There should be two new keys in this folder: Forms and Security

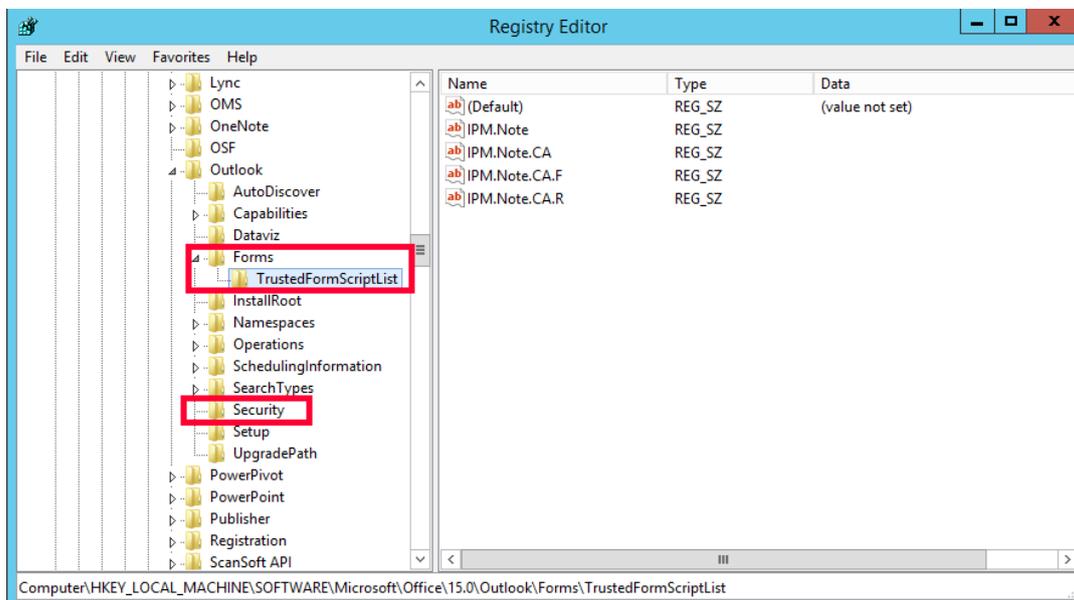
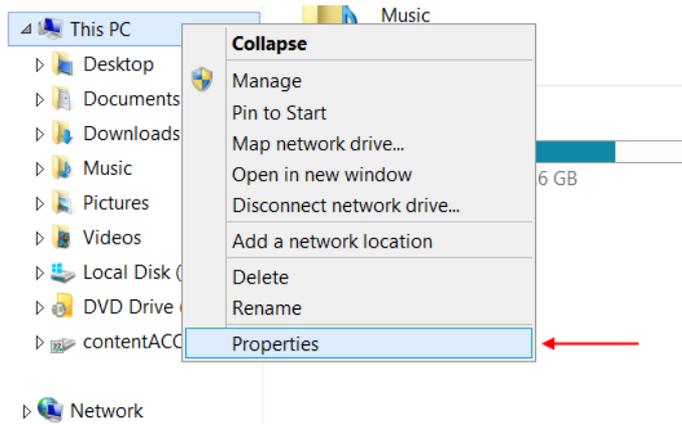


Figure 4: The deployed registry changes

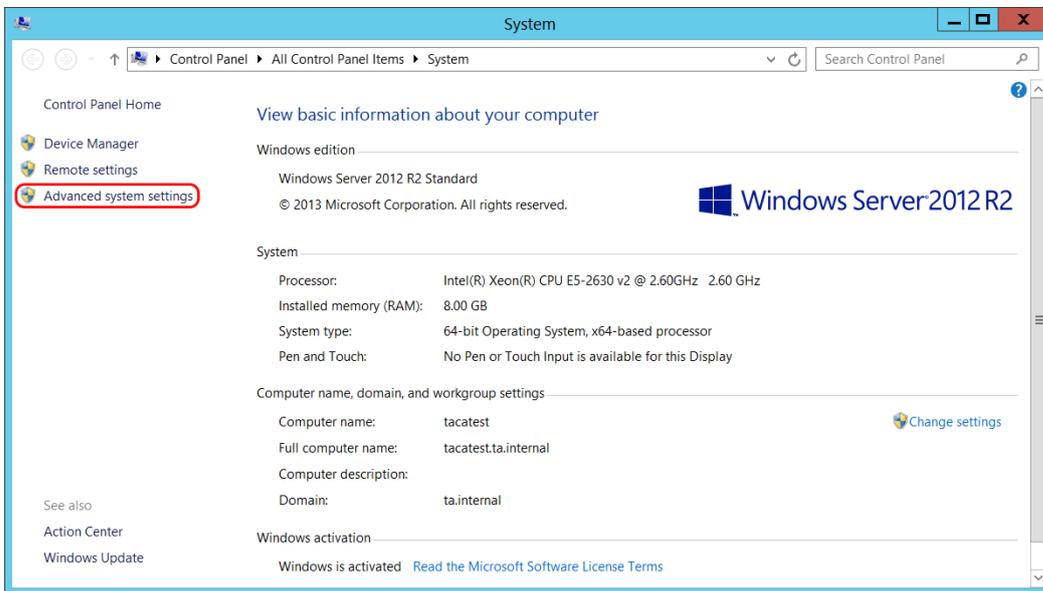
Solution for indexing PDF files

Here is how to set the **Path** environment variable for the Adobe PDF iFilter:

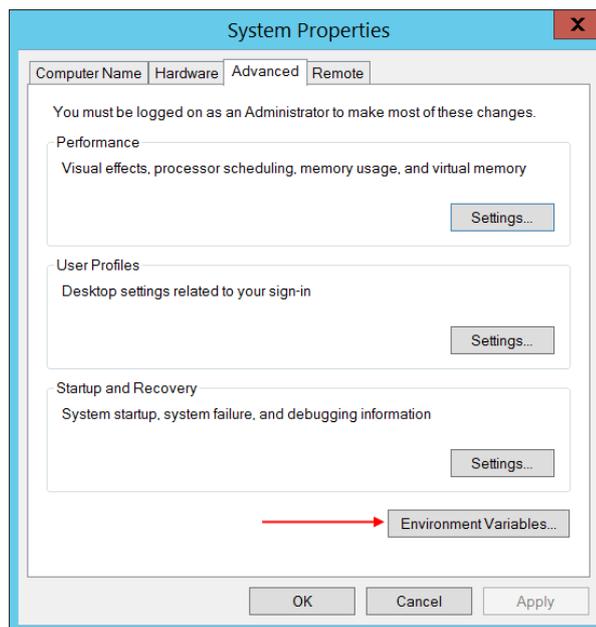
- 1) Open File explorer.
- 2) Right-click on This PC (or My computer) and select Properties.



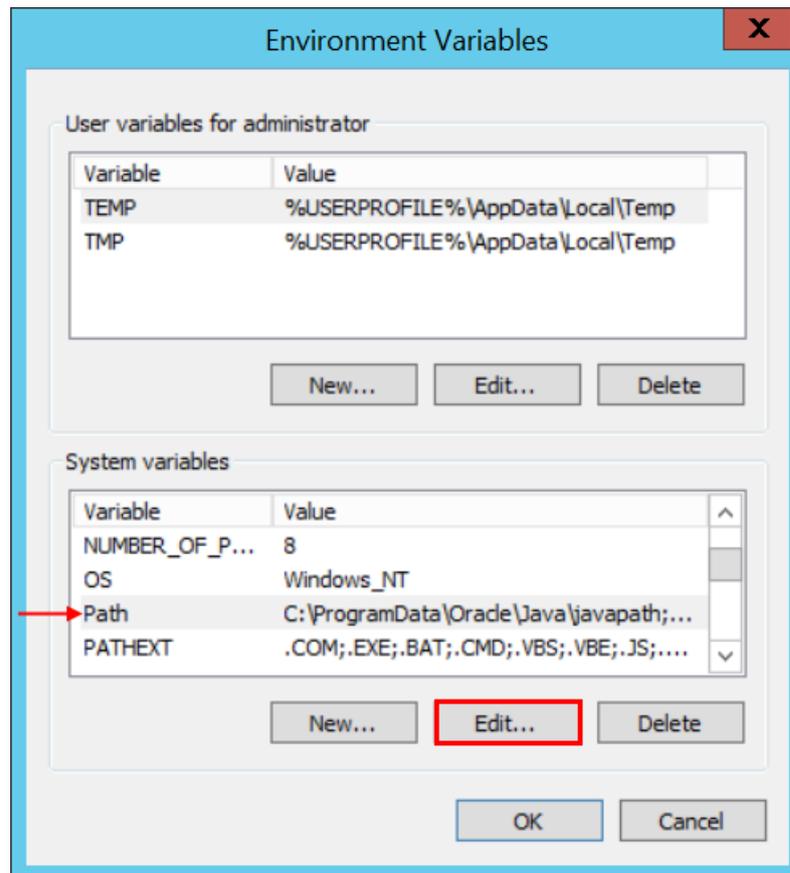
3) Click on Advanced system settings.



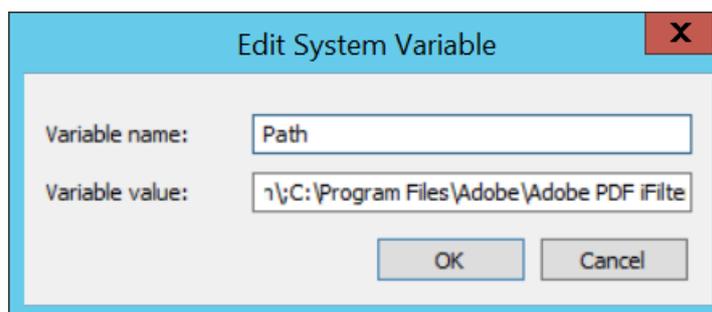
4) In the lower right corner click on Environment Variables.



- 5) Find the variable named **Path**. Click on **Edit**.



- 6) Append the path **C:\Program Files\Adobe\Adobe PDF iFilter 11 for 64-bit platforms\bin** to the variable value separated by semicolon. Click OK.

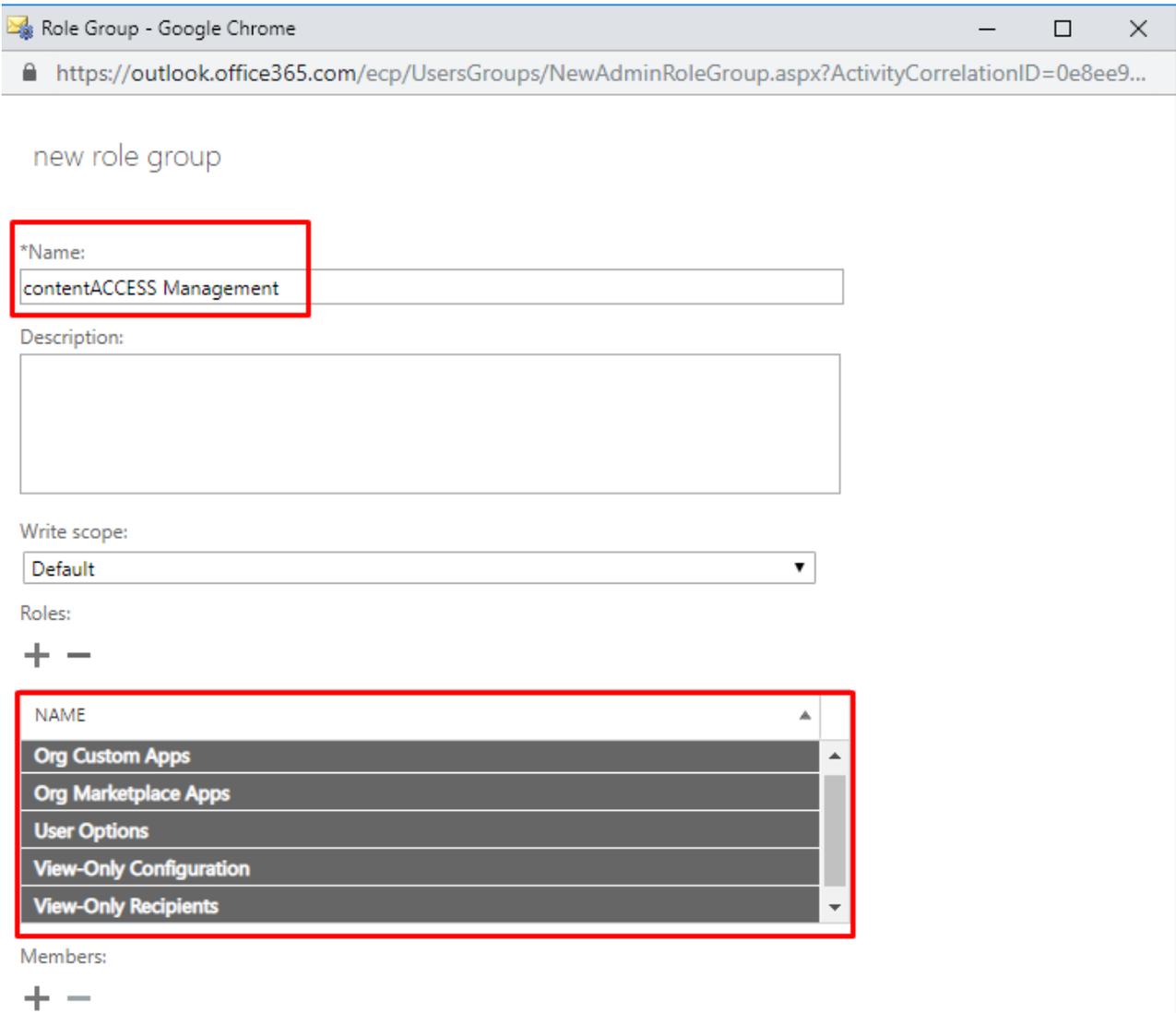


O365 SuperUser mailbox configuration

In this part we will explain what needs to be configured for the "SuperUser" mailbox, which can be later used for archiving.

1. Set permissions in Online Exchange

5 roles are recommended for the SuperUser: *View-Only Recipients*, *View-Only Configuration*, *Org Custom Apps*, *Org Marketplace Apps* and *User Options*. The easiest and most secure way is to create an **Admin role group** called **contentACCESS Management**, assign the roles mentioned above to the group and put the **SuperUser** to the group as a member. For more information about how the role group should look like, please see the screenshot below.



new role group

*Name:
contentACCESS Management

Description:

Write scope:
Default

Roles:

+ -

NAME
Org Custom Apps
Org Marketplace Apps
User Options
View-Only Configuration
View-Only Recipients

Members:

+ -

2. Grant Full Access rights for the SuperUser on all mailboxes

The easiest way to grant the full access rights for the SuperUser is through PowerShell. First, you have to login to the Exchange Online and run this one line command after changing the "SuperUser" for the real SuperUser account:



```
Get-Mailbox | Add-MailboxPermission -User SuperUser -AccessRights  
fullaccess -InheritanceType all
```

To connect to Exchange Online PowerShell, please click [here](#).

Important: This user will have access to all mailboxes, so a strong password has to be set for him.

Office365 journaling

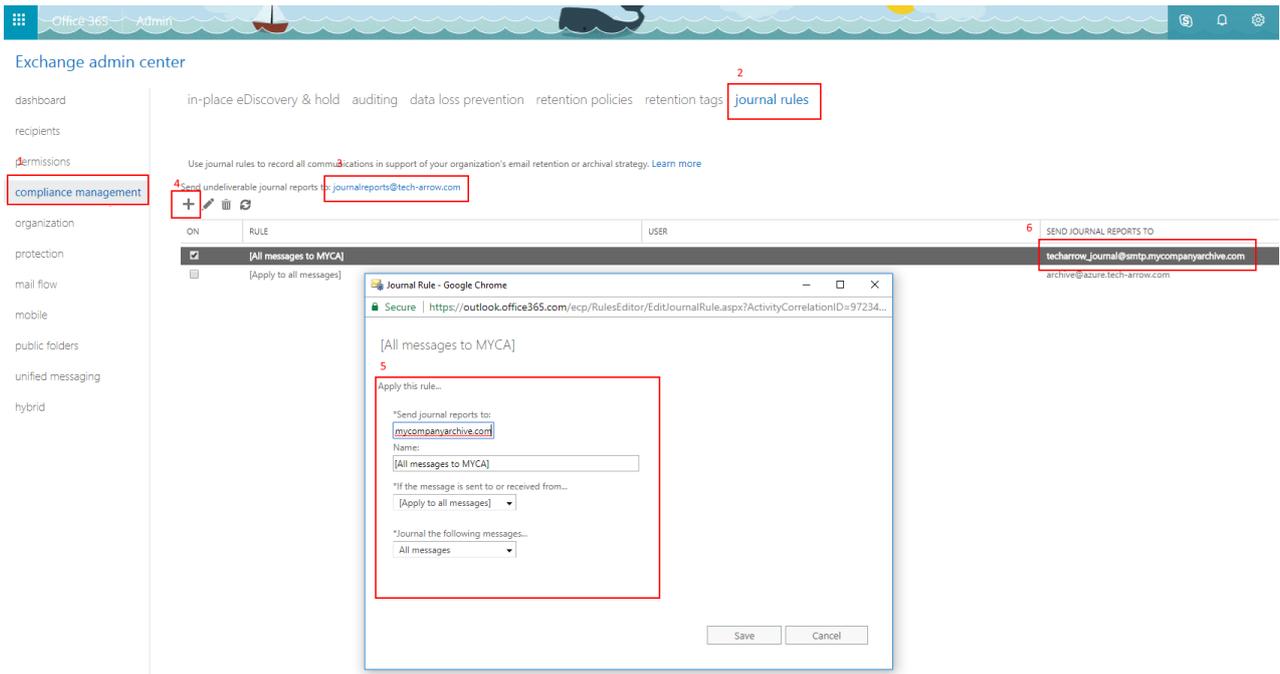
In this section we will explain how to correctly set up the O365 journaling and sending of the undeliverable reports.

Steps to follow:

- 1, Open the compliance management page in O365
- 2, Open the **journal roles** sheet
- 3, Set the "Send undeliverable journal reports" mailbox – **emails of this mailbox will not be forwarded to the journaling**

Note: The emails that are sent to the email address configured to get the undeliverable journal reports will not be sent to the journal. If you configure your mailbox to get the undeliverable reports, then any email sent to you will not be forwarded to the journal, so these emails will not be archived by contentACCESS. This means that a production mailbox, which must be archived, **SHALL NOT** be set as undeliverable report receiver.

- 4, Add a new rule
- 5, Configure the rule
- 6, In case of using the mycompanyarchive, the journal mailbox domain is @smtp.mycompanyarchive.com



Organizational forms

Organizational forms folder was included by default in **System Folders**. With the changes to public folders in newer versions of Exchange, the Organizational Forms folder was removed. This may also cause some troubles when [installing contentACCESS Outlook forms](#).

Exchange 2010

To learn how to create the removed folder and how to publish a **Form** with **Outlook**, please, read this article: <https://www.slipstick.com/exchange/2010-exs/organizational-forms-library-exchange-2010/>.

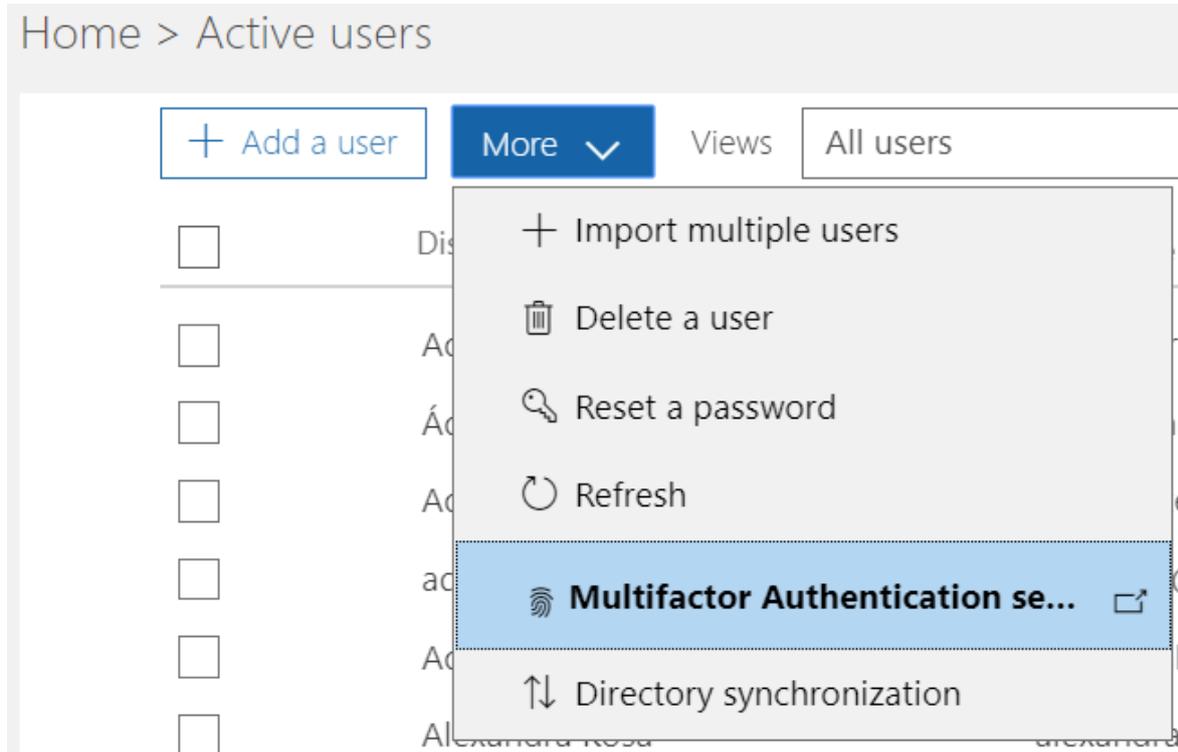
Exchange 2013+

To learn how to create the removed folder and how to publish a **Form** with **Outlook**, please, read this article: <https://support.microsoft.com/en-us/help/3109076/create-an-organizational-forms-library-in-exchange-online>.



Multifactor authentication

For the MFA you need to go to <https://portal.office.com/adminportal/home#/users> (the O365 admin portal) and open the **More** option on the **Active users** site. Select the **Multifactor Authentication (MFA) setup** option from the menu.



On the MFA site you can see all the users and their configuration – whether the MFA is enabled or not.

MULTI-FACTOR AUTH STATUS	
Disabled	
Disabled	
Disabled	tech-arrow@tech
Disabled	noreply@tech-arrow.com
Disabled	quick steps
Disabled	Enable
Disabled	Manage user settings
Disabled	



After enabling MFA through the **Enable** option in **quick steps** on the right side (see screenshot above), you need to confirm your choice by clicking on the **enable multi-factor auth** button.



About enabling multi-factor auth

Please read the [deployment guide](#) if you haven't already.

If your users do not regularly sign in through the browser, you can send them to this link to register for multi-factor auth: <https://aka.ms/MFASetup>

enable multi-factor auth

cancel

On the **MFA** site, switch from **users** to **service settings** and under **app passwords** click on **Allow the users to create app passwords to sign in to non-browser apps**. Click on **save**.

multi-factor authentication

users **service settings**

app passwords

- Allow users to create app passwords to sign in to non-browser apps
- Do not allow users to create app passwords to sign in to non-browser apps

verification options

Methods available to users:

- Call to phone
- Text message to phone
- Notification through mobile app
- Verification code from mobile app or hardware token

remember multi-factor authentication

- Allow users to remember multi-factor authentication on devices they trust
Days before a device must re-authenticate (1-60):

save

The user will have the MFA enabled. However, for MFA to work properly, the user needs to log in and create an “app password”.



Note: In case the user is also Admin for email archiving, the user must use the app password instead of the regular password in the **Email archive -> System settings -> EWS settings**.

Region setting

Microsoft Azure is hosting multiple instances of the **Azure cloud services**, which are isolated from each other. The most commonly used Azure instance is the **Azure Public Cloud**. This Public Cloud has several data centers around the world. The data hosted in the Public Cloud are replicated/stored in these data centers. However, some government regulations in some countries have special requirements. Microsoft has deployed **isolated Azure instances** for such scenarios. One of these isolated instances is the so called **German cloud**, which is hosted by the Deutsche Telecom in Germany. Another isolated instance of Azure is the **Government Cloud**, which is hosted in USA.

The Region setting is used to specify in which Azure instance is the current tenant located. Choose:

- **Global** - if your tenant is hosted in the Azure Public instance
- **Germany** - if your tenant is hosted in the German Cloud (hosted by Deutsche Telecom)
- **Custom** – if you need to specify custom values

Exchange connection settings

Exchange server type:	Exchange Online (O365)
Region:	Custom
Exchange server interface version:	Global Germany Custom
EWS Url:	
Use impersonation:	<input checked="" type="checkbox"/>
EWS authentication mode:	Basic
PowerShell Url:	https://ps.outlook.com/PowerShell
PowerShell auth:	Basic

Important: Users located inside an isolated Azure instance will **NOT** be able to log in to other instances, like Azure Public Cloud or Government Cloud.



contentACCESS Mail app installation issue

PROBLEM

Error message “The app couldn’t be downloaded.” during [Mail app](#) installation (Provisioning job run).

SOLUTION

This problem occurs when the Exchange server can’t download the Mail app’s .xml manifest file from the contentACCESS server. To successfully install the Mail app, the Exchange server must have access to the contentACCESS server and to the Mail app’s .xml manifest file. The manifest file can be accessed using the following links:

- [https://\[SERVERNAME\]/contentACCESSWS/Mailapp/Mailapp.xml](https://[SERVERNAME]/contentACCESSWS/Mailapp/Mailapp.xml)
- [https://\[SERVERNAME\]/contentACCESSWS/Mailapp/Mailapp_no_ribbon_button.xml](https://[SERVERNAME]/contentACCESSWS/Mailapp/Mailapp_no_ribbon_button.xml)

The administrator should be able to browse the file using the links above without any issues.

Azure app registration

In this section, we will explain how an app is registered on the Azure portal.

Navigate to portal.azure.com. Go to **All services** -> **App registrations** -> **+ New registration**. Fill in the details of the new application. The only mandatory field that needs to be changed is the name of the application, the other options can be left as-is.



All services > App registrations > Register an application

Register an application

* Name

The user-facing display name for this application (this can be changed later).

contentACCESS ✓

Supported account types

Who can use this application or access this API?

- Accounts in this organizational directory only (contentACCESS EarlyAccessDE only - Single tenant)
- Accounts in any organizational directory (Any Azure AD directory - Multitenant)
- Accounts in any organizational directory (Any Azure AD directory - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox)

[Help me choose...](#)

Redirect URI (optional)

We'll return the authentication response to this URI after successfully authenticating the user. Providing this now is optional and it can be changed later, but a value is required for most authentication scenarios.

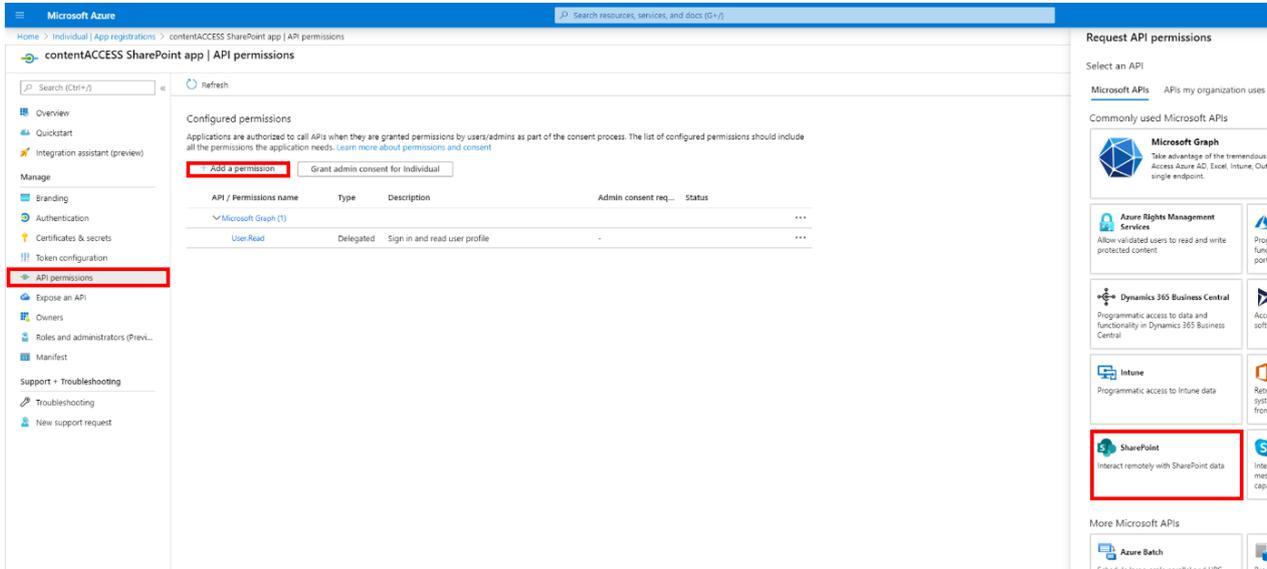
Web ▼

After the app is successfully registered, you will be able to see the **Application ID** and **Directory ID** in the app's **Overview**.

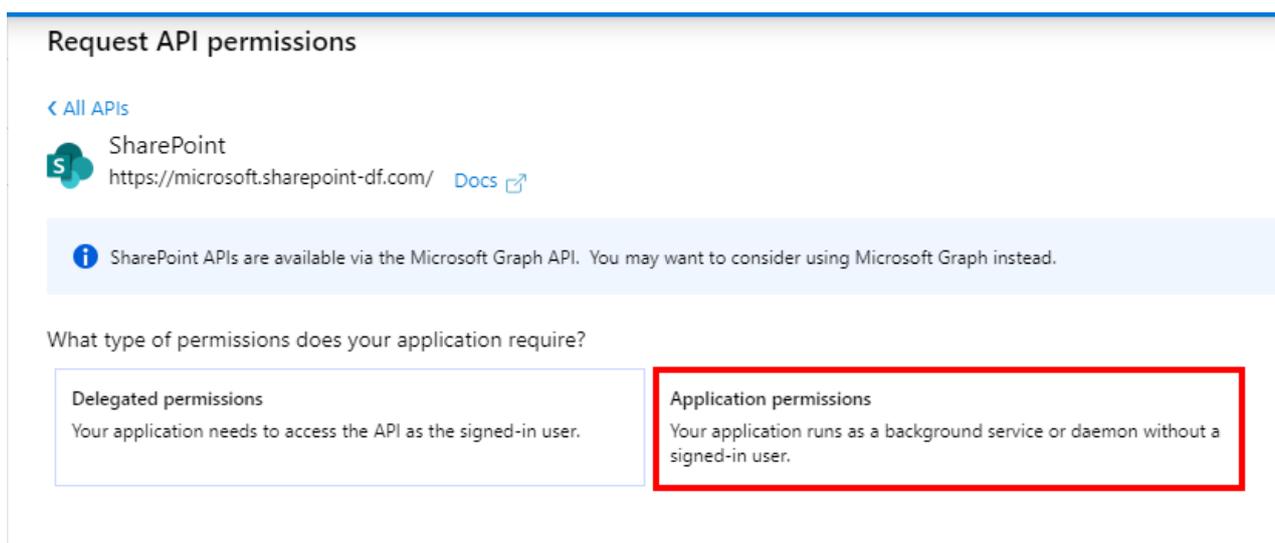
The screenshot shows the 'Overview' page for an application named 'contentACCESS'. The left sidebar contains navigation options: Overview, Quickstart, Integration assistant (preview), Manage (Branding, Authentication, Certificates & secrets, Token configuration, API permissions, Expose an API, Owners, Roles and administrators (Previous), Manifest), Support + Troubleshooting (Troubleshooting, New support request). The main content area shows details for the application: Display name: contentACCESS, Application (client) ID: 4124, Directory (tenant) ID: 9bab, Object ID: 517005. There are red arrows pointing to the Application (client) ID and Directory (tenant) ID fields. On the right, there are links for Supported account types (My organization only), Redirect URIs (Add a Redirect URI), Application ID URI (Add an Application ID URI), and Managed application in... (contentACCESS). Below this is a 'Call APIs' section with a 'View API permissions' button and a 'Documentation' section with links to Microsoft identity platform, Authentication scenarios, Authentication libraries, Code samples, Microsoft Graph, Glossary, and Help and Support.



In this step, the necessary permissions will be granted to the application. On the application details page, click on the **API permissions** button on the left menu. When the configured permissions page loads in, click on the “Add a permission” button, then select “SharePoint” from the right-side menu (when registering **Teams archive app**, select **Microsoft Graph**).



On the next screen we can decide whether we want to grant **Delegated** or **Application** permissions to our app. We need the **Application** permissions.





After the application permissions option is chosen, a list with the available permissions will appear. Select:

- for SharePoint - to support all the functions of contentACCESS and other client applications (including AAD groups support in SharePoint archive), all the following permissions need to be added:

API / Permissions name	Type	Description	Admin consent req...	Status
<ul style="list-style-type: none"> Microsoft Graph (9) 				...
Application.Read.All	Application	Read all applications	Yes	✔ Granted for TECH-ARRO... ...
Application.ReadWrite.All	Application	Read and write all applications	Yes	✔ Granted for TECH-ARRO... ...
Group.Read.All	Application	Read all groups	Yes	✔ Granted for TECH-ARRO... ...
Mail.Read	Application	Read mail in all mailboxes	Yes	✔ Granted for TECH-ARRO... ...
Mail.ReadBasic	Application	Read basic mail in all mailboxes	Yes	✔ Granted for TECH-ARRO... ...
Mail.ReadBasic.All	Application	Read basic mail in all mailboxes	Yes	✔ Granted for TECH-ARRO... ...
Mail.ReadWrite	Application	Read and write mail in all mailboxes	Yes	✔ Granted for TECH-ARRO... ...
Mail.Send	Application	Send mail as any user	Yes	✔ Granted for TECH-ARRO... ...
User.Read.All	Application	Read all users' full profiles	Yes	✔ Granted for TECH-ARRO... ...
<ul style="list-style-type: none"> SharePoint (8) 				...
Sites.FullControl.All	Application	Have full control of all site collections	Yes	✔ Granted for TECH-ARRO... ...
Sites.Manage.All	Application	Read and write items and lists in all site collections	Yes	✔ Granted for TECH-ARRO... ...
Sites.Read.All	Application	Read items in all site collections	Yes	✔ Granted for TECH-ARRO... ...
Sites.ReadWrite.All	Application	Read and write items in all site collections	Yes	✔ Granted for TECH-ARRO... ...
TermStore.Read.All	Application	Read managed metadata	Yes	✔ Granted for TECH-ARRO... ...
TermStore.ReadWrite.All	Application	Read and write managed metadata	Yes	✔ Granted for TECH-ARRO... ...
User.Read.All	Application	Read user profiles	Yes	✔ Granted for TECH-ARRO... ...
User.ReadWrite.All	Application	Read and write user profiles	Yes	✔ Granted for TECH-ARRO... ...

- for Teams archive – some permissions need to be selected from the **Delegated** option, some from the **Application** option



API / Permissions name	Type	Description	Admin consent req...	Status
▼ Microsoft Graph (12) ...				
ChannelMessage.Read.All	<u>Delegated</u>	Read user channel messages	Yes	✔ Granted for TECH-ARRO... ...
ChannelMessage.Read.All	<u>Application</u>	Read all channel messages	Yes	✔ Granted for TECH-ARRO... ...
Directory.Read.All	<u>Application</u>	Read directory data	Yes	✔ Granted for TECH-ARRO... ...
Group.Read.All	<u>Delegated</u>	Read all groups	Yes	✔ Granted for TECH-ARRO... ...
Group.Read.All	<u>Application</u>	Read all groups	Yes	✔ Granted for TECH-ARRO... ...
Group.ReadWrite.All	<u>Delegated</u>	Read and write all groups	Yes	✔ Granted for TECH-ARRO... ...
Group.ReadWrite.All	<u>Application</u>	Read and write all groups	Yes	✔ Granted for TECH-ARRO... ...
GroupMember.Read.All	<u>Application</u>	Read all group memberships	Yes	⚠ Not granted for TECH-A... ...
TeamsTab.Read.All	<u>Delegated</u>	Read tabs in Microsoft Teams.	Yes	✔ Granted for TECH-ARRO... ...
TeamsTab.Read.All	<u>Application</u>	Read tabs in Microsoft Teams.	Yes	✔ Granted for TECH-ARRO... ...
User.Read	<u>Delegated</u>	Sign in and read user profile	-	✔ Granted for TECH-ARRO... ...
User.Read.All	<u>Application</u>	Read all users' full profiles	Yes	✔ Granted for TECH-ARRO... ...

Click on **Add permissions**.

After the permissions have been assigned to the application, the administrator must grant consent for these permissions. Click on the **Grant admin consent for "TENANTNAME"** button.

Refresh

⚠ You are editing permission(s) to your application, users will have to consent even if they've already done so previously.

Configured permissions

Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The list of configured permissions should include all the permissions the application needs. [Learn more about permissions and consent](#)

+ Add a permission **Grant admin consent for Individual**

API / Permissions name	Type	Description	Admin consent req...	Status
▼ Microsoft Graph (1) ...				
User.Read	Delegated	Sign in and read user profile	-	...
▼ SharePoint (8) ...				
Sites.FullControl.All	Application	Have full control of all site collections	Yes	⚠ Not granted for Individu... ...
Sites.Manage.All	Application	Read and write items and lists in all site collections	Yes	⚠ Not granted for Individu... ...
Sites.Read.All	Application	Read items in all site collections	Yes	⚠ Not granted for Individu... ...

When the permissions are assigned to the application and the admin consent is granted, the client access certificate needs to be assigned to the application. Click on the **Certificates & secrets** option in the left side menu. On the certificate management screen click on the **Upload certificate** button. Browse the client certificate you want to use and upload it. It can be a self-signed certificate or an already existing one. PowerShell script for creating a self-signed certificate can be downloaded [here](#).



Home > Individual | App registrations >

contentACCESS SharePoint app | Certificates & secrets

Search (Ctrl+/)



Credentials enable confidential applications to identify themselves to the authentic scheme). For a higher level of assurance, we recommend using a certificate (instead

Overview

Quickstart

Integration assistant (preview)

Manage

Branding

Authentication

Certificates & secrets

Token configuration

Certificates

Certificates can be used as secrets to prove the application's identity when request

[↑ Upload certificate](#)

Thumbprint

Start date

No certificates have been added for this application.

Next, add a new client secret by clicking on the **+ New client secret** button. This is necessary for some plugins and client applications.

All services > App registrations > contentACCESS | Certificates & secrets

contentACCESS | Certificates & secrets

Copy the new client secret value. You won't be able to retrieve it after you perform another operation or leave this blade.

Credentials enable confidential applications to identify themselves to the authentication service when receiving tokens at a web addressable location (using an HTTPS scheme). For a higher level of assurance, we recommend using a certificate (instead of a client secret) as a credential.

Certificates

Certificates can be used as secrets to prove the application's identity when requesting a token. Also can be referred to as public keys.

[↑ Upload certificate](#)

Thumbprint	Start date	Expires
No certificates have been added for this application.		

Client secrets

A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

[+ New client secret](#)

Description	Expires	Value
Email Archive Secret	12/31/2299	4FQ6...