

# contentACCESS Remote File archiving Manual - version 3.9



**NOVEMBER 26, 2019**

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



## Table of Contents

|   |    |
|---|----|
| Introduction to Remote File archiving.....                  | 3  |
| Installation.....   | 3  |
| How to use the Remote File Archiver .....                   | 6  |
| Connection tab.....   | 7  |
| Archive tab.....  | 13 |
| Recovery tab.....   | 23 |
| Active Directory tab.....                                   | 29 |
| PST import tab.....   | 33 |
| RFA use-cases .....   | 38 |
| Archiving common shares .....                               | 39 |
| Archiving user workstations (domain joined).....            | 41 |
| Archiving common shares and domain joined workstations..... | 44 |
| Archiving workstations in a workgroup.....                  | 44 |

## Introduction to Remote File archiving

The Remote File archiving feature is used to archive files located on network shares, even if these shares are not accessible to contentACCESS (when installed in cloud). It can be also used to upload PST files to contentACCESS server.

**Note:** To use Remote File archiving, contentACCESS must be installed first.

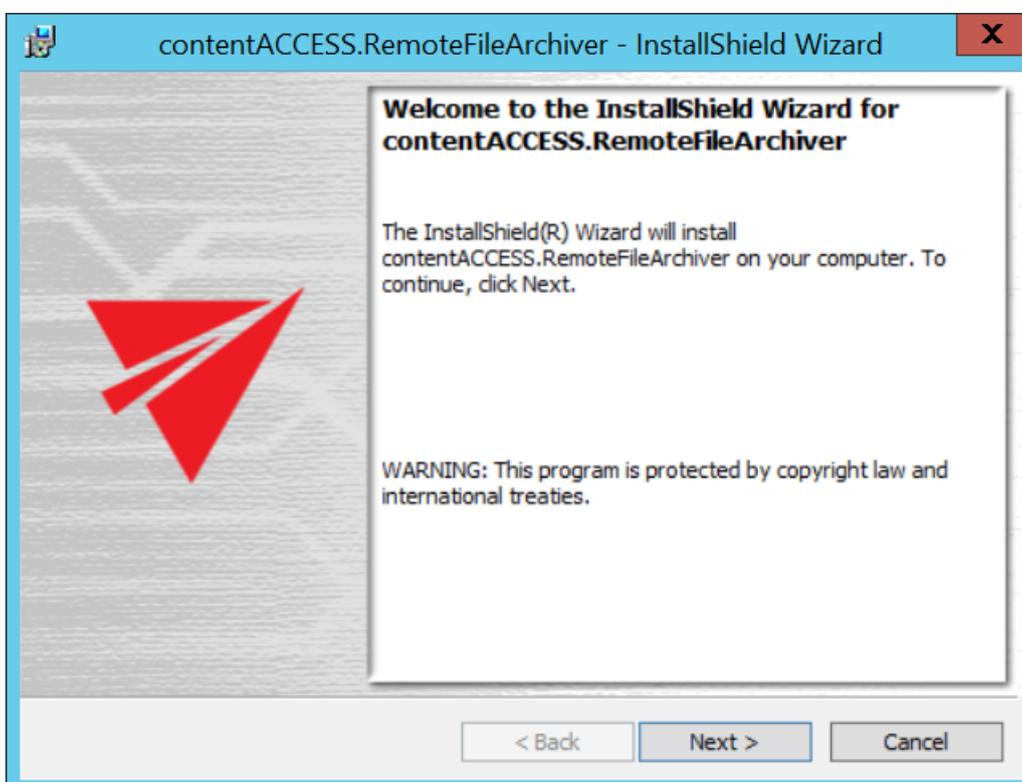
## Installation

There are two ways to reach the setup:

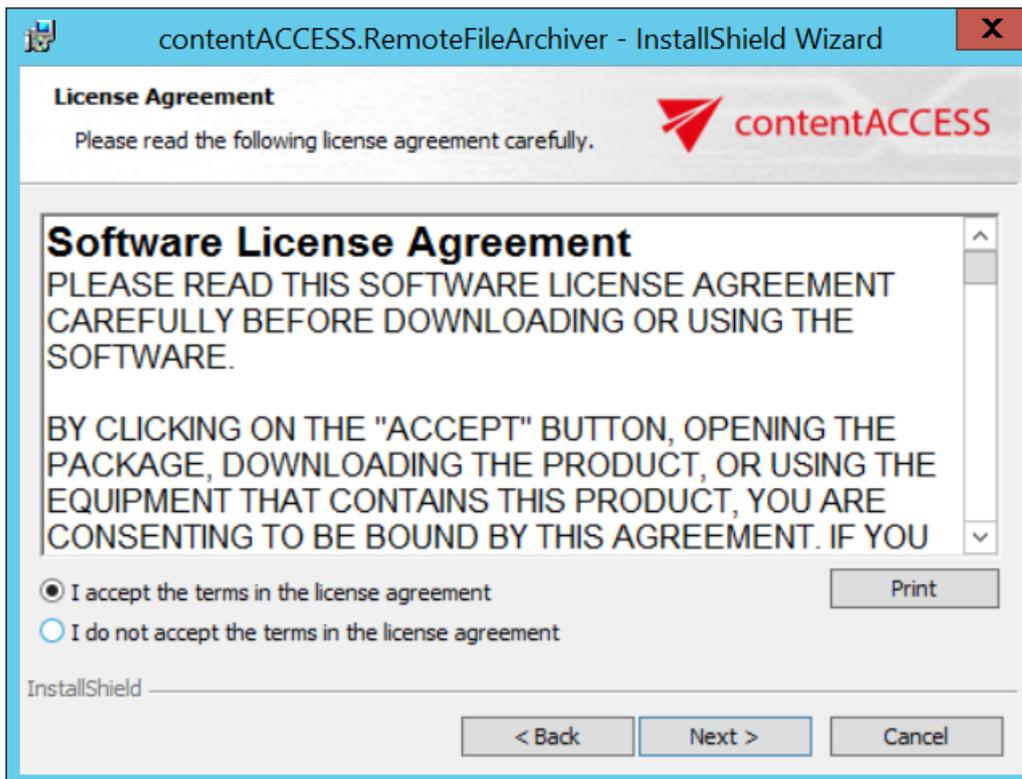
- download it from the [Remote agents](#) tab in Central administration (**File archive** => Remote agents => Remote agents)
- download it from the [Remote agents](#) tab in Central administration (**Email archive** => Remote agents => Remote agents)

Run the setup. The installation process goes as follows:

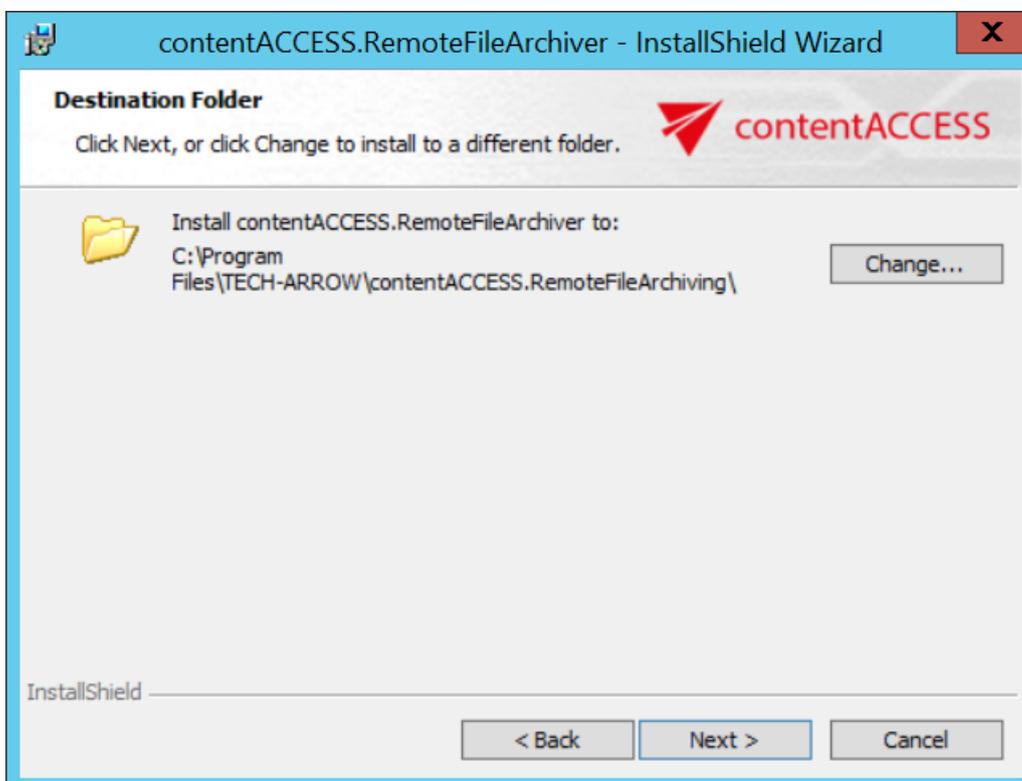
1. Click **Next**.



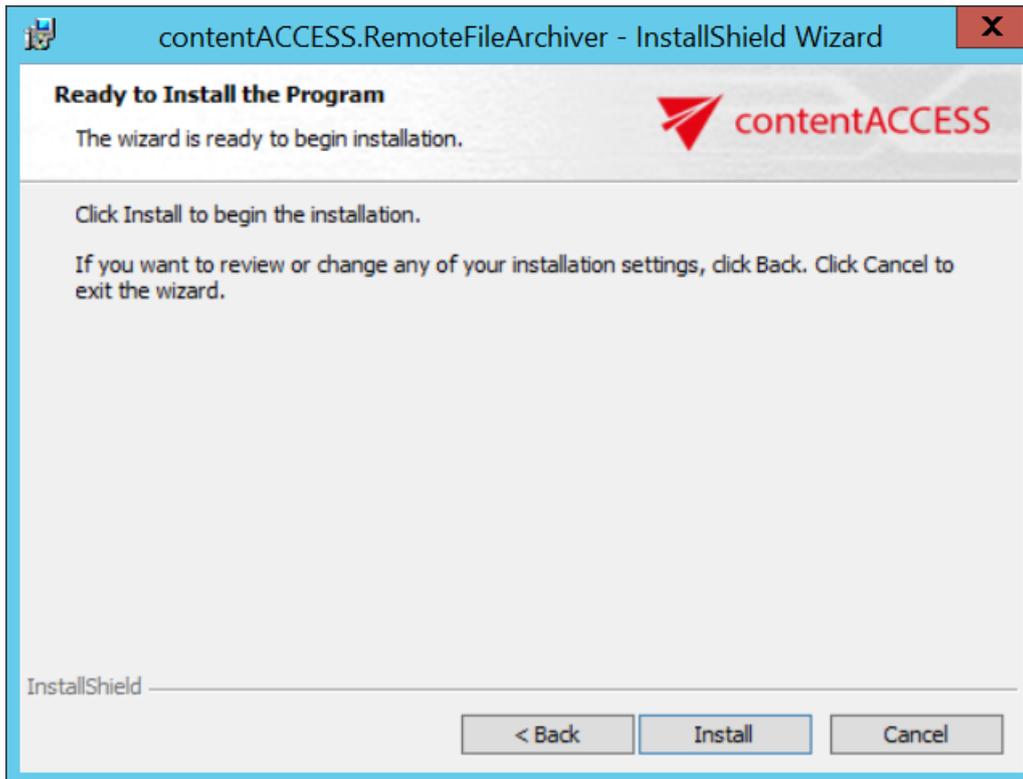
2. Choose **I accept the terms in the license agreement** and click **Next**.



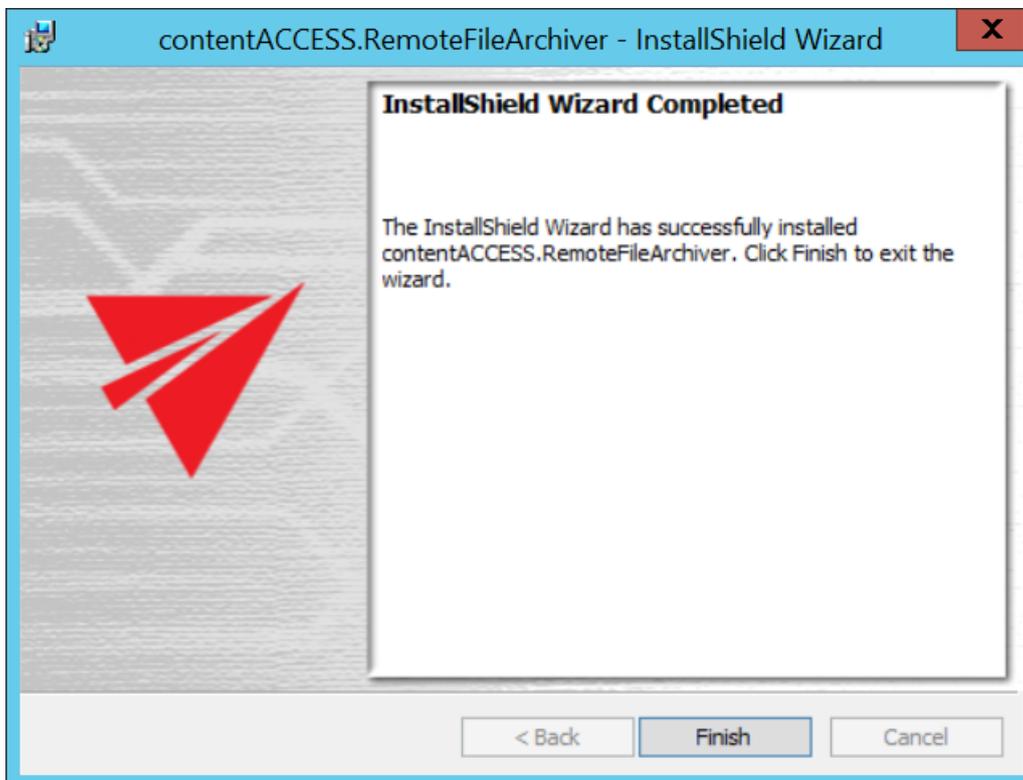
- Here you can choose the folder, to which Remote File Archiver (Remote FA further in text) will be installed. We recommend to leave it like this. Click **Next**.



- Click on **Install**.



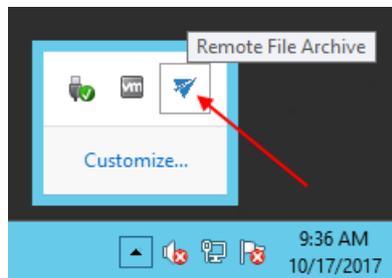
5. Click on **Finish** to complete the installation process.



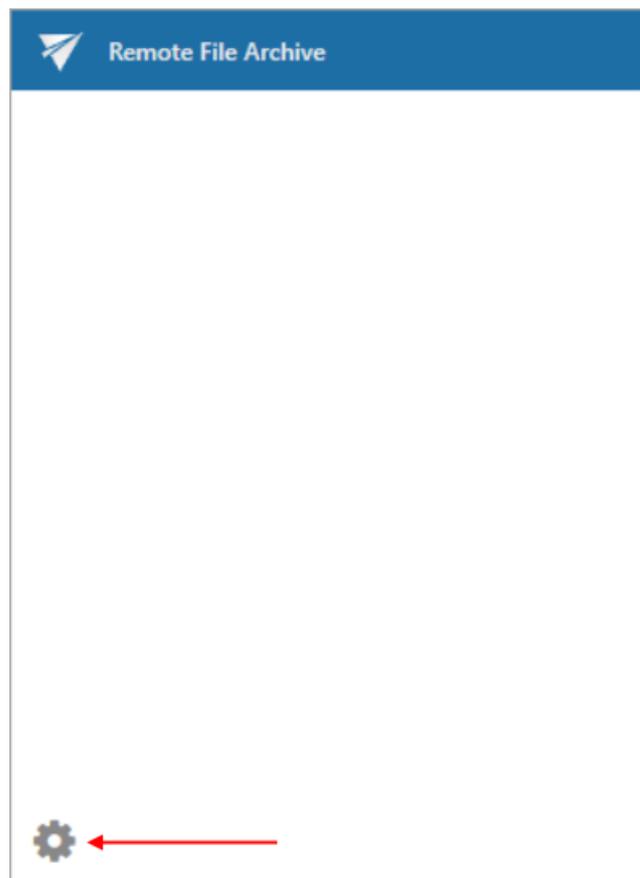


## How to use the Remote File Archiver

In the lower right corner on the taskbar (sometimes it's needed to click on **Show hidden icons**), a blue arrow will appear – this is the icon of Remote FA. Click on it.

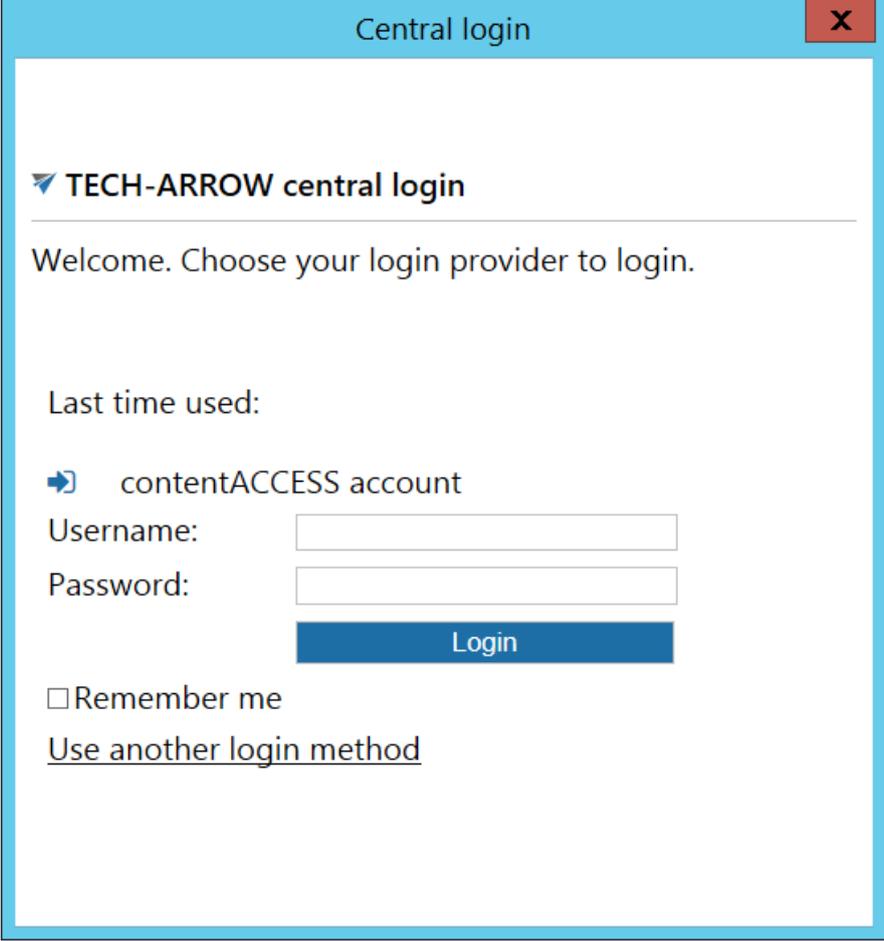


A pop-up window will open. Here it's possible to see the list of items archived by Remote FA (since we haven't archived any files yet, it is empty in our case). Click on the settings button to open the Remote FA settings. It is also possible to open the settings window by right-clicking on the icon and selecting **Settings...** in the context menu.



**Note:** If you were previously logged in, but you logged out of the app, the login pop-up window will appear after this step. You can log in now or you can close the window. If you close it, you will be

able to log in the way as if you were using Remote FA for the first time (read more about logging in in the section [Connection tab](#)). The app will open after this.

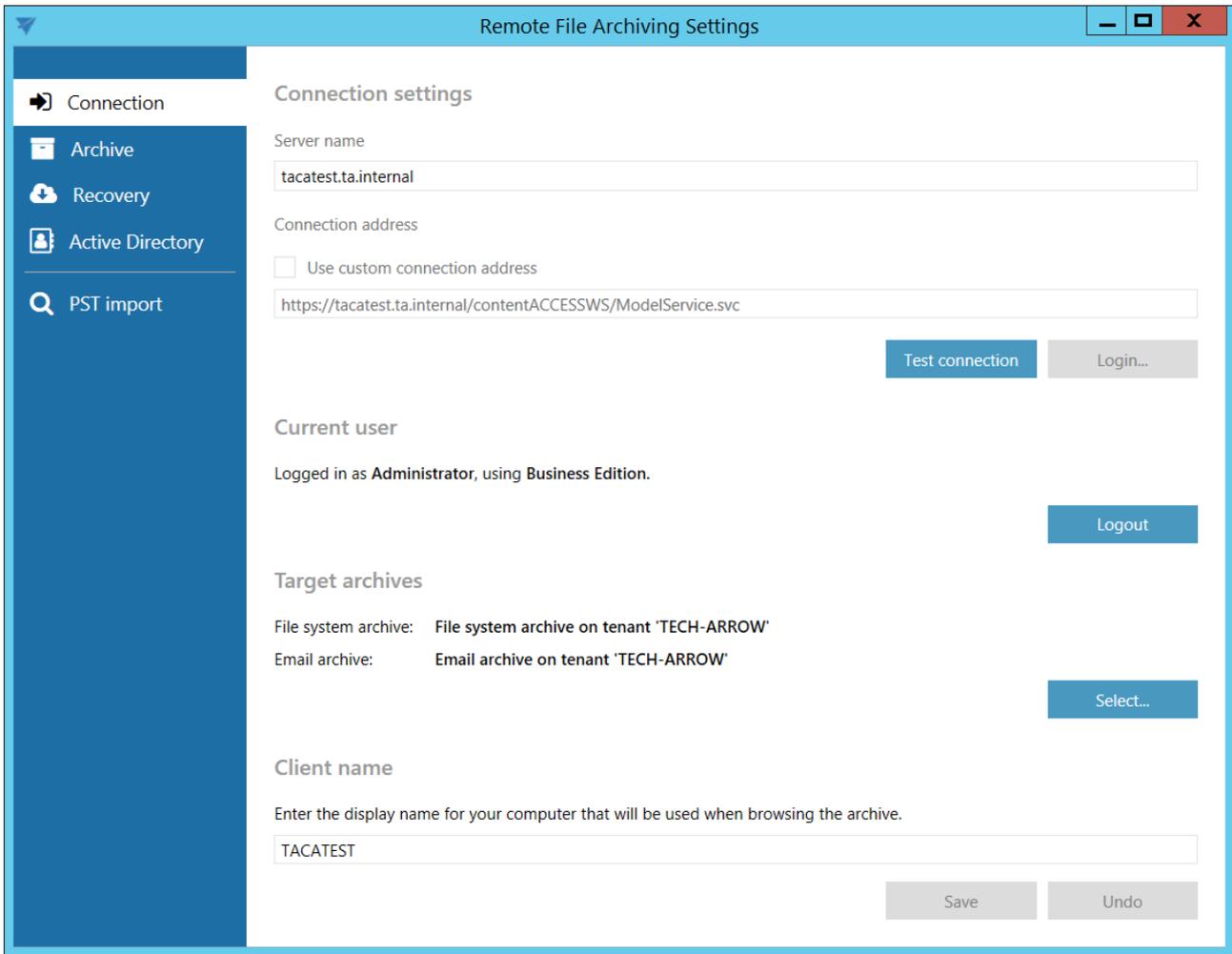


The screenshot shows a dialog box titled "Central login" with a close button (X) in the top right corner. The dialog contains the following elements:

- A header: **TECH-ARROW central login**
- A message: "Welcome. Choose your login provider to login."
- A section titled "Last time used:" with a blue arrow icon pointing to "contentACCESS account".
- Input fields for "Username:" and "Password:".
- A blue "Login" button.
- A checkbox labeled "Remember me".
- A link: [Use another login method](#)

### Connection tab

On the connection tab, the server, where contentACCESS is installed, must be specified.



If you use proxy (contentACCESSWS) with secure (HTTPS) connection to connect to contentACCESS, configure the connection as follows:

- Leave the **Use custom connection address** checkbox unchecked
- Enter the contentACCESS server name into the **Server name** field - with this action the connection URL will be generated automatically

If you use proxy (contentACCESSWS) with unsecure (HTTP) connection to connect to contentACCESS (i.e. you use proxy but do not have a valid certificate), configure the connection as follows:

- Enter the contentACCESS server name into the **Server name** field
- Check the **Use custom connection address** checkbox

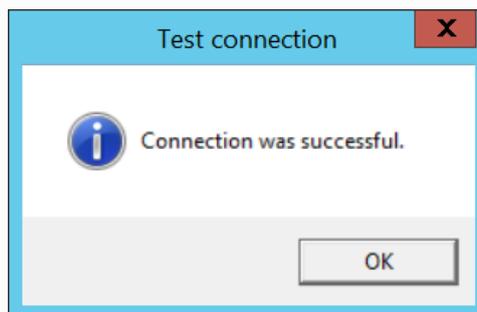


- Enter the HTTP connection URL with the correct server name into the **Custom connection address** field: [http://\[ServerName\]/contentACCESSWS/ModelService.svc](http://[ServerName]/contentACCESSWS/ModelService.svc) (or just delete the “s” from https)

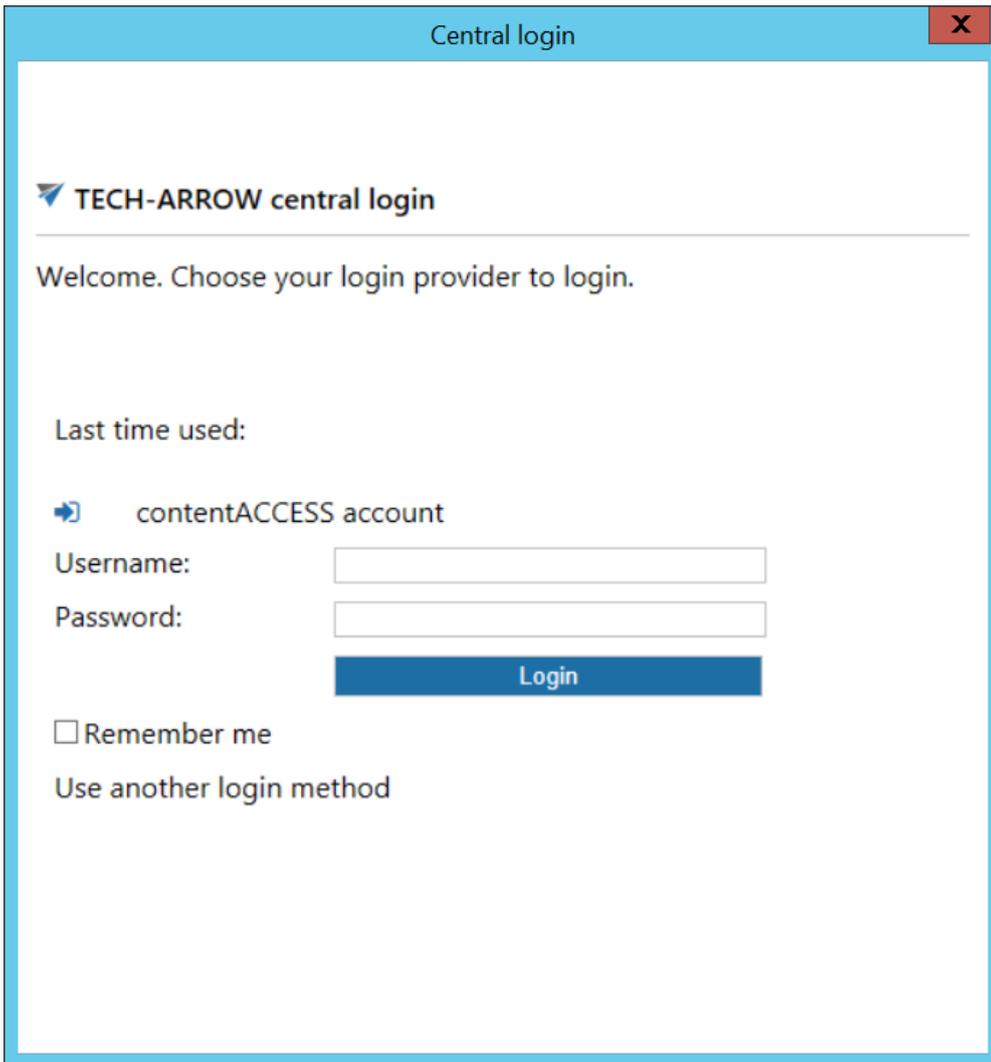
If you use direct connection to connect to contentACCESS (no proxy is installed), configure the connection as follows:

- Enter the contentACCESS server name into the **Server name** field
- Check the **Use custom connection address** checkbox
- Enter the HTTP/HTTPS (appropriate to your configuration) connection URL with the correct server name into the **Custom connection address** field: [http://\[ServerName\]:8736/contentACCESSWS/ModelService.svc](http://[ServerName]:8736/contentACCESSWS/ModelService.svc) (delete the “s” from https and add 8736 port) or [https://\[ServerName\]:8736/contentACCESSWS/ModelService.svc](https://[ServerName]:8736/contentACCESSWS/ModelService.svc) (add the 8736 port)

After setting the connection, click on the **Test connection** button under the custom connection address textbox. If everything was set correctly, this message will appear:



Click on the **Login...** button next to the **Test connection** button. Log in using the Forms method, or choose another login provider previously configured in contentACCESS by clicking on **Use another login method**.



The screenshot shows a window titled "Central login" with a close button (X) in the top right corner. The window content includes the "TECH-ARROW central login" header, a welcome message, and a section for the "contentACCESS account". This section contains fields for "Username:" and "Password:", a "Login" button, a "Remember me" checkbox, and a link for "Use another login method".

After successfully logging in, the current user's name will be displayed. The **Logout** button becomes accessible.

#### Current user

Logged in as **Administrator**, using **Business Edition**.

Logout

In the **Target archive** section, click on the **Select...** button. If you want to use remote file archiving, check the **Enable file archiving** checkbox. From the archive dropdown list, select one of the **previously configured tenants** with **File system archive model**. From the respective dropdown lists, select one of the available **Databases**, one of the available **Storages** and one of the available **Index zones**.



If you want to use PST importing, check the **Enable PST importing** checkbox. From the archive dropdown list, select one of the **previously configured tenants** with **Email archive model**.

**File archive** is allowed by default for every tenant, **Email archive** must be first specifically allowed in the license. In the next tabs, only retentions and schedules that were configured for these tenants can be selected from the dropdown lists.

**Important:** The **Archive tab** and **PST finder tab** will be displayed depending on archives selected in this section – if no tenant with File system archive was selected here, **Archive tab won't be visible**; if no tenant with Email archive was selected here, **PST finder tab won't be visible**.

### Target archives

File system archive: **File system archive on tenant 'TECH-ARROW'**

Email archive: **Email archive on tenant 'TECH-ARROW'**

Select...

X
Select archiving targets

### Select archiving targets

Enable file archiving

Select an existing archive where files will be stored.

File system archive on TECH-ARROW

↻

Database

MNEtestDB

↻

Store

TestingStorage

↻

Index zone

Default index zone

↻

---

Enable PST import

Select an existing archive where PST files will be imported.

Email archive on TECH-ARROW

↻

OK

Cancel

The **Client name** displays the name of the computer that will be shown when viewing the archive. It is possible to change it.

#### Client name

Enter the display name for your computer that will be used when browsing the archive.

TACATEST

**Save your settings.**

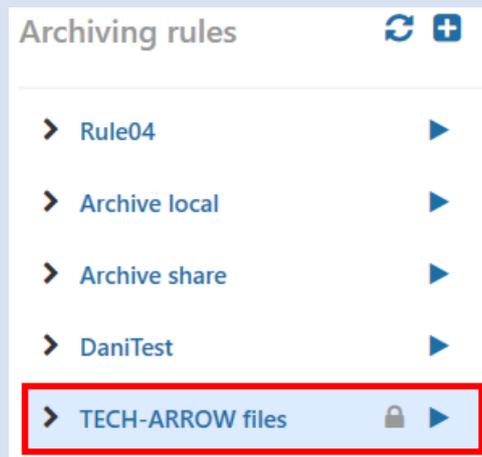


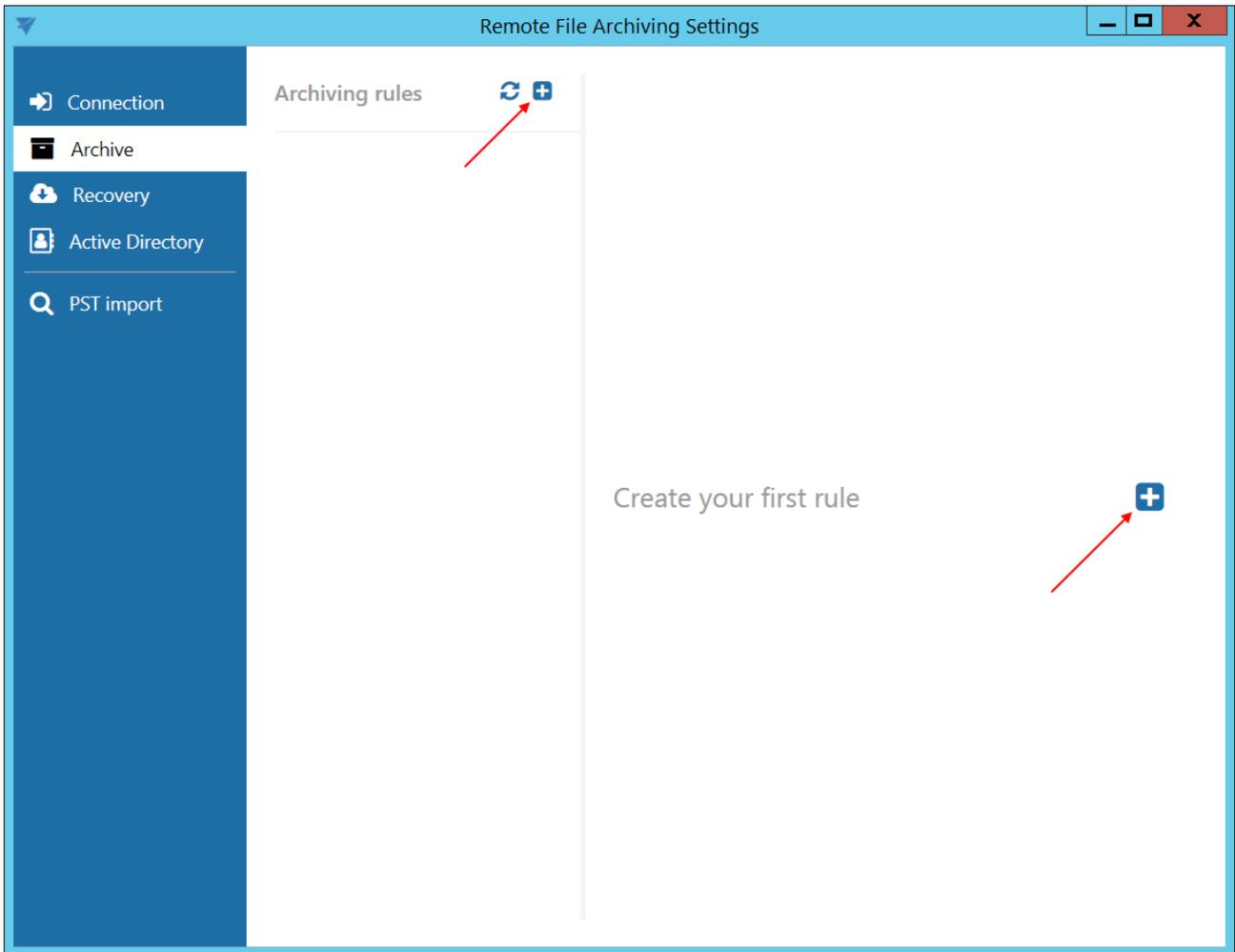
## Archive tab

The archiving rules can be configured on the archiving tab.

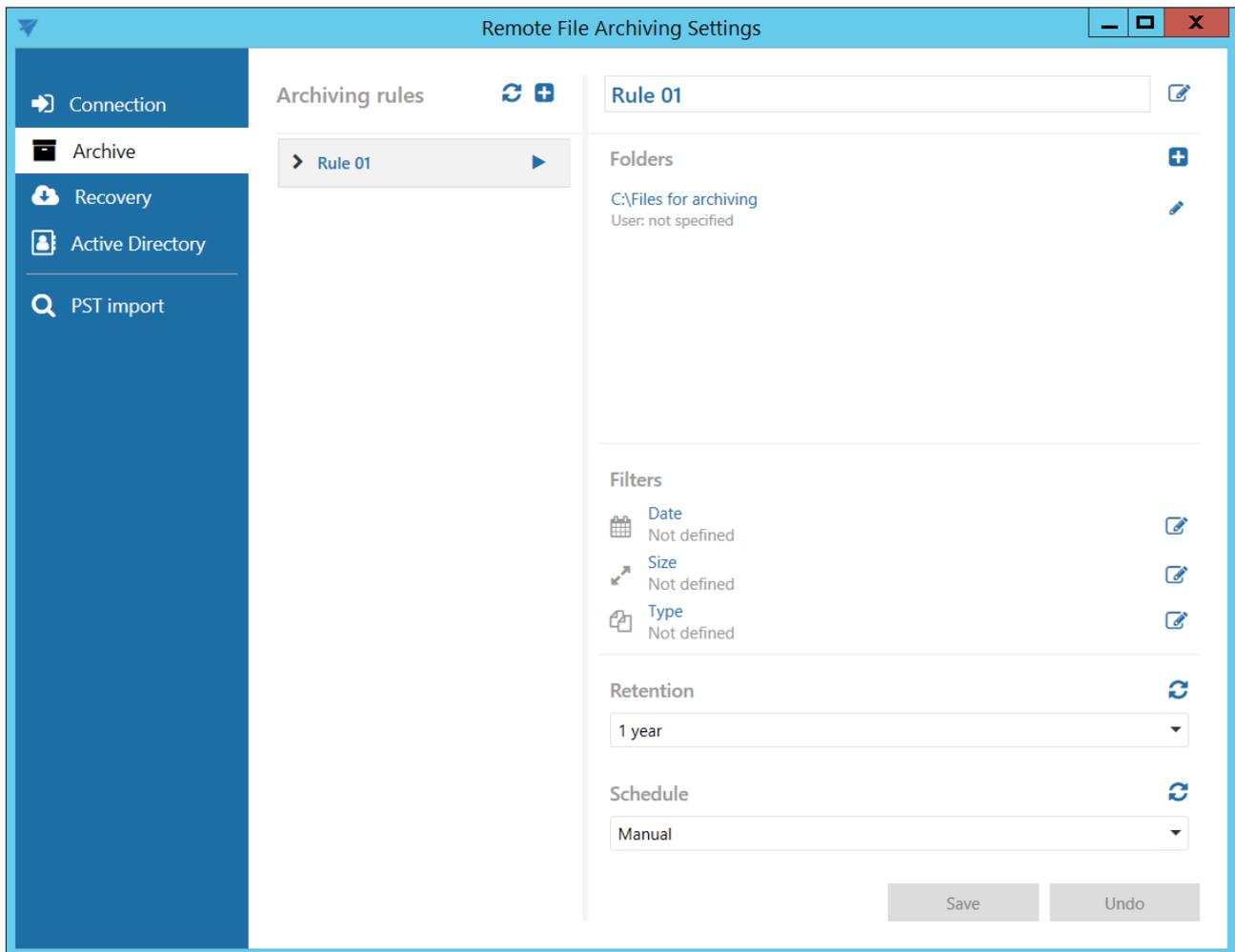
Add a new rule by clicking on the **+** button (the **+** button next to the **Create your first rule** is available only when creating the first rule).

**Note:** A new rule can be also added from **Central Administration**. To read more about this possibility, please check [this](#) section.



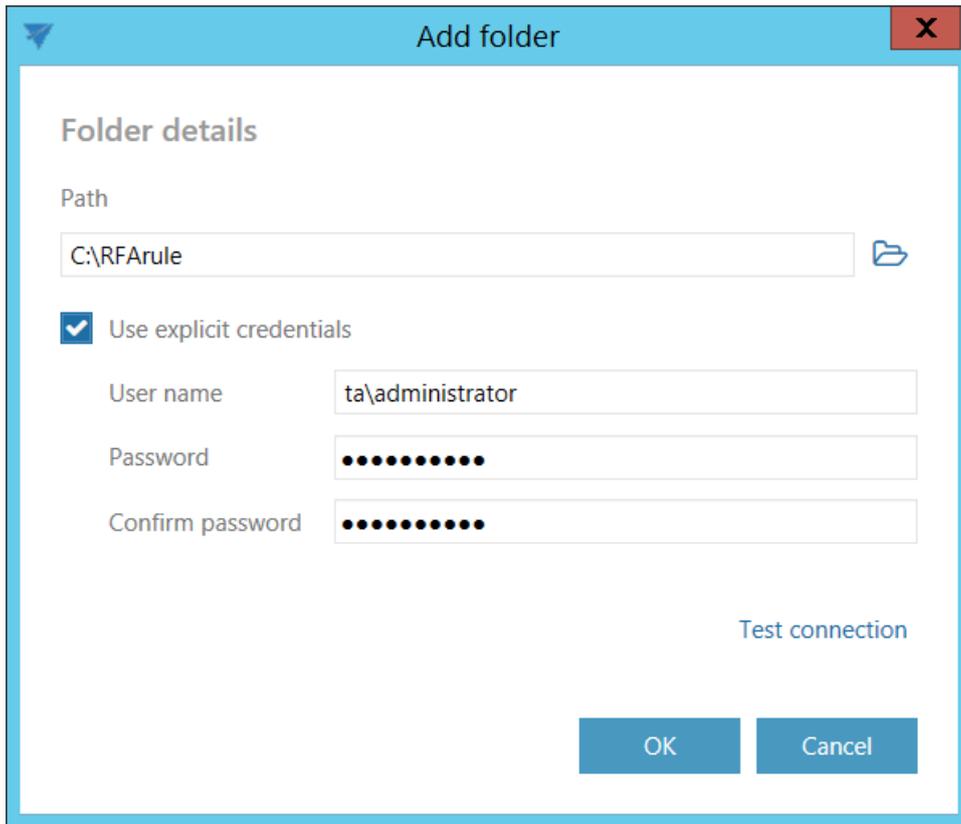


The archiving rules have very similar properties to [File archive jobs](#) in contentACCESS.



### ✓ Folders

In this section the user is required to select the folder(s) where the data to be archived are located. Click on  to specify the folder to be archived.



Enter the UNC path of the shared folder or path of a local folder to the **Path** textbox, or click on the  Browse button and select the folder that you want to archive.

The **GATE.contentACCESS.RemoteFileArchiving.Agent** service is responsible for running the rules. The service is approaching the specified folder under account, under which the service is running. If the folder is accessible to the user running the service, the **Use explicit credentials** checkbox doesn't need to be checked. If the folder is **not** accessible to the user running the service, check the checkbox and enter the credentials of the user/account, which has access to the folder you want to archive.

**Note:** A folder cannot be assigned to a single rule multiple times, so if the user will try to set a new archiving rule with the same folder assigned multiple times, he will get an error when saving the settings at the bottom of the Archive tab.

## ✓ Filters

### Date filter

With this filter the user may select files to process with a specific age. **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 **“Use the creation date for filtering if it is younger than the**



**modification date**” 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 is 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 enhancement can solve the problem. With this feature it is possible to exclude the file with the newer creation date from the archiving process.

The **Modification date** can be **Absolute** or **Relative**. If **Absolute** was chosen, the Remote FA will process files younger/older than the specified date or files with date from the interval set. If **Relative** was chosen, the Remote FA will process files that were created/modified the specified number of days/months/years before the run of the Remote FA. If **Process all files** is selected, the Modification date does not count.

Examples of **filtering**:

**Filter settings**

**File age filter**

- Process all files
- Process files modified before the specified date
- Process files modified after the specified date
- Process files modified between the specified dates

**Modification date**

- Absolute  
10/18/2017
- Relative  
0 days

Use the creation date for filtering if it is younger than the modification date

OK Cancel

### Filter settings

**File age filter**

- Process all files
- Process files modified before the specified date
- Process files modified after the specified date
- Process files modified between the specified dates

---

**Modification date**

- Absolute
- Relative

---

- Use the creation date for filtering if it is younger than the modification date

Filter settings
✕

### File age filter

Process all files  
 Process files modified before the specified date  
 Process files modified after the specified date  
 Process files modified between the specified dates

---

**From**

Absolute

10/18/2017
15

**To**

Absolute

10/21/2017
15

---

Relative

2

and

5

days

---

Use the creation date for filtering if it is younger than the modification date

OK
Cancel

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 and save space. You can choose from the filtering types (**All**, **Larger than**, **Smaller than**, or **Having size between**), enter the size in kilobytes, megabytes or gigabytes and click **OK**.

Examples of **filtering**:



**Filter settings** [x]

**File size filter**

Process all files

Process files larger than

0 [up/down] KB [v]

Process files smaller than

0 [up/down] KB [v]

Process files having size between

0 [up/down] KB [v]

0 [up/down] KB [v]

OK Cancel

**Filter settings** [x]

**File size filter**

Process all files

Process files larger than

0 [up/down] KB [v]

Process files smaller than

0 [up/down] KB [v]

Process files having size between

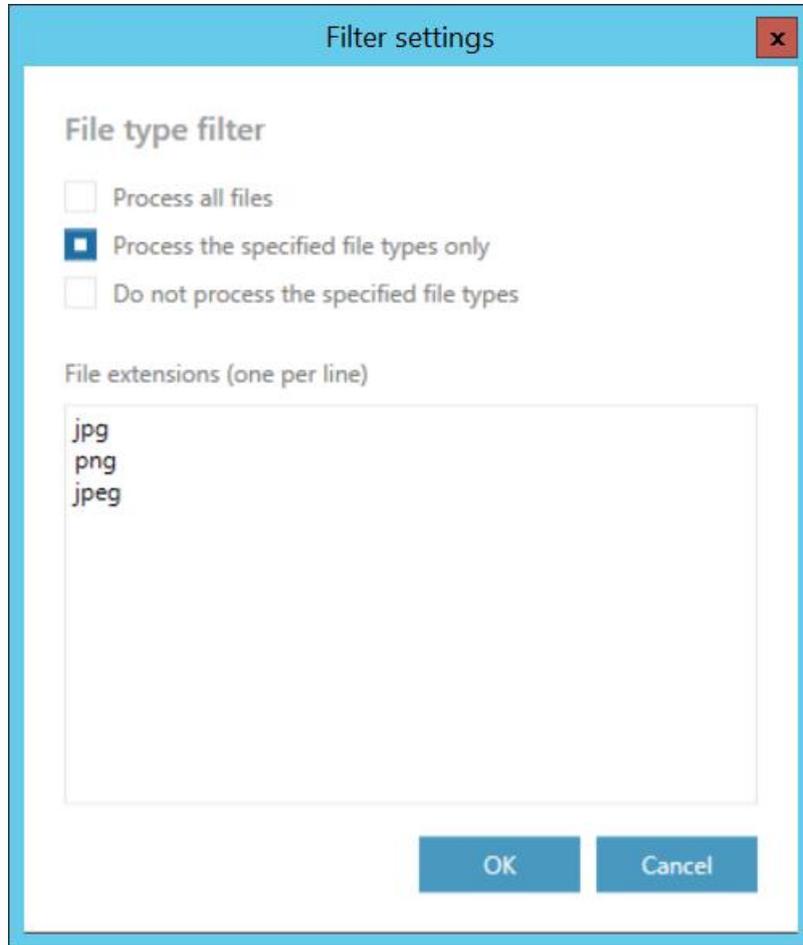
64 [up/down] KB [v]

2 [up/down] MB [v]

OK Cancel

## Type filter

This filter was improved to select certain file types for processing. The user may select and specify the file types, which will be/won't be processed.



### ✓ Retention

Under retention settings the user may select a previously configured time period from the dropdown list. During this time it will be disabled 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. It is possible to refresh the list of retentions by clicking on the  button.

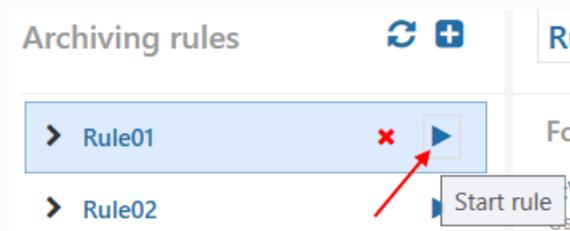


### ✓ Schedule

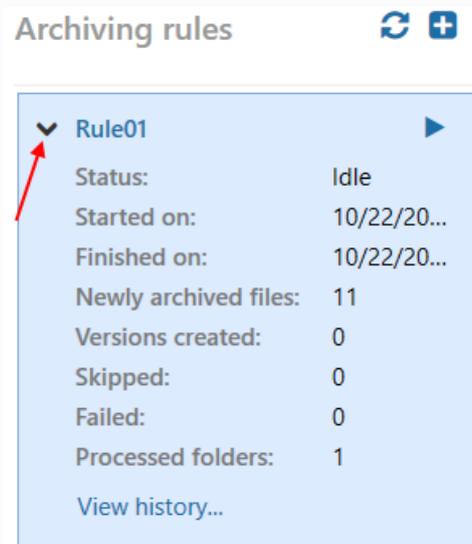
In this step the running times of the archive rule must be selected. It is possible to select only a schedule that was previously configured in contentACCESS. It is possible to refresh the list of schedules by clicking on the  button.



After setting all the parameters, **save your settings**. Start the rule by clicking on the button next to its name.



It is possible to view the details of the last run of the selected rule.



By clicking on [View history...](#), it is possible to view the last run of the rule in more details. The pop-up window will show exactly which file was newly archived, which file had a version created and which file couldn't be processed (was failed) on the respective tabs. The **general error** shows the error message if the rule suddenly crashed (connection fail etc.).

Execution history

-
□
X

Execution history of "Test"

|                   |                      |
|-------------------|----------------------|
| Started on        | 6/14/2018 3:40:39 PM |
| Finished on       | 6/14/2018 3:40:48 PM |
| Duration          | 0:00:09              |
| Processed folders | 1                    |
| Skipped files     | 0                    |
| General error     | None                 |

| Newly archived files (11)                                   | Versions created (0) | Failed files (0) |
|---|----------------------|------------------|
| Path  | Date processed       | Size             |
| C:\00\microsoft-e1452011064246.jpg                          | 6/14/2018 3:40:44 PM | 230              |
| C:\00\ms-office.jpg   | 6/14/2018 3:40:46 PM | 21 K             |
| C:\00\MS_cloud.jpg  | 6/14/2018 3:40:46 PM | 81 K             |
| C:\00\myca_185325812-small.jpg                              | 6/14/2018 3:40:47 PM | 172              |
| C:\00\office-101-badge.png                                  | 6/14/2018 3:40:47 PM | 4 KB             |
| C:\00\office-insider-pc.jpg                                 | 6/14/2018 3:40:47 PM | 43 K             |
| C:\00\office-search.jpg                                     | 6/14/2018 3:40:47 PM | 66 K             |
| C:\00\pros-and-cons-2028471_1920-e1493803542700-300x179.jpg | 6/14/2018 3:40:47 PM | 14 K             |

Close

### Recovery tab

On this tab, the already archived folders can be explored. The view and actions are similar to those in [contentWEB](#).

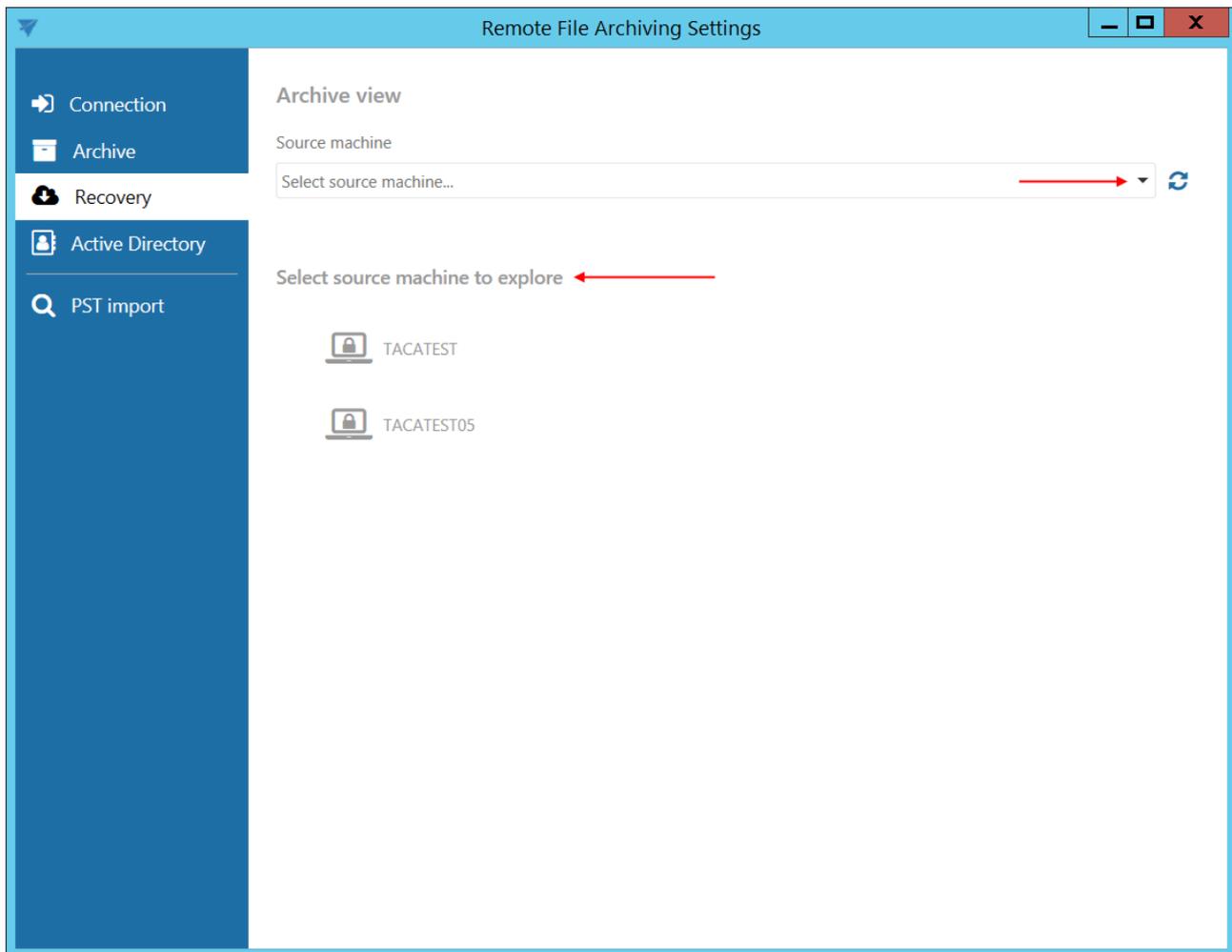
Select a source machine from the dropdown list or from the list under **Select source machine to explore**. The machines are marked as follows:



- fully accessible



- read only, archived by other agent



The following tasks are available:

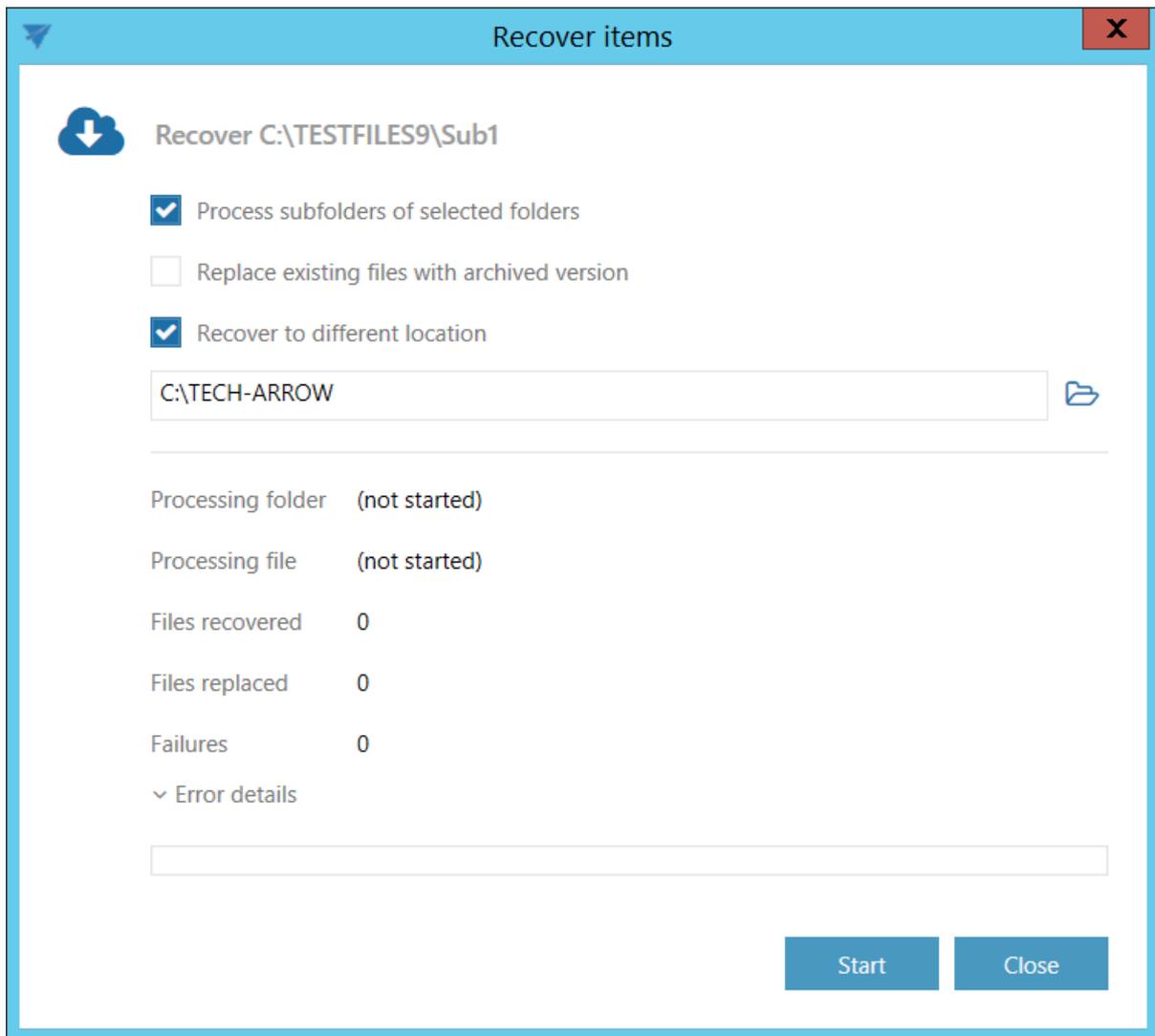
**1. Recover** – recover deleted files from the archive or restore file versions from the archive.

It is also possible to recover the files to location different from the original one. To do this, check the **Recover to different location** checkbox, enter the UNC path of the shared folder or path of a local folder to the textbox, or click on the  Browse button and select the target folder.

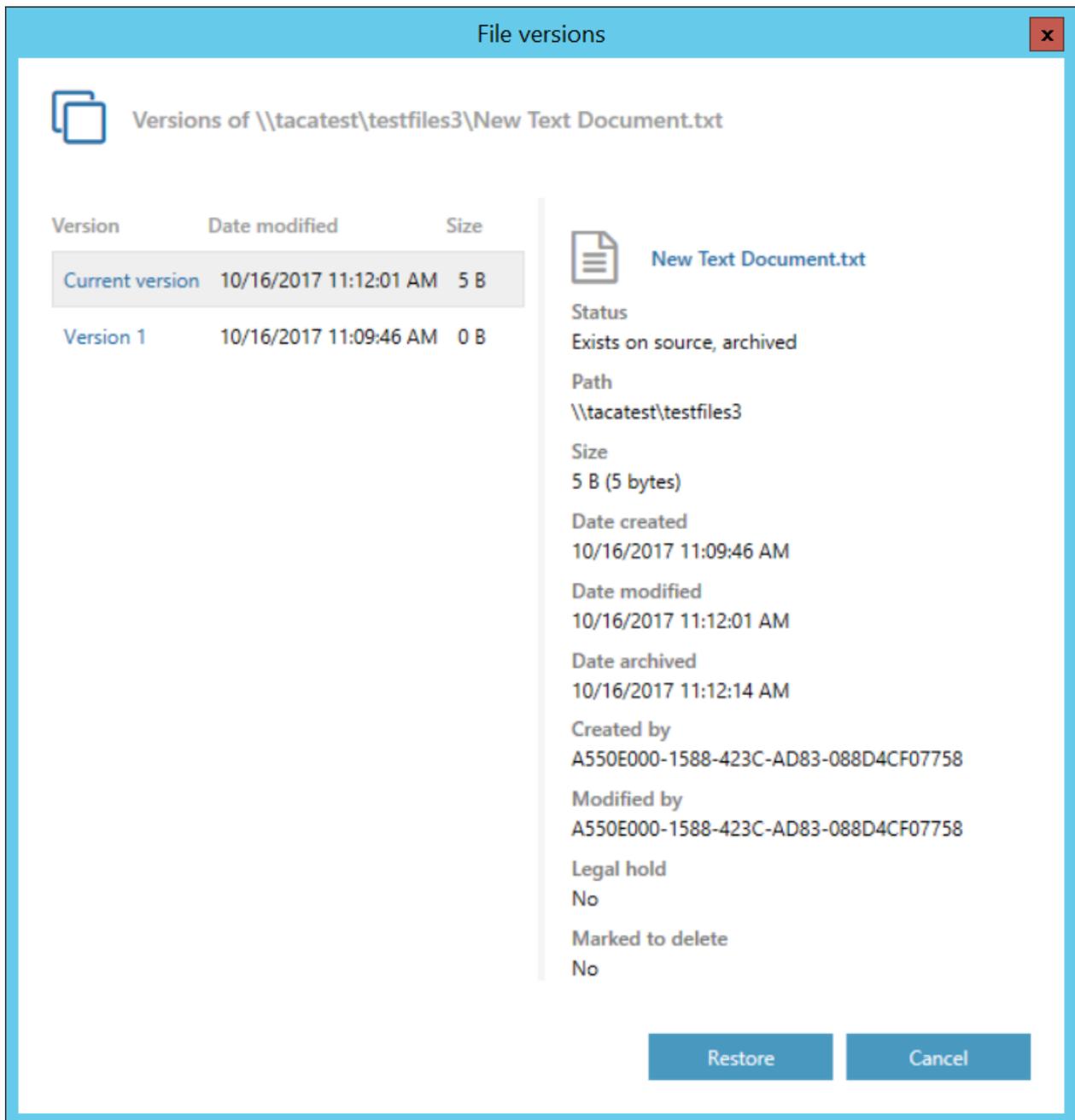
**Note:** The recover function works only for the files and folders selected on the right side, not for the folder structure on the left side.



| Name  | Date modified       |
|---|---------------------|
| Sub1  |                     |
| Sub2  |                     |
| 38010_mahou.jpg                             | 5/10/2017 1:11:44 F |
| 960x0.jpg                                   | 1/18/2017 4:25:52 F |
| a35bb6d3af7c808a.jpg                        | 6/5/2017 1:10:08 PI |
| Address book modifications.docx             | 1/22/2018 6:18:11 F |
| bdb3d7041f7adb74399289a440f0f275.jpg        | 2/1/2017 12:13:19 F |
| business and burgers.png                    | 3/3/2017 1:32:49 PI |
| cloud.mail_jpg                              | 2/7/2017 2:40:14 PI |
| contentACCESS.Email_Archive.be_safe_1-1.jpg | 1/20/2017 2:41:03 F |
| Testing.rar                                 | 1/19/2018 5:26:43 F |
| Versions testing.txt                        | 6/20/2018 11:20:43  |



2. Show versions – if the file has versions, this will show them



**3. Show properties** – shows properties of the selected item, like date, path, size, etc.

**Note:** Properties can be viewn also by clicking on the three dots button on the right side.

|   |                        |        |
|---|------------------------|--------|
| business and burgers.png                    | 3/3/2017 12:32:49 PM   | 52 KB  |
| camera.png                                  | 6/21/2017 11:56:31 AM  | 647 KB |
| cloud.mail_jpg                              | 2/7/2017 1:40:14 PM    | 15 KB  |
| contentACCESS.Email_Archive.be_safe_1-1.jpg | 1/20/2017 1:41:03 PM   | 135 KB |
| New Text Document.txt                       | 10/16/2017 11:12:01 AM | 5 B    |

4. **Hide/show inactive items** - active/inactive item view can be applied from here

5. **Refresh** - the button is used to manually update the item list

Items are marked with different colors, depending on their availability:

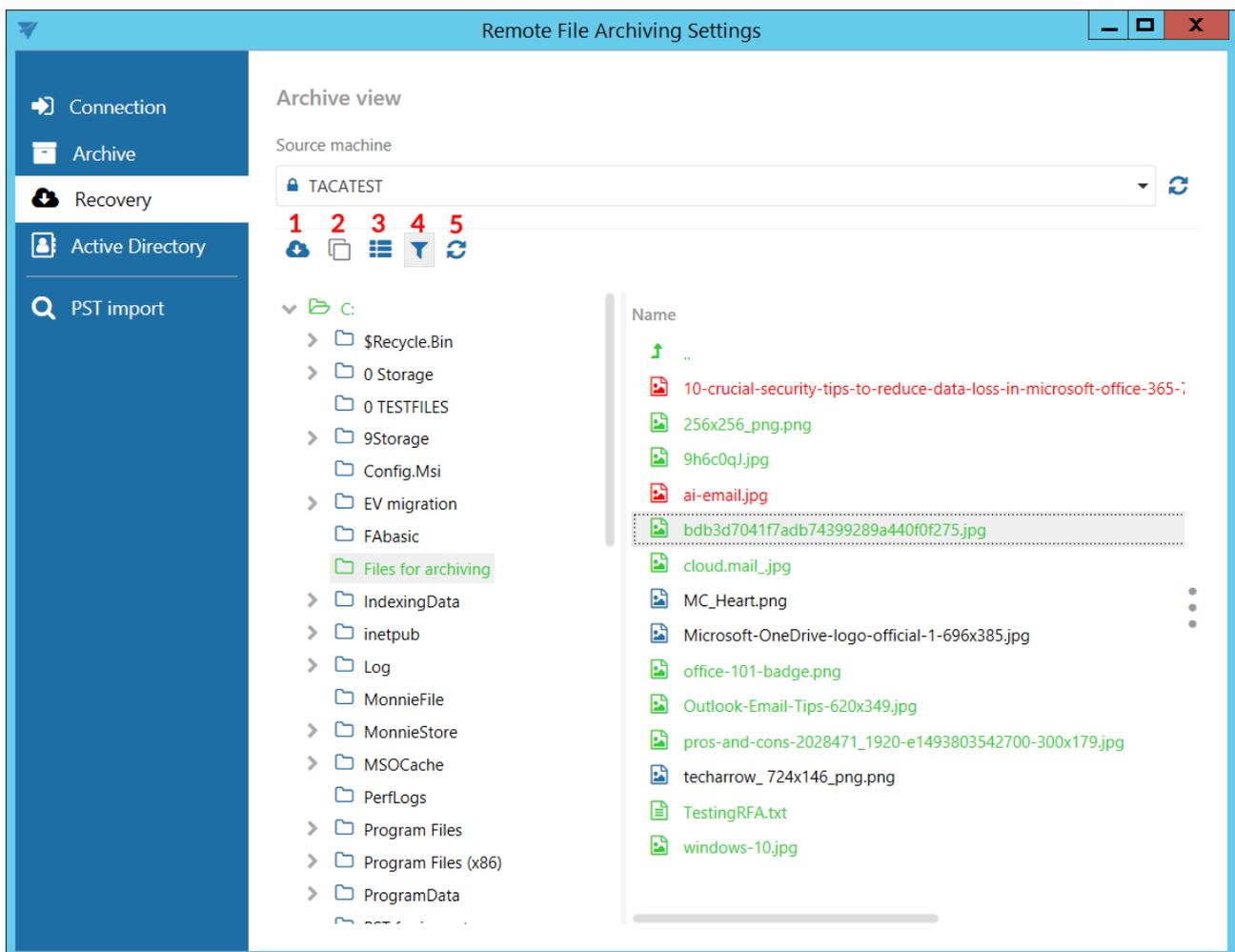
Black – item is available in the source location

Red – item is available only in the archive

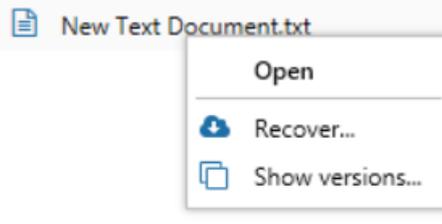
Green – item was archived, available also in the source location

Gray – inactive item - available in the source location, but was deleted from the archive

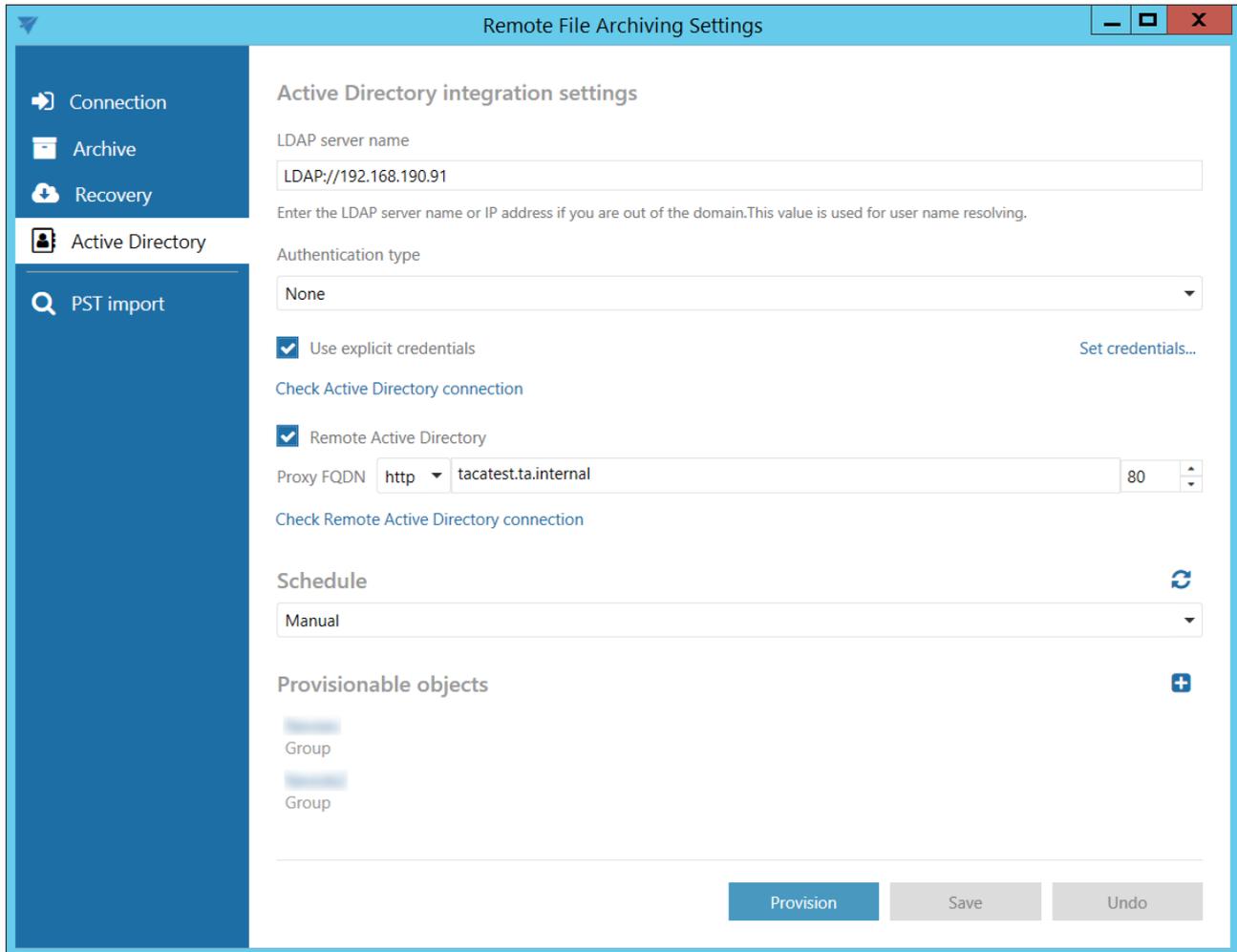
The selected item can be opened by double-clicking on it.



After right-clicking on an object, the context menu with available tasks opens.



## Active Directory tab



Remote File Archiving Settings

**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 Set credentials...

[Check Active Directory connection](#)

Remote Active Directory

Proxy FQDN

[Check Remote Active Directory connection](#)

**Schedule** ↻

**Provisionable objects** +

### Active Directory integration settings

The remote agent needs to access Active Directory in order to be able to provision local Active Directory users to contentACCESS. During the provisioning process, the local users are re-created in contentACCESS with **External Active Directory** authentication. This will allow the users to log in to contentACCESS using their local AD credentials.

Enter the required LDAP server name. If explicit credentials need to be used to connect to the active directory, check the **Use explicit credentials** checkbox and click on **Set credentials...** on the right.

LDAP server name

LDAP://192.168.190.91/dc=ta,dc=internal

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

Set credentials...

Check Active Directory connection

Enter the credentials and then click on **Check credentials** to verify if they are valid. If yes, click **OK**.

**Set credentials** ✕

**Enter credentials**

User name

Password

Confirm password

[Check credentials](#)

OK
Cancel

Click on **Check Active Directory connection** to see, if everything was set correctly.

LDAP server name

LDAP://192.168.190.91/dc=ta,dc=internal

Enter the LDAP server name or IP address if you are out of the domain. This value is used for user name resolving.

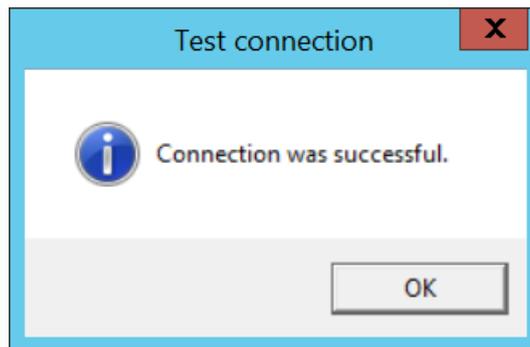
Authentication type

None

Use explicit credentials

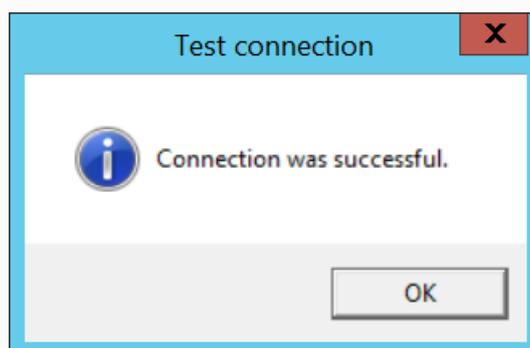
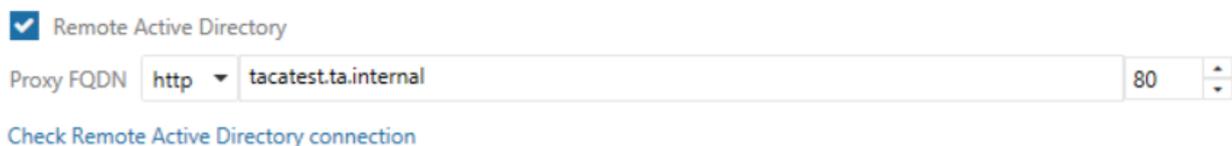
Set credentials...

Check Active Directory connection



During the provisioning, **External Active Directory type logins** are created for users of the selected groups. To allow the users to log in to contentACCESS using their local AD account, the authentication provider (contentACCESSWS) must be installed into the local domain and must be accessible for contentACCESS from outside. The external URL of the authentication proxy should be set here (for example: <https://caAuth.company.com:981>). **Please note, that this public URL must be then forwarded to the machine (and port), where contentACCESSWS was installed and through which contentACCESS can reach the service.** The URL must be published over HTTPS to avoid sniffing the user's credentials.

Click on **Check Remote Active Directory connection** to see, if everything was set correctly.



## Schedule

In this step the running times of the archive rule must be selected. It is possible to select only a schedule that was previously configured in contentACCESS. It is possible to refresh the list of schedules by clicking on the  button.

## Schedule



TaskRunnerScheduler

### Provisionable objects

The provisioning job synchronizes the Active directory with contentACCESS. When the provisioning job is started, it automatically **adds the new Active Directory users into contentACCESS** based on provisioning settings. The provisioned users will automatically get **log on rights for Remote FA** and the **External AD login provider** will be assigned to them.

**Note:** External AD login provider must be enabled in contentACCESS before provisioning.

To add object, click on **+** and specify the object(s) in the respective dialog. You can select a **group**, of which objects will 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)

Add provisionable object
✕

### Provisionable object

Select objects that will be automatically provisioned. You can select a group to synchronize its members or an Active Directory container to synchronize all users inside that container.

Object name

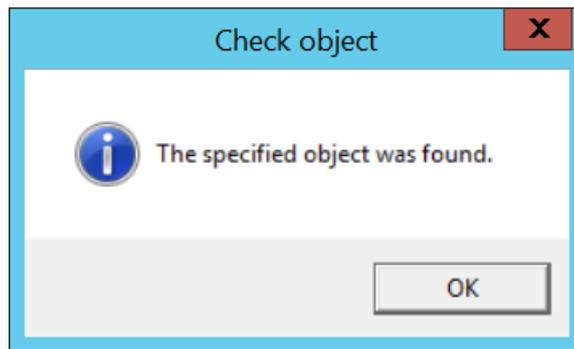
Example: Administrators or CN=Users,DC=domain,DC=com

Object type

[Check object](#)

OK
Cancel

Click on **Check object** to verify if the specified object can be found.



**Note:** Do not specify some built-in groups (such as Domain Users, Users etc.) as provisionable objects. These groups use a computed mechanism based on the primary group of the user to determine membership and most probably will not contain any members by default.

After specifying the objects to be provisioned, click on **Save** and then on **Provision**. After the provisioning is finished, you can verify the created users and logins in [contentACCESS Central Administration](#).

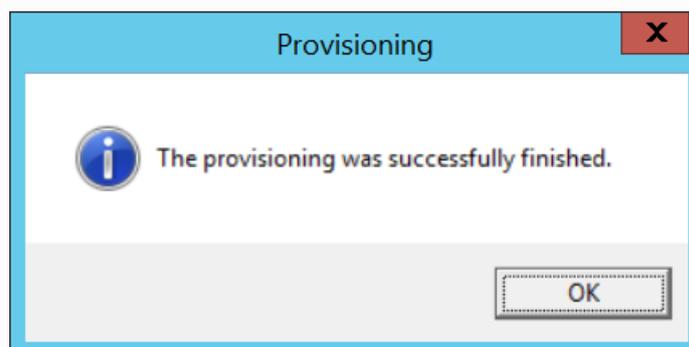
#### Provisionable objects

Administrators  
Group

Provision

Save

Undo

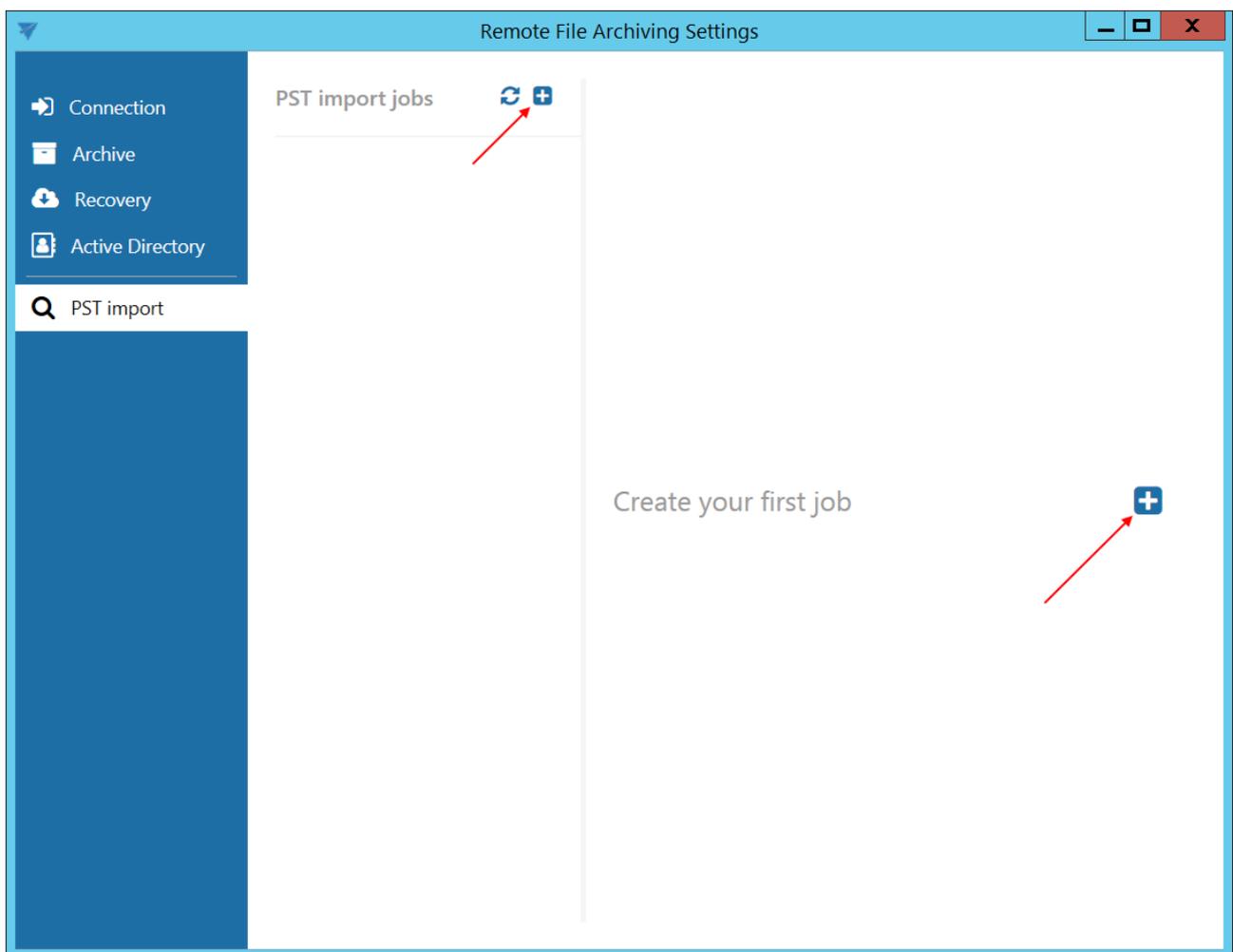
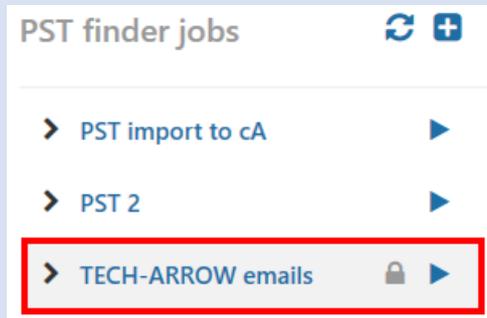


#### PST import tab

A new job can be added by clicking on the  button (the  button next to the **Create your first job** is available only when creating the first job). This job is used for uploading PST files to the contentACCESS server.

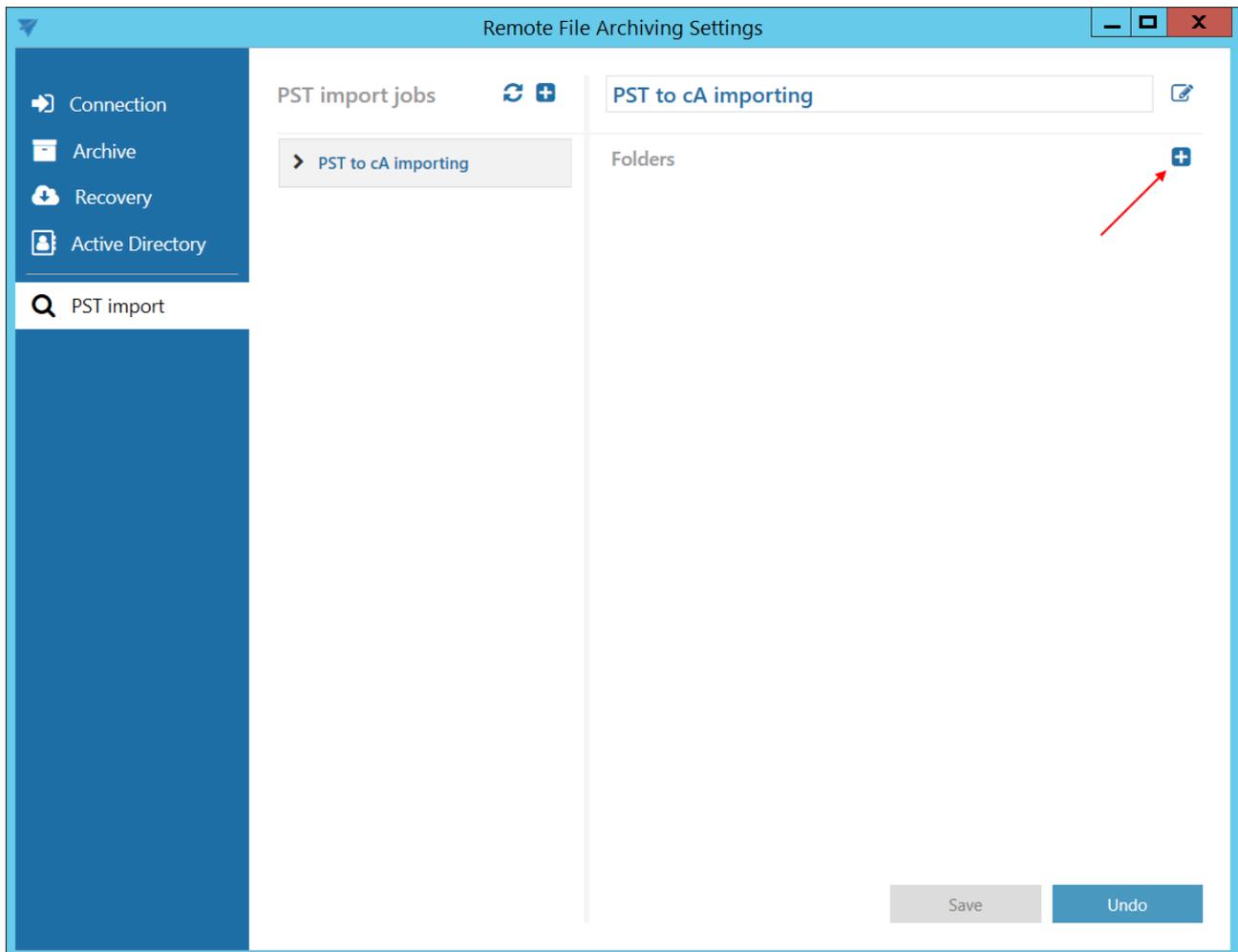


**Note:** A new job can be also added from **Central Administration**. To read more about this possibility, please check [this](#) section.



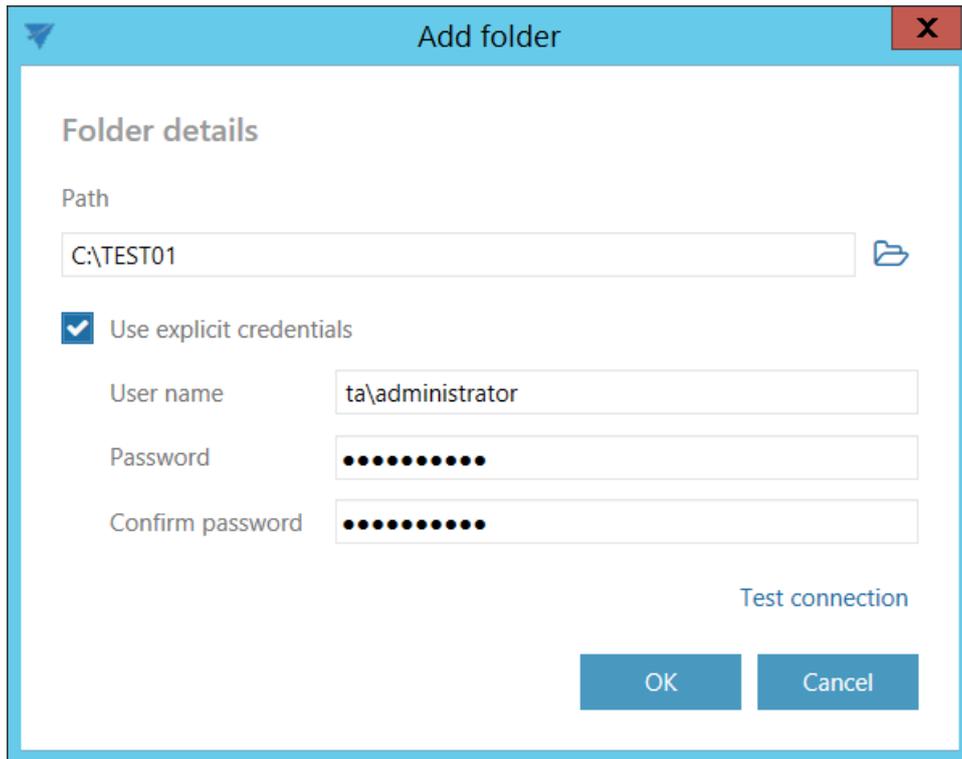
✓ **Folders**

In this section the user is required to select the folder(s) where the PST files to be uploaded are located. Click on **+** to specify the folder.

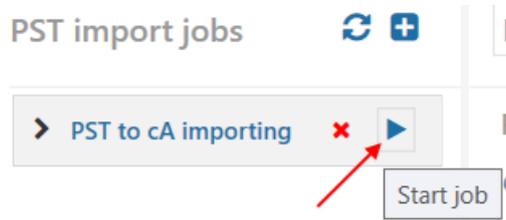


Enter the UNC path of the shared folder or path of a local folder to the **Path** textbox, or click on the  Browse button and select the folder containing the PST files that you want to process.

The **GATE.contentACCESS.RemoteFileArchiving.Agent** service is responsible for running the jobs. The service is approaching the specified folder under account, under which the service is running. If the folder is accessible to the user running the service, the **Use explicit credentials** checkbox doesn't need to be checked. If the folder is **not** accessible to the user running the service, check the checkbox and enter the credentials of the user/account, which has access to the folder with PST files that you want to process.



Save your settings. Start the job by clicking on the button next to its name.



It is possible to view the details of the last run of the selected job.



## PST import jobs



▼ PST to cA importing ▶

|                    |             |
|--------------------|-------------|
| Status:            | Idle        |
| Started on:        | 10/22/20... |
| Finished on:       | 10/22/20... |
| Added:             | 3           |
| Updated:           | 0           |
| Uploaded:          | 0           |
| Skipped:           | 0           |
| Failed:            | 0           |
| Processed folders: | 1           |

[View history...](#)

By clicking on [View history...](#), it is possible to view the last run of the job in more details. The pop-up window will show exactly which file was newly processed and which file couldn't be processed (was failed) on the respective tabs. The **general error** shows the error message if the job suddenly crashed (connection fail etc.).

Execution history
-
□
X

### Execution history of "PST import to cA"

|                   |                      |
|-------------------|----------------------|
| Started on        | 6/28/2018 3:26:28 PM |
| Finished on       | 6/28/2018 3:26:34 PM |
| Duration          | 0:00:05              |
| Processed folders | 2                    |
| Skipped files     | 0                    |
| General error     | None                 |

**Processed files (3)**

| Path                         | Date processed       | Size |
|------------------------------|----------------------|------|
| C:\PST import\ABAL.pst       | 6/28/2018 3:26:29 PM | 0 B  |
| C:\PST import\████_Inbox.pst | 6/28/2018 3:26:32 PM | 0 B  |
| C:\PST import\Lsl.pst        | 6/28/2018 3:26:34 PM | 0 B  |

**Failed files (0)**

Close

PST files processed here can be later used in contentACCESS PST import.

## RFA use-cases

RFA serves many different types and sizes of customers and many different configurations. The goal of this section is to describe the basic use-cases and the possible configurations for RFA.

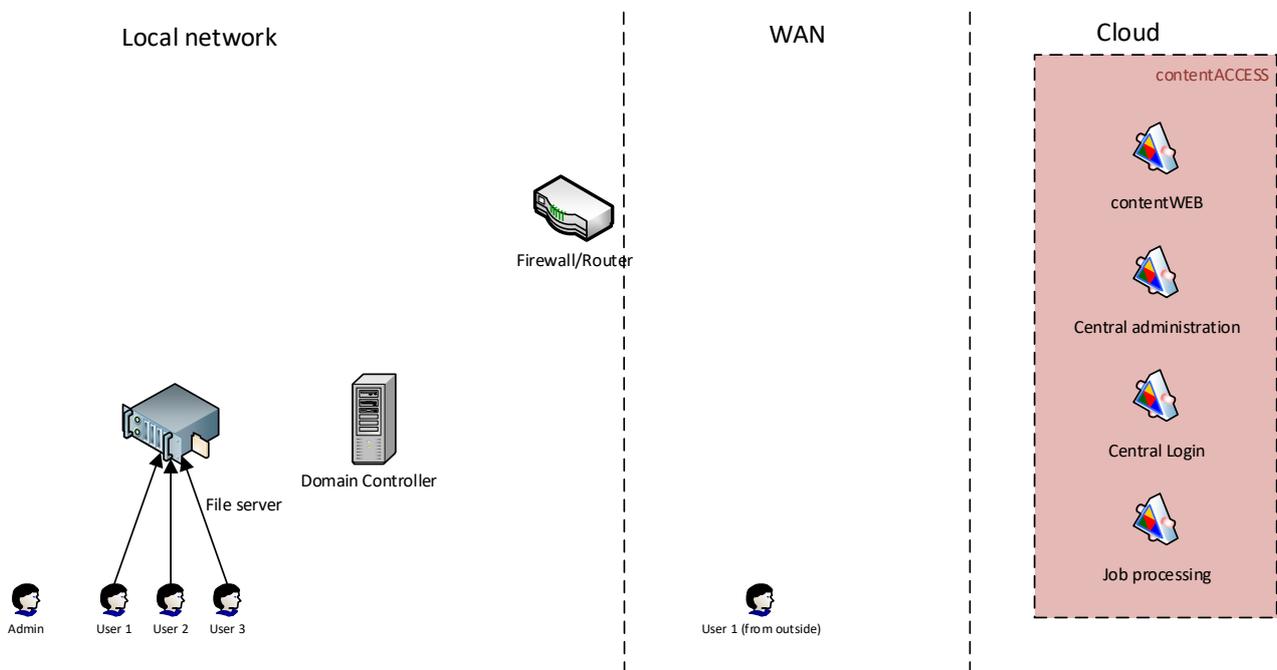
The RFA component for contentACCESS was initially developed to allow on-site customers to archive their local file systems into a contentACCESS environment hosted in the cloud (as a



service, SaaS). The solution allows archiving local file servers, workstations that are domain joined and also single workstations without a domain (small companies, up to 20 employees).

## Archiving common shares

In this use-case, the customer has a domain, into which the users and workstations are joined. The domain has one or more file shares, where the users are storing their documents. The shares are commonly accessed by all users, while the different access levels are handled by the **Windows file security**. The access levels are mostly set on folder level, mainly on higher levels, while the files and subfolders are inheriting the permissions from the parent levels. The users are assigned to different groups and the file security is set based on groups.



## Solution

In this approach, the administrator will choose a server (the so called “archive server”), where RFA will be deployed. RFA will connect to contentACCESS (running in the cloud) using a user with at least tenant administrator level permissions. This user will be able to register the root folder (i.e. the UNC share to archive) and will do the archiving as well.

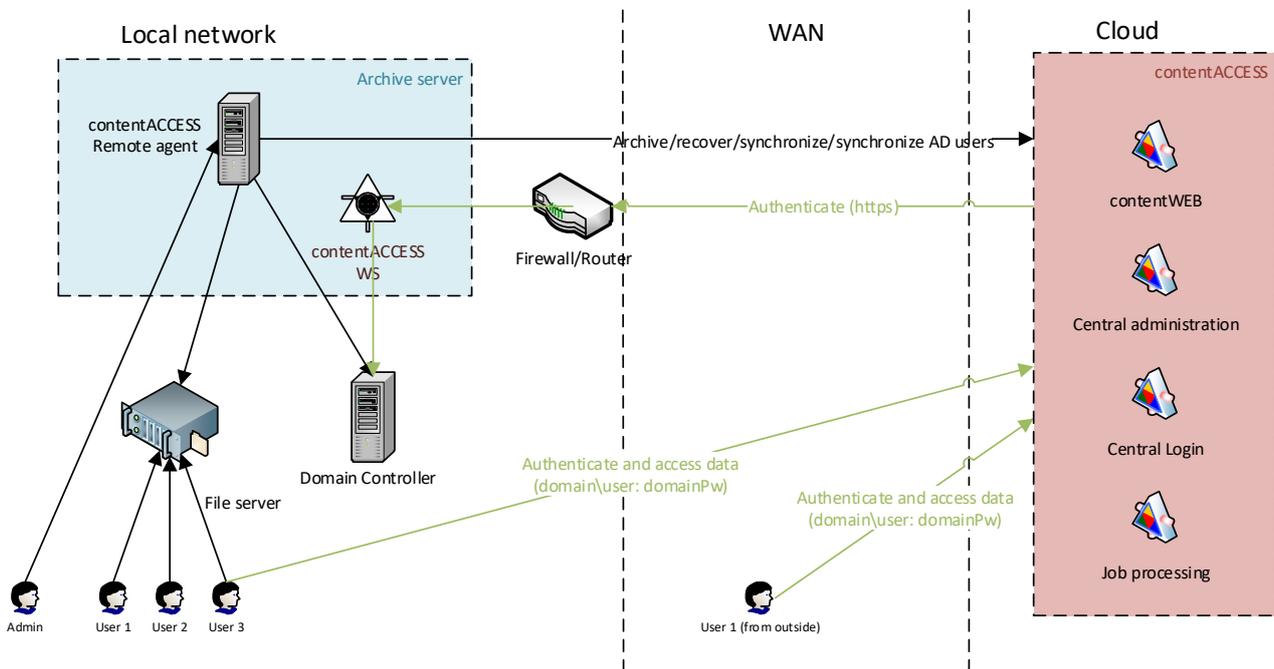
Once RFA is connected, **the administrator can configure the rules:** which folder will be archived and the archiving criteria. He can define as many file shares and rules as he wants. At this point, the

archiving is already achieved, the configured folders will be periodically scanned and archived to contentACCESS.

The only person who has access to the archived data at this point is the **administrator**. He can use the RFA client from the “archive server” to access the data or any other contentACCESS client application (contentWEB, officeGATE, contentACCESS Mobile). To log in, he will use his privileged contentACCESS account.

If the administrator wants to grant access to archived files for end users, **the user provisioning and authentication proxy** must be configured (part of RFA). The user provisioning will automatically create contentACCESS users for all configured users (with External active directory login type) and the authentication proxy will allow the users to log in with their domain credentials to contentACCESS. In this scenario, the user must select **External Active Directory** login type on the contentACCESS login page and enter his AD credentials (domain\user and the password).

Once the users are logged in to the system, the server will apply security trimming on the files and folders based on the source permissions, considering the AD group membership as well. This means that **the user will see only those folders and files to which he has access on the source system**.



## Authentication



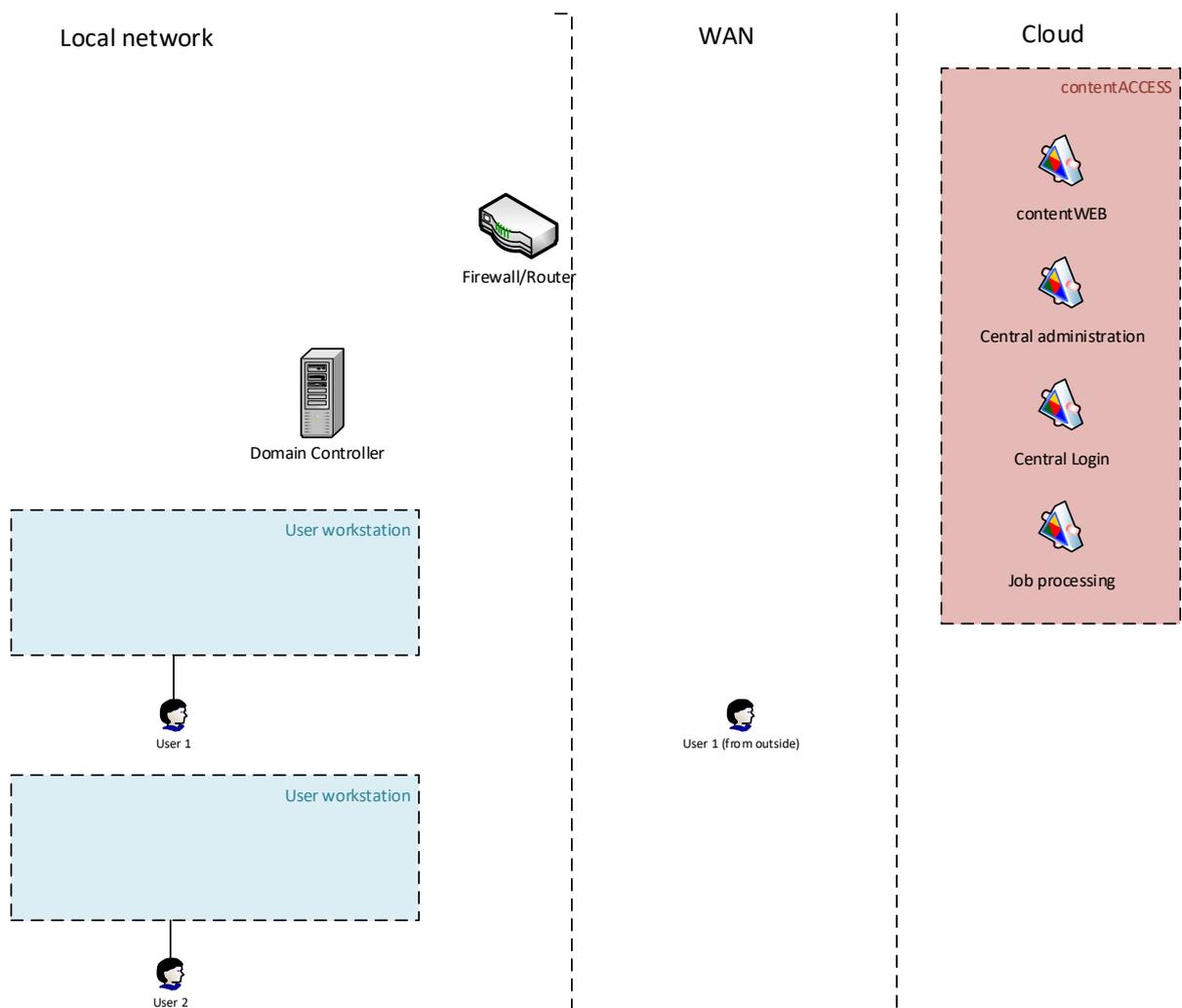
External Windows logins are created for the users that are provisioned using the RFA provisioning. The authentication is performed via the RFA authentication proxy.

### Data access

The users have automatic access to all accessible folders and files in the archive. The built-in domain groups like domain admin and domain users are not supported. Local users and groups are also not supported by the permission evaluation.

### Archiving user workstations (domain joined)

In this use case, the customer does not have a common file share where the users are storing data, but **every single user is using his workstation(s) to store files**. As these files are not backed up regularly, it is very critical to have an automated solution that will archive the files to avoid data loss during hardware crashes. The workstations are joined into a domain and the users are using their domain accounts to access their files and workstations.



## Solution

The administrator needs to prepare a GPO package, which will deploy the RFA together with the configuration file on workstations. The configuration file can be downloaded from [Central Administration](#) (File archive -> remote agents). The configuration file will specify the connection parameters and the default settings for the archiving. The configuration file must be deployed together with the RFA setup and must be copied to folder “C:\Windows\SysWOW64\config\systemprofile\AppData\Roaming\TECH-ARROW\RFAConfiguration.xml” (on the workstation). Please note that the configuration file path can be different based on the user under which the RFA service is running. By default, the RFA service will run under “local system” user.

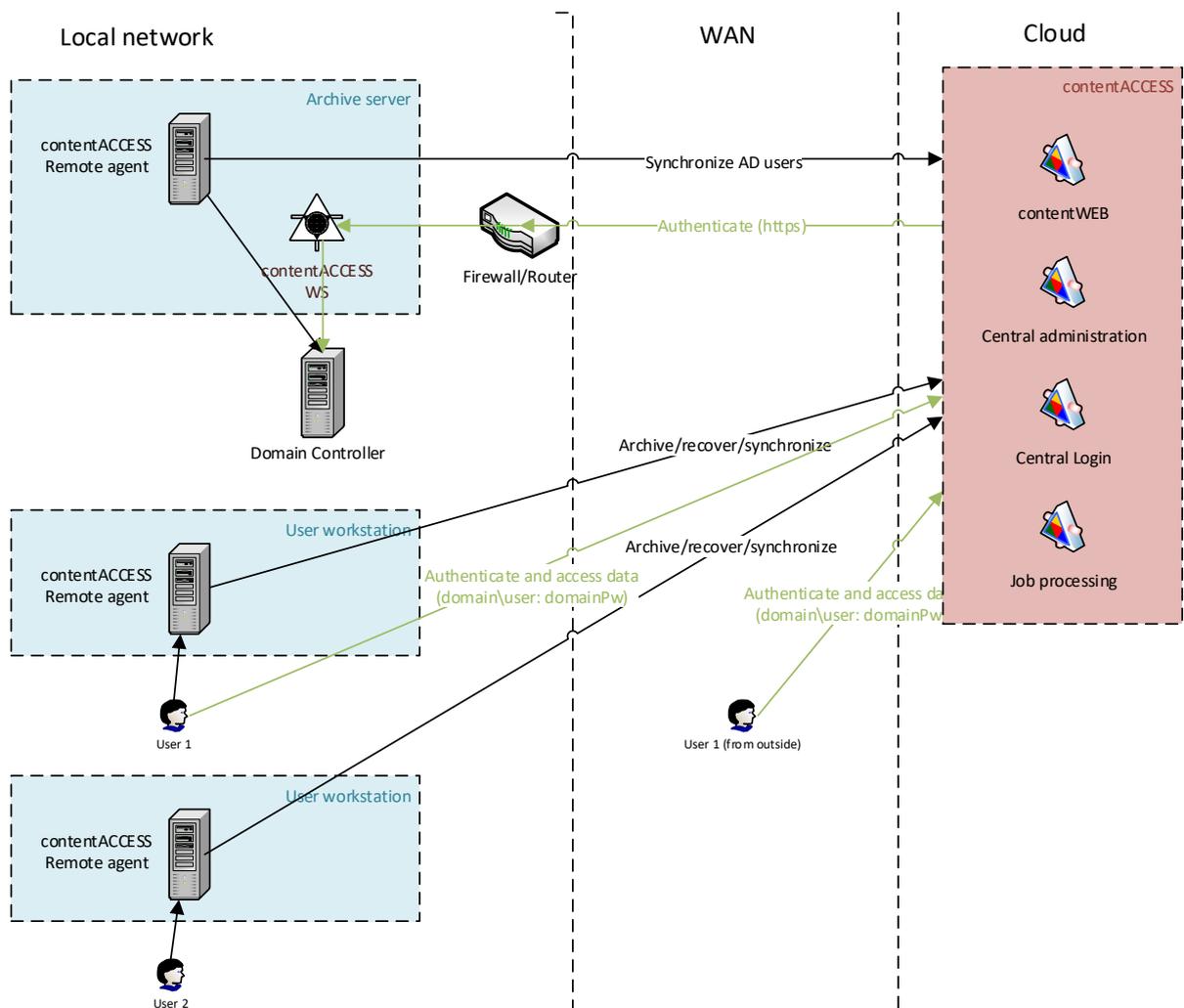
Once RFA is deployed, the agents will appear in [Central Administration](#), where the admin can create global rules and assign them to specific agents or all agents. In global rules, the administrator can use



well-known user folders like %My documents%, which will be then automatically translated to the real path on the machine. In case of well-known user folders, RFA will automatically process all user profiles from the machine, except system ones. The global rules are visible for users, but can't be changed by them.

Regarding the data access, this solution is the same as the [use-case 1](#). If the users need web access, then a global RFA together with the authentication proxy must be installed inside the local network. This RFA will create the necessary contentACCESS users and will allow the External AD authentication (for more info see [use-case 1](#)).

As an addition, each user will have RFA installed on his workstation. The RFA client can be used to access files from the archive directly. This will eliminate the need to use the authentication proxy and user provisioning.





## **Authentication**

If RFA provisioning is not configured, the only way to access the archive is through the RFA client.

If RFA provisioning is configured:

- the users are provisioned using the RFA provisioning, External Windows logins are created for the users
- the authentication is performed through the RFA authentication proxy.

## **Data access**

The users have automatic access to all accessible folders and files in the archive.

### Archiving common shares and domain joined workstations

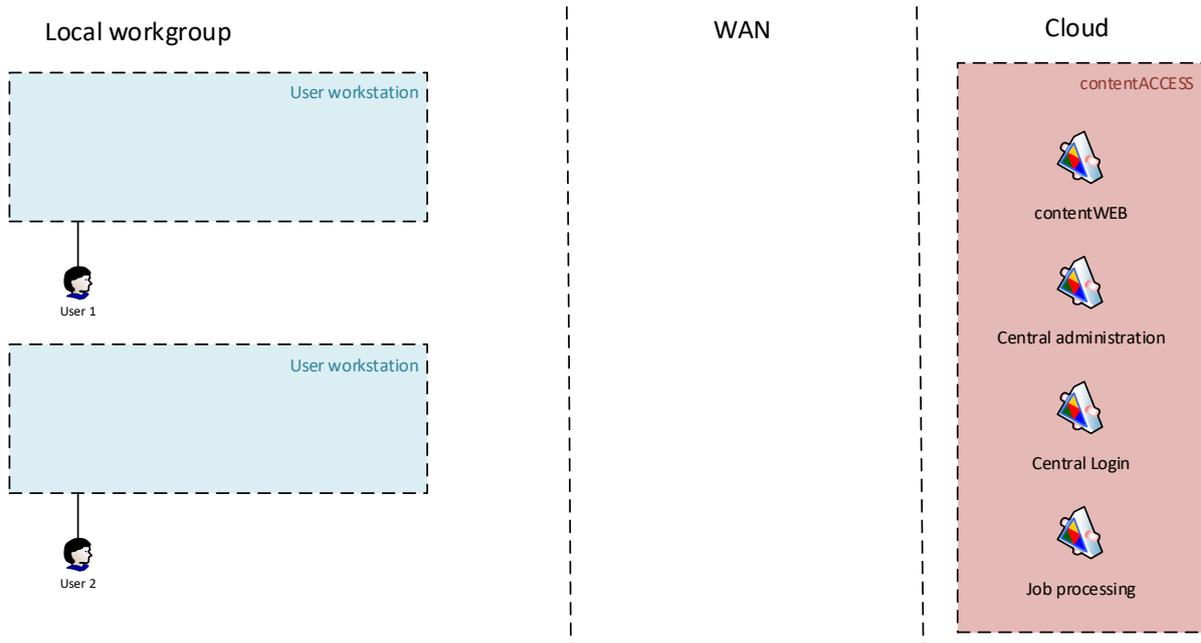
This use case is a combination of the previous two use cases, which means that the company is using a domain, where all resources are located. The company has one or more file shares, where the users are storing the common documents, but each user is also storing some (important) files locally on his workstation(s).

## **Solution**

From RFA point of view, this solution is a combination of [1.](#) and [2.](#), so RFA needs to be deployed on a common “archive server”, the authentication proxy must be installed and set up and RFA clients must be deployed through GPO (for more details, see the sections above).

### Archiving workstations in a workgroup

This use case is mostly used at very small companies. In this case, there are no common resources in the company, there is no domain. Each user owns a workstation, where he is logging in with a local user (exists on that machine only) and is working with local files.



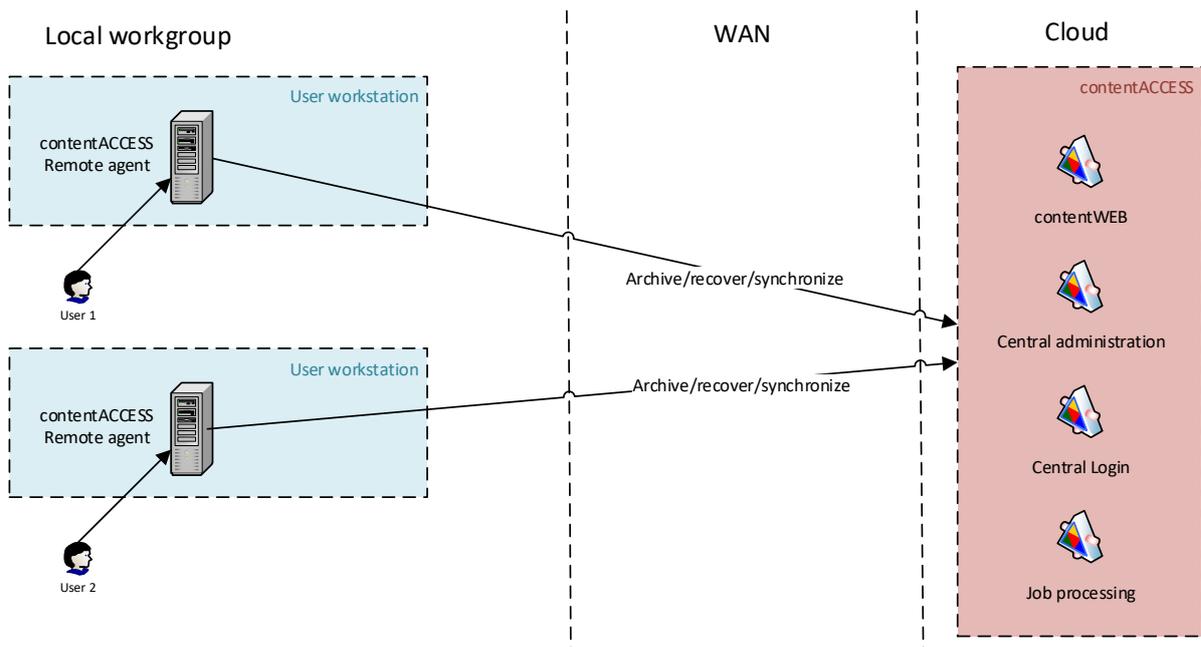
## Solution

The RFA deployment and configuration in this case must be done **manually**: by the user or by the administrator. As the first step, the administrator needs to create contentACCESS users in [Central Administration](#) for every user and grant the necessary rights (System -> Users).

**Note:** When using contentACCESS 3.8 and/or older version, the user must have at least Tenant administrator rights to be able to register his machine to contentACCESS.

**Then RFA must be installed on each workstation and the connection to contentACCESS must be configured.** For the connection, each user must use his own contentACCESS user which was created by administrator in the previous step. Once everything is configured, then the users can create their own archiving rules, or the administrator can create **global rules** in contentACCESS and assign to any or all agents.

The users can use RFA client to manage their files in the archive or use any contentACCESS client application (contentWEB, officeGATE, contentACCESS Mobile).



## Authentication

Each user must be manually registered in contentACCESS by the administrator. The choice of login is up to the administrator: Forms, Azure. **Windows login can't be created for these users.**

## Data access

The user has access to own resources only, i.e. to the archived workstation.

Access to other resources must be granted by the administrator. If the administrator grants access to a different workstation, the granted user has full access to that workstation.