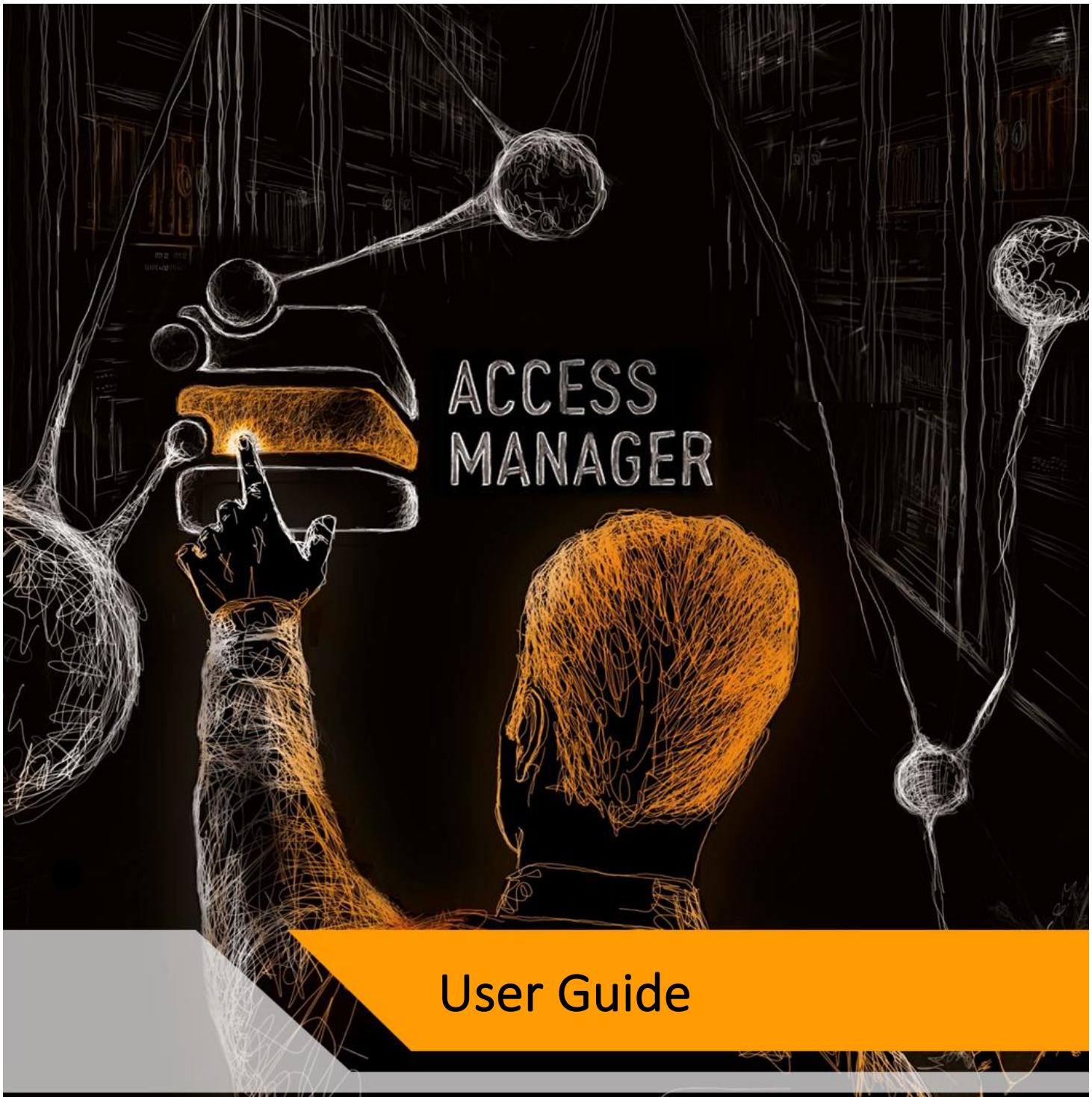


User Guide

Management Portal

Access Manager 2024.2

Manual for End Users and Administrators

BAYOOSOFT
MANAGEMENT SOFTWARE

Content

ACCESS MANAGER

1 Glossary

Term	Meaning
AM	BAYOOSOFT Access Manager
AMPR	Access Manager Password Reset – module for resetting user passwords
IDM	Identity Management Module – optional extension for managing employee accounts
Resource	General term which includes rights folders, managed SharePoint sites and 3rd Party elements.
Item	Logical resource like a printer, web application etc. on which access is managed by AD group membership (3rd Party Management Module).
Rights Folder	A folder whose access rights will be managed and monitored by AM.
Managed Site	A SharePoint site whose access permissions will be managed and monitored by Access Manager.
Free Folder	A directory that is not explicitly managed by Access Manager.
Workflow	A complete set of filing a request from an end user to a decider, processing it and giving feedback about the decision.
AM-Agent	A Windows service that takes various work orders from the Access Manager Server and processes them.
AD	Active Directory
DFS	Distributed File System
ABE	Access Based Enumeration: The functionality of a file server that show only such files and folders to a user on that he has access permissions.
Share, Folder Collection	A directory shared in the file system
Site Collection	Collection of SharePoint sites
Site	A SharePoint Site
Item Collection	A group of items (AD Group Management Module)
NTFS	New Technology File System
ACL	Access Control List
API	Application Programming Interface
IIS	Internet Information Server
MS SQL Server	Microsoft SQL Database Server

Term	Meaning
EU-GDPR	European General Data Protection Regulation

2 The Access Manager

2.1 Welcome to automated Rights Management

The Management Portal provides users access to different types of resources (folders in network directories and, by utilizing the respective module, SharePoint sites or item collection items) in a simple manner. Depending on the users' role, they can apply for certain access permissions and new addresses, which may be granted or revoked. Various additional features round out the support for the necessary management tasks. For this reason, not all of the pages described here will be available to all users. Their visibility depends on the respective role of the user after login

2.2 General Usage Instructions

Access Manager is a technically advanced client-server solution that uses state-of-the-art software technology. However, the infrastructure requirements remain moderate, especially for the Management Portal described here. Being a pure web application, the SSP only requires a current web browser without any additional plug-ins like Adobe Flash Player, Microsoft Silverlight or PDF Viewer. Currently, the following browsers are supported:

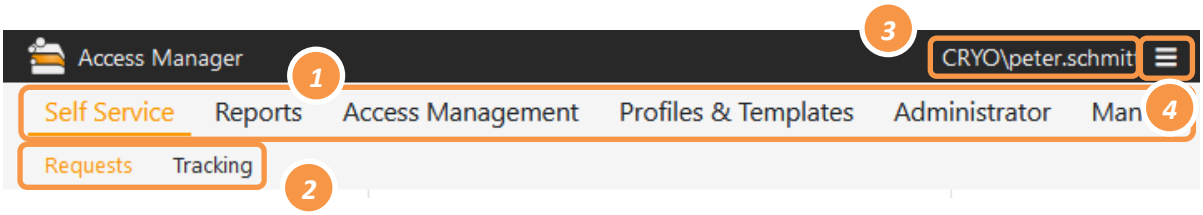
- Microsoft Edge
- Mozilla Firefox 70 or later
- Google Chrome 78 or later

Correct depiction & execution are not guaranteed for older browsers or browsers other than those indicated above.

In case you are using an adblocker software, please allow any action for the Management Portal by whitelisting its web URL, otherwise some features will not be available.

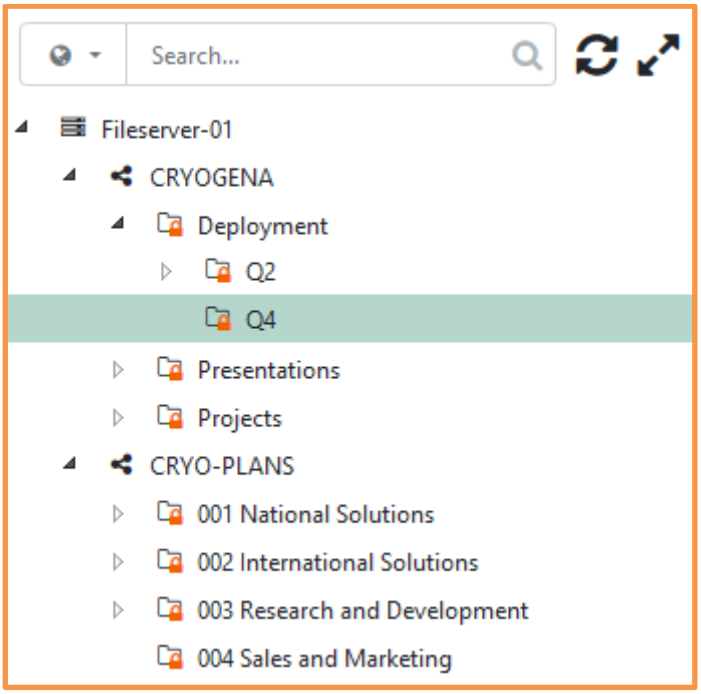
2.2.1 User Interface

The basic structure of the Self Service Portal simplifies navigation within the application:



1) The main menu – using these menu options, the user can access the respective pages. Only the options dedicated to the logged in user will be visible, meaning that a pure user would not see, for example, the *Reports* menu option.
2) The sub-menu – additional menu options will be displayed here as needed, which will refer to the sub-pages. The sub-menu is always visible and will be populated based on the option selected from the main menu. It may be empty if no alternate sub-pages are available.
3) The account name of the currently logged in user.
4) The burger icon (three dashes) opens a window with information about the version of the program and the interface language can be switched between English and German.

2.2.2 Resource Tree



As with the Windows File Manager, a resource tree shows the hierarchical structure of the available Folders, SharePoint Sites and Items. Clicking on the triangle icons will fold or unfold the level below the associated icon. If a triangle is not displayed, the node does not contain any sub-nodes.

Additional icons will be displayed to indicate the type of node:

- Server
- Server (DFS)
- Share
- Rights Folder
- Common Folder (without permission management)
- Managed SharePoint Site
- Common Site (without permission management)
- Item Collection (icon can be chosen by users)
- Managed item
- User Profile

2.2.2.1 Multi-functional toolbar

The multi-functional toolbar above the resource tree serves several purposes:

Use the DropDown list (globe icon) to specify the search boundaries: By default, the full resource list is searched. If you have selected a node (e.g. Server, Share or Folder) before, you can also search only within this resource.

The text entry field is used to search for resources by partial name and supports find-as-you-type by ad-hoc highlighting all found nodes in bold italic font.

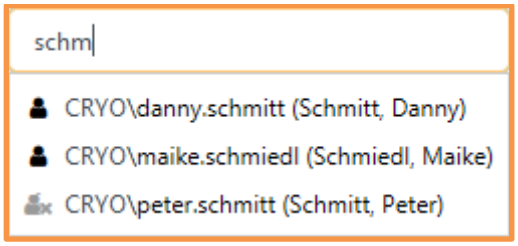
Moreover, following functions are available:

Refresh: Clicking on this icon will refresh the entire folder tree, displaying newly created and removing deleted folders from the list.

Expand: This icon will display the top folder level for all folder collections and serves to quickly view the managed resources contained at that address.

2.2.3 Search for Users

2.2.3.1 Individual Users

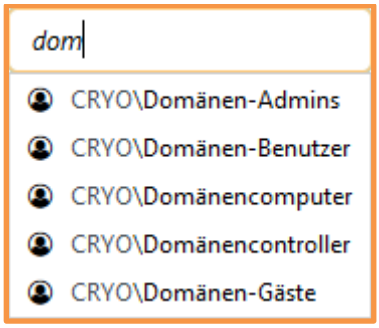


The user search control can be used to quickly find a user to grant additional rights to their account.

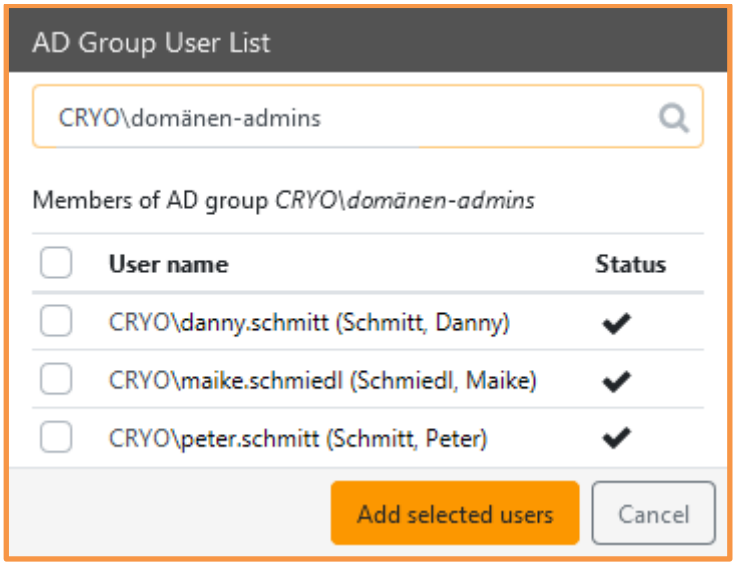
Simply enter part of the account name or last name in the text field and, starting with the second character, Access Manager will display the matching user accounts in the selection list. Entering more characters will refine the match list. The mouse or keyboard can be used to select and accept the matching account once the selection list displays it.

2.2.3.2 Multiple Users (Group search)

Using the Group feature is recommended when adding multiple users. The search process is identical to searching for single users. Instead of entering the name of a single user account, provide the name of a group that includes the desired user(s):



The group will first be added to the list like an individual user. Clicking the *Save* button will display the users currently contained in the group for selection from a dialog:



The header in the list provides the ability to select or unselect all users at once in order to invert this selection for several entries in a targeted manner. Users can only be selected if the checkbox next to the user entry has been enabled (depending on the status).

The status icons for the user accounts have the following meanings:

✔ The user can be added
The user account has been disabled in Active Directory and cannot be added

2.2.4 Displaying additional AD User Data

When displaying a user account, Access Manager may display additional information about this person. If this is the case, the mouse pointer changes over the user name. If you click on the name, a tooltip with the additional data appears:

The information displayed is provided by the administration and may vary. For example, the entry “Phone” is not displayed if the phone number is not defined in AD. Additional user data are not confidential and can be viewed by any user.

2.3 User Roles

Each Management Portal user performs a specific task and will receive specific access to the necessary pages for that task according to the role(s) assigned to him.

2.3.1 Role Description

In principle, Access Manager defines three basic roles:

- *Users*: Pure users who need access to various resources on the company network for their activities. They will apply for the desired access permissions using the Management Portal or make an application for a new resource.
- *Owners*: Persons who are obligated to manage a resource. In addition to making decisions about the creation or deletion of managed resources, this includes: the determination of *Responsibles* (see below), the reporting system and, if necessary (for the use of the optional *Accounting* module), the specification of the participating cost centers. *Owners* explicitly do not make decisions about granting access permissions.
- *Responsibles*: Persons who are appointed by the owner to process user requests so that access permissions can be granted to the respective managed resources. They can also grant or revoke permissions without a request as well as create reports. *Responsibles* explicitly do not have the ability to create or delete new managed resources.

There are additional roles that only collaborate with those indicated above, including the ability to process and use profiles for permission management (*Profile Administrators* and *Profile Responsibles*) and the ability to apply for access permissions for other employees (*Assistants*).

2.3.2 Role Overview

The following table lists all the roles with their access rights and duties in the Self Service Portal. *If a user has multiple roles, the rights are additive* for fulfilling all tasks.

Role	Tasks & Rights
User	- Apply for permissions to existing resources - Apply for changes or revocation of permissions to resources - Apply for the creation of a new managed resource - Apply for the revocation of permissions management for a resource - Ability to track their current and prior applications
Assistant	Same rights as a user with the ability to submit applications for other users.
Global Reports User	Same rights as a user with the ability to view also global reports (person independent)
Responsible	- Process open requests for their resources (allow or reject) - Add, revoke or modify user permissions to all of their resources

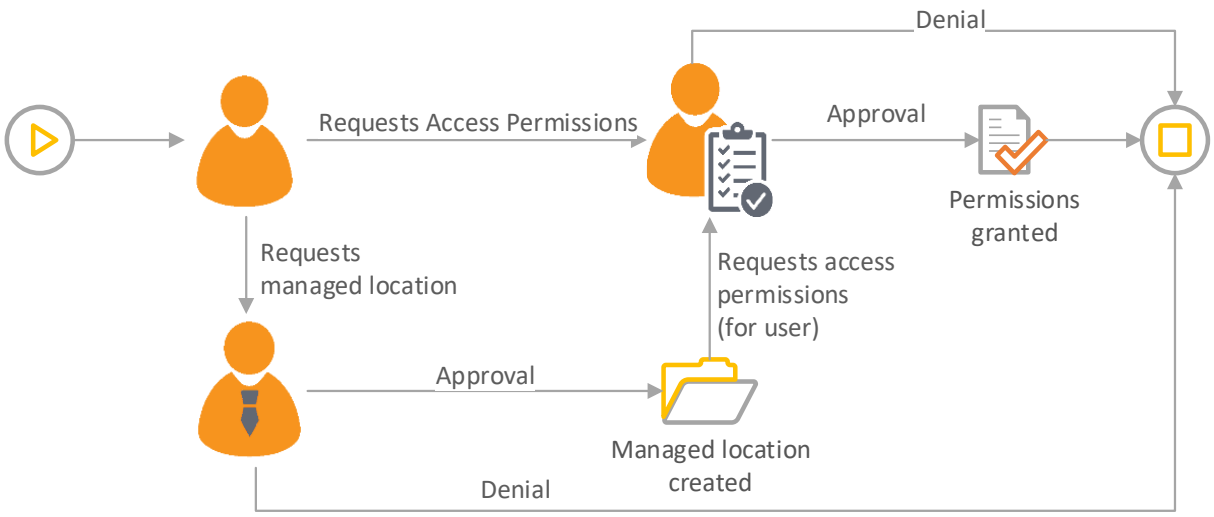
Role	Tasks & Rights
	- Create reports about their resources, profiles and users - Appoint and remove their own substitutes - Create, delete and modify templates of permissions for their folders
Responsible (Substitute)	The same rights as the Responsible they represent, however without the right to appoint a substitute
Owner	- Process open requests for the creation of new resources and for the removal of the managed resource status that are in their area of responsibility - Grant and withdraw Responsible rights for resources in their area of responsibility - Create various reports about their resources - Appoint and remove their own substitutes
Owner (Substitute)	The same rights as the Owner they represent, however without the right to appoint a substitute.
Administrator	A combination of the rights for Owners and Responsibles. The Administrator cannot appoint substitutes, but can process requests for all resources
Template Administrator	- Create and edit global templates - Choose other users who can use the global templates - Uses global templates
Global Template User	- Uses global templates
Profile Administrator	- Create and edit profiles - Grant and withdraw Responsible rights for profiles
Profile Responsible	- Add, revoke or modify memberships to all of their profiles
Classification Administrator	- Create and edit classifications that may contain categories according to EU-GDPR

3 Self Service for End Users

3.1 Operational Principle: Workflow requests

Users who require access to a certain network directory or SharePoint Site will select it from a list and apply for the desired permission using a simple entry form. The responsible person for the resource, who the user does not need to know, will be notified immediately. As soon as they have processed the request (allowed, allowed with restrictions or rejected), the applicant will be notified by email. In the ideal case, access can be made available within minutes.

If a user applies for a resource that does not already exist, the so-called owner for the parent resource will first be notified. If he agrees with the request, the owner will perform the necessary management tasks in AM. The desired resource will automatically be created by Access Manager and the permission management will be set up; deep understanding of IT is not required for this. Once the new resource has been created, the responsible chosen by the owner will automatically receive a request to set up the access permissions for the applicant (see previous chapter) as specified in the applicants´ request.



3.2 Workflow requests

Menu:

Self Service → Requests

All users have access to this page. All requests for the creation of new folders and site, for granting access permissions and so on will be made from here. Therefore, this is the central and most important page of the Management Portal. Depending on the usage of further modules, the submenu may also contain SharePoint Sites, 3rd Party Items etc.

The desired entry will be selected from the tree view and a menu bar with the available action tabs will be displayed on the right side. The request forms are identical for all resource types except SharePoint (Classic mode). Therefore, the following chapters will describe the functionality based on the file system request type by example. Differences in detail affect, for example, the available permission types:

- **Folder:** Available permissions: Read / Write
- **SharePoint Sites (on premise):** Available permissions: Read / Write / Design
- **Microsoft Entra (Office 365):** Regards SharePoint (Cloud) and MS Teams
- **Items (3rd Party):** Available permissions: Differing, defined by customer
- **User Profiles:** Available permissions: Membership
- **Passwords:** Several options to change your password

With the support of Microsoft Entra accounts, an application for access permissions for your AD or Microsoft Entra account now depends on the target resource: "On Premise" resources such as file servers, classic self-hosted SharePoint sites, AD groups, etc. can only authorize AD user accounts (and thus also can be applied for), Microsoft Entra accounts only work on cloud resources (O365-SharePoint, Teams). Even if you are signed in with your AD account, Access Manager will populate your appropriate account when you apply. The only exception is Profile Membership: because a profile can contain a mixture of all resource types, Access Manager always proposes both account types together here.

3.2.1 Requesting Access Permissions

You can use this form to request access permissions for yourself. If you have the *Assistant* role, you can also request permissions for other people. If enabled by your administration, you may also be able to request access to cloud components such as SharePoint or Teams. When you start typing a name, you will see, among other things, a clickable *Invite guest user* entry at the end of the suggestion list. A dialog will open in which you must enter the name and email address of the user to be invited. After you have submitted the application for this person and the decision-maker has approved it, a corresponding guest account will be created in the Microsoft Entra cloud and the invited user will receive an automatic email from the cloud system through which they can log in and legitimize themselves . These final steps are beyond the control of Access Manager. If you have any problems, please contact your cloud administrator.

The optional *Valid through* entry will assign an expiration date to the necessary access permission, after which the user will automatically lose the permissions. If a maximum permission duration was predefined, it is only possible to apply for shorter time but not for longer.

The *Permission* group distinguishes between the *Read* and *Write* permissions. Thereby, *Write* also includes creating, deleting, and changing files and sub-folders. If you already have permissions to the selected resource, a notification is displayed and an additional option for removing permissions is added. Other resource types may have customized rights listed; A different allocation logic may be used here:

3.2.1.1 Supplementary Permissions

Supplementary Permissions usually consist of a set of multiple single permissions. In contrast to the commonly used exclusive permissions, you can select more than one permission at a time and they will add up. This variant is often used if such permissions are independent of each other, they are not contradicting.

Please note: If you already own distinct permissions of an item and want to change the selection in a new application, the currently given permissions are pre-selected. If you deselect them, they will be revoked later on.

You will only get the permissions you have selected from the list.

3.2.1.2 Apply inclusion in Profile

If you have the role *Assistant*, you have the additional option of requesting that the selected resource with the desired authorization be included in a profile of your choice. The application is decided by the *resource responsible*, not by the *profile responsible*. Similar to selecting another person, enter part of the profile's name and select the one you are looking for from the auto completion. Here, too, you can select and request multiple profiles at once.

Please note that you can request the permissions set for people and profiles at the same time if you specify both target types. So, for example, if you only want to request inclusion in a profile, remove all personal details from the *User* field.

3.2.2 Public Elements

You can tell so called public elements by their special icon . For such elements, no manual approval process is needed but access is granted instantly. The application form states “Automatic” for the decider (“Approval by”).

3.2.3 Requesting a new Resource

This form is used to apply for the creation of a new rights folder, SharePoint Site or an individual resource (Item).

You must specify a resource name, and it must comply with the naming rules for resources.

You must also specify who will be responsible for the new directory. By default, you will be entered yourself, but you can also remove yourself if you specify at least one other person.

3.2.4 Requesting Responsible Role

Using this form, you can apply for the role of a *Responsible* for the selected resource to assign access permissions to other people in the future.

The *Owner* being responsible for the folder will be displayed for informational purposes.

The *Reason* entry may be mandatory under certain circumstances. It should provide an explanatory message.

3.2.5 Requesting Removal of Rights Folder status

This form is used to request the removal of the rights folder status from a folder. There are several consequences bound with this: possible loss of control over the access permissions of other users, possibly loss of invoicing control if the optional *Accounting* module is licensed, etc. The *Owner* should take these consequences into consideration when making the decision about the request. This applies particularly to the existing access permissions. If a folder is no longer being managed by Access Manager, it will automatically inherit the access permissions of its parent directory.

3.2.6 Requesting Profile Memberships

As Profiles contain various permissions for a multitude of resources, it is not possible to request a distinct permission here. Instead, you may apply for membership of a Profile, giving you access to all specified resources of that Profile. You as an applicant are not able to determine the underlying resources and permissions.

If you also have an Microsoft Entra account, this will be entered automatically in addition to your AD account when you apply. You can also remove it if you wish.

If you have the assistant role, you can also enter any number of other users (both AD and Microsoft Entra accounts).

3.2.7 Password Management

This function allows you change, reset or unlock your password for a distinct application or system environment. First, enter the account in question and then authenticate yourself using one of the pre-configured options (see chapter 3.5).

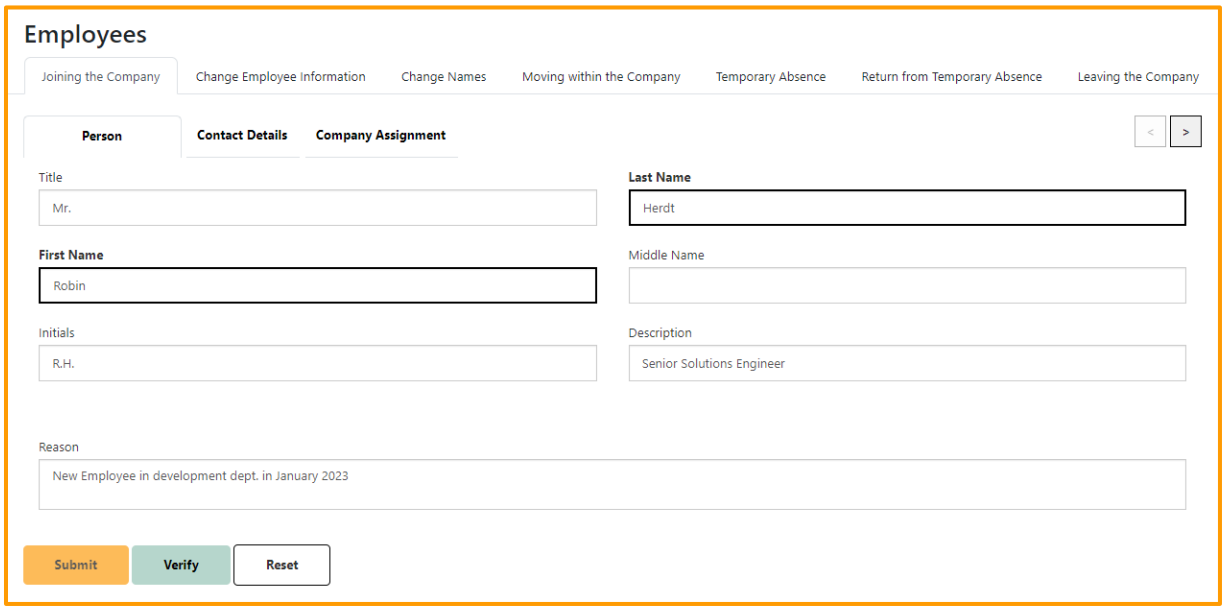
If you own the role *Service Desk* within AMPR, you can initiate a reset for other users without explicit legitimation (menu item *Reset Password for other user*).

This menu item provides the functionality of the AMPR application.
Please find a more detailed description in the corresponding manual.

3.2.8 IDM Dialogs

Behind the dialogues of the IDM module are processes that create or modify identities and their associated AD accounts and Exchange mailboxes. These processes are only triggered when a dialog has been successfully sent and accepted by the assigned approvers. The dialogs are located under the *Identity & Users* tab in the *Self Service* area. Users with the *Personnel Manager* role can view and send these dialogs.

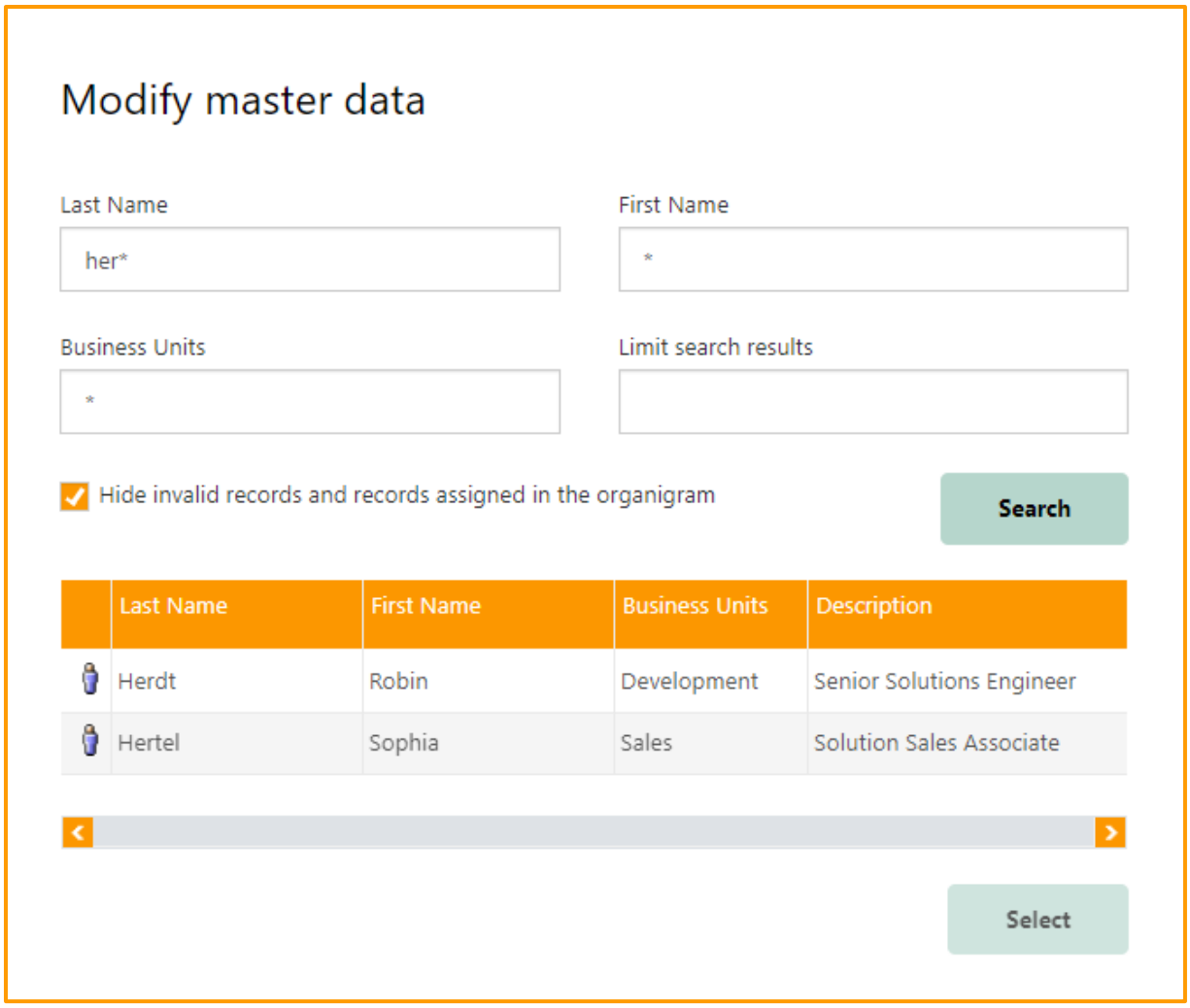
Seven dialogues (tabs) are available for you to manage your company's employees. Each dialog can be divided into tabs. To send a dialog, all marked **mandatory** fields must be filled with valid data. Then press the *Verify* button and – if there are no problems – click *Submit* afterwards. You can use the *Reset* button to reload the dialog and thus, for example, select a new identity in a change dialog. Entries previously made will be lost.



The *Joining the Company* dialog allows you to create new identities. The personal data in the first tab contains the name of the new identity and a description. The latter is not only displayed in the IDM module itself with the identity, but also entered in the corresponding AD field. The contact data of the second tab can be divided into a private and a business part. Note that the address listed here is that of the identity. The postal address of the new identity's work location is assigned to it by its organization chart affiliation. In the company assignment tab, in addition to an assignment in the organization chart, you can also choose whether an Exchange mailbox should be created for the new identity. The *Manager* and *VIP Employee* fields are used for administration. They have no impact on the IDM processes. Note that if an employee number is not selected, this field in AD will be filled with a random character string.

If your administration decided to use free text fields when choosing a pattern, you will also see all the fields that have been set accordingly. Each of them is a mandatory field and must be filled with a valid entry. With the *Verify* button, the IDM module will validate your entries according to common conformity rules and adjust them if necessary. Adapted fields are marked as such and the reason given, e.g., too many characters.

In the Change *Employee Information* dialog, you can adjust the metadata of an identity. To do this, select one of the IDM identities from the search mask. Note that only identities created or imported in the IDM can be edited here. Identities, or better AD accounts, which are only available to the Access Manager through the AdUserImport, are not listed here. You can also select AD accounts here that have not been imported into the IDM but have been assigned as Responsibles or have logged on to the IDM. Changes to these only result in adjustments to the data within the IDM module. The AD account of these identities is **not** changed.



After the selection, you can now, among other things, adjust the contact details, the employee number and the entry and exit dates of the selected identity. Any changes made are then also propagated to the AD.

In the *Change Names* dialog, you can make changes to an identity's name after selecting it. Note that in contrast to the *Change Employee Information* dialog, this can also result in adjustments in the calculated fields of the template. If you do not use free text fields and your patterns contain the parts of the name that you want to adapt here, this means that these fields will also be recalculated and updated. If you have set free text fields instead, you can edit the values here.

The *Moving within the Company* dialog allows you to update the assignment of the selected identity in the Organigram.

The two dialogs *Temporary Absence* and *Return from Temporary Absence* are used to manage inactive identities. In contrast to the previous dialogues, the specification of a reason for the request is mandatory here. If the identity to be deactivated has an Exchange mailbox, you can enter a forwarding email address here. Regardless of any rules within the mailbox, all incoming E-Mails are then passed

on to the forwarding address. Alternatively, you can set an out-of-office message that is sent to all senders of incoming E-Mails. If you do not select a start and end time for this, the setting remains in place until the return workflow is executed. This also disables automatic forwarding if set. Apart from that and regardless of the existence of a mailbox, the AD account of the selected identity is deactivated or reactivated. It is therefore not possible to Log in with the account of a temporarily absent identity. In addition, absent identities are also not considered as approvers for new workflows. The selection of approvers of an already created workflow is not updated when a relevant identity is returned.

In the *Leaving the company* dialog, the AD account and, if applicable, the Exchange mailbox are permanently and irrevocably deactivated in the IDM. It is no longer possible to log in with the account, but administrators still have access to the mailbox – the latter, however, can no longer receive or send emails. Other than that, the identity will be moved to one of the configured Tombstone-OUs if configured. After an identity has been permanently deactivated, it can no longer be managed by the IDM and can no longer be activated.

If you submit a dialog, you will be informed about the status of the workflow via E-Mail. If requestors have been configured as recipients of onboarding mails, you will receive a corresponding E-Mail for the onboarding of the new employee upon completion of a *Joining the Company* process. This E-Mail contains account data including the new employee's password and should therefore be handled with care.

3.3 Overview of own data

Menu:

Self Service → My Overview

You can check your current permissions on the resources managed by Access Manager as well as several other information at any time on the *My Overview* tab.

3.3.1 Tab "User Information"

The basic overview includes a quantitative listing of your permissions, separated by resource types.

3.3.2 Tab "Individual Permissions"

Here, you will find a concrete breakdown of the accessible resources for which you are given personal access. This also includes permissions that your associated Microsoft Entra Cloud account has. Access Manager distinguishes between *AD User* and *Microsoft Entra User*.

3.3.3 Tab "Profile Memberships"

If enabled by the administrator, there is also a *Profile Memberships* tab that lists the profiles you belong to. You can use the info icon **i** to display the resources to which you have access through that profile.

3.3.4 Tab "Substitutes"

If you have a decider role (Owner, Responsible), this page allows for appointing another person as your substitute for a limited or unlimited period (such as during a vacation). Your substitute will get the same possibilities that you have, but you will not lose your capabilities and are still able to perform all tasks.

A period of validity may optionally be specified for the *Substitute* role, whereby the beginning and end dates are also optional. If a start date is not entered, the *Substitute* role will take effect immediately. If an ending date is not specified, the *Substitute* role will be in effect until you manually revoke it.

It is not possible to assign substitution role to an AD group.

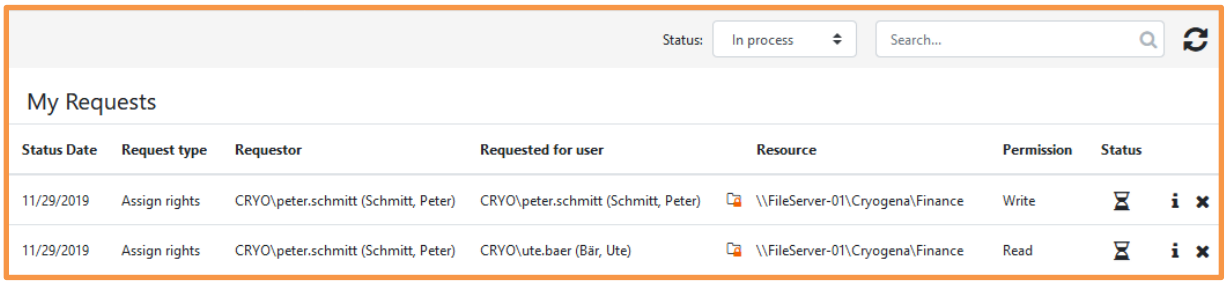
3.3.5 Tab "Roles"

This tab shows you which system-wide or resource-related roles you have. This is a purely informative view; roles cannot be changed here.

3.4 Tracking Requests

Menu:

Self Service → Tracking



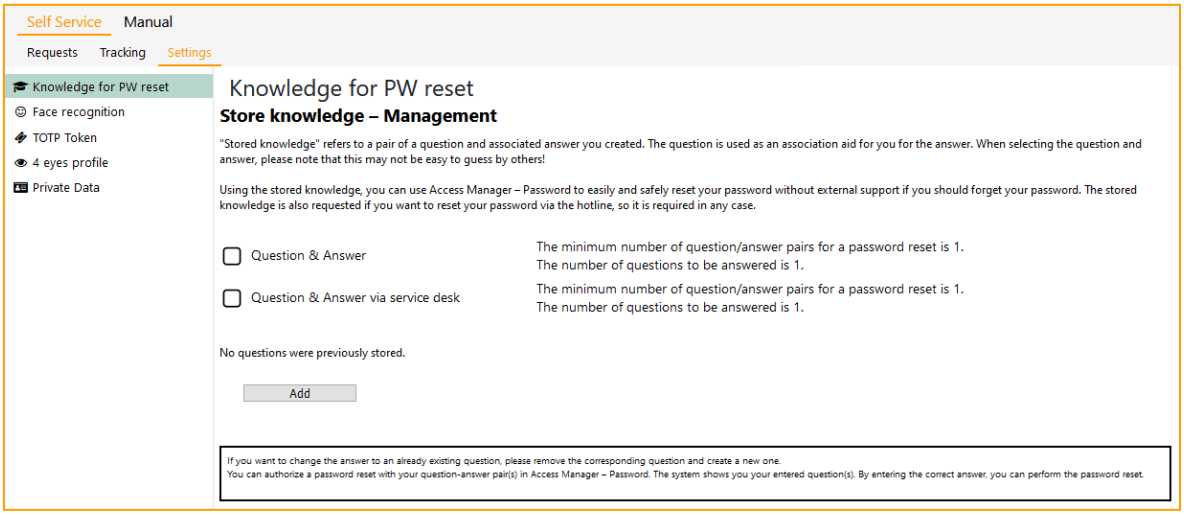
The *Tracking* page provides the user with a list of his open and processed requests, which can be reviewed and filtered by their states. The individual columns provide information about the various details of the individual requests. The cancel button ✖ will be displayed when there are open applications (the status is *in process*), in order to withdraw them.

For better overview several application information are grouped in an additional window which is displayed when clicking the *Details* button ℹ. Here, information about the application and decision is listed – the latter is empty if the request is not yet processed. Moreover, the applicant finds information about the involved deciders.

3.5 Settings for Password Management

Menu:

Self Service → Settings

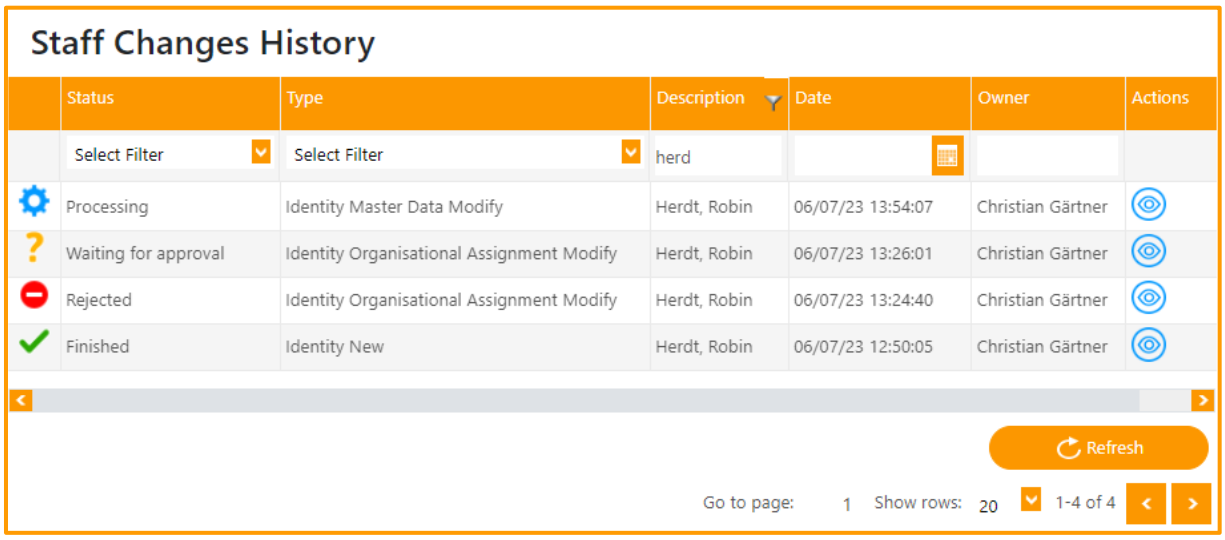


These functions are available only if application AMPR is present. They allow you to setup various ways of authenticating yourself when using the password management function (see chapter 3.2.7), e.g. secret questions, One-Time Tokens or second account of a colleague (four-eyes-profile).

This menu item provides the functionality of the AMPR application.
Please find a more detailed description in the corresponding manual.

3.6 IDM Workflow Views

The IDM module offers several views for inspecting and managing workflows. Here you can view the processed, planned and executed workflows and find more details by clicking on the eye symbol on the right of the respective workflow. You will also find all the data or changes that the applicant entered in the dialog. The selection of workflows displayed depends on the selected view.



The Self Service workflow view under *Tracking* shows you the workflows that you have initiated yourself. By default, only workflows in progress are displayed. You can show completed workflows via the filter selection in the status column.

4 Permission Management for Data Owners

4.1 Operational Principle: Responsibles & Owners

In addition to the role *User* (everyone using the Access Manager has this role automatically), there are two more basic roles, the *Responsible* and the *Owner*. These roles are used to reflect the competencies in your company, strictly separated to support the division of powers concerning the accessibility management:

The *Responsible* takes the decision about permission requests of users for all resources he is responsible for. He also manages access permissions independently of user applications and checks permissions in case of *Reapproval* cycles (see next chapter).

The *Owner* is in charge of managing the basic structure of “his” resources. For example, he decides about the creation of new Rights Folders and their assigned *Responsibles*. He also flags distinct resources with *Classifications*, used for marking resources as sensible in terms of the EU-GPDR (including definition of resources to be checked within a *Reapproval Run*, see next chapter).

An *Administrator* can always perform the tasks of all *Responsibles* and *Owners*, should they not be available. This includes having insight to applications and altering existing permissions as well as changing *Owners* and *Responsibles* for distinct resources.

4.2 Responsibles Tasks

As a Responsible you have access to the main menu item *Access Management* which allows further sub items for managing your resources.

Using this overview and editing page, you can review and modify other users’ access permissions for resources in the Responsibles´ scope of responsibility without a request from those users. This is an important difference compared to the normal processing of user, because all changes made here occur without automated email notifications to the participants. The normally intended workflow processing does not happen in this case.

4.2.1 Processing Requests

Menu:
Access Management → Requests

This page shows the user requests for access permissions. First, select from the left if you want to work on open (that means yet unprocessed) or closed requests. They are listed on the right side and can be searched or filtered based on various criteria.

When processing requests, they may be granted (un-)changed or rejected entirely. Once processing has been completed, both the user and applicant receive an automated email message with the results of the request.

Processing requests may require additional information, i.e. a mandatory comment to justify the decision.

To check and process a request, unfold the entry with the DropDown icon ⌄. If all necessary information is already available, you may immediately grant (icon ✔) or reject (icon ✖) the request without confirmation.

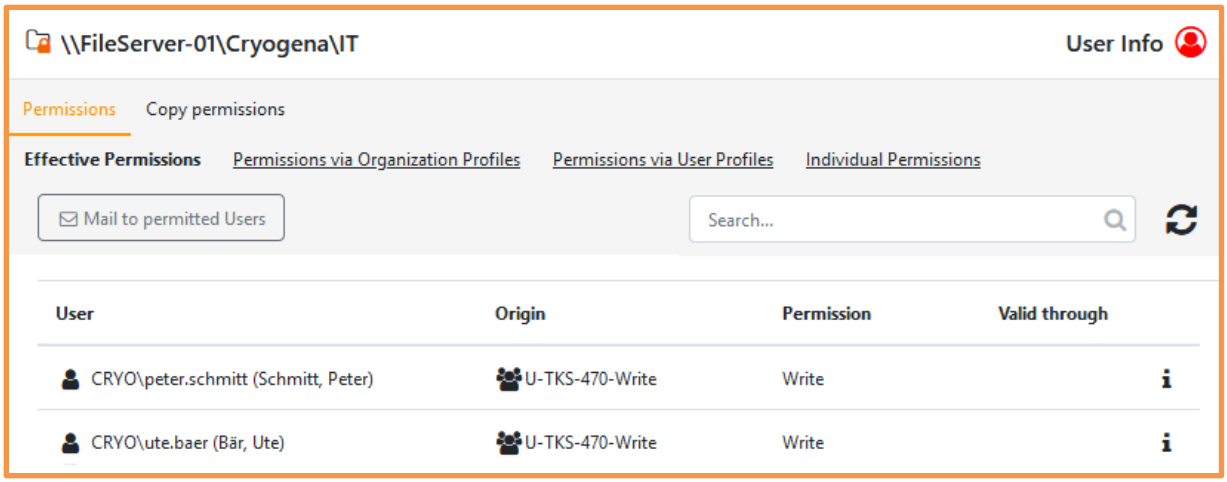
4.2.2 Manage Permissions of Resources

Menu:
Access Management → Permissions

Select *By Resource* from the list at the left side. The tree view will now display the managed resources that you can choose for processing as desired.

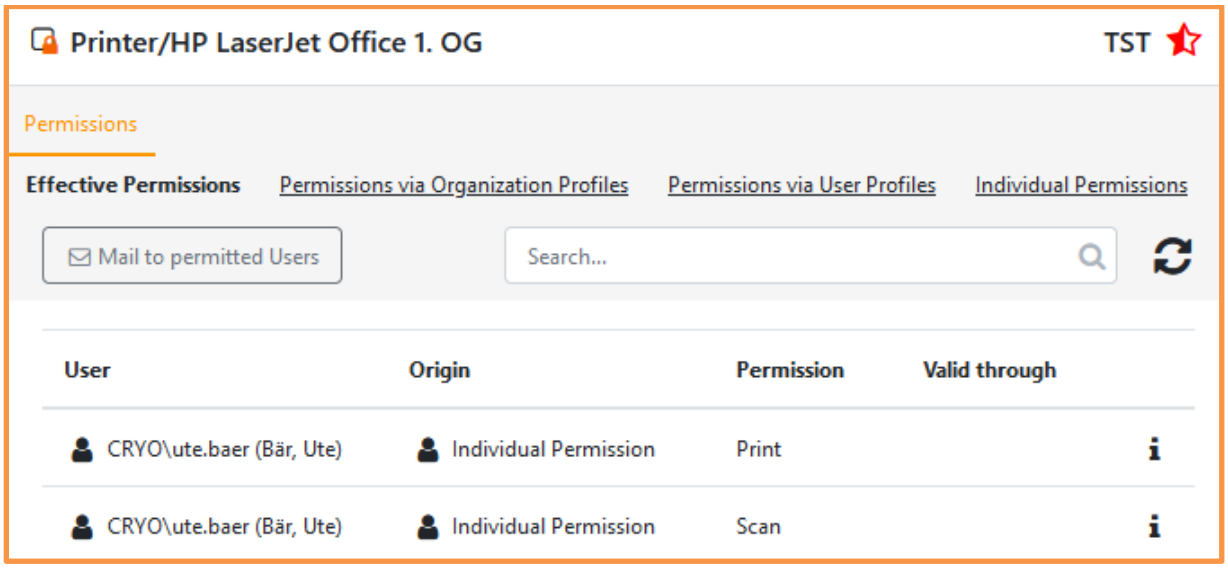
The right Details pane has a header row, containing the resource´s address and a potentially set classification. The Details pane itself offers two tabs, “Permissions” and “Copy permissions”:

4.2.2.1 Section “Permissions”



This section displays a list of users with their access permissions for the selected resources, having one row per user.

In case of Supplementary Permissions (see chapter 3.2.1.1), also every single permission of a user has its own row. This is needed because different permissions granted may have different origins:



Because of the possibility to grant access permissions by the use of *Profiles*, there are several ways a user can get access to a resource. Therefore, this area is separated into four different views:

- Effective Permissions
- Permissions via Organization Profiles
- Permissions via User Profiles
- Individual Permissions

4.2.2.1.1 Effective Permissions

Effective Permissions are composed of the various options to permit access (*Profiles*, *Individual Permissions*) at the current point of time with the highest permission winning. If, for example, a user was granted read access via individual permission onto a resource and a user profile (which the user is a member of) defines write access, the user will effectively encounter write access.

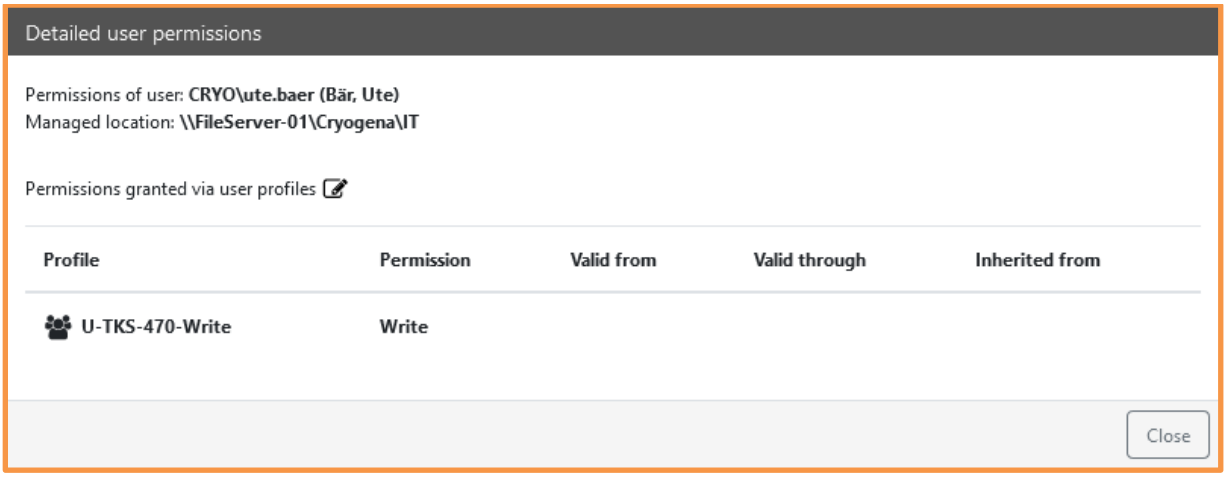
Because of the nature of this view, information shown here are read-only data. Every user is listed exactly once. Besides the effective permission also its origin is displayed.

The origin of the effective permission can be one of the following:

- Individual Permission – The permission was personally granted to this user.
- User Profile – The permission was granted to a user profile which the user is currently a member of.
- Organization Profile – The permission was granted to an organization profile. The user displayed is member of a user profile which in turn is a member of the organization profile.
- Special permission group – The permission was explicitly granted by the *Folder Management Administrator* and lies outside the responsibility and competence of the *Responsible*. It cannot be changed nor deleted here.

Access permissions that have been granted to a parent rights folder (not necessarily the immediate parent folder, but potentially a folder at a higher level), are displayed in a separate foldable list and cannot be edited here (but only in the folder where they are set).

Further permission-related information can be retrieved via the corresponding info icon. The opening dialog shows more details about all permissions set for the selected user with the effective permission being highlighted. Clicking the *Edit* icon the Responsible can jump directly to the origin and alter permission settings.

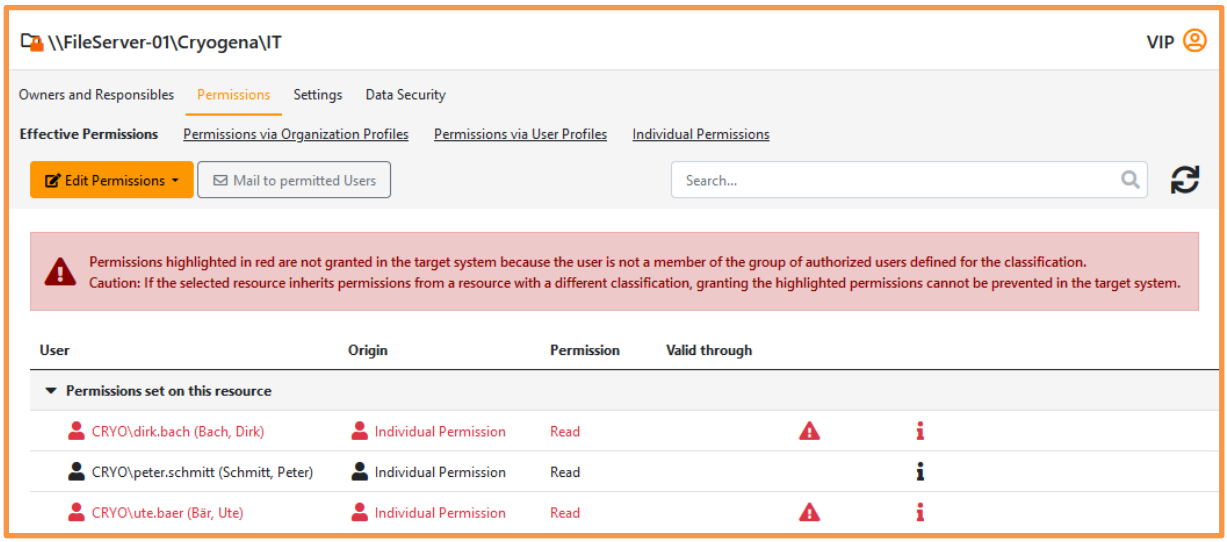


Mail to permitted Users:

Use this button to send an email to all users who have access permission / membership for this resource. In the dialog window you may alter the given email subject and enter your message in the text area. Although the sender address will display as the one configured for Access Manager, a reply mail will be sent to your own mail address.

Note: Special cases when using classification with set authorized users

If a resource has an assigned classification that holds a defined group of authorized users (see chapter 7.2), it may happen users were permitted onto this resource who are not members of the respective group and are therefore not eligible for access permission. Solely in this view of effective permissions, such users are displayed with a warning notice:



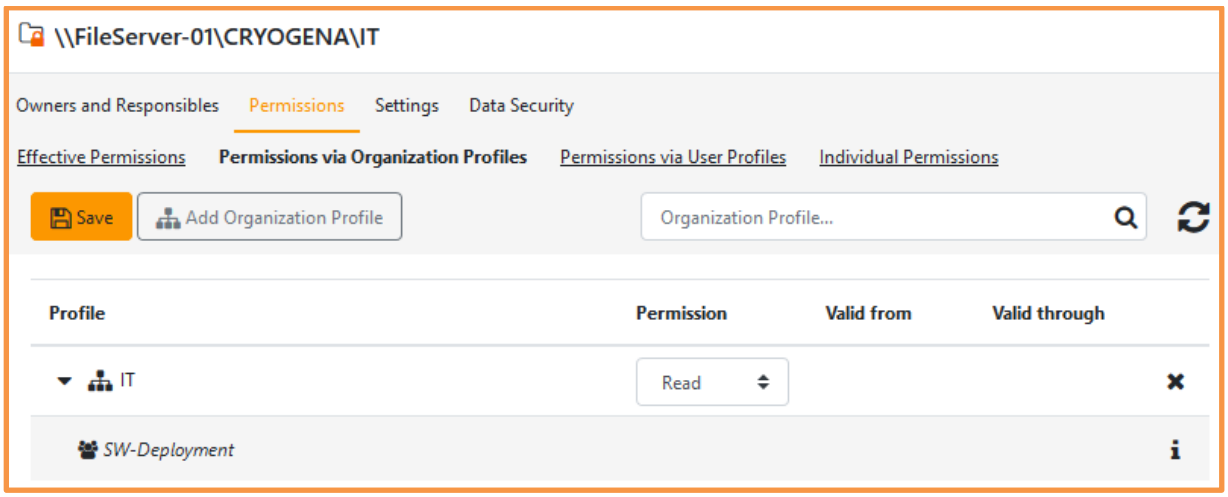
Access Manager still saves this permission grant but will not give true access in the target system (AD group, file system, depending on the resource type).

Take this as a reason to check if either the user was erroneously permitted or if he needs to be added to the authorized user group.

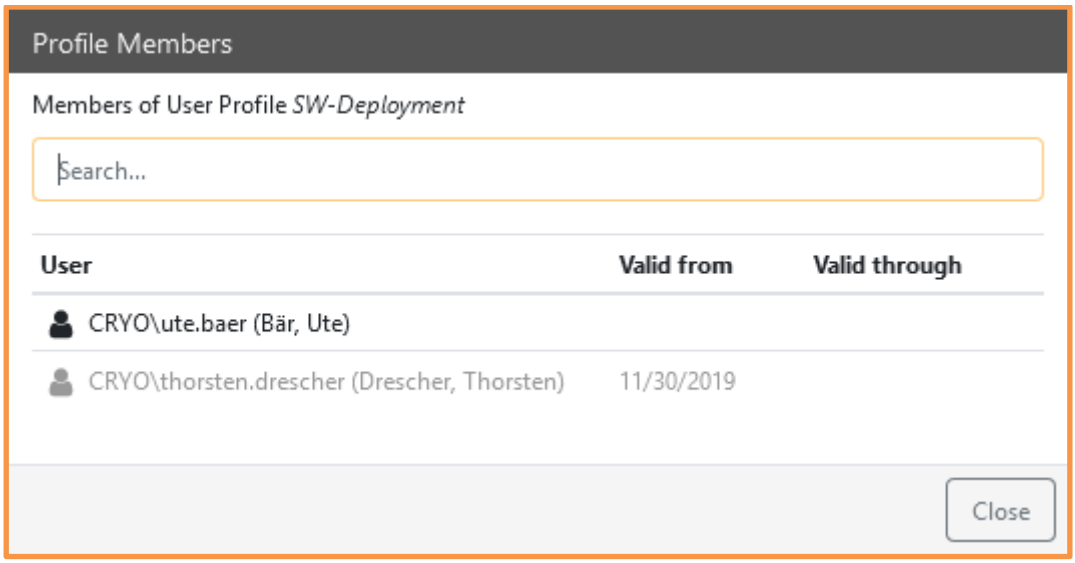
4.2.2.1.2 Permissions via Organization Profiles

This view shows the *Organization Profiles* that have been granted access to the selected resource. For every profile, the members (User Profiles) are listed along with the start and end date of the validity if the Profile is unfolded using the expander icon.

Please find more information about the functionality of Profiles in chapter 6.



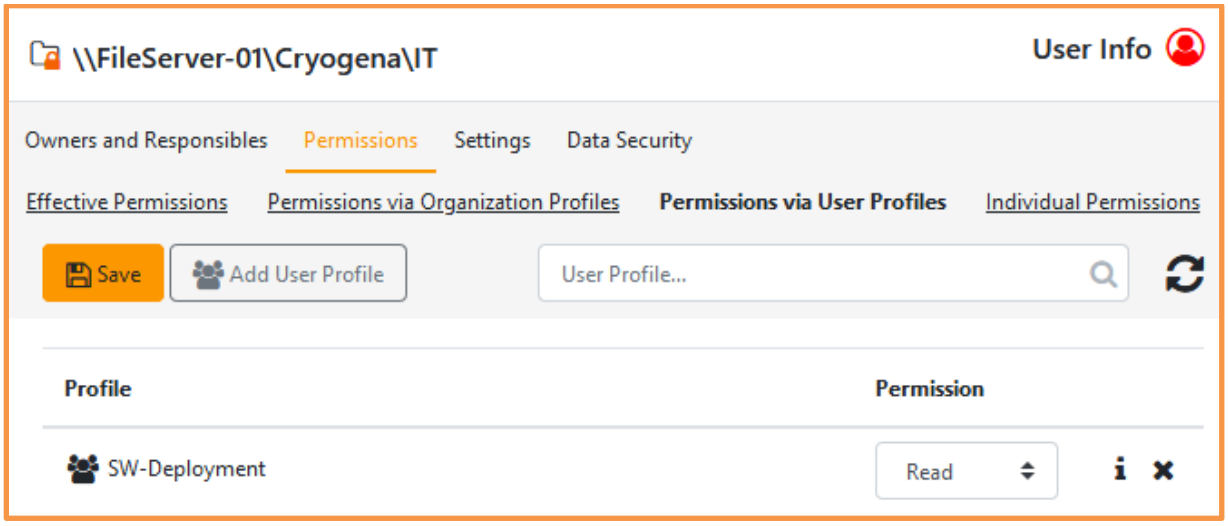
Clicking the Info icon of a User Profile will open a dialog showing its members (user accounts).



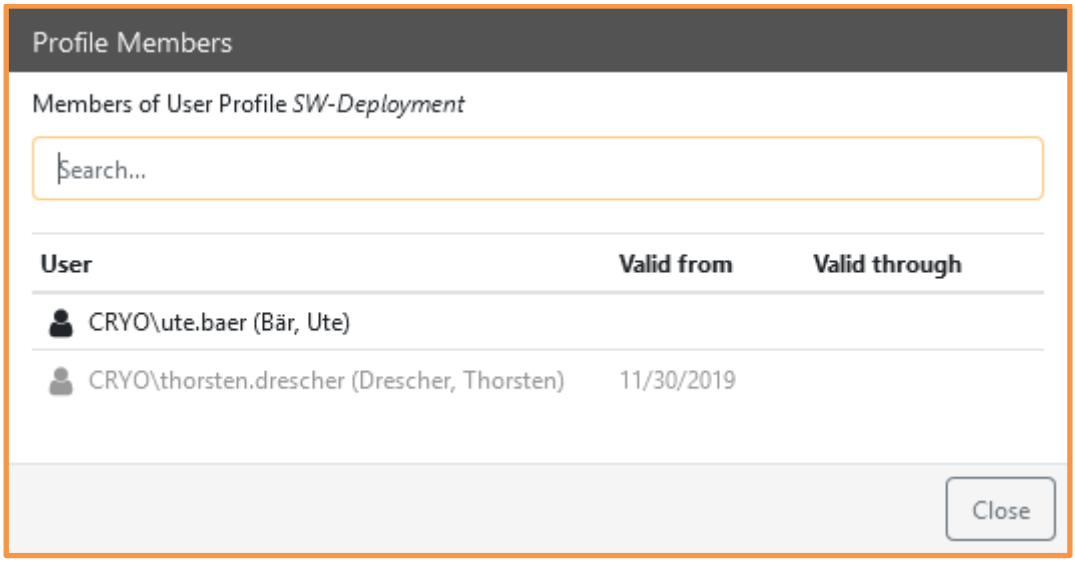
The Responsible can add further Organization Profiles and grant access to them (button *Add Organization Profile*). He has the power to change or delete all listed access permissions. With every change of the profiles the belonging user accounts will receive / lose permissions.

4.2.2.1.3 Permissions via User Profiles

This view shows the User Profiles that have been granted access to the selected resource. Please find more information about the functionality of Profiles in chapter 6.



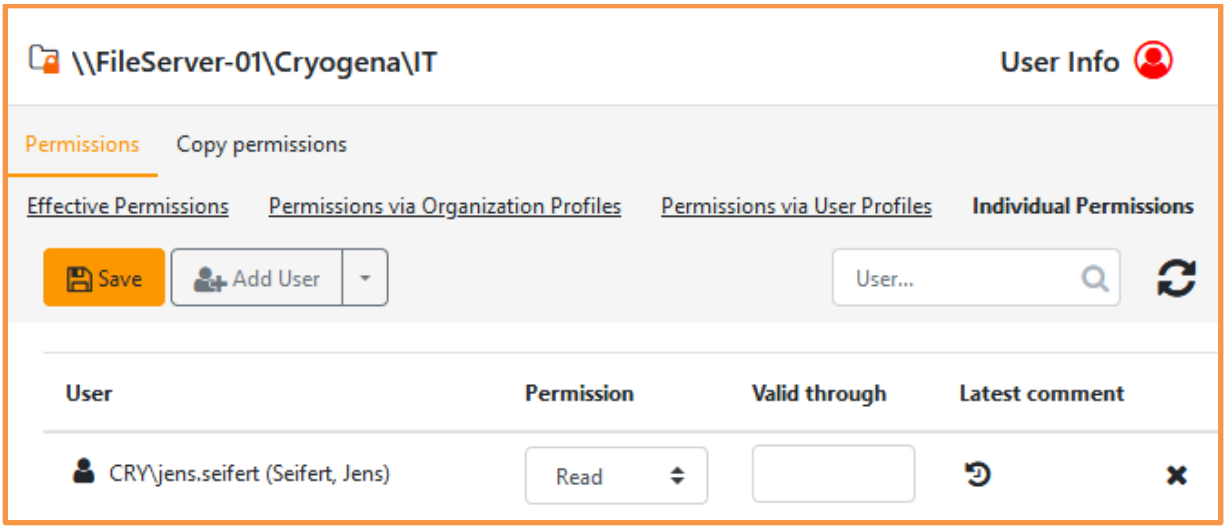
Clicking the Info icon of a User Profile the members (user accounts) are listed along with the start and end date of the validity.



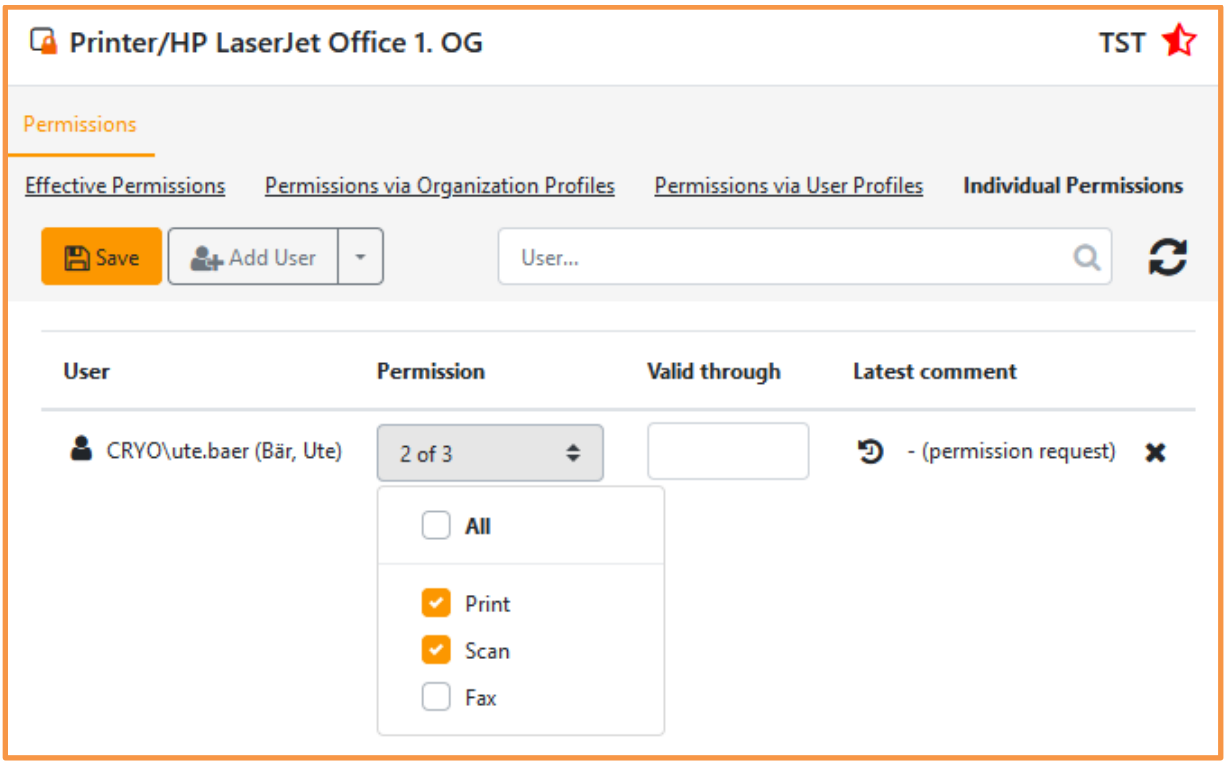
The Responsible can add further User Profiles and grant access to them (button *Add User Profile*). He has the power to change or delete all listed access permissions. With every change of the profiles the belonging user accounts will receive / lose permissions.

4.2.2.1.4 Individual Permissions

This view shows the personally assigned access permissions of a user for a resource with their possibly set end date and comment.



Supplementary Permissions of 3rd Party Items are listed depending on their amount (“All”, some (“2 of 3”)):

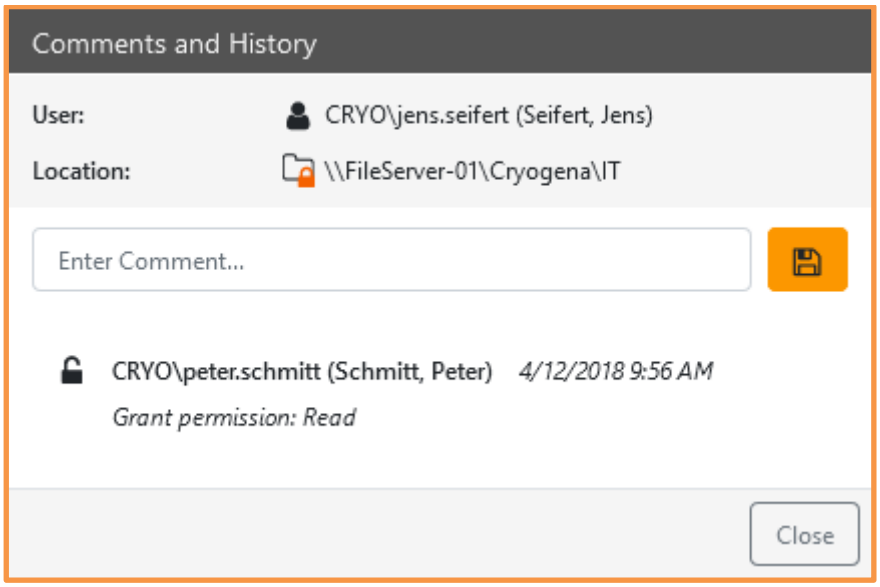


The Responsible has the power to change or delete all listed access permissions and can add further users and grant access to them. This is accomplished by the following buttons:

Add User: The Responsible can add a single user account with the desired permission and an optional end date and comment. If enabled by an administrator, it is possible to alternatively permit an AD group. The difference to the following option is that here the group itself is permitted, without checking for its members. This means that neither right now nor in the future you have control over which accounts will get access – only use this option if you absolutely certain.

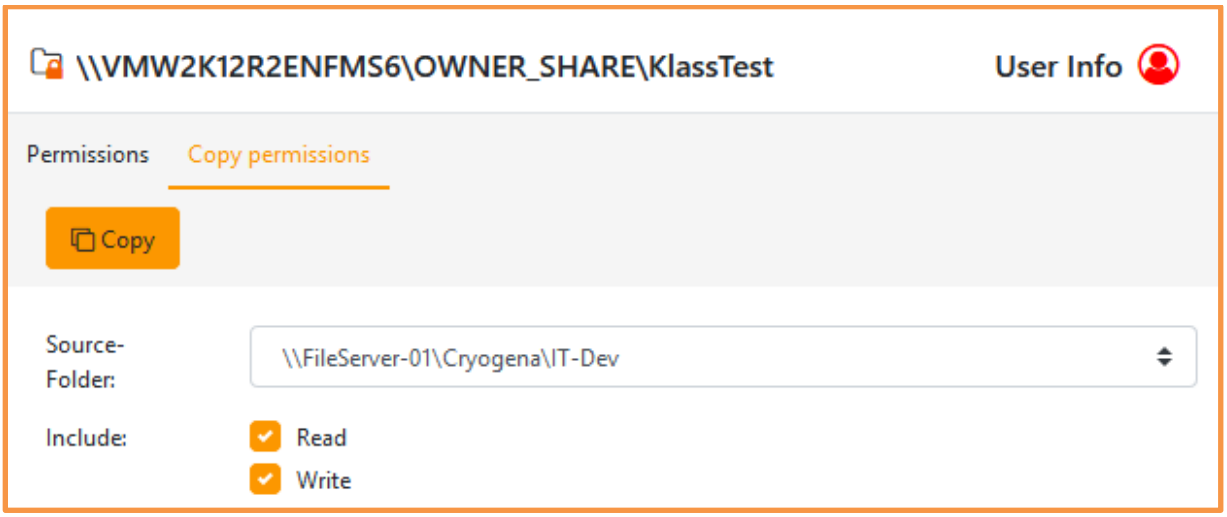
Add Users from AD Group: The Responsible can use this function to specify an Active Directory group. Its members will be listed in a dialog window from which the Responsible can select multiple users for granting them the same access permission. This does not permit the group itself but only its selected members.

A comment must be entered for each permission change if this is required by the respective administrative setting. This setting affects adding / removing a user account as well as changing an existing right (e.g. changing from reading to writing, adjusting the expiration date). The icon opens a dialog in which all previous comments and permission changes can be viewed and new ones can be entered without applying any modification:



All comments will also be shown in the reports with exception of the historic reports.

4.2.2.2 Section "Copy permissions":



This section simplifies authorization of multiple users with a few mouse clicks on a Rights Folder (currently not available for 3rd Party items). The resource[1] from which the users should be copied to the current resource can be determined using the *Source* selection list. From that resource, the *Include* selection list will filter only those users who have either only read or only write permissions. If the *Read + Write* option is selected, all users will be copied with respect to their permissions. However, only users who have been assigned access permissions to the source resource will be taken into consideration. Users with inherited permissions and/or special permission groups will be ignored. The users and their respective permissions will be copied to the current resource by clicking the *Copy* button.

4.2.3 Managing User Permissions

Menu:
Access Management → Permissions

While the sub-page *By Resource* shows a permissions overview from a folders point of view, this page shows which permissions a single user has.

Select *By User* from the list at the left side. The list shows all user accounts, offering various filtering options. Searching for a specific account is possible as well as limiting the display on permitted accounts and active / inactive accounts. After each filter selection, only the first 100 accounts are displayed with the possibility to also load all accounts. Depending on the amount of accounts, this may take a few seconds.

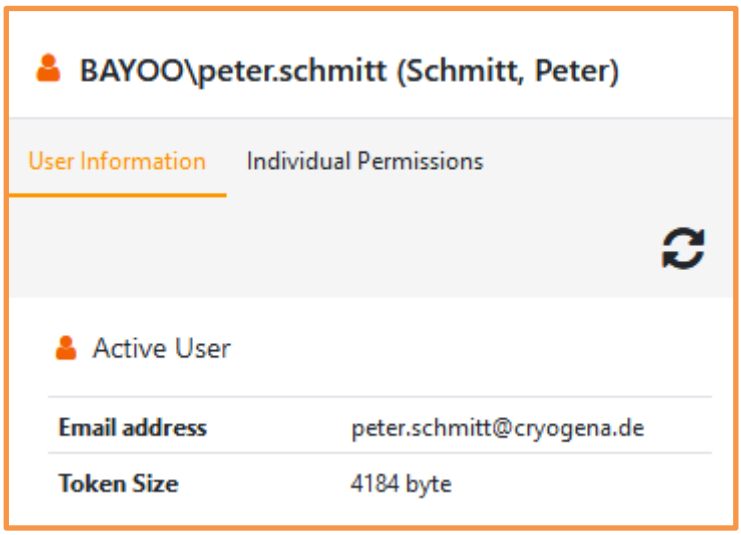
[1] Only the locations will be displayed that are currently assigned to the responsible.

All user accounts are prepended by an icon, informing about their current status:

- Active account with permissions / roles
- Active account without permissions / roles
- Inactive account with permissions / roles
- Inactive account without permissions / roles
- Blacklisted account with permissions / roles
- Deleted account with permissions / roles (may be marked by "***" also)

So called *Blacklisted Users* are usual accounts that are included by the AM Administrator in a blacklist. Therefor they are not handled within search masks and find-as-you-type functionality and are only shown if they already own permissions or roles. Without a request, permissions cannot be granted but only revoked. Existing permissions are still maintained by AM and blacklisted users still have access to the Management Portal to request access permissions.

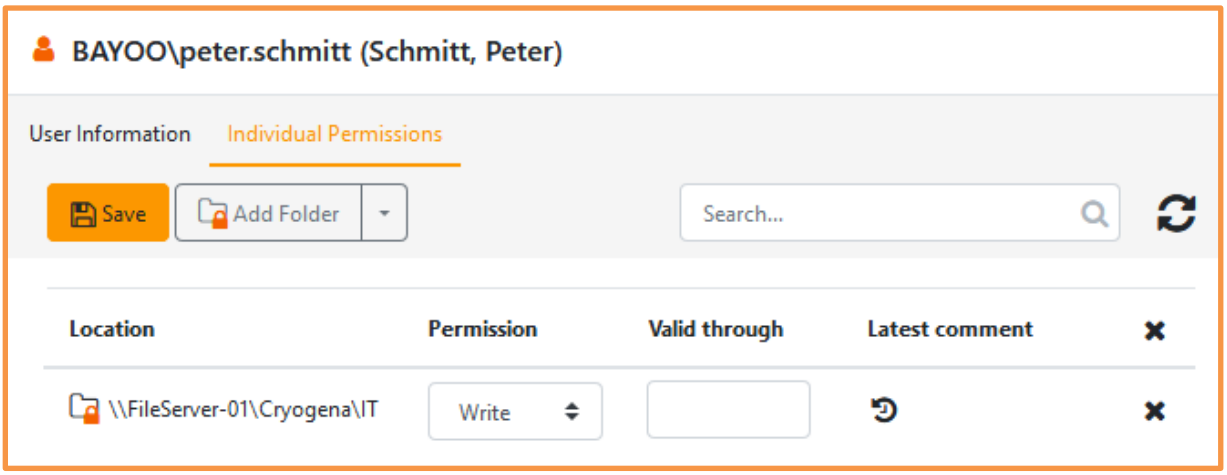
4.2.3.1 Section "User Information"



The section *User Information* contains common information about the user account. This includes e.g. the email address, the home folder (if available) and further technical data.

4.2.3.2 Section "Individual Permissions"

If the section *Individual Permissions* is selected, all resources of the user including the according permissions and, if available, the date of expiry are shown.

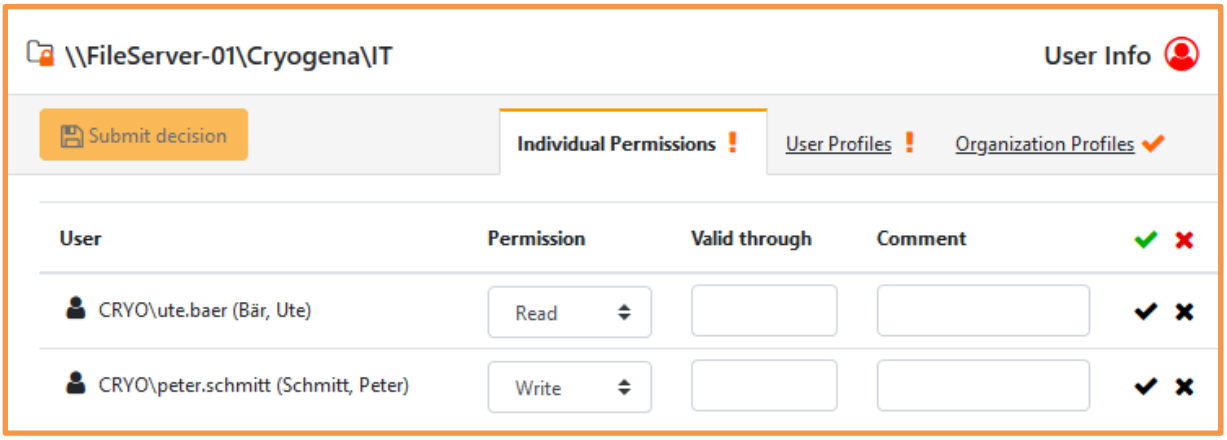


For every resource, the access permission can be changed (Drop Down Menu), a date of expiry can be set (but not longer than a possibly predefined maximum duration), comments can be viewed and added, and the permission can be removed entirely (X icon). Via the X icon in the table header it is possible to remove all permissions for the selected user at once. Permissions for additional resources can be added via the *Add Folder / Add Site* button. All changes are delayed, and the changed row is shown in a different color until the *Save* button is clicked. No automatic emails are sent to the affected parties, since for all these actions no requests are needed.

4.2.4 Performing Reapproval

Select *Permission Reapproval* from the list at the left side.

According to the Reapproval concept (see chapter 4.4), the currently set permissions for users and profiles on managed resources are to be checked and approved on a regular basis. The Owner decides for himself, if and which resources are to be re-checked by assigning a specific classification. This page shows all resources the Responsible oversees and that are chosen for Reapproval. Resources not yet approved within a run are marked by an exclamation mark.



When selecting a resource from the left tree view, the right area lists the currently set permissions grouped by Individual and Profile Permissions. To perform a Reapproval of a resource, all permissions of all tabs (*Individual Permissions*, *User Profiles*, *Organization Profiles*) must be approved to activate the button *Send Decision*. The term “approve” in this context comprises the decisions about keeping permissions as-is, modifying or even withdraw them. To complete a resource reapproval, the specific decision does not matter; simply the fact *that* a decision is taken is relevant. As soon as all permissions within a tab are approved, the exclamation mark changes into a checkmark. Once all tabs are checked the Reapproval of this resource is finished and can be saved – it is not possible to save a partly approved resource.

The option *Show all resources* will also list resources already reapproved.

Depending on your organization´s decision, all yet unapproved permissions may be automatically deleted when a Reapproval run finishes.

4.2.5 Template Management & Assignment

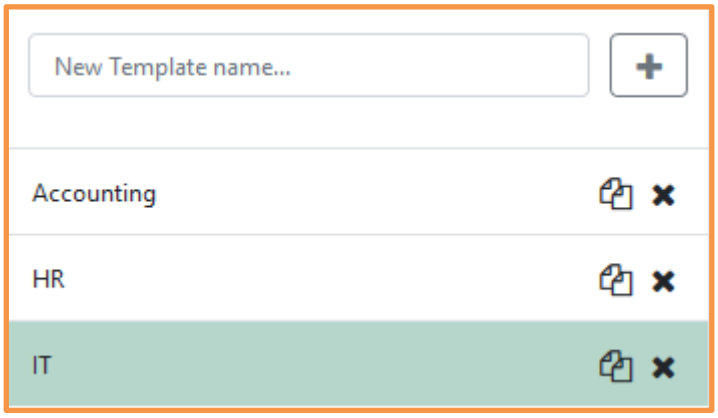
Menu:
Access Management → Templates

4.2.5.1 Creating Templates

As a Responsible you can create templates using the *Templates* page. Responsibles and Substitutes can use these templates to assign a large number of identical permissions and Rights Folders to various users in a simple manner with just a few mouse clicks. This can be helpful when, for example, an employee switches between departments, a new trainee is hired or access should be granted based on user participation in a project. These templates are explicitly private, meaning only visible to and useable by the Responsible who creates them. To make similar functionality available to several users use the *Global Templates* tab page (see chapter 6.4ff).

Templates can only be used for Rights Folders. Managed SharePoint Sites and 3rd Party items are not supported. Consider using Profiles for support of all resource types.

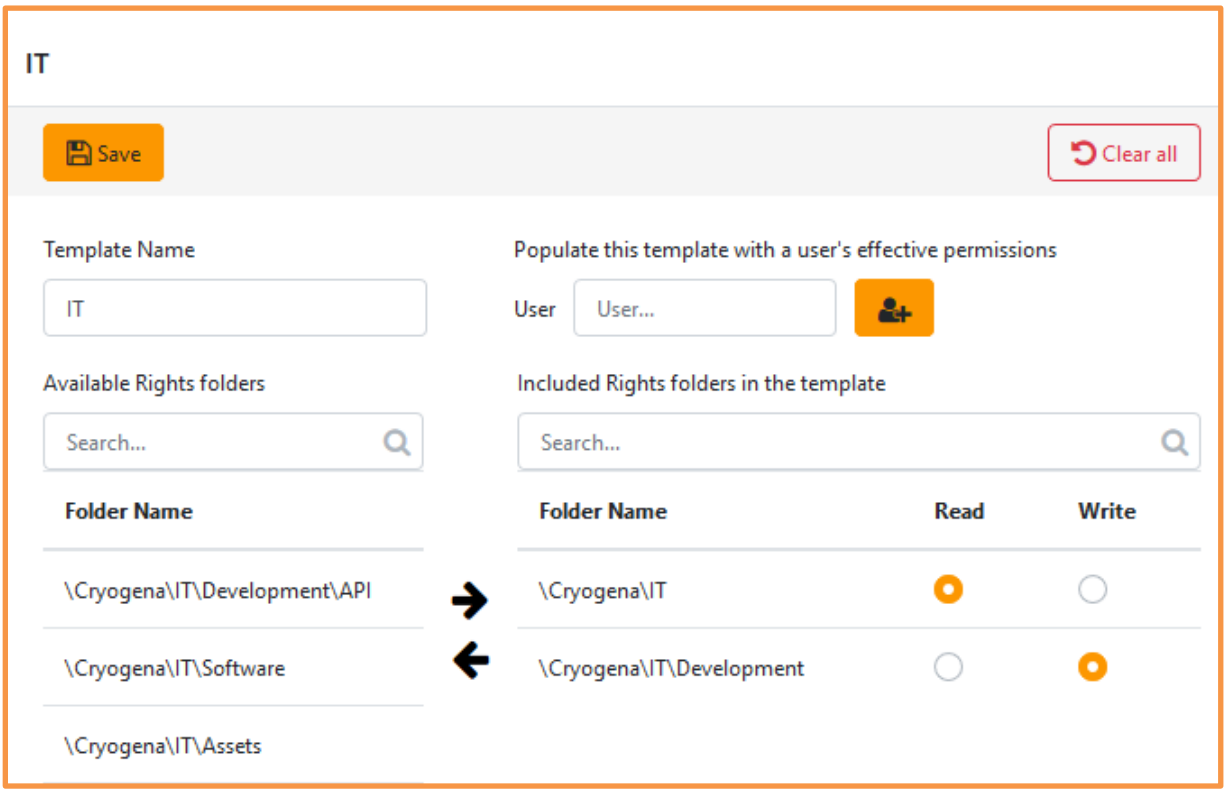
Select *Template Management* from the list at the left side. The list aside has an entry for creating new templates and lists the existing ones:



By clicking the respective icon, actions may be taken for each template:

- *Duplicate*: create a true copy of the template to save it under a different name. During the copy process, all rights folders contained in the template will be kept along with their access permissions.
- *Delete*: remove the template from the system without possibility to recover it.

After choosing a template, all settings are displayed in the details area at the right. You can change the name and specify the desired folders and permissions, either selecting them manually from the list at the left or take over folder permissions from a specific user. Please note that this is not a true copy of all user permissions as you only have access to folders you are the Responsible for.



4.2.5.2 Assigning Templates

Select *Template Assignment* from the list at the left side. All available templates can be executed from this page. The reason for separating the template creation and execution action is the fact that while both Responsibles and their Substitutes can execute templates, only true Responsibles shall be allowed to create templates.

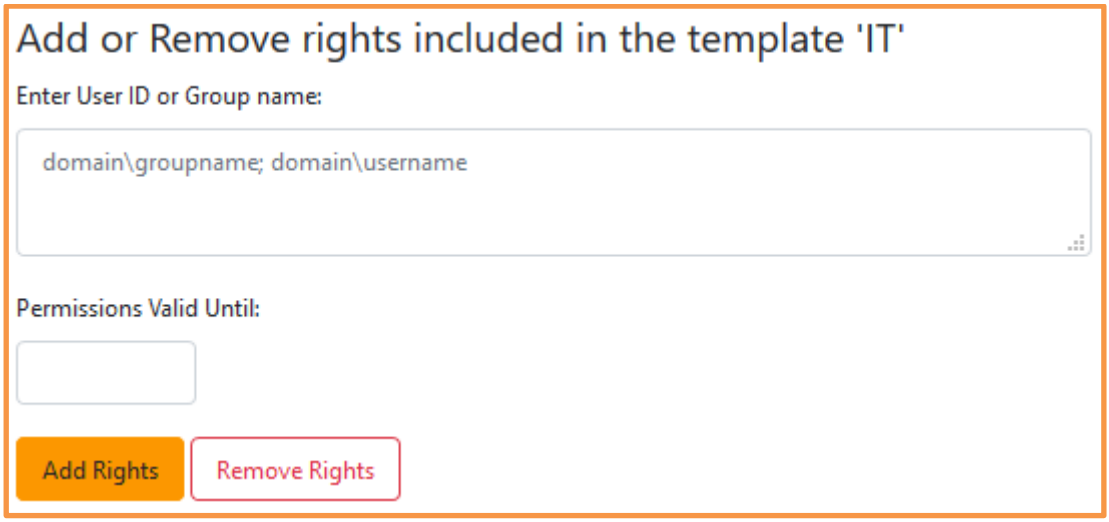
The page is divided into three panes:

- Template selection
- Determining the affected users and access durations
- Displaying the included folders and permissions

4.2.5.2.1 Selecting a Template

The example above shows the potential visibility of templates. The *HR* template was created by the current user, who is also a Responsible. The *IT* template was created by a different Responsible (Peter Schmitt) and is only visible here because you are currently a Substitute for Peter Schmitt. Empty templates without assigned folders will not be displayed in this list, because they cannot be reasonably used.

4.2.5.2.2 Specifying Users & Access duration



The user accounts for which the template should be used will be determined in this section. Use semicolons (;) to separate a list of accounts. You can also specify one or more user groups. The members included in the group will then be listed in a selection list afterwards. The expiration date for the permissions can also be specified.

Buttons *Add Rights* / *Remove Rights*:

As assigning permissions using a template can affect users who may already have access permissions for one or more folders included in the template, it may be important to know that any existing permissions will not be reduced by such assignments; existing permissions that grant higher access rights to users will always have precedence[2] over assignments made by templates.

[2] This means that if a user already has the write permission for a folder, the right will be retained even if the template grants a read permission to the user.

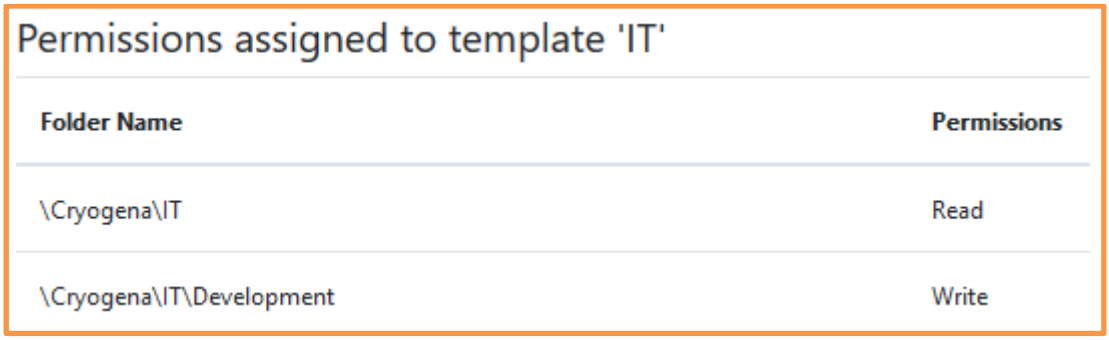
If an expiration date has not been specified, the change to the permissions will take the rule above into consideration immediately and permanently. Otherwise, the following rules will apply:

- *Add Rights*: All users and groups specified will immediately be assigned the respective access permissions to the folders and the expiration date will be set (in consideration of the rule above). If necessary, the previous or existing expiration date will be extended by the template.

- *Remove Rights*: New rights will not be set, however already existing user and group permissions will be assigned an expiration date, if the setting involves same permission as the one in the template (meaning only an existing read permission is updated by a read permission in the template or the same will apply with regards to a write permission). An existing expiration date would first take effect later. This means that the time frame for a permission will be reduced at most but can never be extended.

If either the *Add Rights* or *Remove Rights* button is clicked, the permissions will be set for all specified users and they will be notified by email as will the responsible.

4.2.5.2.3 Displaying Folders of a Template



For the purpose of checking, the folders defined in a template and their access permissions will be displayed after the template has been selected but they cannot be modified.

4.3 Owners Tasks

As an Owner you have access to the main menu item *Access Management* which allows further sub items for managing your resources.

A user will receive the *Owner* role through explicit assignment by an *AM Administrator* or another *Owner* of this resource. The *AM Administrator* role is a special role for AM system permissions which lies outside of the role design for regular operation. There is no intention of being able to apply for this role through the Access Manager Management Portal itself. Usually, a person will be appointed *Owner* for a top-level folder (at most, at Share/Site Collection/Item level) through an organizational decision. He will then be the Owner of all resources below the assigned one at first. For a certain resource (and its sub-resources) at a lower level, the role will be granted when another person should get ownership.

4.3.1 Processing Requests

Menu:

Access Management → Requests

This page shows the user requests. This includes the creation of new managed resources, removal of the status as a managed resource and applications for responsible rights. First, select from the left if you want to work on open (that means yet unprocessed) or closed requests. They are listed on the right side and can be searched or filtered based on various criteria.

When processing requests, they may be granted (un-)changed or rejected entirely. Once processing has been completed, both the user and applicant receive an automated email message with the results of the request.

Depending on the type of request, the folder owner may have to perform more or less additional tasks, such as the determination of a responsible as an additional step in the creation of a new managed resource.

To check and process a request, unfold the entry with the DropDown icon ⌄. If all necessary information is already available, you may immediately grant (icon ✔) or reject (icon ✖) the request without confirmation.

4.3.2 Structure Management

Menu:
Access Management → Permissions

Select *Structure Management* from the list at the left side. The tree view will now display your own resources[3] that you can select for processing as desired.

The right Details pane has a header row, containing the resource´s address and a potentially set classification.

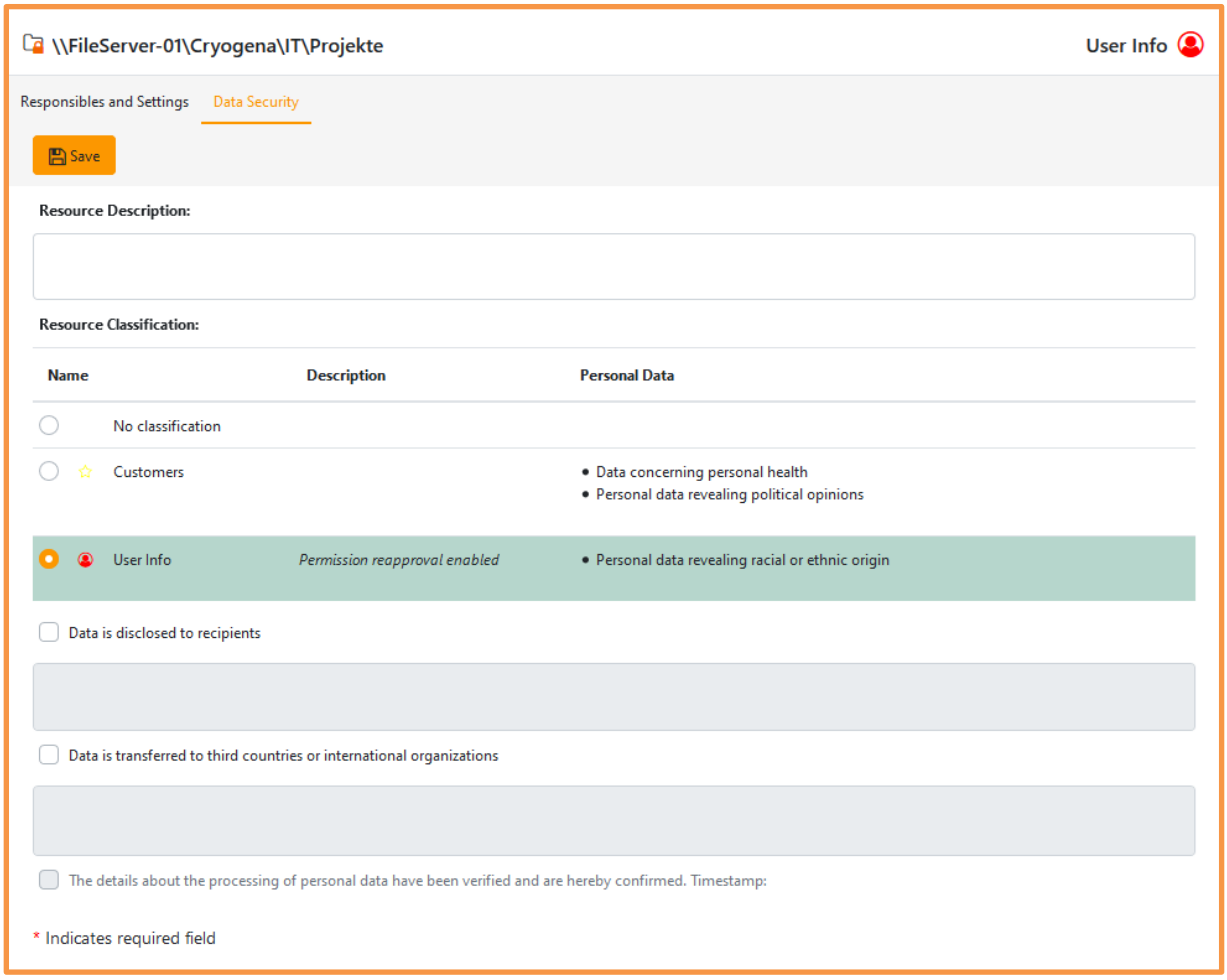
4.3.2.1 Section "Owners and Responsibles"

This is where the Owners and Responsibles for the directory are managed, i.e. you can use the *Add User* button to make other people Owners - or also Responsible if it is a managed folder. If the folder is not currently managed, you must first switch on the Permission Management via the *Settings* tab (see the following chapter 4.3.2.3).

As the owner, you may also withdraw the owner role from other people. If permitted by the administrator, you can also revoke the role for yourself. Please note that if you do this you will lose all management rights of an owner and you will no longer be able to give yourself this role again!

[3] In contrast with other tree views, this will display not only the managed locations, but also existing unmanaged ones.

4.3.2.2 Section "Data Security"



Resource Description: Depending on the administrative setting done by the *AM Administrator*, a description may or must be entered.

Resource Classification: The Owner can assign a given classification to the resource or switch to another one. Removing a classification from a resource is accomplished by selecting the option *No classification*. Available classifications can only be defined by a *Classification Administrator*. For more details about Classifications, please see chapter 7.1.

Activating the checkbox *Data is disclosed to recipients* or *Data is transferred to third countries or international organizations* saves this EU-GPDR related information along with an optionally entered comment in the context of the resource selected. It may also be altered by a *Classification Administrator*.

The option *The details about the processing of personal data have been verified and are hereby confirmed* informs the *Owner* that the above information are validated by another party. The *Owner* cannot set this option (and its timestamp) himself, but changing the above-mentioned options will reset it, stating it is not validated anymore (needs to be re-validated by a *Classification Administrator*).

Click button *Save* to confirm the changes.

Assigned classifications are not visible to normal users (applicants). The Responsible of a classified resource can tell the classification from the icon displayed on new permission applications. It is also displayed in resource details pane of a selected resource.

Concerning Reapproval:
In case the *Classification Administrator* has enabled *Reapproval* (chapter 4.2.4) for a classification, all resources that the Owner has assigned, the respective classification will be added to the Responsibles´ list of Reapproval resources. The Owner can tell whether a classification is marked for Reapproval or not by a corresponding information within the selection list.

4.3.2.3 Section "Settings"

If the folder is not yet managed, there are no settings that can be changed. To do this, first click the *Add Permission Management* button. The directory is now immediately, without further prompting, converted into a managed folder. All owners of the parent folder are entered, as well as you as the *Responsible*. From this point on, you can access the settings described below.

4.3.2.3.1 Visibility in Self Service Portal for Applicants

The following options define the visibility of managed resources for requestors in the resource tree view:

Visible in Self Service shows the resource. A Requestor can submit any application.

Visible in Self Service, Requests not enabled also shows the resource but displays it as unmanaged, so users cannot file a request. This option is not available for 3rd Party Elements.

Not visible in Self Service fully hides the resource from users. This also applies to resources having managed child resources.

It is important to know that the visibility and the access options for the resource will not have any effect on the actual resource in the share/site.

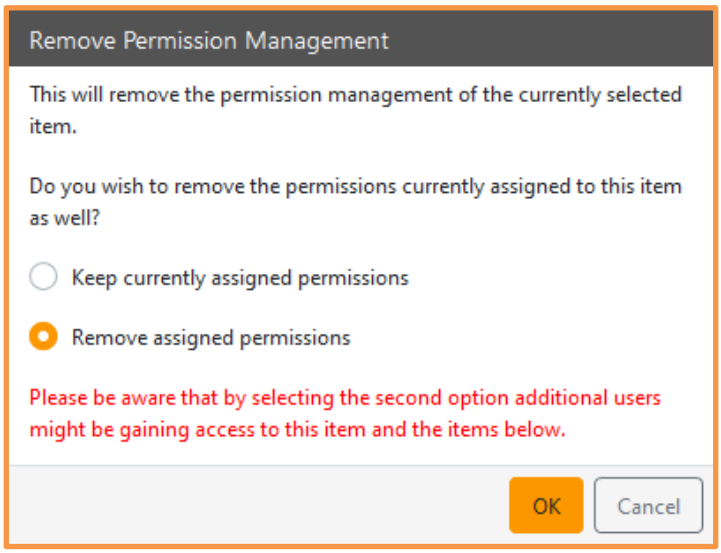
4.3.2.3.2 Inherit or not Permissions from Parent Folder

Using the *Enable Permission Inheritance* button (only available for directories, not for SharePoint Sites) you can set for this managed folder that the user permissions of the parent folder shall be inherited. This is indeed an inheritance, even in the NTFS file system – the rights are not just copied from above. This button is not present if the current folder is the first in the permissions hierarchy because it cannot inherit from anyone. In the case of a normal folder (not a permissions folder), inheritance cannot be switched off because such folders always inherit their permissions from the parent directory.

If the folder is already inheriting, the button is called *Disable inherit permissions*. To stop inheriting, you must decide in the following dialog whether the inherited permissions should be removed or converted into explicitly set rights. In the latter case, Access Manager ensures that any existing rights are summarized for each user. The higher or longer lasting permission is adopted.

4.3.2.3.3 Removing Permission Management of a Folder

Alternatively, the folder can be converted into a free, unmanaged one by clicking the *Remove Permission Management* button. When doing this, the owner must take a decision regarding the management of the permissions:

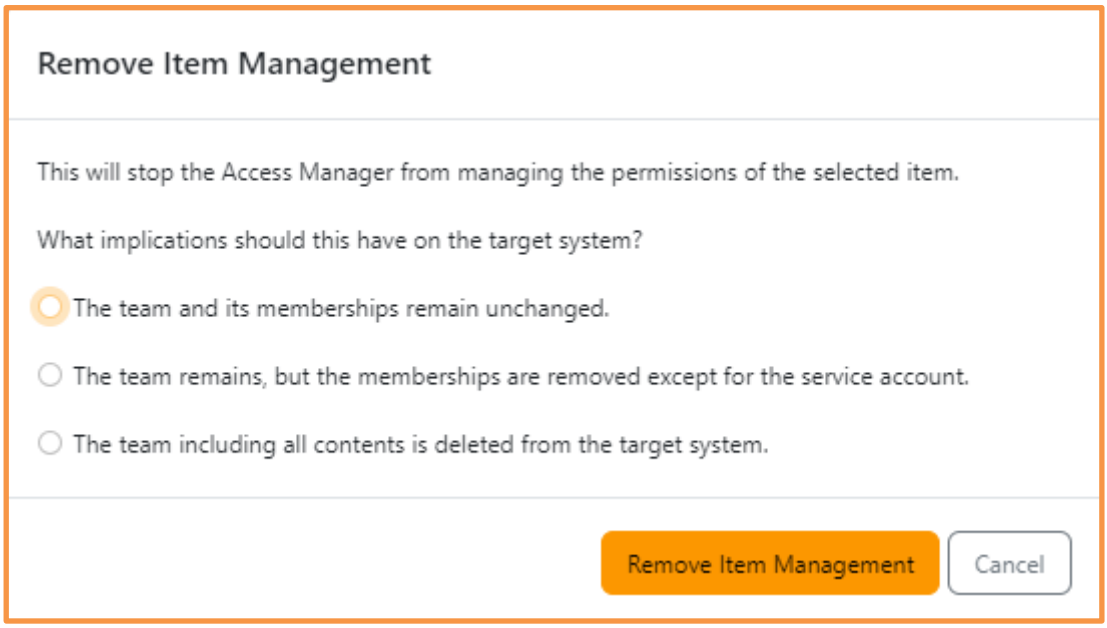


The user permissions set for this folder can either be removed completely or optionally be retained. If permissions are removed, the folder will remain accessible to users nonetheless (however for different users than before, possibly), because it will inherit the parent folder´s permissions. If the current permissions are retained, inheritance will not be used, and the same people will continue to have access to the resource.

For consistency and clarity compared to other unmanaged resources,
it is advised to remove assigned permissions.

4.3.2.3.4 Removing Permission Management of a SharePoint (online) Site or MS Teams

On such an element type, removing the administration works in principle as described above, but you have further options:



Essentially you have to decide if you just want to remove the item from Access Manager administration (1st option) or if the removal should also affect SharePoint / Teams.

4.3.2.4 Delete Folder

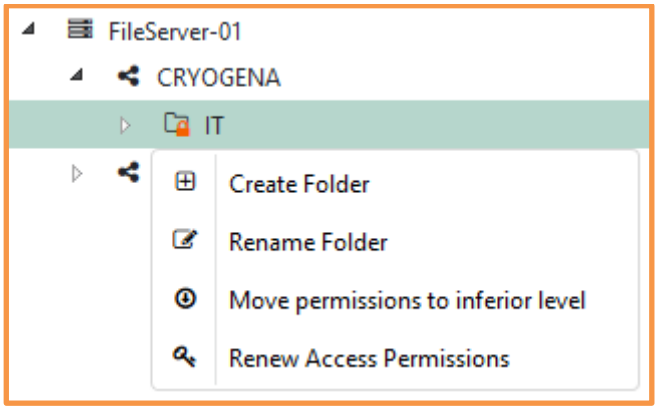
It is possible to physically delete a folder – regardless of being managed or not – directly out of Access Manager. Click button *Delete Folder* and acknowledge the confirmation dialog.

Firstly, the system will check if further managed folders exist with different owners. If so, you are informed and are not allowed to proceed. Else, deletion is started as a background job, as this may take a while, depending on the number of included files and folders. The folder / folder structure will be deleted recursively, beginning with the innermost folders. If an error occurs, all further processing is cancelled, and the cause is stated in the finishing email. All deletions up to this point a final, there will be no restore.

For all successfully deleted folders, not only the management status is removed, but also open applications are abandoned an, depending on administrative setting, AD groups are deleted as well. In any case, a finishing email is sent to you as the owner who triggered the deletion – other co-owners will not receive this email.

4.3.2.5 Context menu

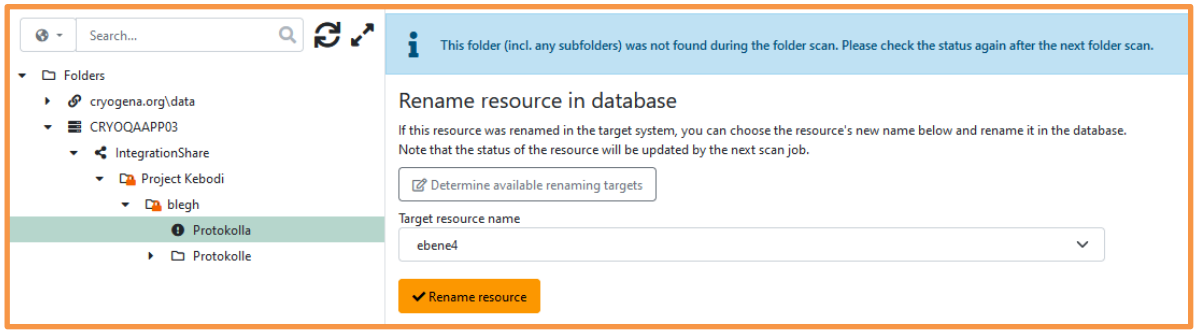
In addition to the Detail section, a context menu can be opened from the tree view by right clicking on a folder. The menu provides the following options, depending on the depth and type of the resource:



- *Create Folder:* Selecting this option will create a new, initially unmanaged folder in the file system. Per definition, it will inherit all access permissions from its parent rights folder. The naming rules globally set by the *AM Administrator* will be used to validate the chosen name. The similar function is available also for SharePoint Sites.
- *Rename Folder:* The name change will also be made to the file system. The naming rules globally set by the *AM Administrator* will be used to validate the chosen name. The similar function is available also for all modules. In the case of SharePoint and MS Teams, please note that the renaming also applies there, not just in Access Manager. This also applies to the description field.
- *Move permissions to inferior level:* If the folder is a Rights Folder, this status can be transferred to all *immediate* child folders and removed from the current folder. If a child folder has been an unmanaged folder until this time, it will be converted into a Rights Folder with the same settings (assigned Responsibles, user access permissions and so on). If the sub-folder has already been a Rights Folder, it will retain its previous settings and also receive the settings of the parent folder (through logical concatenation).
- *Renew Access Permissions:* Usually this function is only available to Administrators. If the AM Administrator has activated this feature also for Owners, you can force AM to update access permissions on the selected resource immediately.

4.3.2.6 Repairing missing Rights Folders

It may happen managed folders are renamed, moved or deleted in the file system without Access Managers´ knowledge. The periodically running scan job will encounter this and mark the missing folder with a distinct icon. As such errors cannot be repaired automatically, the Administrator may have granted you the possibility to do so yourself. If you are sure the folder still exists here and was simply renamed, you can select one of the sibling unmanaged folders and thereby instruct Access Manager to handle that folder as the missing one. Your decision is processed not before the next planned run of the scan job.



For any other cases, please contact your administrator.

4.3.3 Managing Responsibles

Menu:

Access Management → Permissions

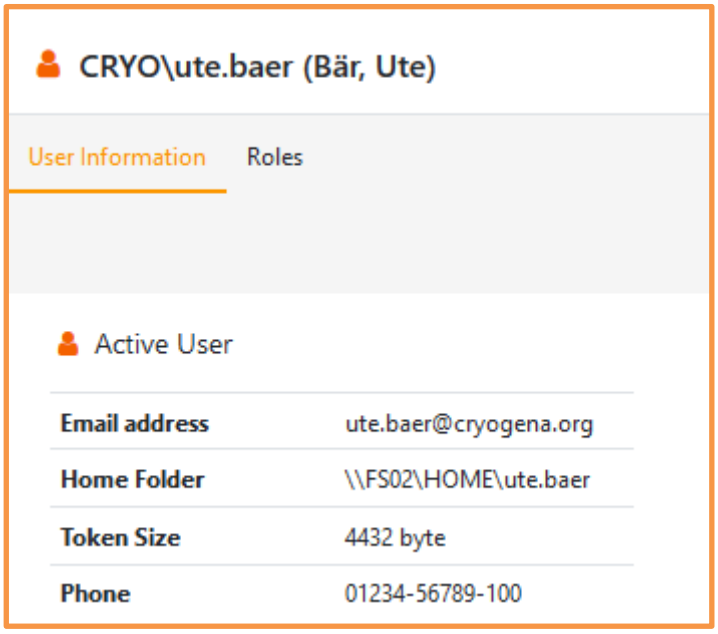
Select *By User* from the list at the left side. The list aside shows all Responsibles of the logged in Owner, offering various filtering options. Searching for a specific account is possible as well as limiting the display on permitted accounts and active / inactive accounts. After each filter selection, only the first 1000 accounts are displayed.

All user accounts are prepended by an icon, informing about their current status:

- Active account with permissions / roles
- Active account without permissions / roles
- Inactive account with permissions / roles
- Inactive account without permissions / roles
- Blacklisted account with permissions / roles

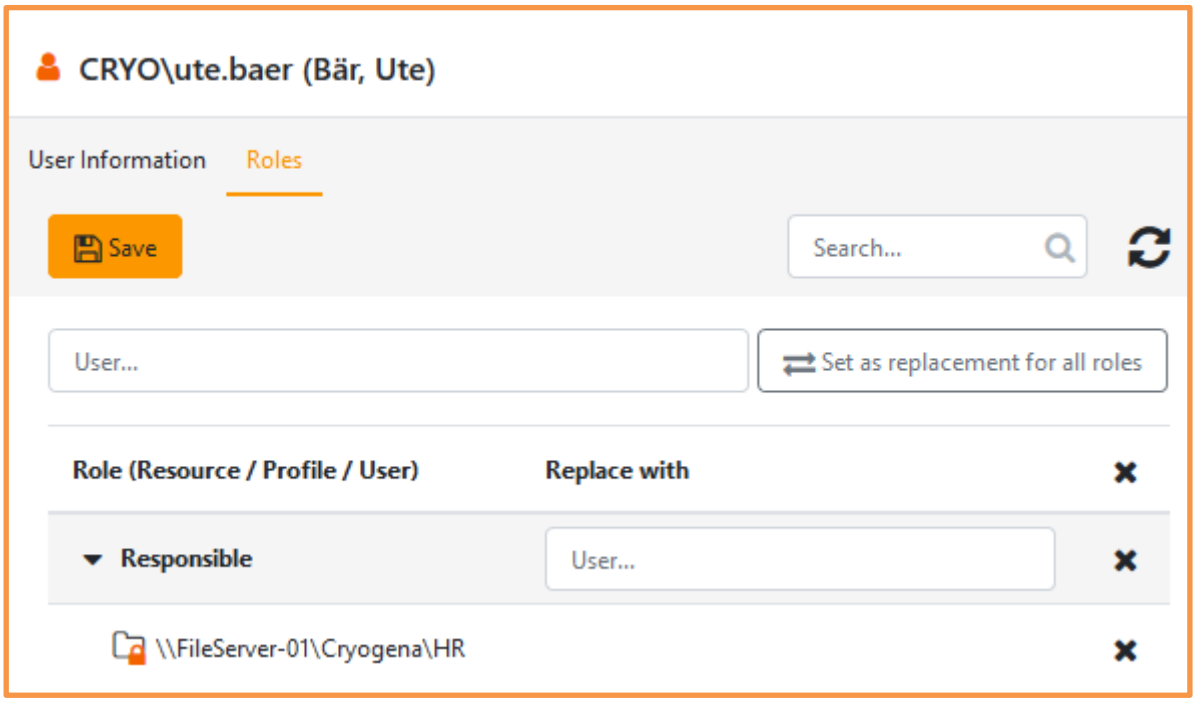
So called *Blacklisted Users* are normal accounts that are included by the *AM Administrator* in a blacklist. These accounts are not handled within search masks and find-as-you-type functionality and are only shown if they already own permissions or roles. Without a request, permissions cannot be granted but only revoked. Existing permissions are still maintained by Access Manager and blacklisted users still have access to the Management Portal to request access permissions.

4.3.3.1 Section "User Information"



The Tab *User Information* contains common information about the user account. This includes e.g. the email address, the home folder (if available) and further technical data.

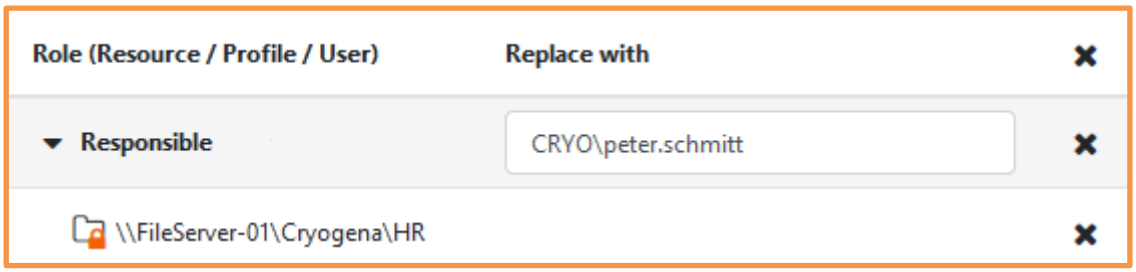
4.3.3.2 Section "Roles"



If the tab *Roles* is selected all resources of the selected user which are managed by the logged in Owner are shown under the category *Responsible*. Via the **X** icon next to every resource it is possible to

remove the according *Responsible* role for the selected user. However, this is not possible (**X** icon grayed out) if the selected user is the only one with this role for the according resource. All changes have to be confirmed by clicking the *Save* button.

Alternatively, a user can also be replaced by another user:



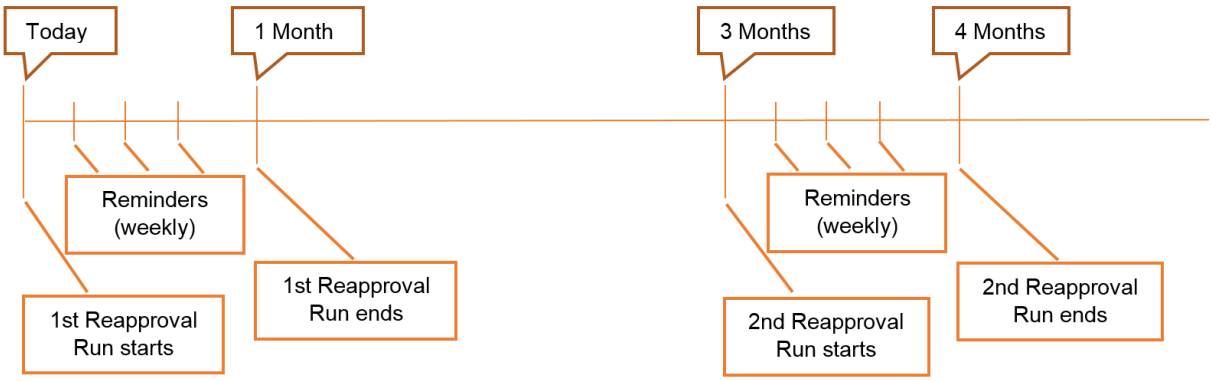
This replacement will also only happen after the *Save* button has been clicked. All affected users will be informed via email.

This functionality is especially helpful for discovering deactivated user accounts and migrate their management roles to other persons.

4.4 Reapproval – Workflow for repetitive Permission Checks

The *Reapproval* function is used to regularly check certain resources (folders, SharePoint Sites, 3rd Party items) for set permissions still being necessary / desired.

A Reapproval run is defined by an *AM Administrator*. The run starts in fixed intervals (i.e. every three months) and lasts for a specific duration (i.e. four weeks). Within this period, the accounted resource *Responsibles* are reminded multiple times by email as long as they have not yet finished the needed checks.



Generally, a Reapproval is always performed per resource. It includes a confirmation, update or removal of current permissions for user accounts and profiles. As soon as a Responsible has approved all of his resources he has finished his task for the current run.

Reports offer the current status of the resources to be checked at any time during an active run. If there are still unapproved resources at the end of a run, user permissions may be removed automatically, depending on your company´s decision.

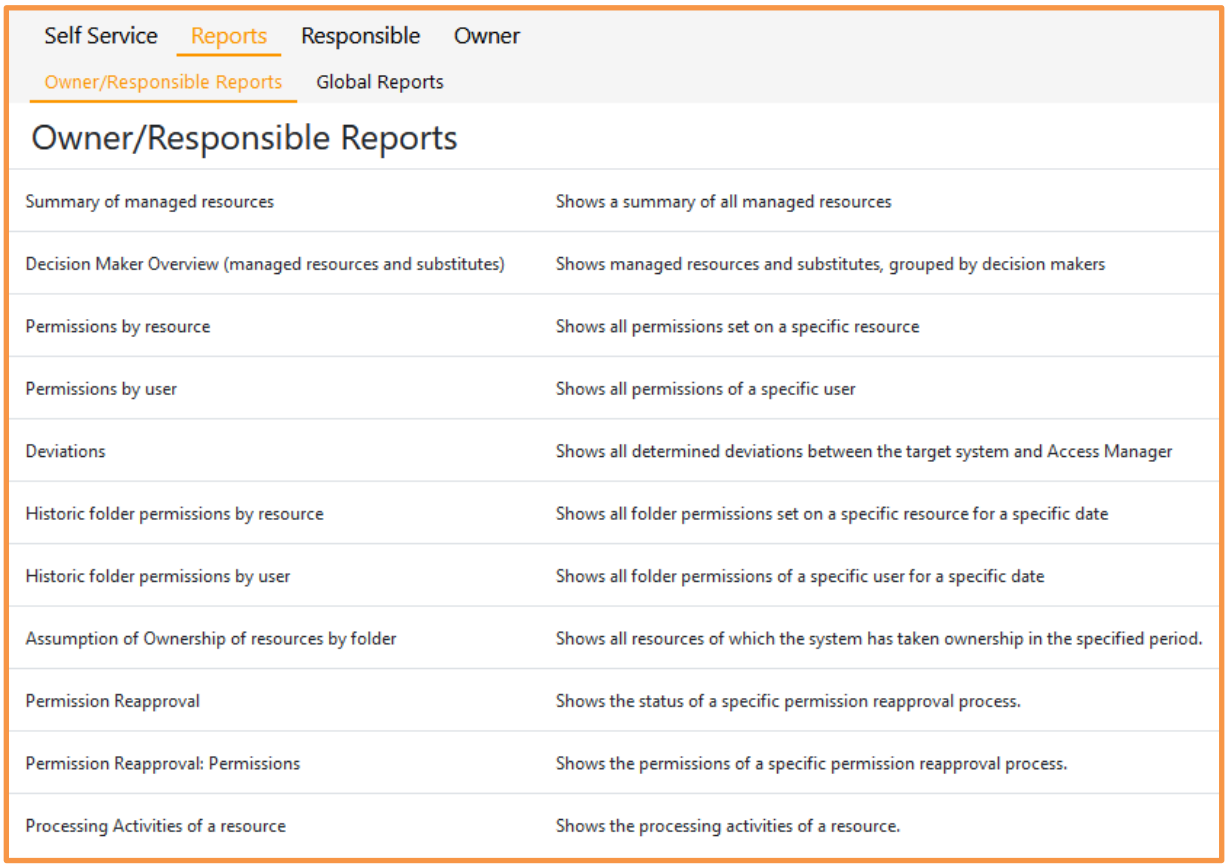
4.4.1 Responsibilities

While the *AM Administrator* defines the repetition interval and duration of a Reapproval run, the *Owner* decides which resource is to be included in a Reapproval run for regular permission checks that will be performed by the corresponding *Responsibles*.

4.4.2 Reapproval Assignments

Firstly, the *Classification Administrator* creates new classification entries with the option activated for Reapproval. The *Owner* then has the possibility to assign such classifications to the desired resources. Starting a run, the *Responsible* automatically receives a request for reapproving his resources and performs this task.

5 Reporting



Reports provide information about various aspects of the resources managed by deciders (Responsibles, Owners). Using this feature, all resources for which the current user is responsible can be summarized. The descriptions of the reports make them self-explanatory. The summarized data will be current at the time when the report is generated.

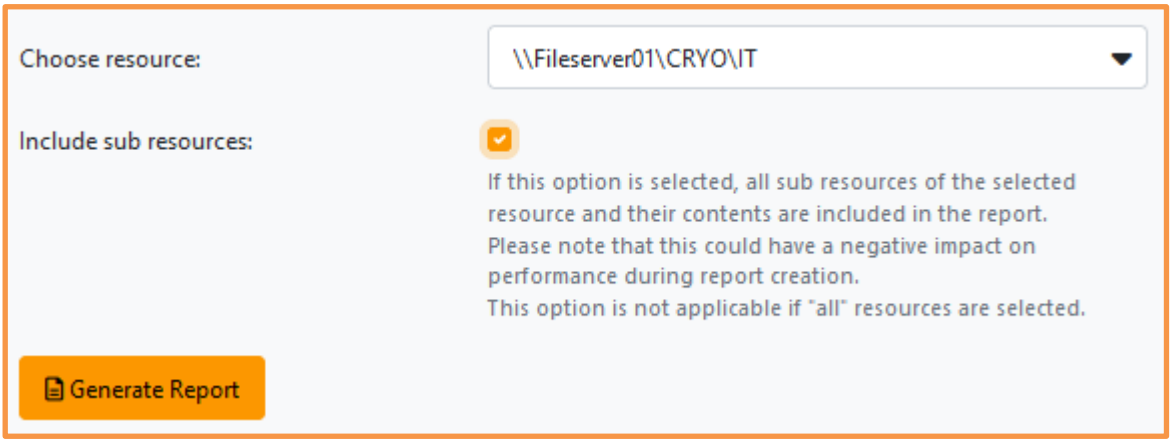
When selecting a report from the list, a filtering area occurs at the bottom with options to limit reported data by means of the users´ role, specific categories, or user ID / AD group and more.

5.1 Reports for Data Owners

Usually, deciders who have the role *Owner* / *Responsible* only get reports covering their own (personal) managed resources – all other data is kept away.

If a user owns both kinds of roles, he can choose the necessary type from the sub menu. Both report types are identical, they just differ in the amount of data returned.

For some distinct report types, an additional option is available to choose whether reporting only the selected resource or also its subsequent ones (not possible for 3rd Party Item Collections):



For these report types the option is available:

- Permissions by resource
- Deviations
- Permission Reapproval: Permissions
- Processing Activities of a resource

In the *Permissions by User* report, exactly one user account can be specified in the *Choose User/Group* field; The authorizations for this account are then displayed.

If you do not specify a user, you can use additional filters to limit the number of user accounts that will then appear in the report.

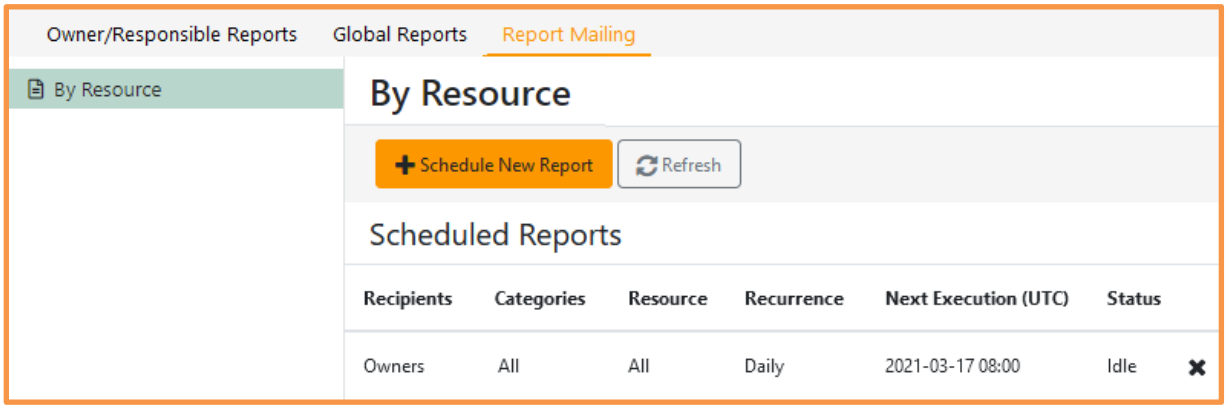
5.2 Global Reports

Users having the role *Administrator* / *Report User* will receive person-independent (global) reports, including all resources.

If you own both the roles *Administrator* / *Report User* and *Owner* / *Responsible*, you can choose the report type (*Owner/Responsible Reports* or *Global Reports*) from the sub menu. Both report types are identical, they just differ in the amount of data returned.

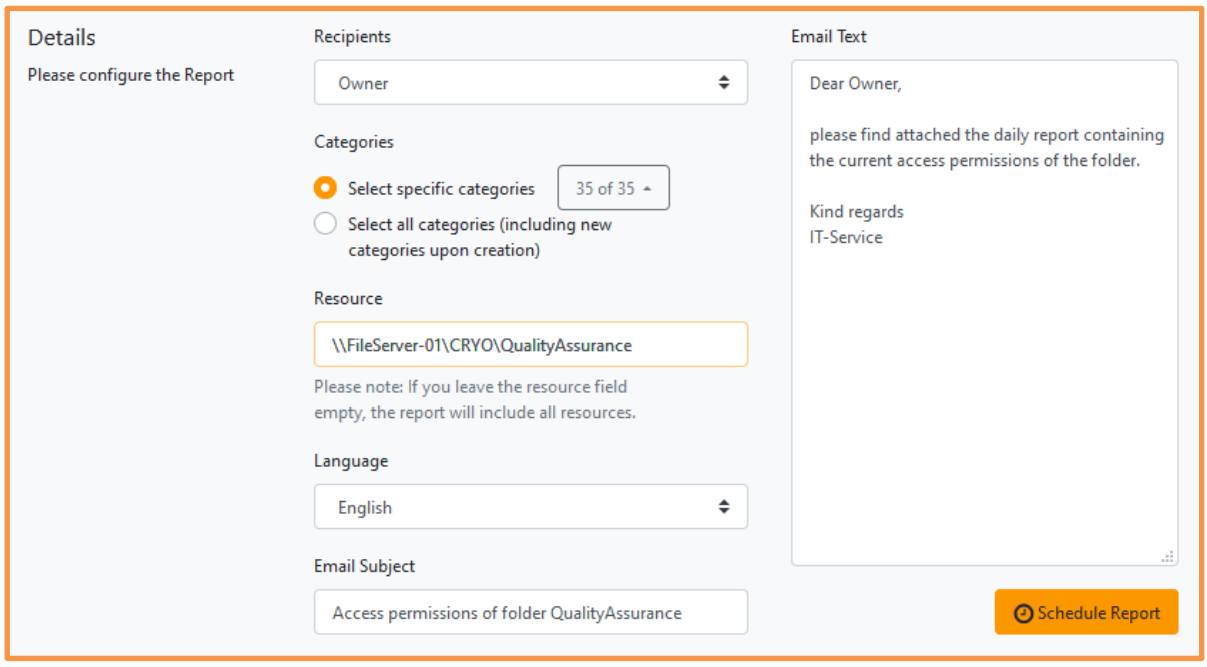
5.3 Report Mailing

Being an *Administrator*, you have one more option available: *Report Mailing*. Here, you send the report *Permission by Resource* to a distinct audience as PDF document by email, optionally only once or repeatedly based on a schedule. Existing mailing plans are displayed in the overview:



5.3.1 Creating Mailing Plan

To create a new Report Mailing, click button *Schedule New Report*. At the bottom screen, enter the necessary mailing information:



5.3.1.1 Recipients

Select the audience to receive the report. When selecting *Owners* or *Responsibles*, only the persons receive the report who are in charge of the included resources – not all users having this role.

5.3.1.2 Categories

Choose which type of resource your report will cover.

Using the first option, you can select distinct categories (resource types) that will be included in the report. This is a static selection, meaning that it will not change even if new resource types are added to Access Manager in the future. In contrast, the second option will dynamically evaluate all categories available at the very time of creating the report.

5.3.1.3 Resource

If you leave this field empty, all resources of the above selected categories are reported. Alternatively, specify exactly one resource here. For more resources, create a mailing plan for each resource separately.

5.3.1.4 Language

Select the language of the report (English / German). This option has no effect on the email subject and email text described below.

5.3.1.5 Email Subject

Enter your email subject here.

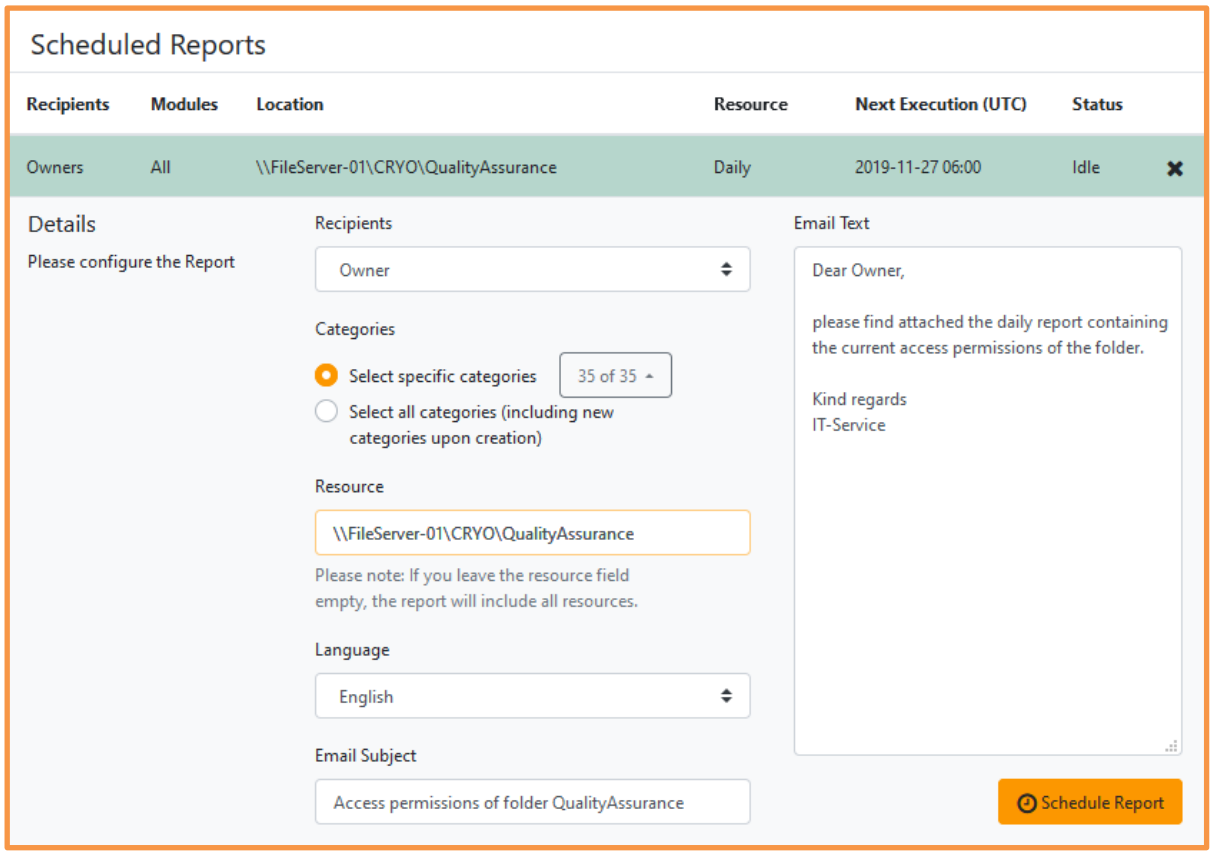
5.3.1.6 Email Text

Enter your email text here. Currently, no variables and formatting options are supported.

5.3.2 Adding / changing Schedule

After you have entered all information for your new mailing, click *Schedule Report*, bringing you to the scheduling dialog window. This is the same interface that you have for *scheduling jobs* (chapter 11.4). Finish the mail planning with the button *Schedule Job*. Afterwards, you will find this in the *Job Queue* (chapter 11.7) with the name *SendReports*.

To alter an existing mailing, click the respective record in the overview list. At the bottom screen the mailing details are displayed and editable. Click Change Report Scheduling to proceed to the time planning. You must finish that dialog to save also the (textual) changes made before.



5.4 Report "Permission Reapproval"

Besides *AM Administrators*, this report is available only for *Owners* and their *Substitutes*, while the latter will only have access as long as they have the *Substitute* role. The DropDown List *Select Date* offers the start time of each Reapproval run. The report shows the current reapproval status, Owner and Responsibles for each resource marked for Reapproval.

5.5 Report "Permission Reapproval: Permissions"

Besides *AM Administrators*, this report is available for both the *Owners* and *Responsibles* (including their *Substitutes* while they have this role). The DropDown List *Select Date* offers the start time of each Reapproval run. After selecting a run, specific / all resources can be specified having a Reapproval-enabled classification assigned. The report shows the current status, previously permitted objects (user accounts / profiles) and the approver and his decision (approved / withdrawn) for each resource marked for Reapproval.

5.6 Report "Processing Activities of a Resource"

This report is only available for *Classification Administrators* and shows privacy-relevant information for managed resources. Besides the list of all *Classification Administrators*, each classification used is shown with its details and the resources assigned to the respective classification.

Filtering options include filtering by module and by classifications that a resource should have.

5.7 Report "Deviations"

This report lists all permissions the system has discovered for managed resources after an executed maintenance job that differ from what is defined in AM.

The generated report contains the following columns per resource:

Date:
Timestamp of deviation discovered.

Type of deviation:
Not authorized user – User / Group object which must not have been included in the Access Manager AD group.

Not authorized permission – User / Group object which must not have resided in the file system.

Missing user – User / Group object which was missing from the Access Manager AD group.

Missing AM AD group – AM group object which was missing from the file system.

Principal:
The AD object which was edited / deleted from the file system.

Permissions:
Details on the incriminated permissions of the mentioned AD object.

Deny rule:
Flag if the deviation was a deny rule.

Inherited:
Flag if the permission was inherited.

Additional information:
In case of *Missing user* and *Not authorized user* in column *Type of deviation*, this column states the user / group object that was missing / superfluous in the Access Manager AD group.

5.8 Report "User accounts by organization structure"

This allows you to create reports that provide information about all identities and accounts registered and managed in the IDM module and their position in the organizational chart. You can choose between the responsibilities in the organizational structure.

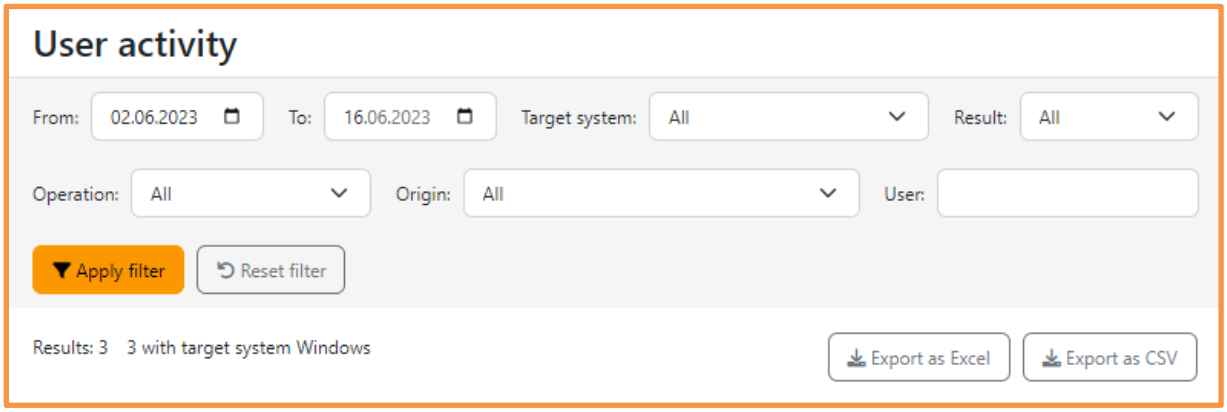
If there are identities without accounts in the report, this does not mean that the user does not have any accounts, but that IDM does not manage any accounts for this identity. The identity is then known to the IDM module through possession of the personnel manager system role and may be assigned as a team leader.

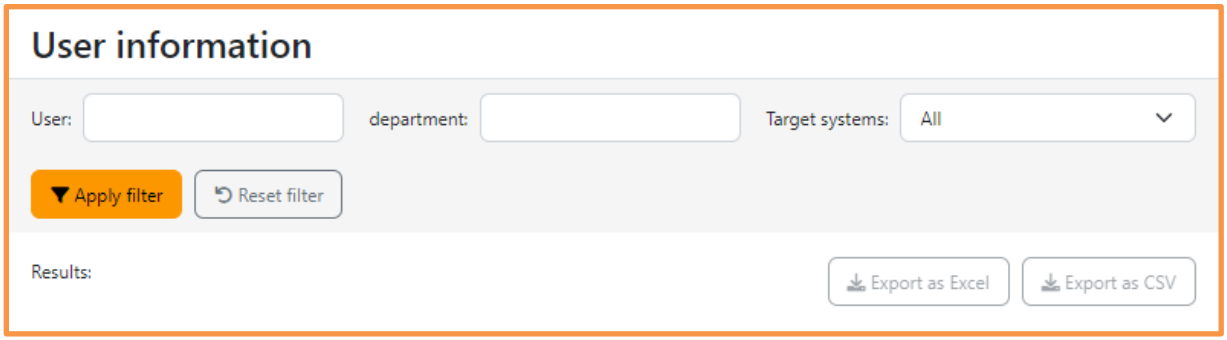
5.9 Password Reports

As an AMPR Administrator you may let the system create reports, listing information about user accounts or their actions within a specific timeframe.

Menu:

Reports → Analysis → User Activity
Reports → Analysis → User Info





These menu items are part of AMPR.
For more information, see the AMPR manual.

6 Permission Management with Profiles & Templates

Menu:

Profiles & Organization

Profiles and Templates make permission management more flexible and can save a lot of manual effort. One can distinguish between *Profile* and *Template* Management.

Using *Profiles*, the *Profile Administrator* can define groups of users and resources and assign permissions to a number of users. Profiles offer a flexible way for assigning, revoking and grouping by self-defined hierarchies.

The user can create templates using the *Global Templates* page. Other users can use these templates to assign a large number of permissions and Rights Folders to various users in a simple manner with just a few mouse clicks where those permissions and Rights Folder are always the same. This can be extremely helpful when, for example, an employee changes department, a new trainee is hired or access should be granted based on user participation in a project. These templates are public as per definition, meaning they are visible and useable by several people. To create private templates as a *Responsible*, see chapter 4.2.5.

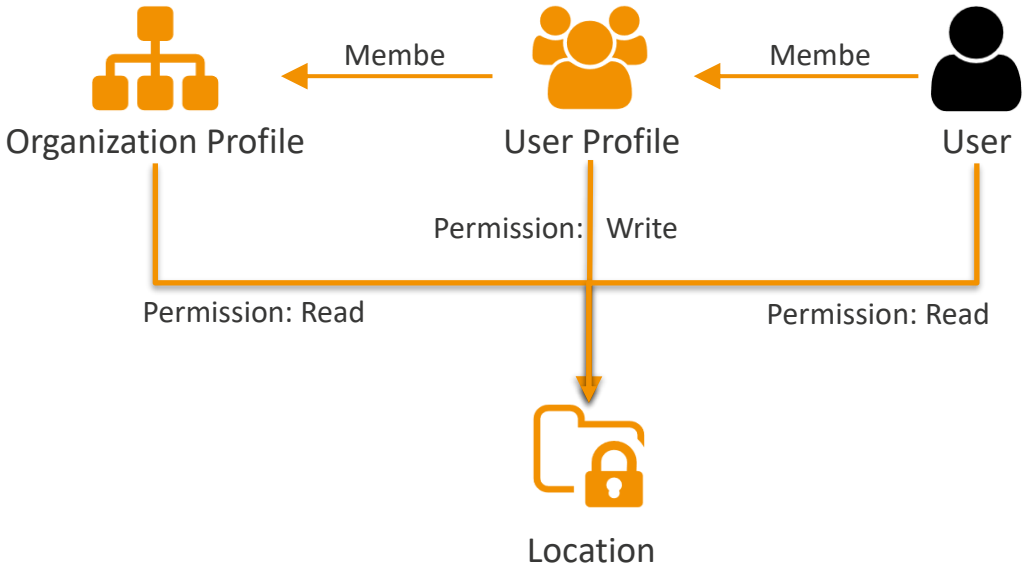
Currently this functionality is only available for Rights Folders – SharePoint Sites and 3rd Party Elements are not supported.

6.1 Operational Principle: User & Organization Profiles

Profile permission management enables matching your company´s HR structure to file storage organization by connecting permissions to user groups. Logical grouping of users and resources may significantly ease permission processes for employee changes (new / leaving, switching departments etc.) by simply adapting user membership of profiles.

Profile management supports three ways to permit access:

- *User Profiles:* Here, multiple users can be arranged in a User Profile, i.e. all colleagues of a project group. By assigning permissions to a resource within this profile, all profile members will automatically have these permissions. When altering permissions, all members are affected accordingly.
- *Organization Profiles:* To support complex organizational structures, Organization Profiles add another level of grouping. Organization Profiles may also define access permissions on resources but only User Profiles are accepted as members, not single users. All users being members of a User Profile which itself is a member of an Organization Profile will automatically have these additional permissions. When altering permissions, all members are affected accordingly.
- *Individual Permissions:* In addition to access permissions received by profile membership users may get “personal access”. This is accomplished by assigning permissions explicitly to a user. If permissions of a profile are altered, this has no effect on such individual permissions.

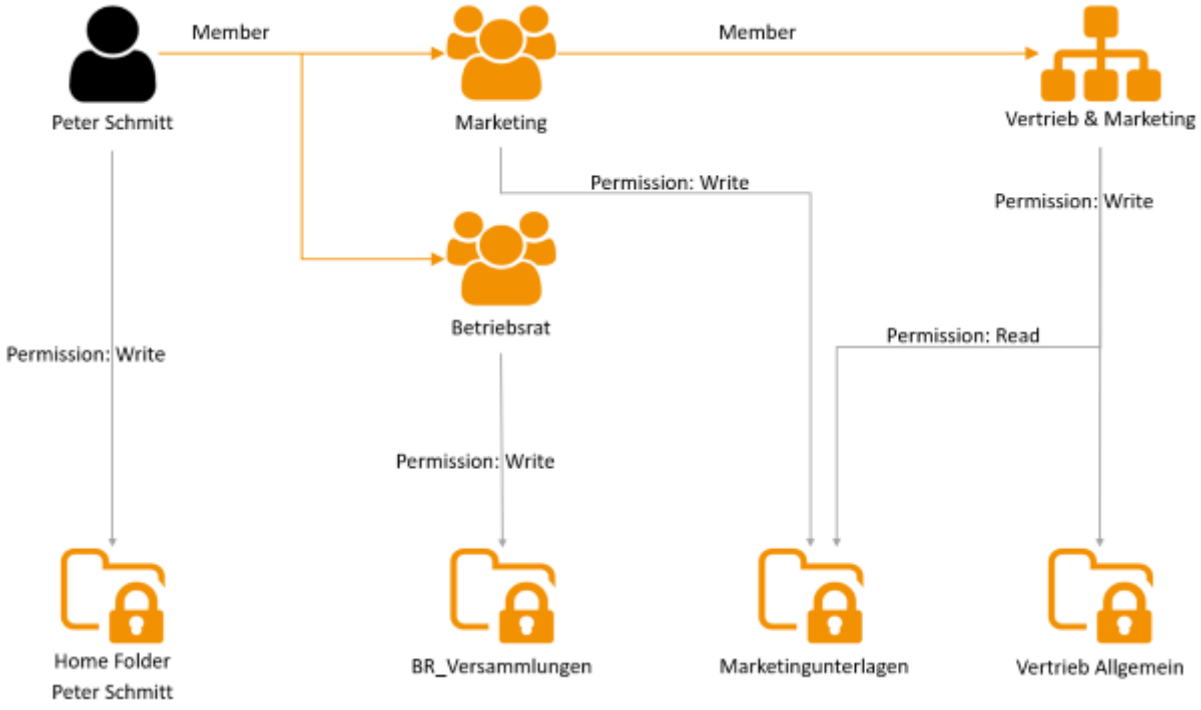


Using profiles enables for supporting differently organized working structures. It is likely to happen that users receive multiple permission assignments onto the same resource by various profile memberships. Access Manager will calculate the *Effective Permission* that does result for each resource. When combining multiple permissions, the highest permission is granted (where *Write* supersedes *Read*, and *Design* supersedes *Write* in case of SharePoint sites).

Example:

The employee Peter Schmitt is a member of User Profile *Marketing* because he works in this department. This profile, because of the logical affiliation, is also a member of the Organization Profile *Sales & Marketing*. Additionally, Peter Schmitt is a member of the Work council and therefore his user account is a member of the User Profile *Work Council*, accordingly. Because of these affiliations to the various profiles he will receive permissions on folders *WC_Meetings* (via User Profile Work Council), *Sales* (via Organization Profile Sales & Marketing) and on folder *Marketing* where he has permissions not only because of his membership in User Profile *Marketing* but also because of Organization Profile *Sales & Marketing*). He encounters Write permission because this is the highest effective permission AM has computed. The Read permission is not directly relevant for him but further User Profiles may be members of Organization Profile *Sales & Marketing*, having no additional Write permissions on this folder. In that case, Read permissions will become effective.

Furthermore, Peter Schmitt has individual permissions set for his home folder *Peter Schmitt*.



6.2 Profile and Cluster Management

Menu:
Profiles & Organization → Profile Management

6.2.1 Cluster and Profiles

Sub menu item: *Profile Structure*

Cluster, also called Profile Cluster, are a method for grouping several Profiles. They are only used for better overview with no functional purpose.

Every Profile must be a member of exactly one Cluster – by default, only one Cluster named "/" exist as the root element, all Profiles are created within this one if no further Cluster exists.

To manage Profiles and Clusters, you need to have the role *Profile Administrator*. A Profile Administrator can create, move, modify and delete Profiles & Clusters. He may view and modify all existing Profiles and Cluster, meaning he is able to edit their names and parent containers, manage permitted resources and specify *Profile Responsibles*. A Profile Responsible is shown only the Profiles he was assigned and is not able to create or modify other ones.

The left tree view lists the existing Cluster and Profiles, consisting of two different types:

- *User Profile* – Only user accounts can be assigned as members.
- *Organization Profile* – Only user profiles can be assigned as members, user accounts are not allowed as well as nested organization profiles.

6.2.2 Managing Cluster

Sub menu item: *Profile Structure*

Select the Cluster to manage. In the details area on the right, a list of possible actions are displayed, divided into sections (*Create child element*, *Change profile cluster settings*, *Delete Cluster*) that may contain sub-sections (folded by default). By clicking on its name (gray background) you can unfold this sub-section to provide necessary data.

6.2.2.1 Creating Cluster

In the details area, in section *Create child element*, unfold the sub-section *Create New Cluster* and enter the Cluster name. The new name must not exist within the parent Cluster (but may exist in other clusters already). After clicking button *Create Cluster*, the new record appears immediately in the tree view.

6.2.2.2 Renaming and moving Cluster

In section *Change profile cluster settings*, edit the name or enter another Cluster path. A list of available paths is displayed, so you can select one – other paths are not allowed. Click the appropriate *Save* button and the changes are immediately reflected in the tree view.

You will receive an error message if you move a cluster to another one that already contains a Cluster with the same name.

6.2.2.3 Deleting Cluster

Because contained elements (Profiles and Cluster) of the Cluster to delete are not deleted automatically, specify a target Cluster for these elements at the lower right. If no child elements exist, you do not need to specify a target Cluster.

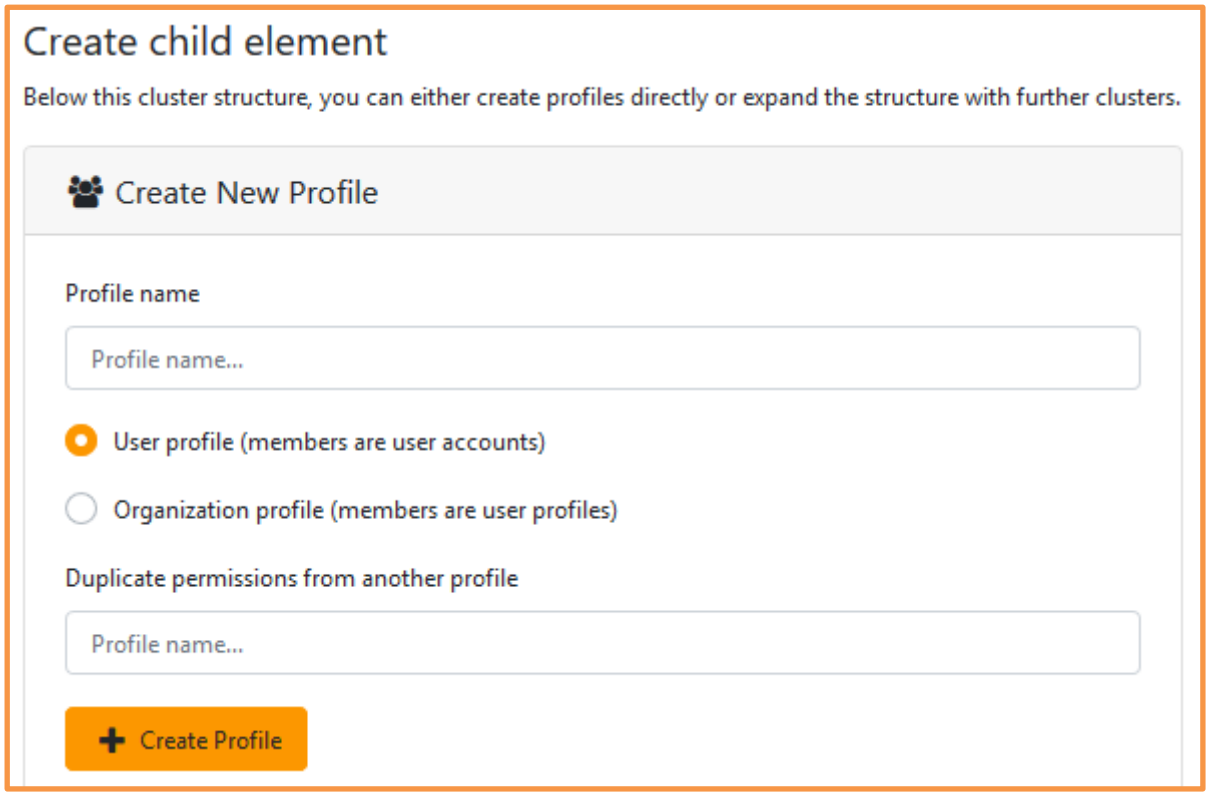
You will receive an error message if a cluster is moved to another one that already contains a Cluster with the same name.

6.2.3 Managing Profiles

Sub menu item: *Profile Structure*

6.2.3.1 Creating Profile

Select the Cluster to create a new Profile in from the tree view. In the right details area, you have the following options:

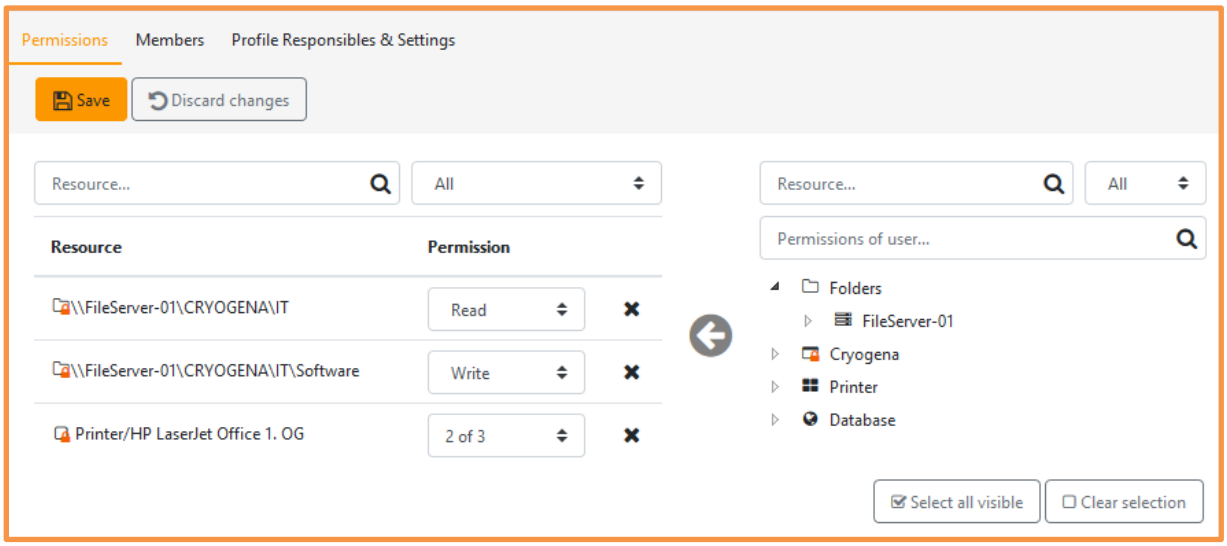


Enter a unique Profile name. It must not exist in any Cluster already. Then select the Profile type, User Profile or Organization Profile – it is not alterable afterwards. In addition, you can enter an existing profile for copying its permitted resources (*Duplicate permissions from another profile*). Members and Profile Responsibles are not taken over.

After saving, the new Profile is immediately displayed in the tree view and the details area shows further management options.

6.2.3.2 Managing Permissions

Select the Profile to manage from the tree view. The sub-page *Permissions* in the details area is available to both the *Profile Administrators* and – with read-only permission – *Profile Responsibles*.



Use this tab to assign managed resources to the profile and define access permissions for each resource separately. Later on, users will get access to these resources once they become a member of this profile. Within a profile, different resource types can be combined, meaning it may contain Rights Folder, managed SharePoint Sites and 3rd Party Items at the same time.

Supplementary Permissions of 3rd Party Items:
*If you do not grant **all** item permissions, the missing permissions are **not** revoked from a user owning such permissions.*

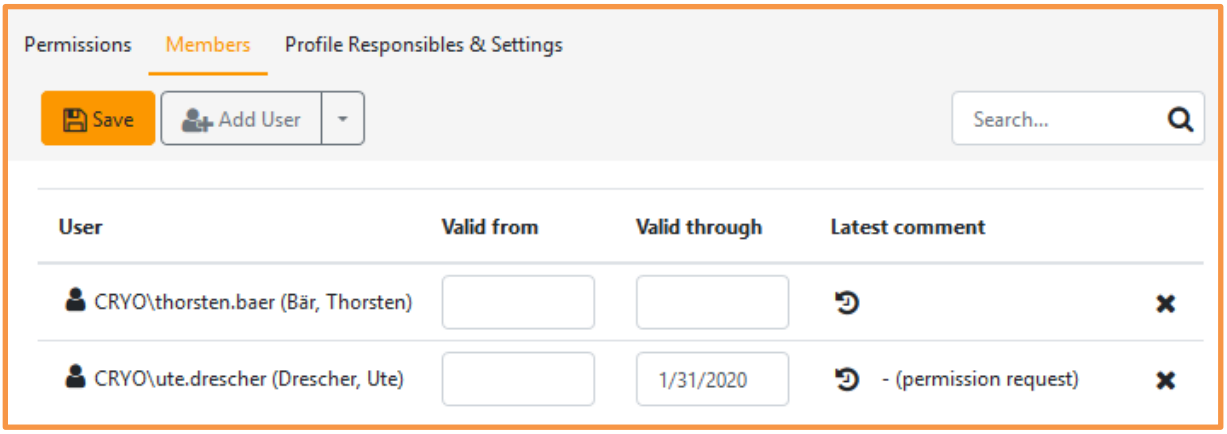
The list at the right side contains all still assignable resources (folders and SharePoint sites) while the left list shows the already assigned ones. Via drag-and-drop or the button resources can be put into the profile list. The button ✖ removes single resources.

Both lists own input fields for searching / filtering their elements. At the right, the search bar *Permissions of user* offers an extra functionality:

When searching for a specific user account, the list shows all resources the user is permitted on. As an extension to the rule above, also such resources will be marked black even if they are managed by AM but the user has no access permissions. Hence, it is very easy to take over all resources of a user by simply clicking the button *Select all visible* below the list.

6.2.3.3 Managing Members

Select the Profile to manage from the tree view. The sub-page *Members* in the details area is available to both the *Profile Administrators* and *Profile Responsibles*, but *Profile Administrators* do only have read access. Member assignment is performed by *Profile Responsibles* only. Here, all members of the selected profile are listed. Members of *User Profiles* can only be user accounts whereas members of *Organization Profiles* are *User Profiles*.



Profile Responsibles specify the members who will have the access permissions that are defined on the tab *Permissions*. For each member a time frame can be given for which the membership is valid. Also, existing accounts / profiles can be removed (button *Remove* ✖) and their access permissions are immediately revoked.

New members are added via button *Add User*, *Add Profile* respectively. A new input field is created to enter the new member name. The Arrow button to the right unfolds a list with further options:

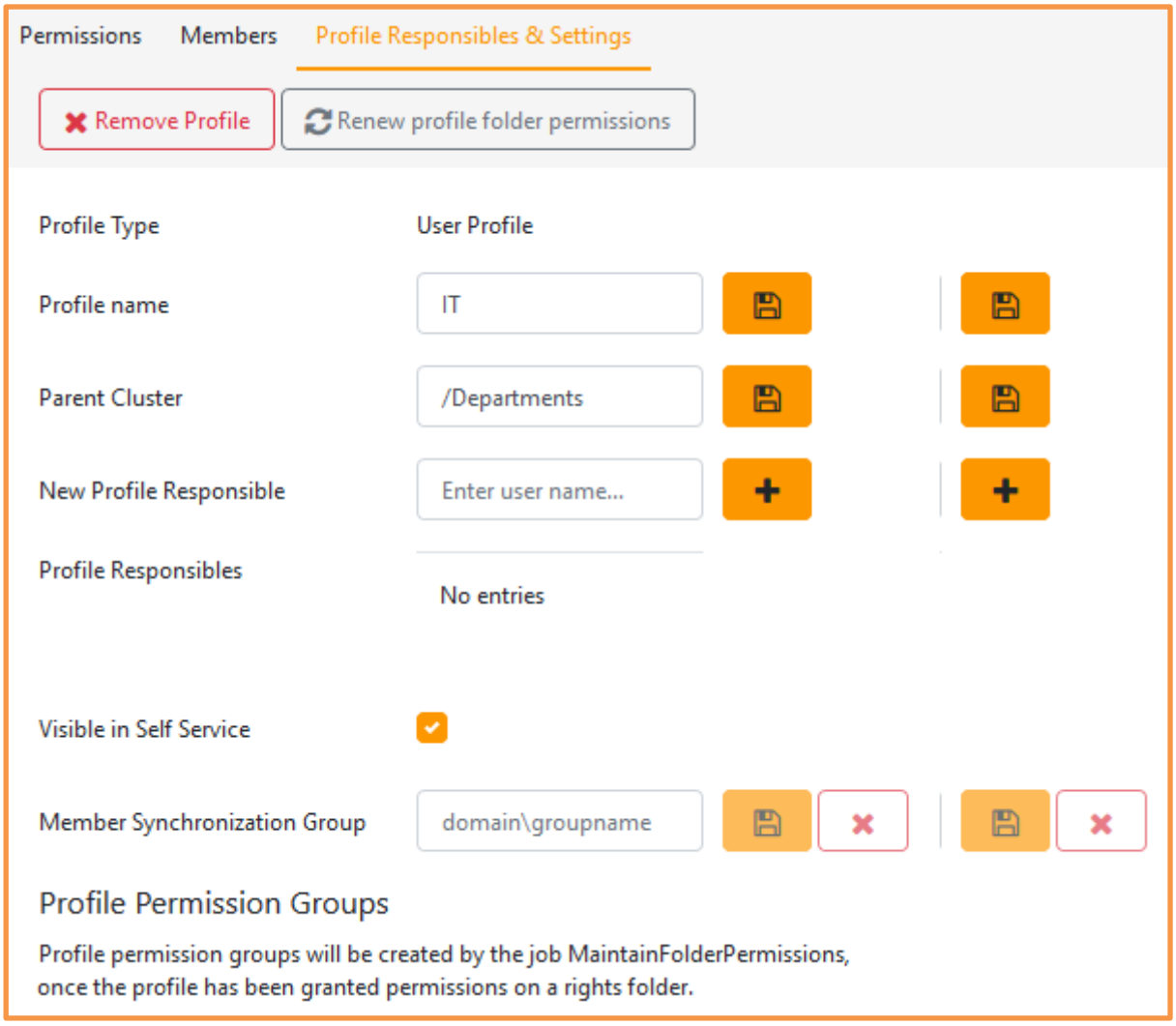
Add members from another profile: Enter the name of a different profile of the same type (user profile or organization profile). Now all members of that profile will be listed. The ones you select will be added as new members to the current profile if not already existing there.

Add users from AD group: For User Profiles the additional button offers a way to add multiple user accounts at once. Enter the name of the containing AD group and select the desired group members. These are added to the user list immediately and can be altered afterwards.

In addition, for each member a comment can be entered and all previous comments can be displayed at any time using the button . Click the *Save* button to take over all changes made.

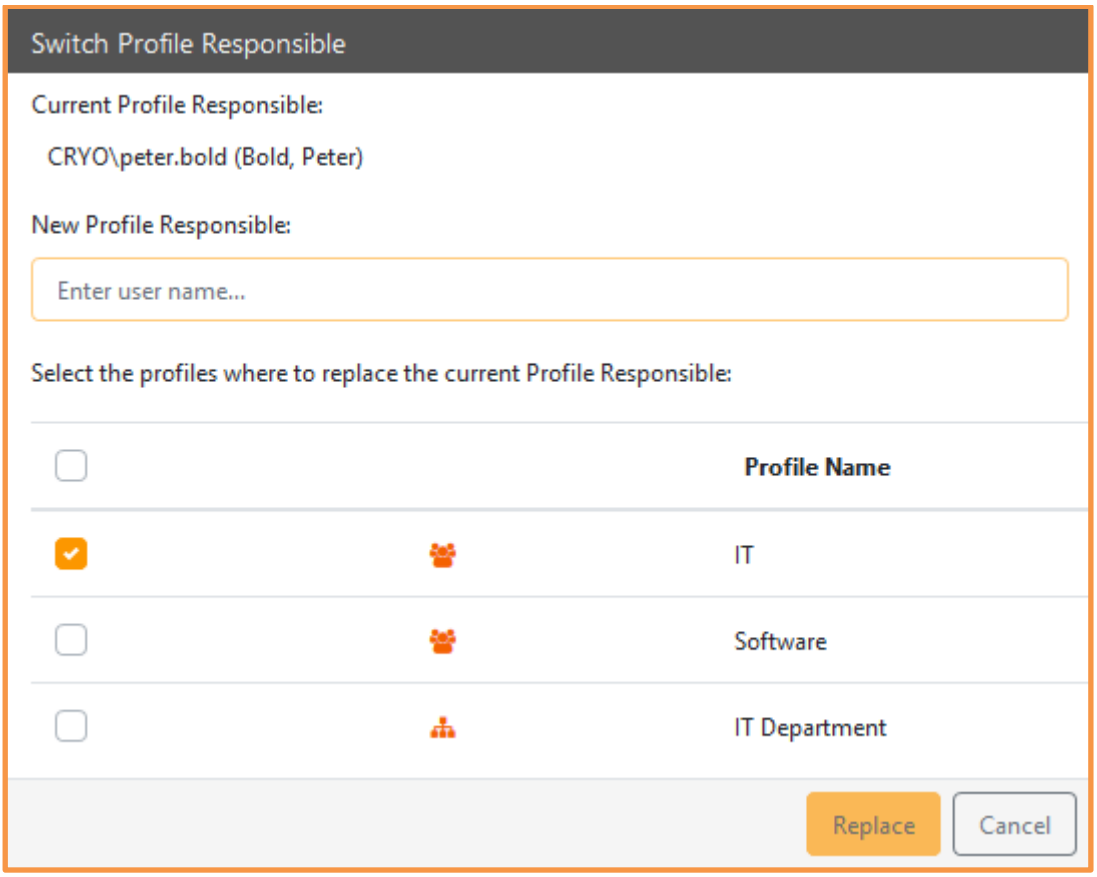
6.2.3.4 Profile Responsibles & Settings

Select the Profile to manage from the tree view. The sub-page *Profile Responsibles & Settings* in the details area is only available to *Profile Administrators*.



Here, you can edit the Profile name and the list of *Profile Responsibles*. An infinite number of Profile Responsibles can be added and are immediately saved and displayed in the list.

A Profile Responsible can be removed (use button *Remove* ✖) or replaced (button *Replace* ⇄) by another person. A list is displayed with all profiles the selected person is a *Responsible* for. Using the checkboxes, the *Profile Administrator* can select for which profiles the person shall be replaced. Initially, only the current profile is pre-selected:



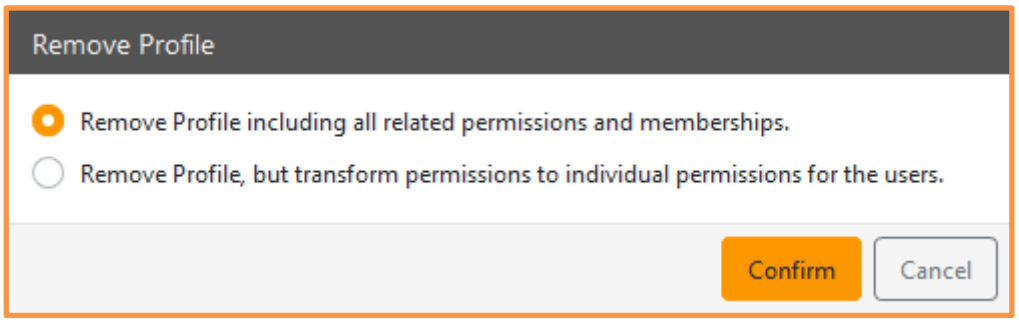
Besides Profile Responsibles management, you can specify if this Profile shall be *Visible in Self Service* so users may apply for membership. This is only possible if the Profile is manually managed by Profile Responsibles – automatically managed Profiles (see next option) are not visible to end users, so they cannot apply membership.

Member Synchronization Group: Instead of specifying *Profile Administrators* who manage profile members, an AD group may be given. This will switch off the manual management. On every run of the profile synchronization job, all members of the given AD group will treated as profile members and access permissions are granted to them. All user accounts that have been members before but are missing now will be removed. Because of this, it does not make sense to show this Profile to end users for application.

The profile list (left side) marks all user profile that are managed by member synchronization groups with a tooth gear icon ( ).

Button *Remove Profile*:

If a profile is to be deleted, there are several options to deal with access permissions of already assigned members:



- *Remove Profile including all related permissions and memberships*
  For each member the permissions on all specified resources will be revoked. If a user has further permissions on one of the resources they will be kept and – depending on the effective permission calculation – become effective.
- *Remove Profile, but transform permissions to individual permissions for the users*
  This option is only available for User Profiles. With it, the profile is deleted and permissions are applied as explicit permissions on every user member.
- *Remove Profile, but transform permissions to User Profile permissions*
  This option is only available for Organization Profiles. With it, the profile is deleted and permissions are applied to all member profiles (User Profiles). In case a resource was already defined within a member profile, the access permission is updated if it specifies a higher access right (e.g. *Write* instead of *Read*).

If the User Profile is using the new profile permission group technology (see chapter 13.3), the associated AD profile groups are removed from the file system and deleted from the AD without further notice.

Therefore, do not use such profile groups outside of Access Manager for your own purposes.

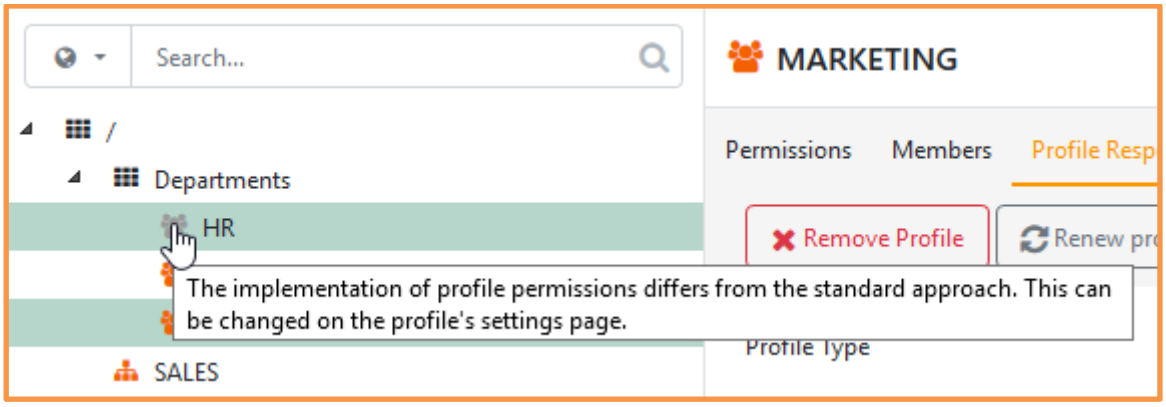
Buttons *Migrate to…*:

With each profile, you have the option of switching the authorization technology used at any time. In addition to the labeling of the button, you can also tell the currently used technology from the color of the profile icon:

- Orange: the profile uses the directory groups
- Black: the profile uses its own profile group

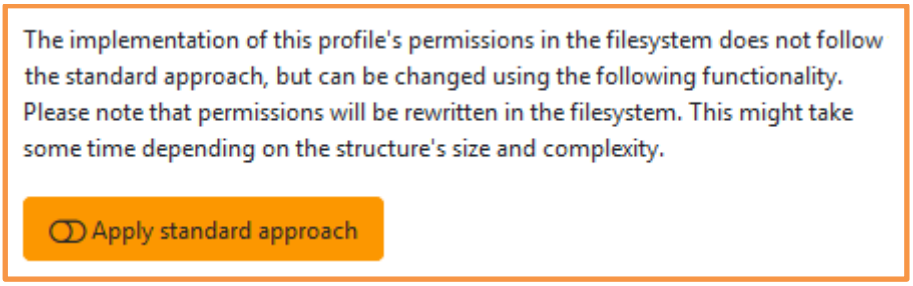
After you have confirmed the migration, a conversion process is started in the background, which, however, can only be completed after 24 hours, otherwise the currently valid physical authorization on the file server would be removed and replaced, and the user's current access would be terminated.

6.2.4 Non-Standard User Profiles



AM Administrators can decide between two different technical implementations of the folder permissions in profiles. If the standard procedure was changed, user profiles that were created before the change appear in gray and are explained by a tooltip. This does not indicate an error and the usage of these profiles is still fully functional. Yet theses profiles can selectively be switched to the new procedure if desired.

Select the respective user profile and go to tab *Profile Responsibles & Settings*:

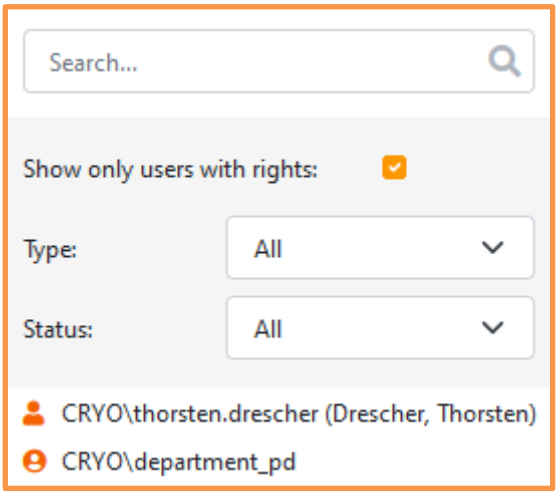


By clicking the button *Apply standard approach* the technical changes for the new permission logic are performed in the background and will be available afterwards. Information about the technical implementation is given in the Administrators´ manual but is not needed to know for utilizing the function.

This is a purely internal technical change; there are no changes to the existing permissions, operating logic or appearance.

6.3 Profile Memberships

Sub menu item: *Profile Memberships*



A *Profile Responsible*, similar to a *Responsible*, can view information on all users and AD groups here, which are members of at least one of his profiles.

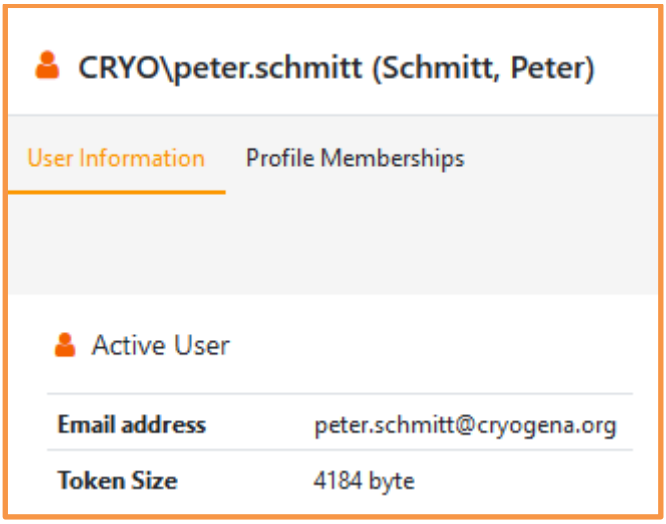
The left side shows a list of all user accounts, offering various filtering options. Searching for a specific account is possible as well as limiting the display on permitted accounts and active / inactive accounts. After each filter selection, only the first 100 accounts are displayed with the possibility to also load all accounts. Depending on the amount of accounts, this may take a few seconds.

All user accounts are prepended by an icon, informing about their current status:

- Active account with permissions / roles
- Active account without permissions / roles
- Inactive account with permissions / roles
- Inactive account without permissions / roles
- Blacklisted account with permissions / roles
- In AD deleted account with permissions / roles (may also be marked by “***”)
- Active AD group with permissions / roles
- Active AD group without permissions / roles

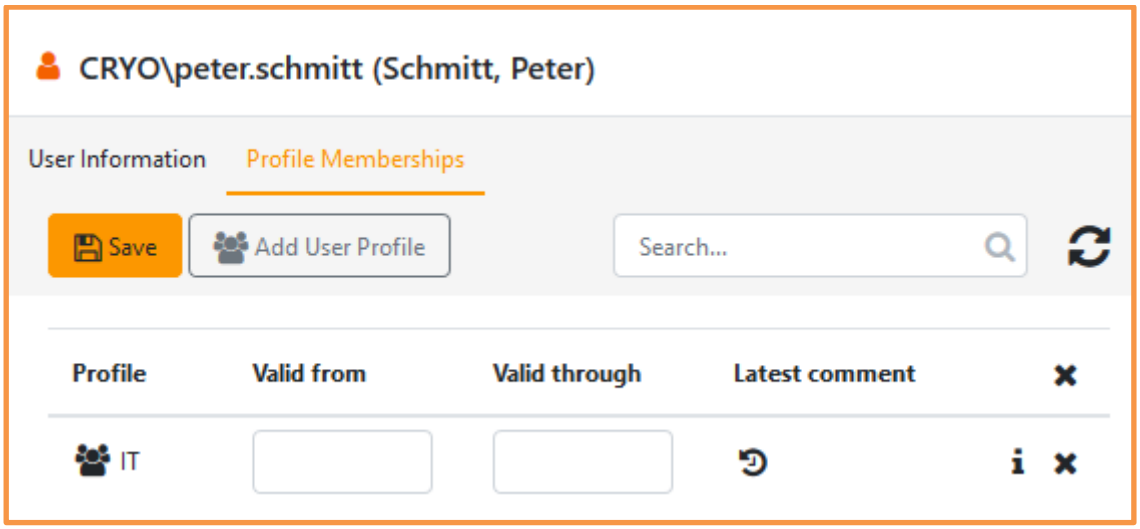
So called *Blacklisted Users* are usual accounts that are included by the *AM Administrator* in a blacklist. Therefor they are not handled within search masks and find-as-you-type functionality and are only shown if they already own permissions or roles. Without a request, permissions cannot be granted but only revoked. Existing permissions are still maintained by AM and blacklisted users still have access to the Management Portal to request access permissions.

6.3.1 Section "User Information"



The tab *User Information* contains common information about the user account. This includes e.g. the email address, the home folder (if available) and further technical data.

6.3.2 Section "Profile Memberships"

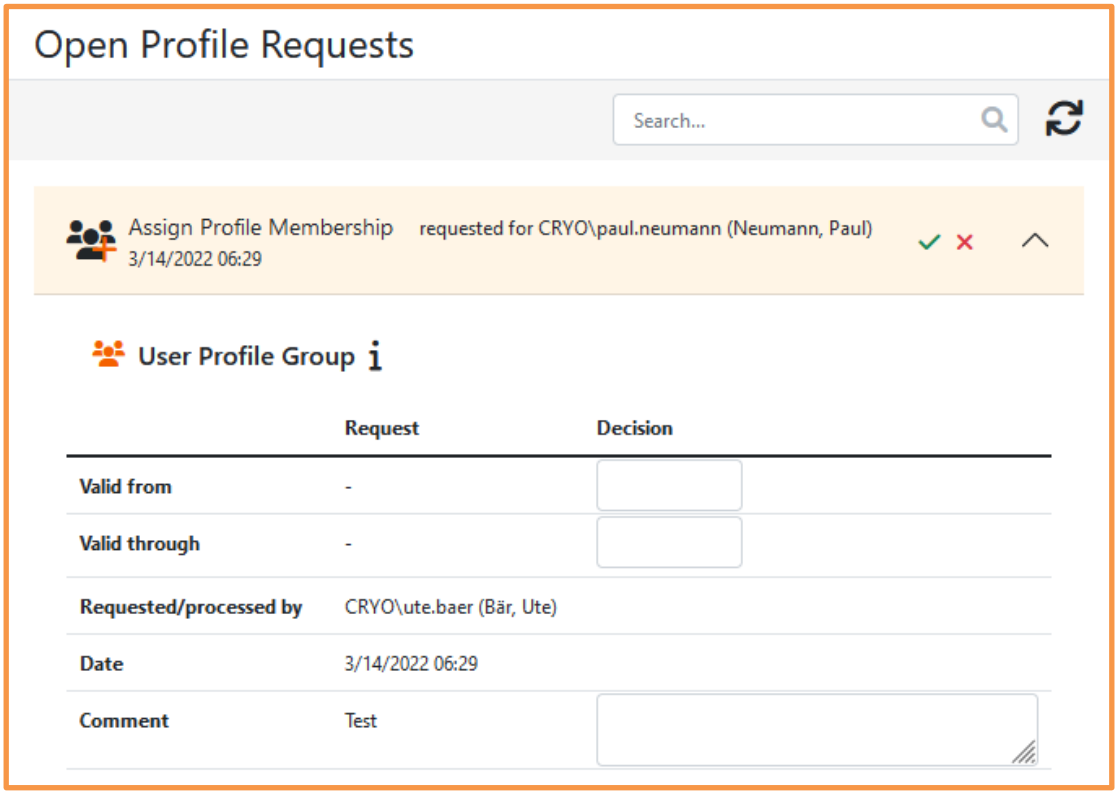


In contrast to the *Responsible* the *Profile Responsible* has a tab to view the profile memberships of the selected user, including also memberships which will start in the future and are not yet active. Changes to the validity period for a membership can also be done on this page. Via the Info icon it is possible to discover folders that are permitted by the according profile. A profile can be removed for the selected user by clicking the X icon next to the profile, which will result in the user losing all permissions granted by the according profile. It is also possible to remove all profiles at once for the selected user by clicking the **X** icon in the table header. Vice versa, by clicking the *Add User Profile* button it is possible to add the selected user to other profiles, granting him the according permissions.

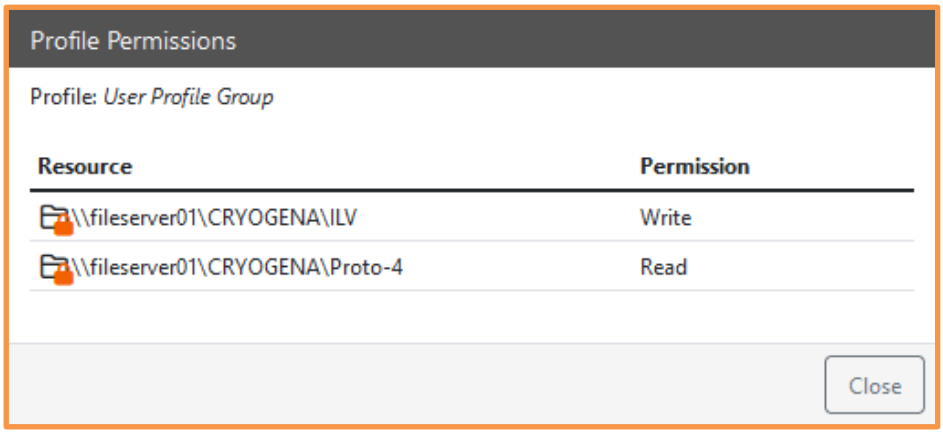
6.4 Profile Requests

Sub menu item: *Requests*

As a *Profile Responsible* or *Profile Administrator*, here you see all requests that users have filed in for Profile memberships, separated into open (unprocessed) and closed applications.

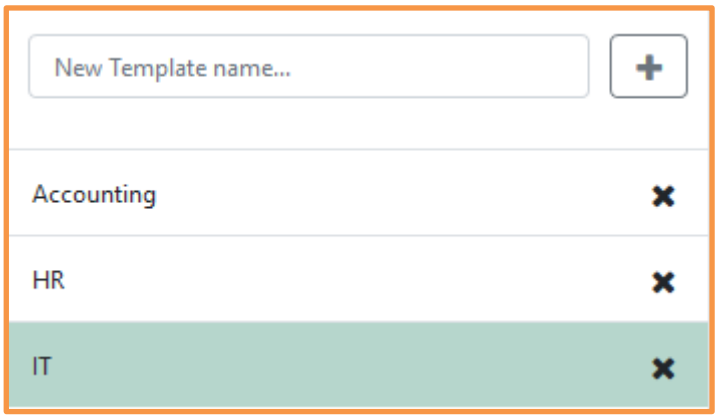


Like processing requests for other resource types (Folders, SharePoint Sites, 3rd Party Items), you may individually set for example start and end date of the membership. While it is not possible to change the resources the applicant gets permitted (this was defined by the Profile Administrator), you can see the list of resources permitted by this profile by clicking the Info icon next to the profile name:



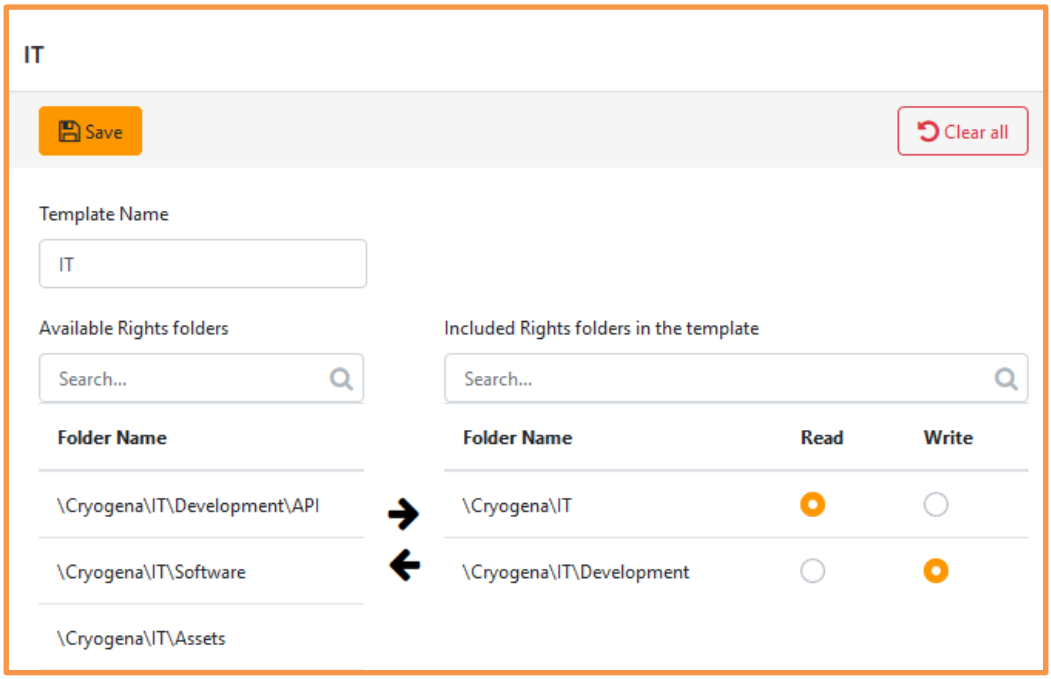
6.5 Global Template Management

A *Template Administrator* may create, modify and delete global templates. The top of the page has an entry for creating new templates. The table below displays the existing templates:

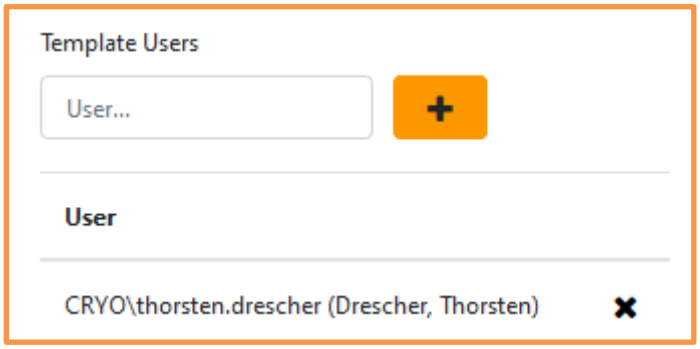


When a template is selected for editing, additional controls will be displayed for editing the template in a flexible manner. As one example, the name can be changed. The *Available Rights Folders* table underneath will display all rights folders known to AM. Any number of folders can be added either by drag-and-drop or using the right arrow button next to the list. Either drag-and-drop or the left arrow button can be used to remove folders from the list.

At the right, the permissions list will display all rights folders contained in the template along with the associated permissions. The list can also be adjusted from here. All folders can be deleted at one time by clicking the *Clear All* button.



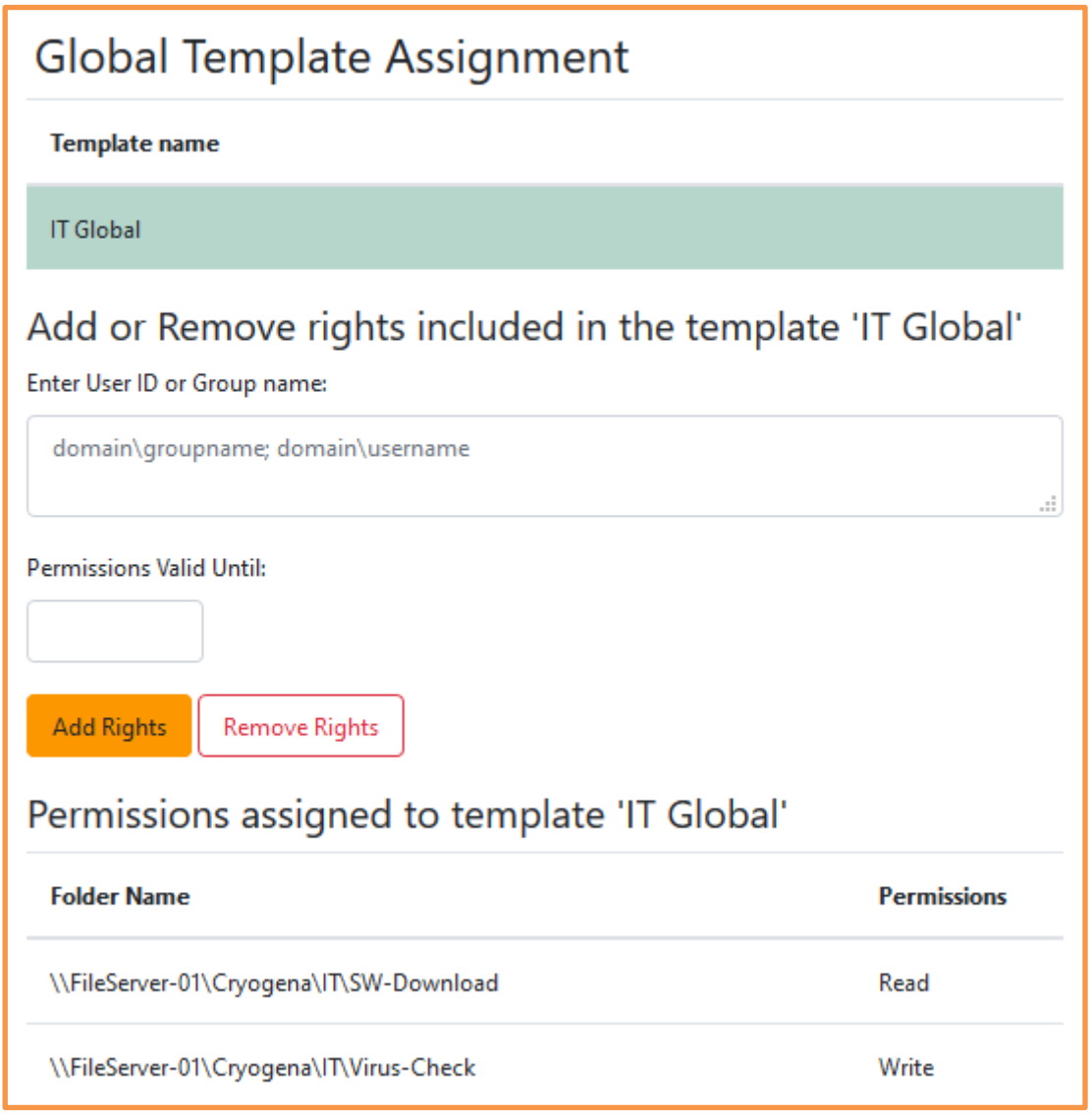
In the last section at the bottom the *Template Administrator* can specify which users can use the template for assignment.



These users will automatically be granted the *Global Template User* role. However, they do not receive additional management rights, like *Responsible* or *Owner*, and cannot apply any deviating rights. However, please take special when selecting such user to avoid unwanted / uncontrollable elevation of access rights.

6.6 Global Template Assignment

The table lists all templates you have been authorized for usage (see the previous chapter). Analogous to a *Responsibles´* private templates, you have the ability to authorize other users on a defined set of rights folders. A user who was assigned the usage of a template cannot modify it afterwards. Only the *Template Administrator* can do this. Please note that the *Global Template User* role does not have the ability to manage permissions.



After choosing a template, two panes will be added. Below, users and groups will be entered, who should be assigned the corresponding permissions or have these permissions revoked. Use semicolons (;) to separate multiple entries. The expiration date for the permissions can be specified optionally. Even below that, the folders and permissions included in the template will be listed for your information.

6.6.1 Assigning & removing permissions

Assigning permissions using a template can affect users who may already have access permissions for a folder contained in the template. Any existing permissions will not be reduced by such assignments; existing permissions that grant more to users will always have precedence[4] over assignments made by templates.

If an expiration date has not been set, the change to the permissions will take the rule above into consideration immediately and permanently. Otherwise, the following rules will apply:

- *Add Rights*: All specified users and groups will immediately be assigned the respective access permissions to the folders and the expiration date will be set (in consideration of the rule above). If necessary, the previous or existing expiration date will be extended by the template.

- *Remove Rights*: New permissions will not be set, however already existing user and group permissions will be assigned an expiration date, if the setting involves same permission as the one in the template (meaning only an existing read permission is updated by a read permission in the template or the same will apply with regards to a write permission), whereby an existing expiration date would take effect later. This means that the time frame for permissions will be reduced at most but can never be extended.

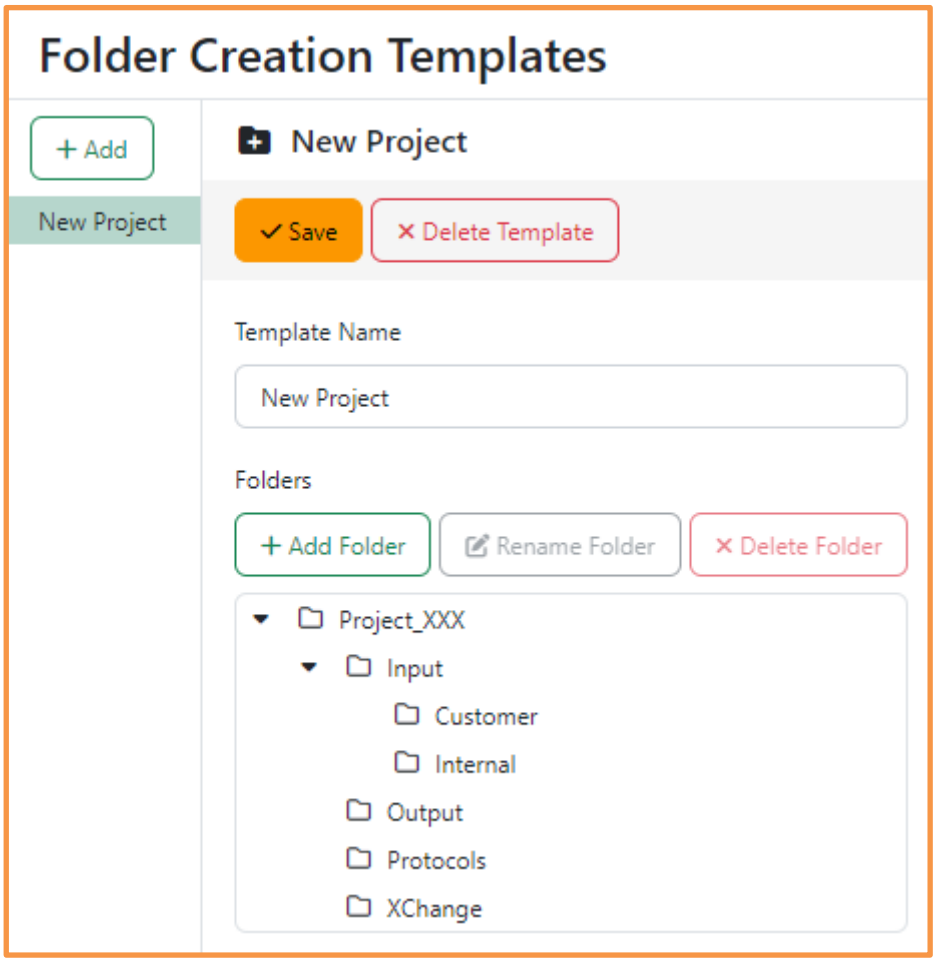
Finally, clicking the respective button for adding / removing, the permissions for the assigned users are propagated by the system and they – as well as you – are notified by email.

[4] This means that if a user already has the write permission for a folder, the permission will be retained even if the template grants a read permission to the user.

6.7 Managing Folder Templates

Menu:
Profiles & Organization → Template Management → Folder Creation Templates

The *Folder Templates* page allows you to manage templates that are used to easily create directory structures that are required several times. Once defined, templates can be used by the administrator in the context menu of a directory (in the *Permissions* tab) as often as desired to create many, possibly nested, directories.



Clicking on *Add* creates a new, empty template. Assign a unique, not yet used name here; you can change this at any time.
The templates created so far are listed under the button. After selecting a template, the details are displayed in the area on the right, and you have various options for defining or modifying any complex directory structure.

7 Data Protection Classification

7.1 Operational Principle: Flagging personal data according to EU-GPDR

The *Classification Administrator* creates so-called *Classifications* which consist of categories concerning user-specific data according to the EU-GDPR. A classification has a name, an icon and a descriptive text. It is used to mark distinct resources that are sensible to user data protection.

Furthermore, *Classifications* could also be used without means of data protection, i.e. to simply categorize specific resource content or to include resources in a Reapproval run.

The *Classification Administrator* maintains Classifications and provides them to *Owners* of managed resources (see chapter 4.3.2.2).

7.2 Defining Classifications

Menu:
Administrator → Classifications → Data Protection Classifications

The *Classification Administrator* maintains *Classifications* and provides them to *Owners* of managed resources.

Besides entering a name (mandatory), it is helpful to select a proper icon and a color to easily identify the classified resources later on. The given categories are preset by the EU-GDPR and cannot be changed. You can derive the protection level from their combination. Once created, classifications can be used by every resource Owner, but they cannot alter them.

Using the button *Set as default* will make this classification preselected whenever a new managed resource is created (Folder Collections, SharePoint Site Collections, 3rd Party Item Collections), but can be changed individually. Selecting another classification as default here will have no impact on already existing resources.

The *Data deletion period* is just an informational specification, purely to serve as a reminder according to the EU-GDPR. Compliance will not be checked by AM.

Group of authorized users: If you enter an AD group, only members of this group (user accounts) are permitted to receive access permission on resources flagged with this classification. It is still possible to add other persons to that resource, but they will not gain true access unless they are included in the above-mentioned AD group.

Special case when using Profile Groups (see chapter 13.8.3.19):
If you are using one or more resources secured by this option within a profile, only such users will be permitted who are allowed to access all of the secured resources. In turn, this means that a user not being permitted on at least secured resource, he will not be permitted on any resource of this profile.

If a profile does not use profile groups, mixed permission are possible as permissions are granted per folder, not per profile.

Deleting a classification:
When using the *Delete* button, the classification will be deleted immediately if it is not yet used. If in use, it cannot be deleted but can still be altered.

7.2.1 Create reapproval for a classification

Next to the *Reapproval* label, you will find the button *Configure reapproval*, which you can use to create a reapproval specific to this classification so that all resources flagged with this classification can be checked individually. You have the following options in the configuration dialogue:

- Activate/deactivate reapproval
- Remove all unconfirmed authorizations from the associated resources after the reapproval cycle has expired. **ATTENTION:** This can result in drastic access restrictions and should be agreed upon with the company management/data protection officer, even if it is the right choice regarding security.
- Start date definition: If the date lies in the past, Reapproval is starting immediately.
- Set a repeat interval: A new cycle starts every X months on the day selected in the start date, for example always on the 1st of the appropriate month. If you specify the 31st, in months with fewer days the cycle will start on the last day of the month.
- Duration of the reapproval cycle – must be shorter than the repeat interval.
- Number of reminder mails within the cycle. The intervals between the emails are determined evenly based on the cycle duration and the number. An additional reminder can be sent three days before the end of the cycle, informing also the Owners.

Please note that at the start of a reapproval run, only those resources that were assigned the corresponding classification at that time are considered. Other resources that are classified in this way during a reapproval run can only be checked in the following cycle.

7.3 Checking Resources

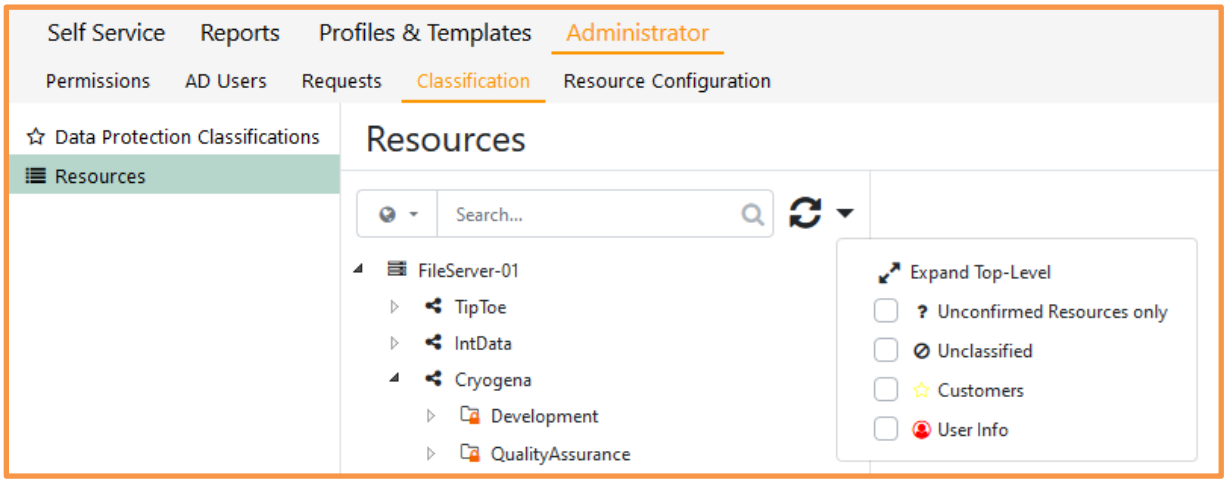
Menu:
Administrator → Classifications → Resources

Here, all managed resources can be viewed by a *Classification Administrator*. For each resource the *Owners* and *Responsibles* are listed (read-only) as well as the resource description and classification (both editable, see chapter 4.3.2.2).

This page is a subset of page *Permissions for Administrators*, reduced to classification information, because a pure *Classification Administrator* has less permissions than an *AM Administrator*.

Address Filter:

Besides the textual search, the dropdown button provides additional options to filter the tree view for classification information:

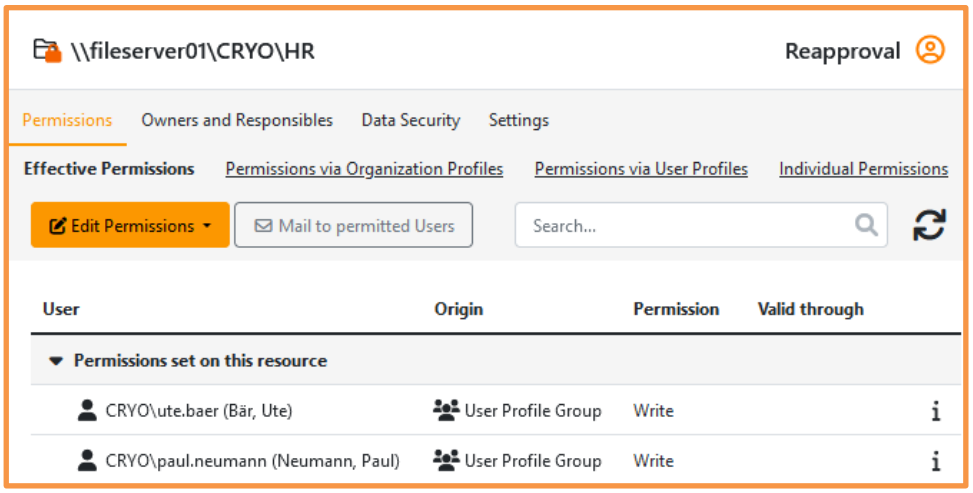


Filtering is possible for one or more classifications as well as for unclassified resources. This filter cannot be combined with the option to filter only for unconfirmed resources, because the latter ones are classified per definition. For further information about unconfirmed resources, please see chapter 4.3.2.2.

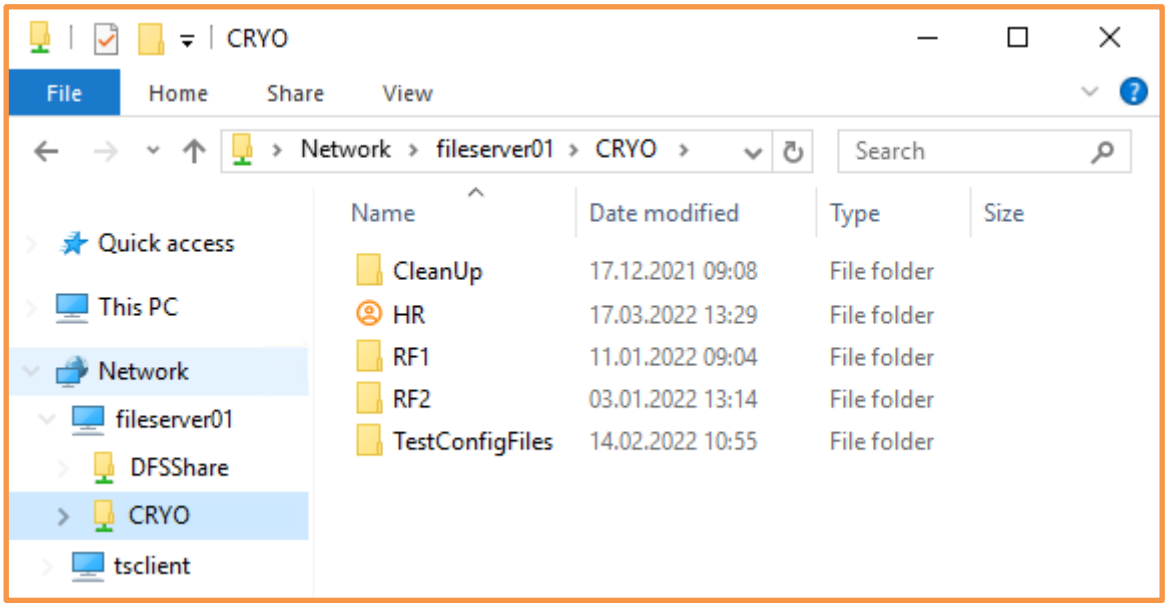
7.4 Classification Icons on File system

A classified folder always has a classification icon (chapter 7.2). If desired, Access Manager can also make this icon displayed in the file system. Therefore, the job *InitializeDesktopClassificationIcons* must be scheduled (chapter 11.6.4.2).

Example: Classified folder in Access Manager:



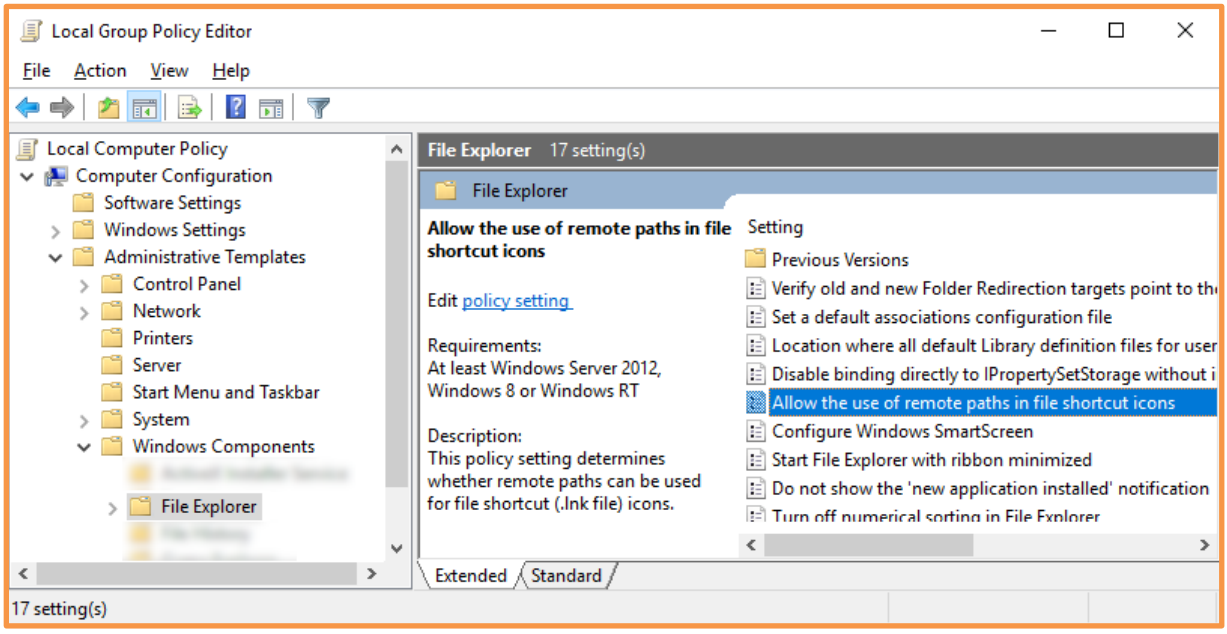
Display in Windows Explorer:



Because of caching mechanisms of Windows, it may happen that after changing the icon in Access Manager, Windows still displays the old icon.

7.4.1 Troubleshooting

Remote icons were deactivated with a Windows update in October 2022. This can be reactivated via a local group policy on the client computers or centrally via a global policy.



8 Resource Administration

The *BAYOOSOFT Access Manager* provides a relief for the corporate IT department regarding the issues and implementation of access permissions for file systems and SharePoint as well as for 3rd Party Services for users. Using a web-based interface, any number of Folder Collections, Site Collections and 3rd-Party Item Collections can be added in an easy manner and their user permissions can be managed independently and flexibly.

Access Manager uses the term *Managed Resource* to indicate that the proper assignment of the desired access permissions for such a resource will be constantly controlled and updated by AM. Furthermore, resources can be targeted to prevent or avoid their management by AM. Such resources are referred to as *Unmanaged Resources*.

Implementing access management using AM does not require any special software tools. All features will be implemented using the server-side tools that already exist in a standard Windows infrastructure (Active Directory groups & users, NTFS Shares and assignment of permissions). Ultimately, Access Manager is a management front end. The actual user authentication and authorization will be ensured by the standard Windows Server features. If the AM system does crash, users' access capabilities will not be affected for that reason; only the management and reporting of existing permissions will be affected.

8.1 Operational Principle: Automatic Permission Maintenance

The Access Manager utilizes its own AD permission groups for managed resources, i.e. a file system folder. All access permission set before are completely deleted and replaced by the AM AD groups, which are granted standard system permissions for Read, Change and Browse (Open folder, but no Read permission for files and sub-folders). All permissions set via the Access Manager User Interface are propagated to the AD and file system and are also stored in the AM database. By this, full control of your set permissions is achieved.

In a constant interval, Access Manager performs target-performance comparison and checks the database information against the status of AD and file system. In case of deviations, AD and file system data are reset to AM database defined permission.

The same approach applies to other resource types like SharePoint Sites and 3rd Party Elements. This working principle also applies to the modern Microsoft Entra SharePoint Sites and MS Teams, but here the Access Manager can take over existing permissions directly when integrating them as a managed resource. Elements can also be renamed in SharePoint / Teams, Access Manager then adopts the new names, so it is only the leading system in terms of access rights.

8.2 Configure Entry Points

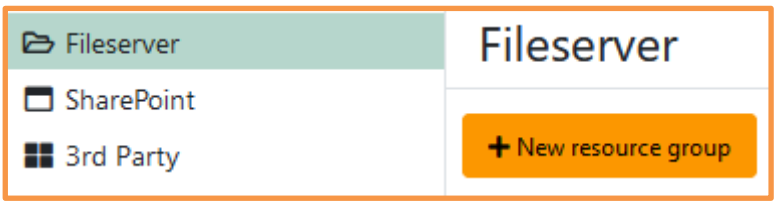
Menu:
Administrator → Resource Configuration

This page allows for assigning your managed resources, so-called entry points, into Access Manager. Only resources that are included and configured correctly can be maintained by the software.

Depending on your license, there are several resource types you can administer in the right pane:

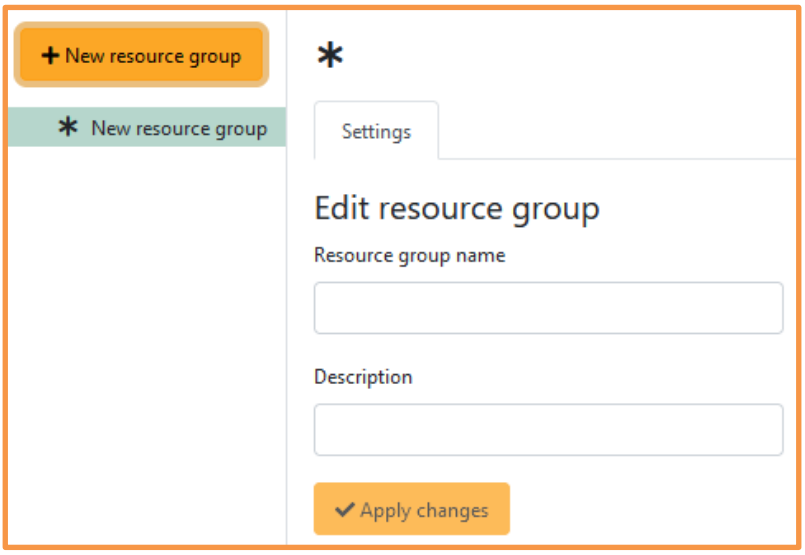
- Fileserver (chapter 8.2.1)
- SharePoint (chapter 8.2.2)
- 3rd Party Elements (chapter 8.2.3)

8.2.1 Fileserver



8.2.1.1 Create new resource group

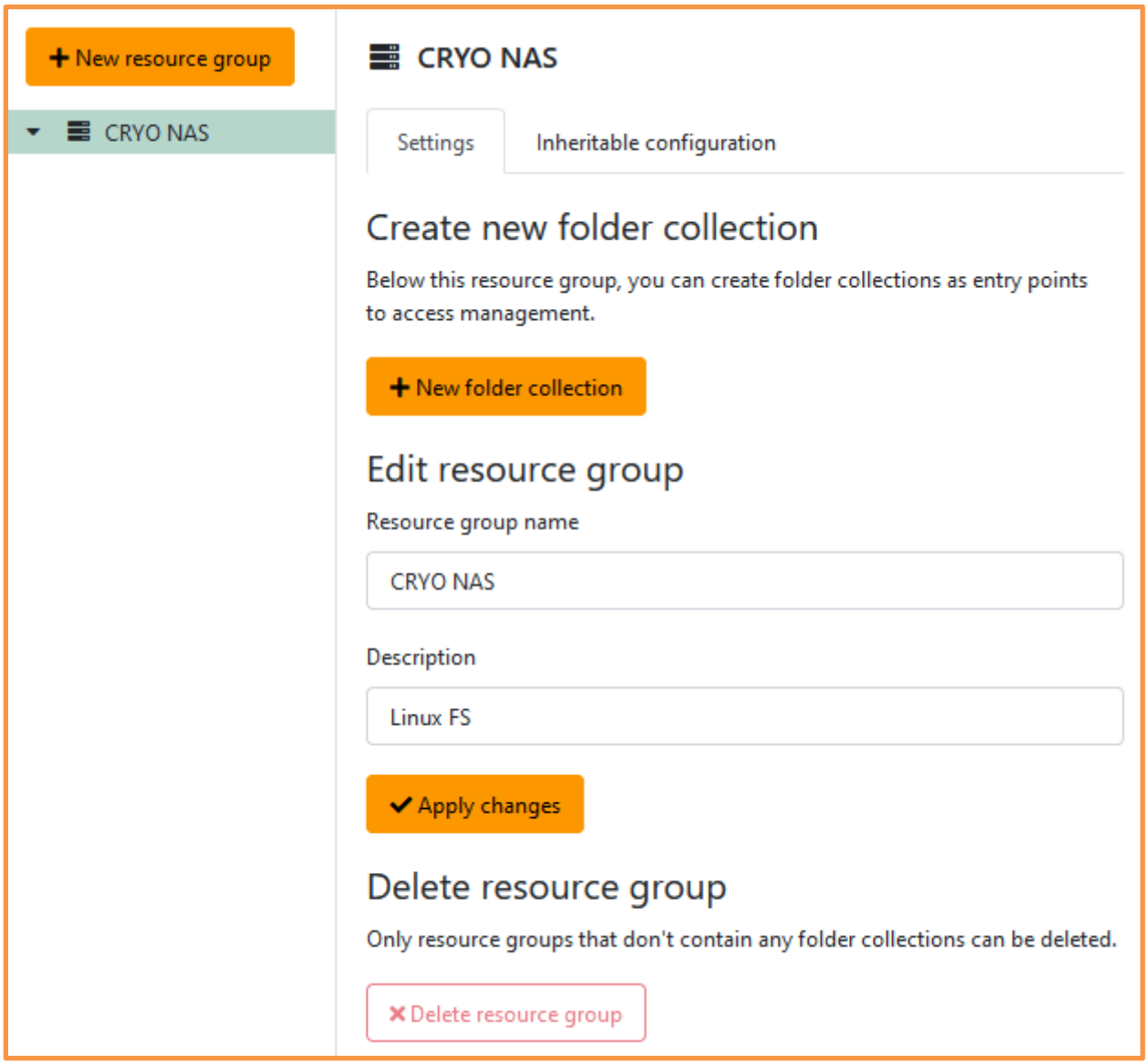
Filesystem resources are grouped into so-called resource groups. This is just an organizational grouping with no technical relation to physical resources. First, create a new resource group using the respective button:



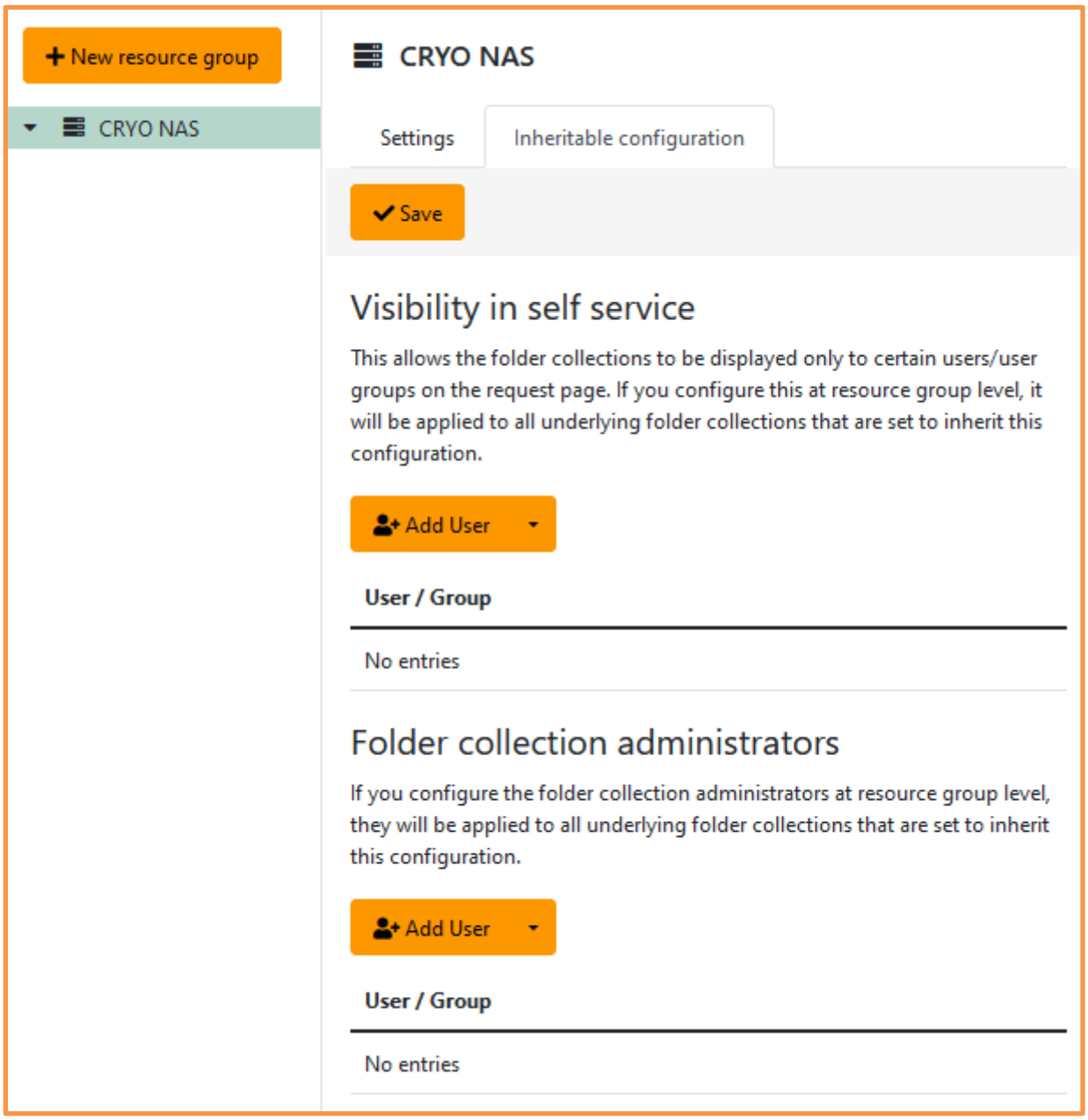
- *Resource group name*: Specify the name of this group, i.e. department location or a file server.
- *Description*: A short text of what this resource group is about.

8.2.1.2 Manage resource group

An existing resource group can be managed, and you can also add the physical folder collections:



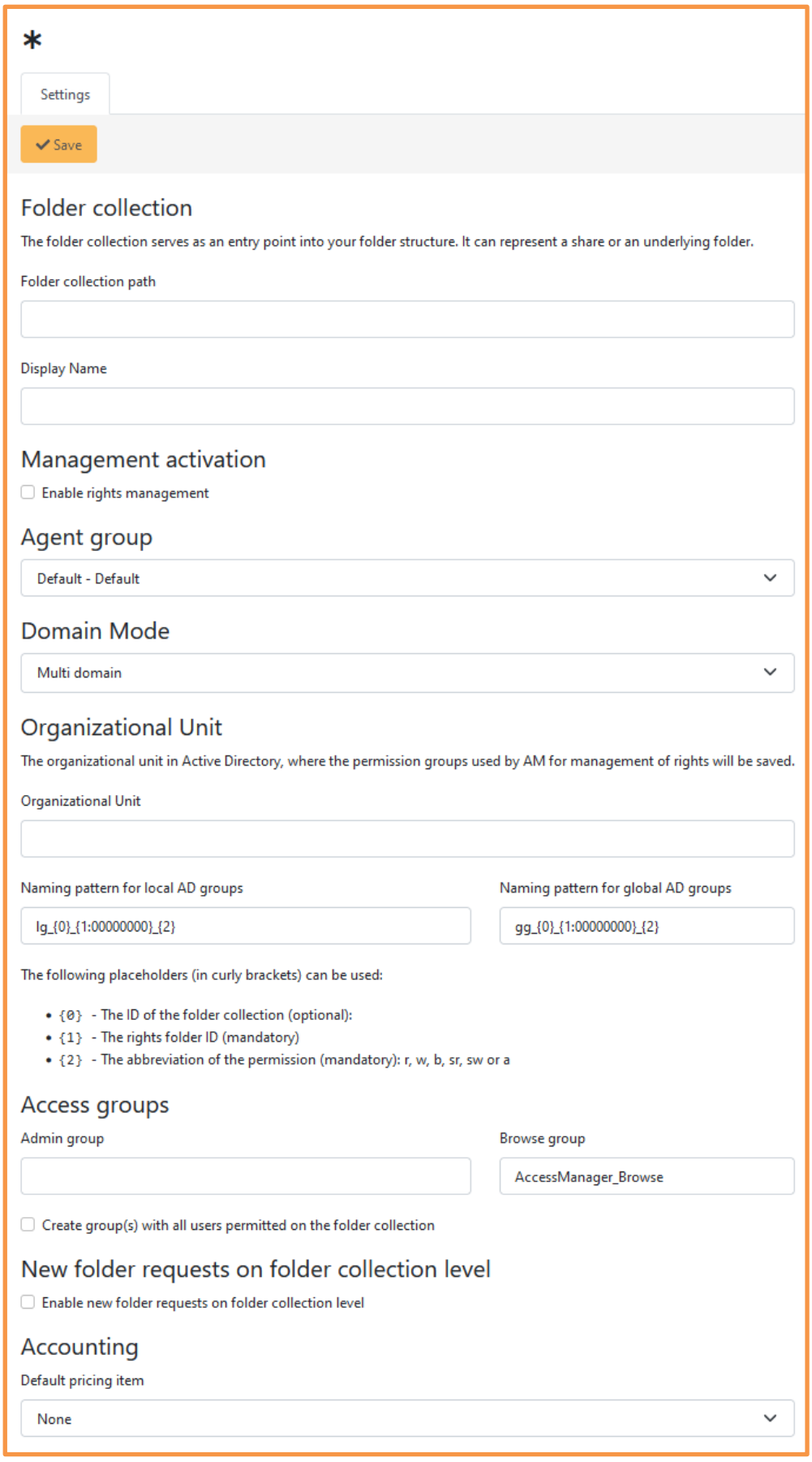
Use the tab *Inheritable configuration* to specify default values that attached folder collections can utilize. This is not a must – every folder collection can even use their own value set:



- *Visibility in self service*: only user accounts and groups specified here will be able to see the folder collection in the self service area. Please note that this setting does not affect visibility in the filesystem!
- *Folder collection administrators*: Besides all full Access Manager administrators, these accounts are allowed to administer the folder collections.

8.2.1.3 Create folder collection

In the settings of a resource group the creation of a *New folder collection* is possible via the corresponding button:


*
Settings
Save
Folder collection
The folder collection serves as an entry point into your folder structure. It can represent a share or an underlying folder.
Folder collection path
Display Name
Management activation
Enable rights management
Agent group
Default - Default
Domain Mode
Multi domain
Organizational Unit
The organizational unit in Active Directory, where the permission groups used by AM for management of rights will be saved.
Organizational Unit
Naming pattern for local AD groups
lg_{0}_{1:00000000}_{2}
Naming pattern for global AD groups
gg_{0}_{1:00000000}_{2}
The following placeholders (in curly brackets) can be used:
{0} - The ID of the folder collection (optional):
{1} - The rights folder ID (mandatory)
{2} - The abbreviation of the permission (mandatory): r, w, b, sr, sw or a
Access groups
Admin group
Browse group
AccessManager_Browse
Create group(s) with all users permitted on the folder collection
New folder requests on folder collection level
Enable new folder requests on folder collection level
Accounting
Default pricing item
None

- *Folder collection path*: Full UNC path of the entry point to the folder hierarchy. This can be a share or a subsequent folder.
  It is not possible to nest such entry points.
  This means, having \\server\share\folderX as a folder collection, you cannot add \\server\share\folderX\folderY as another one.
- *Display Name*: An alternative name to present to users in self service area.
- *Enable rights management*: This checkbox determines whether the folder collection will be actively managed or not. If management has not been enabled, the following restrictions apply:
  - The folder collection will not be displayed in self service
  - The access permissions will not be managed (created, checked, corrected)
  - An informational file will not be created with Responsibles
  - The folder cleanup job will not be executed
- *Agent group*: The group of AM Agents that work on the folder collection. The *Default* group is the default setting. More information about agent groups can be found in chapter 11.2.
- *Domain Mode*: The AD group type to be used depends on the selected mode, which must be selected from the following three options:
  - Single Domain
    AD groups will be of type “Security Group – Global”. Use this if you have only one domain (no sub domains, no external trusts). This mode requires the least space consumption of a users´ Kerberos token.
  - Multi Domain
    AD groups will be of type “Security Group – Local (in domain)”. This is the default setting. Use this if you have more than one domain (sub domains, external trusts) or are planning for more domains. This mode requires more space consumption of a users´ Kerberos token.
  - Multi Domain Optimized
    Both local and global AD groups will be created. The group type to which the user will be added will be determined dynamically depending on the user and server domain. This mode can help to reduce the size of the users' Kerberos tokens.

  If this setting is changed afterwards, all user permissions for this server of foreign domains must be deleted (only when changing the multi- and single domain modes). In any case, the "MaintainAccessPermission" job must be executed again.

- *Organizational Unit*: The organizational unit in Active Directory, where the permission groups used by AM for management of rights will be saved. Enter the exact value of parameter distinguishedName (case sensitive).
- *Naming Pattern for local / global AD Group:* Define how the name of AD groups shall look like. Placeholders (in curly brackets) are available for dynamic value replacement at runtime, all other characters are fix parts of the name. These patterns can be preset by administrative settings and changed here if necessary (chapters 13.8.3.5).

- *Admin group & Browse group*: Access Manager will permit these groups on the filesystem folders for its own and user access, they must already exist in AD (no dynamic creation).
- *Create group(s) with all users permitted on the folder collection*: With this option, AM will create a special AD group containing all users who have read or write access to at least one folder in the folder collection. This group can be used, for example, in a login script to test if the folder collection can be added as a network drive to the users' account. If the servers' domain mode has been set to Multi-Domain optimized, both global and local access groups will be created.
  To make use of this feature, the UpdateShareAccessGroups job must be scheduled.
- *Enable new folder requests on folder collection level*: This option enables end users to apply for a new folder under that folder collection directly. Otherwise, new folders can only be created under an already existing managed folder. To do this, an *Owner* must have been assigned to a folder collection already.

8.2.1.4 Manage folder collection

In existing folder collection can be altered in many further aspects that are available only after creation. Therefore, you should additionally check and revise these settings right after creating it.

For better overview, options are divided into several thematic tabs:

- Settings
- Security settings
- Administrators
- Structure import
- Data Security

8.2.1.4.1 Tab: Settings / Alter folder collection path

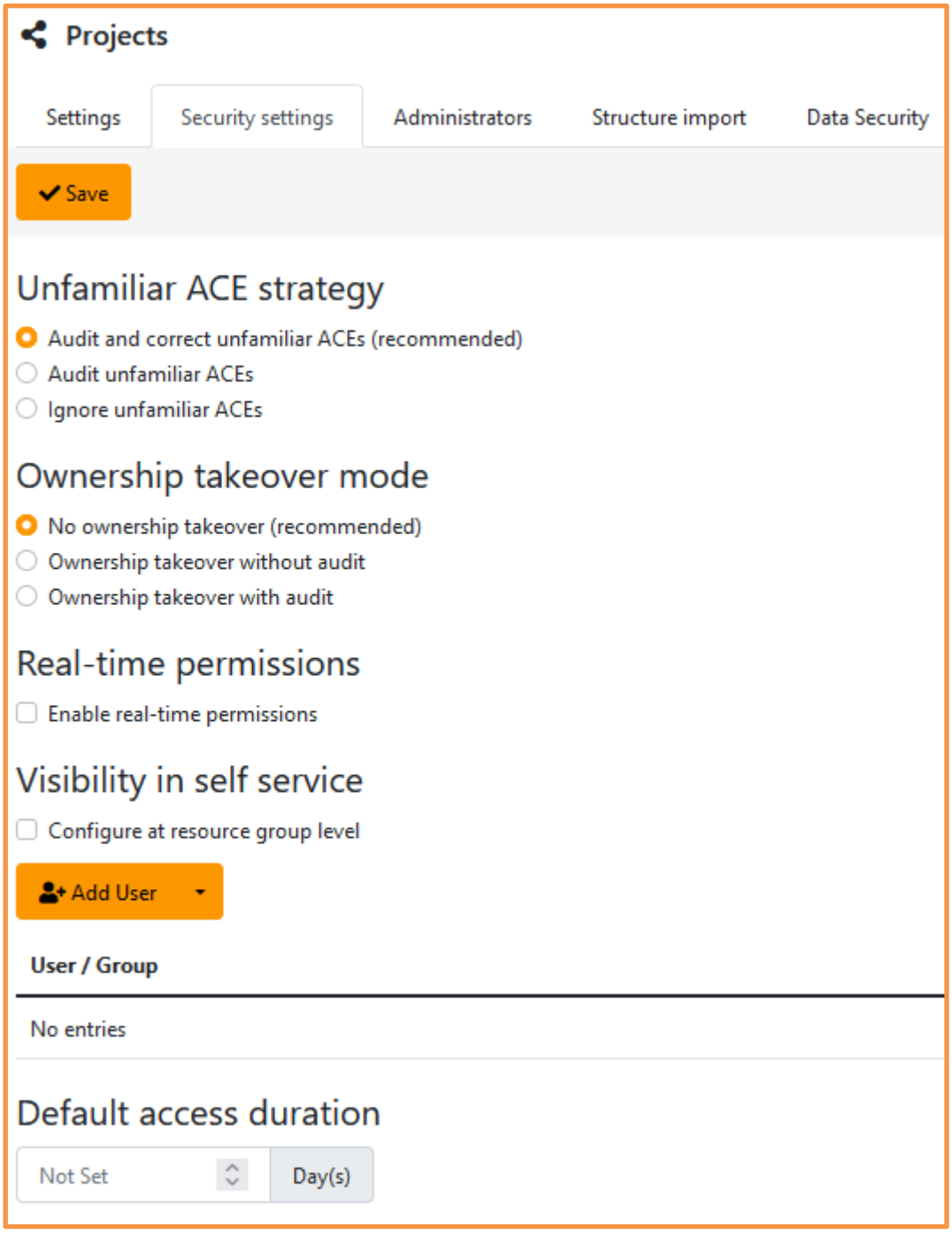
You have the same options as when creating a new folder collection (see previous chapter).

In addition, you may change the UNC path to the folder collection when the entry point has changed in the filesystem (renamed base folder or moved to another server). Because in this case the UNC path changes, you need to reconfigure Access Manager on this matter, otherwise subsequent managed folder cannot be found anymore.

Please definitely take care to follow these tips for successful alteration:

- First, make the change in the filesystem. If you copy the file structure to another location, please make sure to also copy the access permissions (i.e. using the program robocopy that comes with Windows).
- Now click the button *Rename folder collection* and enter the new UNC path. Make sure to follow the information in the dialog window. You will be notified if any jobs are currently executed on this folder structure. Please make sure to wait until they are finished, otherwise this may lead to errors or inconsistencies.
- By renaming the folder collection in the AM database, all affected records are changed, so that, for example, folders referenced in profiles are corrected as well. Depending on the amount of data, this may take a while and is therefore performed asynchronously by an automatically scheduled job.
- To avoid inconsistencies and erroneous access on folders not existing anymore, management of this folder collection management is deactivated (see option *Enable rights management* in the previous chapter).
- Once the job *RenameFolderCollection* is finished, you need to manually reactivate the management.

8.2.1.4.2 Tab: Security settings



- *Unfamiliar ACE Strategy:* This setting usually does not need to be changed as it has direct impact on checking the correct permissions on the file system performed by the job *MaintainAccessPermissions*. The setting lets you choose from the following options:
  - *Audit and correct unfamiliar ACEs:* This is the default value. When the job checks for illegal permissions change on the file system, all deviations compared to Access Manager

definition are not only audited but also corrected. This gives you maximum security against unwanted permission spreading.

- *Audit unfamiliar ACEs:* The job will still check the managed folders and report all permission deviations but will leave additionally set file system permissions for accounts and groups untouched. Missing and incorrectly set permissions (i.e. Write instead of Read) are still revised. This gives space for undesired extent of access rights.
- *Ignore unfamiliar ACEs:* Like above, additional file systems permissions are not corrected. Moreover, they are also not audited but fully ignored. This gives space for undesired and unrecognized extent of access rights.
  This option is not recommended!

- *Ownership takeover mode*: For managed folders, Access Manager has the possibility to take over the ownership of all contained folders and files. This setting lets you choose from the following options:
  - *No ownership takeover:* This option is recommended. AM will leave the current owner untouched when a folder is managed. To avoid unwanted filesystem changes by end users, it is strongly advised to **set up Share permissions** in a way **that end users only have read and change permissions but not full control**.
  - *Ownership takeover without audit:* As soon as Access Manager manages a folder, it will take over ownership of all contained folders and files but does not save this information.
  - *Ownership takeover with audit:* As above, but Access Manager will create an audit record for every object it has taken ownership of, so you can tell the original owner from the report *Assumption of Ownership of resources by folder*. You should use this option only in rare cases where you really need this information, as it has a high impact on both database size and processing performance.

  Regarding this setting, options exist in the System Settings to specify initial default values (see chapter 13.8.3ff).

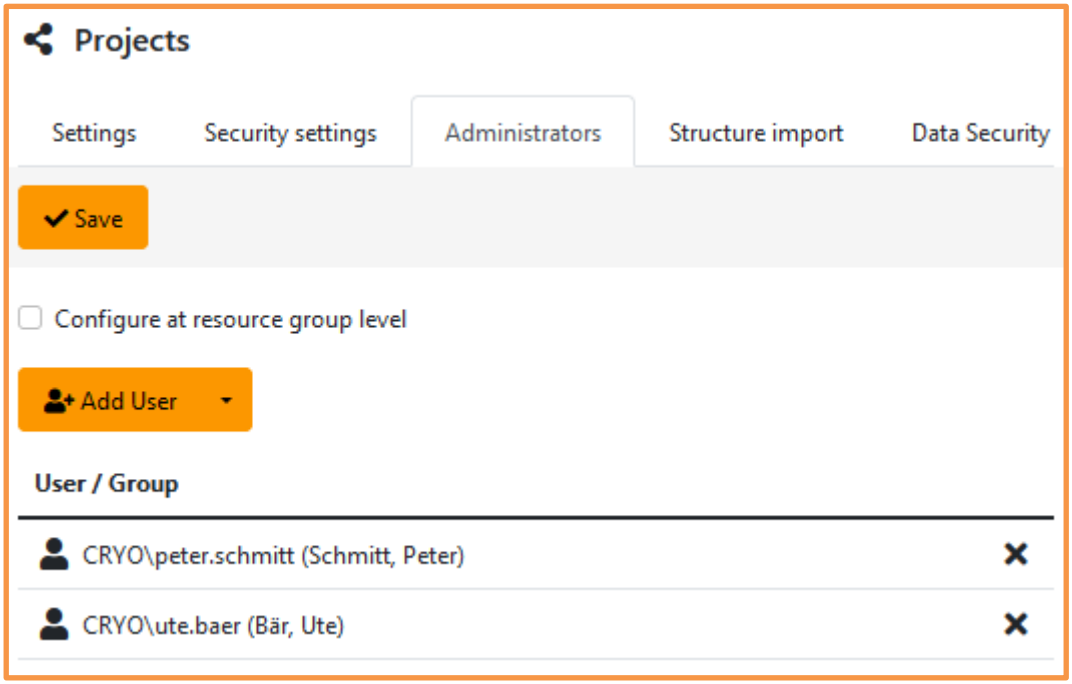
Please note that this setting concerns ownership in the file system, not the role Owner within Access Manager.

- *Enable real-time permissions*: If this option has been checked, AM will not only save new user permissions to the corresponding AD groups but also directly to the file system. This option will give the user immediate access to the folder without having to logoff and logon again with Windows. The ACL entry will automatically be deleted from the file system after 24 hours. It should be noted that this setting might have negative effects on performance, if it has been activated for folders with a large number of files. In addition, subsequent modifications of the same users' permissions within a 24-hour period will not be reflected properly.
- *Visibility in Self Service*: If this option is activated, the folder collection will only show up on the application page for users and groups who have been added to this list. If you don´t specify

any users and have also not enabled checkbox *Configure at resource group level*, all users can see this folder collection.

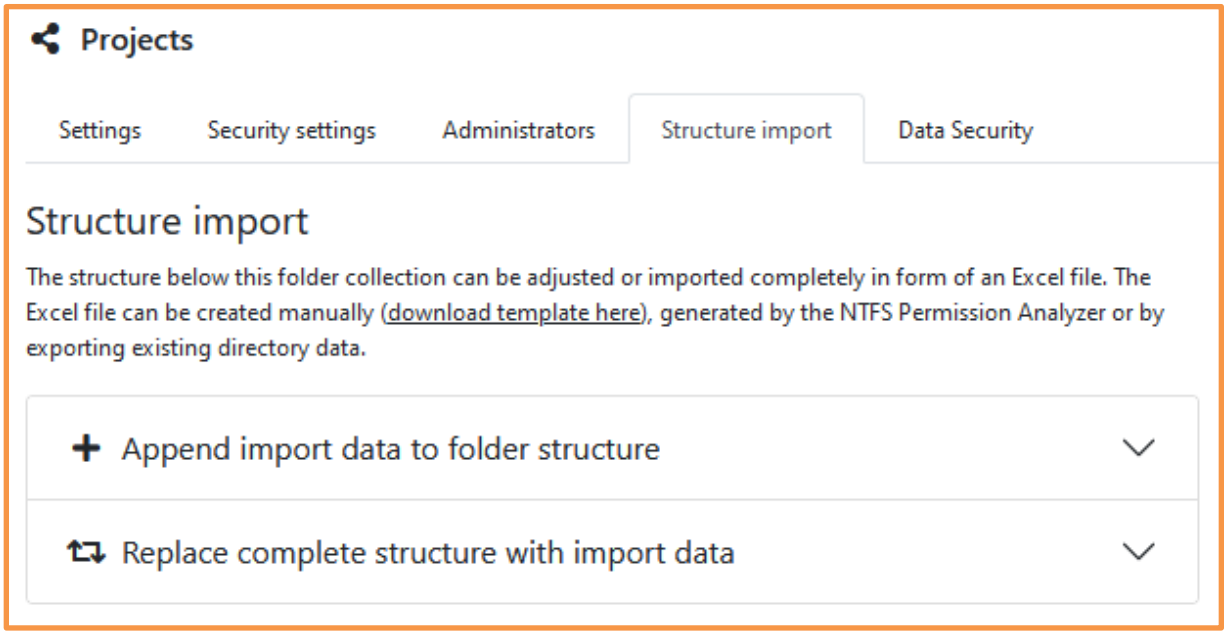
- Default access duration: The number of days set here will be used as the default value for the *Maximum duration period of permissions* for all subsequent managed folders. It can still be altered individually. Newly applied (and granted) managed folders will receive the value set in this option – they will *not* inherit the value set on their parent folder!

8.2.1.4.3 Tab: Administrators



Here, you specify users who may also administer this folder collection. If you leave this list blank, only AM-Administrators can do so. Alternatively, activate the checkbox to inherit the persons defined on the parent resource group.

8.2.1.4.4 Tab: Structure import



Most often, right after creating a new folder collection, you want to re-use your already existing file system permission with Access Manager. This can be accomplished using the Structure import that allows for importing an Excel file with distinct content. Choose whether you want to keep already managed folders (if any) as-is and only append management information for further folders (first option) or if you want to completely wipe managed folder information and start again with only such folders being managed that are contained in the Excel file (second option). By default, the imported information will only affect the AM database. The import process will only create folders in the file system if the option *Insert folders into database and create them in the file system* is activated. The Excel file can be created manually or generated by NTFS Permission Analyzer (separate application) or by exporting existing folder data. In any case, the file must correspond to the format described in the following chapter.

All folder data to be imported must relate to the same folder collection. Correspondingly, all folder names must begin with the correct server and share names, following the UNC naming convention. First, select the Excel file to import and click *Validate file*. The content will undergo an intensive validation process. If the file contains errors, a list of the detected problems will be displayed, and the import will be terminated. Data will not be imported or modified.

If there are no errors, the import process can be started by clicking the *Start import* button.

The new permissions will be stored in the AM database if the import process is successful. The *MaintainAccessPermission* job must be executed to set the permissions in the file system.

The file to be imported must be an Excel file (XLSX file extension created by Office 2007 or later). The first row in the file must contain the column headers. The following columns contain information

needed by Access Manager and are mostly – depending on administrative settings – mandatory. They may occur in any order.

A file may have empty rows that will be ignored by the import process. If several rows list a user account for the same folder with different permissions (read permissions in one row, write permissions in another), AM will grant the higher graded set of permissions to the user. The existence of duplicate user entries in the import file will not cause any problems.

Import files from previous versions are not perfectly compatible but may be used after adapting some columns headers.

These columns will be used by AM during the import process:

Column name: **FOLDER**	Mandatory: **Yes**
Format	**Description**
\\Server\Share\Folder path	UNC path for the folder to be imported including server and share

Column name: **READ**	Mandatory: **Yes**
Format	**Description**
X or empty	The user from the SAM-ACCOUNTNAME field has read permissions. If the SAM-ACCOUNTNAME has been set, the READ or WRITE column must be set also. If the WRITE column has been set, the user will be granted the write permission.

Column name: **WRITE**	Mandatory: **Yes**
Format	**Description**
X or empty	The user from the SAM-ACCOUNTNAME entry has write permissions. If the SAM-ACCOUNTNAME has been set, the READ or WRITE column must be set.

Column name: **SAM-ACCOUNTNAME**	Mandatory: **Yes**
Format	**Description**
Domain\Username or Domain\Groupname	Login name (AD attribute: "SamAccountName") for a user or an AD Group who shall have the read or write permissions. This entry must be filled if the READ or WRITE column has been set. It is possible to not grant permissions to any user. For this, a row must be given containing an OWNER and RESPONSIBLE. This way AM will turn the folder into a Rights Folder but not grant any permissions yet.

Column name: **FULLNAME**	Mandatory: **No**
Format	**Description**
Free text or empty	Display name of the user. Not used by AM, just for your information.

Column name: **OWNER**	Mandatory: **Yes**
Format	**Description**
Domain\Username	Login name (AD attribute: "SamAccountName") for the Owner.

Column name: **RESPONSIBLE 1-X**	Mandatory: **Yes**
Format	**Description**
Domain\Username	Login name (AD attribute: "SamAccountName") for Responsibles 1 to many. At least one Responsible must be provided, further ones are optional.

Column name: **INHERITRIGHTS**	Mandatory: **Yes**
Format	**Description**
X or empty	Indicates if the folder shall inherit the user permissions from a parent Rights Folder. If this is the first managed folder in the hierarchy, inheriting from above is not possible.

Column name: **VISIBLEINSELFSERVICE**	Mandatory: **Yes**
Format	**Description**
X or empty	Indicates if the folder shall be displayed in the Management Portal.

Column name: **COMMENT**	Mandatory: **See description**
Format	**Description**
Free text or empty	For every permitted user a text is entered, displayed later on in the comment column of AM user permission screens. If the administrative setting "CommentsAreMandatoryDuringImport" is activated, this column is mandatory, and every user permission must contain an entry. If inactive, any given comments will be imported but also, the column need not be present at all.

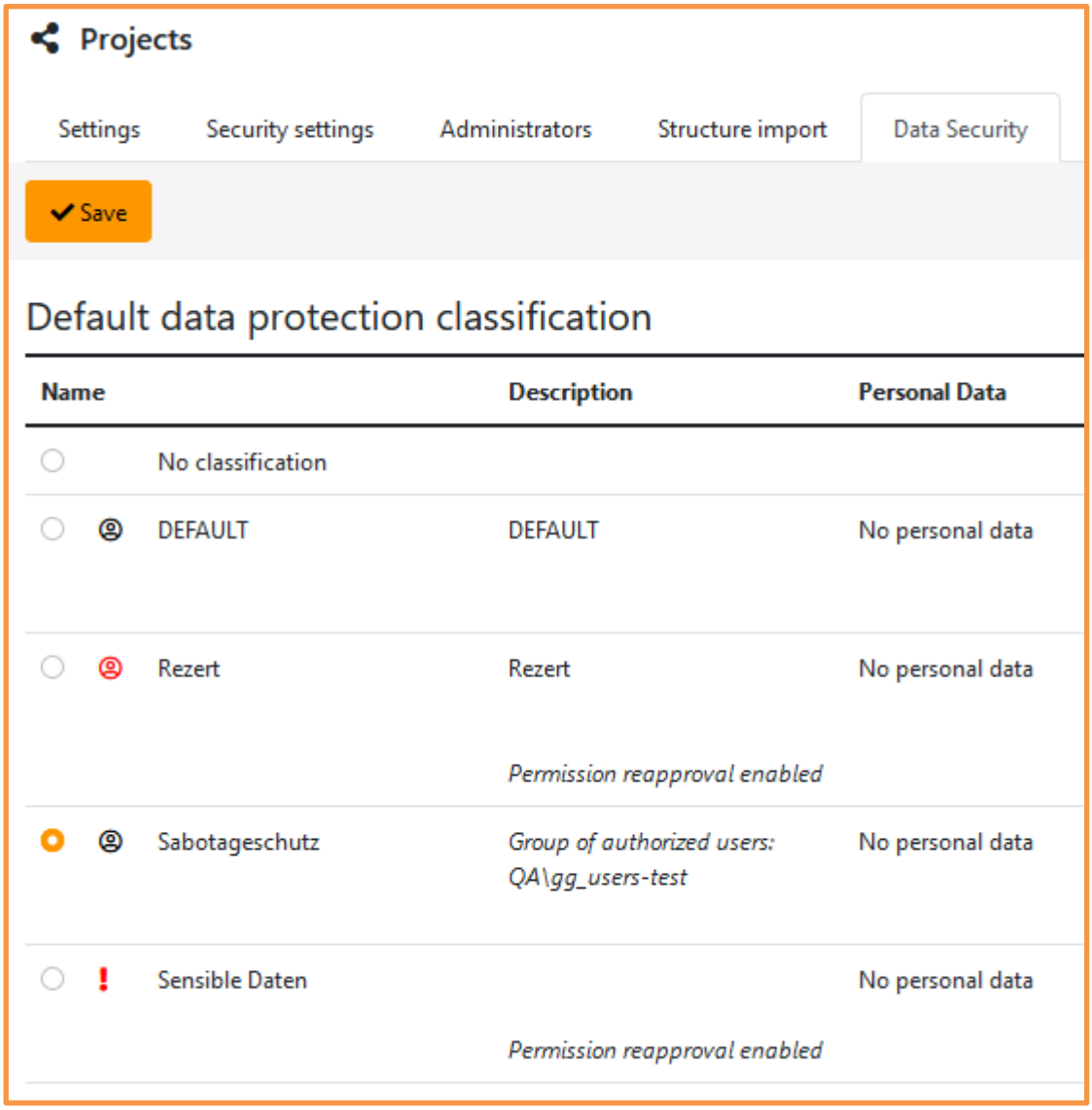
Column name: **VALID-THROUGH**	Mandatory: **Yes**
Format	**Description**
YYYY-MM-DD or DD.MM.YYYY or MM/DD/YYYY	Date until which the permission is valid.

Column name: **DEFAULT-VALIDITY-PERIOD**	Mandatory: **Yes**
Format	**Description**
Integer number	Number of days for maximum permission period. Leave this field blank to use the default permission period set in AM on the Folder Collection. Enter value "NULL" (without quotation marks) to force an indefinite permission period on the folder.

Column name: **RESOURCE-DESCRIPTION**	Mandatory: **Yes**
Format	**Description**
Free text or empty	A brief description of the folder.

Column name: **RESOURCE-CLASSIFICATION**	Mandatory: **Yes**
Format	**Description**
Free text or empty	Name of a classification for this folder. The classification must already exist within Access Manager. Leave this field blank to use the default classification set in AM on the Folder Collection. Enter value "NULL" (without quotation marks) to force having no classification set on the folder.

8.2.1.4.5 Tab: Data Security

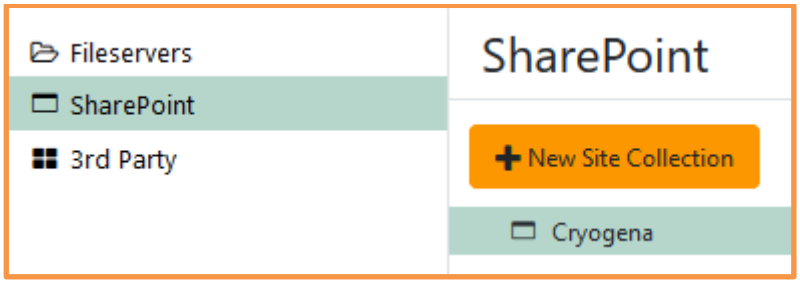


If you have created some classifications before, they will be listed here, and you can select one that will be assigned to every newly set up managed folder from now on (can individually be changed on that respective folder).

When changing the default classification later on, this may or may not affect the classification set on the managed folders:

- A managed folder has had the previous classification assigned: It will have the newly set default classification assigned.
- A managed folder has had a different classification assigned: That classification will stay the same, the new default classification will not be assigned.

8.2.2 SharePoint (Classic Experience)



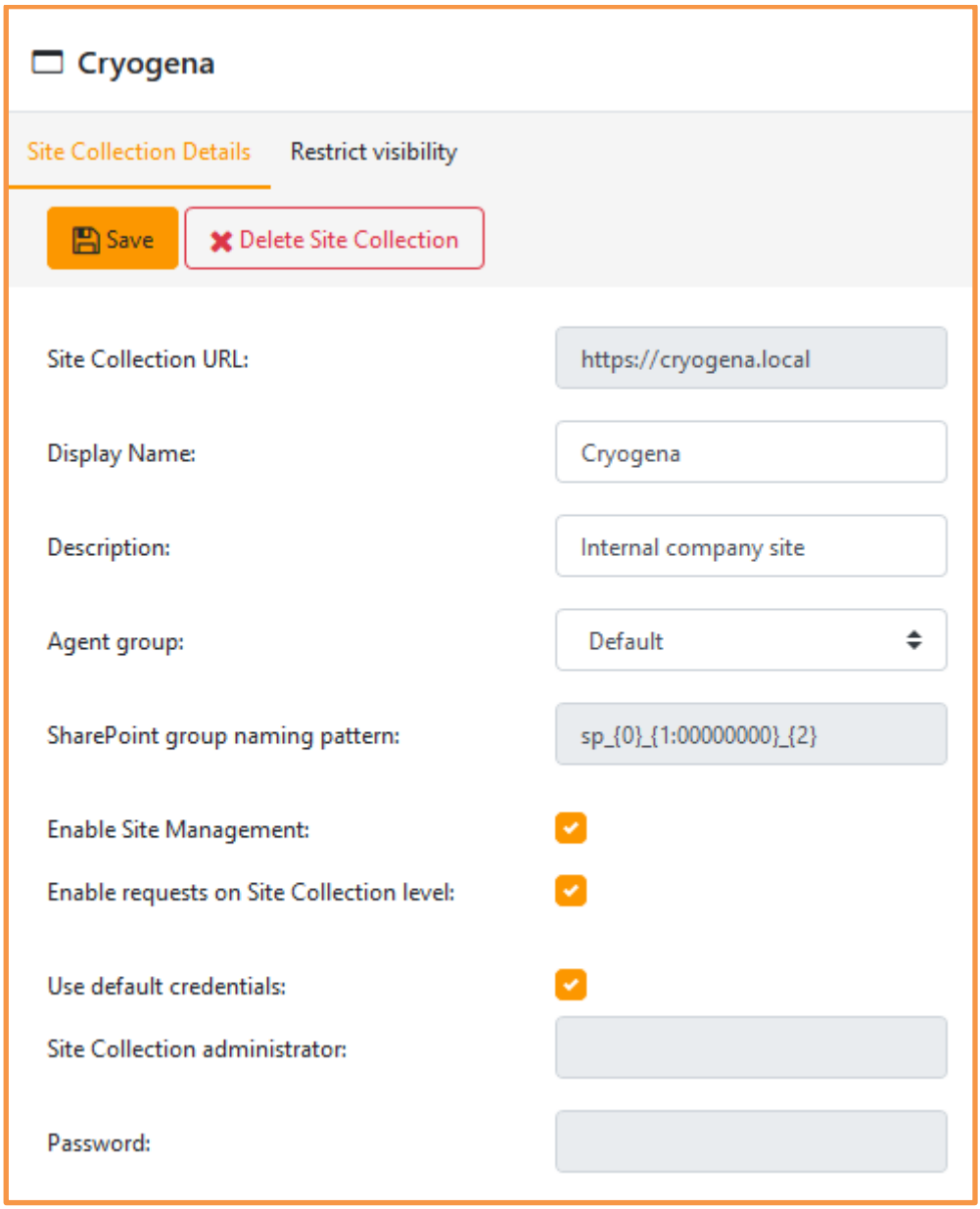
Important distinction: This area only deals with SharePoint Classic Experiences (in Microsoft Entra and on premise).

SharePoint Modern experience in the Microsoft Entra Cloud ("Microsoft Entra SharePoint", "SharePoint online", "SharePoint Modern Experience") cannot be managed here. You can find this in chapter 8.2.4

This section determines which AM access permissions should be managed for which site collections. The section has been divided to display the tree view and the Details list.

The list in the tree view displays all site collections that are managed by Access Manager. A site collection can be selected by clicking on the respective node. The corresponding details will then be displayed in the right pane. A corresponding resource can be added by clicking the *New Site Collection* buttons.

8.2.2.1 Site Collection Details



If a Site Collection already exists within Access Manager, you can change all its parameters except for its URL – in the network, the Site Collection is identified solely by its URL.

When adding a new Site Collection, fill in the following values:

Site Collection URL: The full URL of the Site Collection including the protocol (http, https).

Display Name: This name shows up in the Management Portal (mandatory).

Description: A description of the Site Collection (mandatory).

Agent Group: Shows the group of *AM Agents* which can be edited for the Site Collection. The *Default* group is the default setting. More information about agent groups can be found in chapter 11.2.

SharePoint group naming pattern: When adding a server, these parameter entries can be changed using the corresponding entries. The following placeholders (in curly brackets) can be used:

- {0} The Site Collections´ name as entered in *Display Name*
- {1} The Site Collection ID (automatically increased internal number)
- {2} The abbreviation of the permission (*r*, *w* or *b* for read, write or browse permission)

Use of the {0} placeholder is optional, however, the {1} and {2} placeholders must be used to generate a unique group name.

Enable Site Management: This checkbox determines whether the Site under the Site Collection will be managed or not. If management has not been enabled, the following restrictions apply:

- The Site Collection will not be displayed in the Management Portal.
- The access permissions will not be managed.

Enable requests on Site Collection level: This option enables Management Portal users to select a Site Collection and apply for a new Site under that Site Collection immediately. Otherwise, new Sites can only be created under an already existing Site. To do this, an *Owner* must have already been assigned to a Site Collection.

Use default credentials: If the server of the Site Collection is connected to the Active Directory (e.g. by usage of Office 365) you can activate this checkbox and use the Access Manager user account.

Site Collection Administrator & *Password:* If the server of the Site Collection is not connected to the Active Directory (e.g. by usage of Office 365) there is the possibility to enter alternative credentials here.

The changes will take effect after the *Save* button has been clicked. Once a new Site has been added, it will appear in the tree view. Clicking the *Delete* button will remove the Site so that the it will no longer be managed by AM.

Additional settings for SharePoint Online:

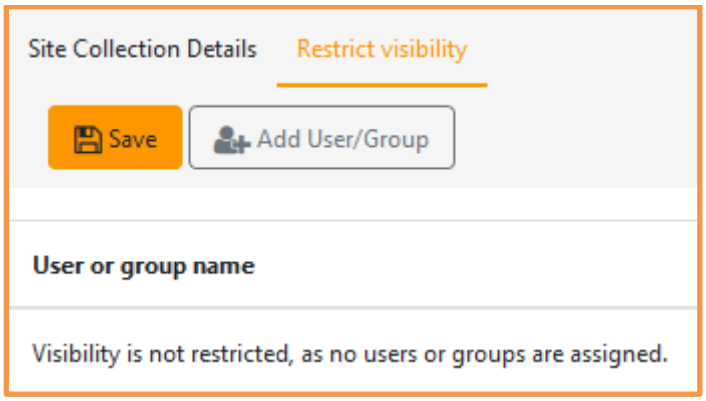
In case you are using the cloud based SharePoint 365, additional settings have to be done.

Access Manager needs to be registered as an application in Microsoft Entra. **While doing so, please make sure to take a note of the following parameters and values as some will not available for you later:**

- Application ID (Client)
- Client key
- Authentication end point

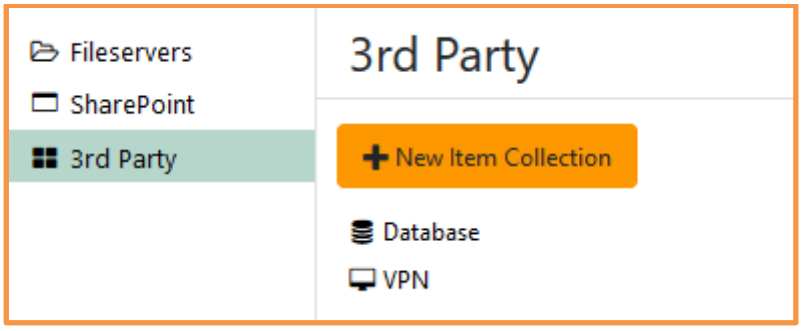
These values are needed when adding a Site Collection in Access Manager:

8.2.2.2 Restrict visibility



If the Site Collection shall be displayed only to a distinct set of users / user groups, enter them in this list and save it.

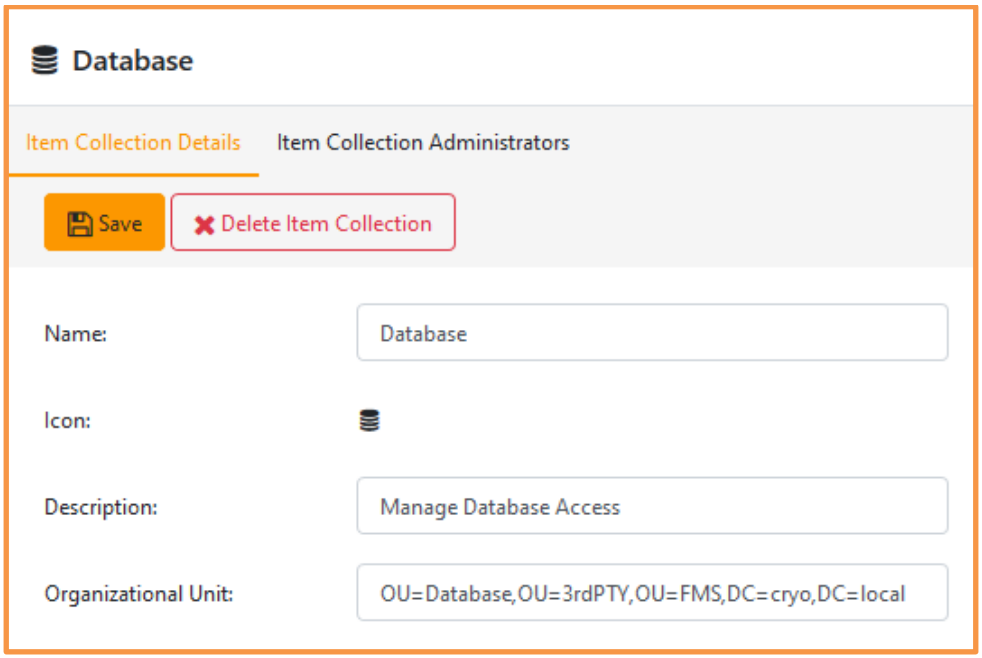
8.2.3 3rd Party



This page determines *Item Collections* for AD groups. AM will manage membership by means of *Items*. The page is divided into *Item Collection List* and *Details*.

The Item Collection pane lists all Item Collections managed by AM. By clicking an entry its details will be displayed in the right pane. The button *New Item Collection* adds a new Item Collection.

8.2.3.1 Item Collection Details



If an Item Collection already exists within Access Manager, you can still change its parameters.

When adding a new Item Collection the following information must be entered:

Name: Name of the Item Collection visible to all users. If this name is already used by another Item Collection please enter a different name.

Icon: Choose from a list of predefined icons that will fit best.

Description: Choose from a list of predefined icons that will fit best.

Organizational Uni: Enter the fully qualified name of the OU in your AD where permission groups of newly created items will be saved. The OU must already exist and the Access Manager (=the user accounts of AM) must have write access for it and all of its sub-objects. It is possible to enter the same OU for different Item Collections.

The changes will take effect after the *Save* button has been clicked. Once a new Item Collection has been added, it will appear in the tree view.

Clicking the button *Delete Item Collection* will remove the Item Collection so that it will no longer be available. Included Items will also be deleted, but the AD Groups bound to them are left untouched. If you want to change / remove such groups, remove the permission management of single Items first (see chapter 8.4.4.3.6).

8.2.3.2 Permission Set – Logic to grant permissions

A *Permission Set* defines a freely customizable amount of permissions of an item which are mapped to specific AD groups when it comes to creating a new item within the item collection. Please note that

Access Manager does not truly manage permissions itself: You only describe by name the permission which your 3rd party application will interrelate to the given AD group. By definition, a Permission Set may consist of at least one permission.

For every Permission Set, a default permission is set. When a Responsible, Administrator or Profile Administrator is permitting an item of this collection, this permission is suggested by default, analogous to *Read* permission when granting permission on a file system folder.

For each right that you define here, further details about the Active Directory (AD) groups are specified in addition to the display name. The *Group Naming Pattern* is explained more explicitly as follows:

If you leave this field empty, you can freely specify its AD group name later when creating a new element. If you enter something here, this entry is automatically used later as the AD group name and cannot be changed. Therefore, you must use the *{ItemName}* parameter in the template to ensure that all AD groups are given a unique name. This parameter will be replaced by the name you give the item when you create a new item. For example:

Suppose you create a new right with the display name "DBO access." You define the group naming pattern as "database_{ItemName}_dbo." If you later create a new element and give it the name "AM-DB," the AD group that is created for this right of this element will be named "database_AM-DB_dbo."

Since element names must not contain certain special characters (to ensure valid AD group names), there is a validation rule for the name input similar to that for directories and SharePoint sites (see chapter 13.8.2.1).

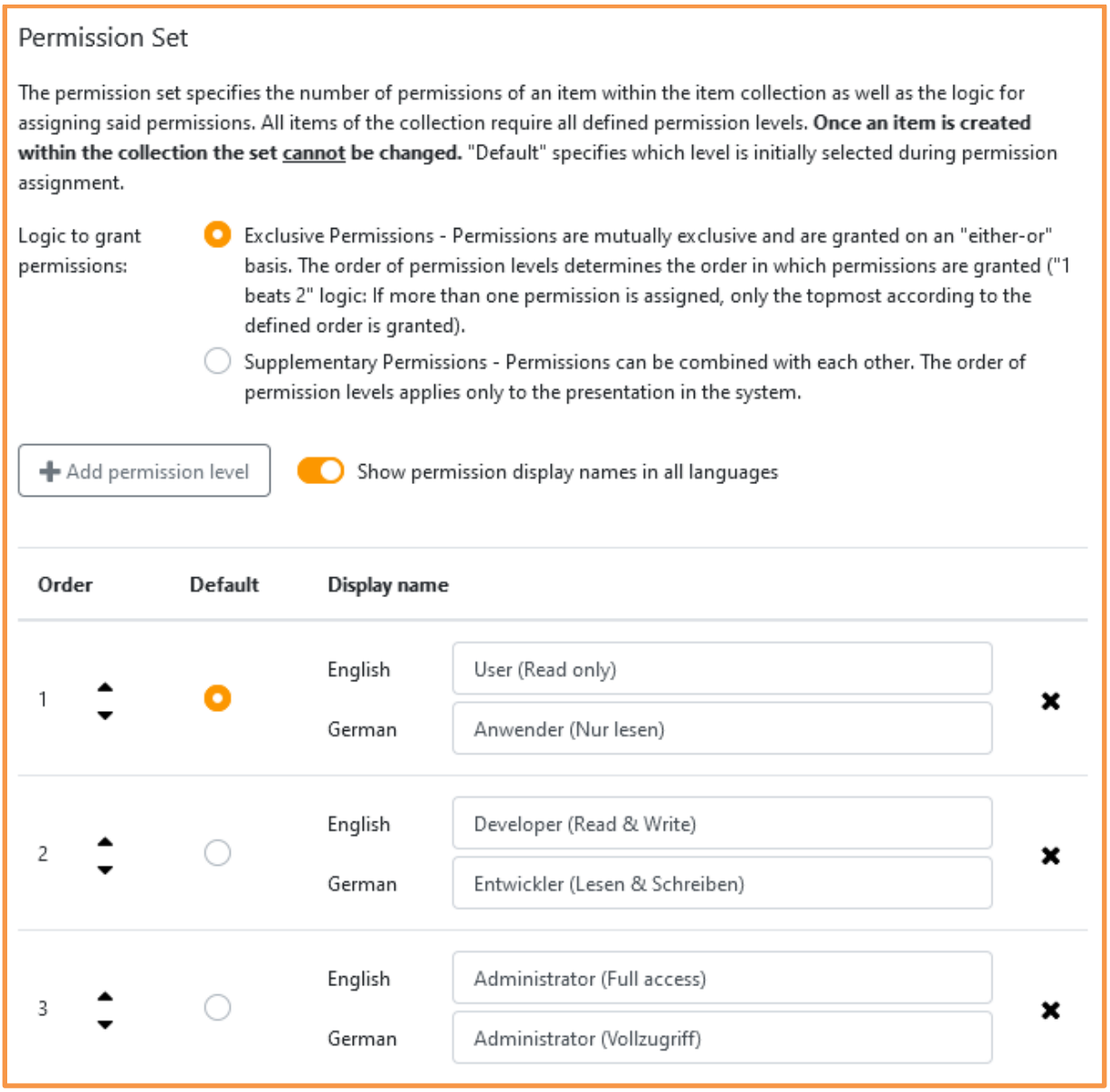
Also consider the maximum length for group names (AD limitation):
The ItemName *you entered plus the characters you entered in the name pattern must not have more than 64 characters!*

There are two kinds of permission logic: Exclusive and supplementary permissions.

8.2.3.2.1 Exclusive Permissions

When using Exclusive Permissions, only one of many permissions within the set can be granted, they cannot be combined.

Example: Database access

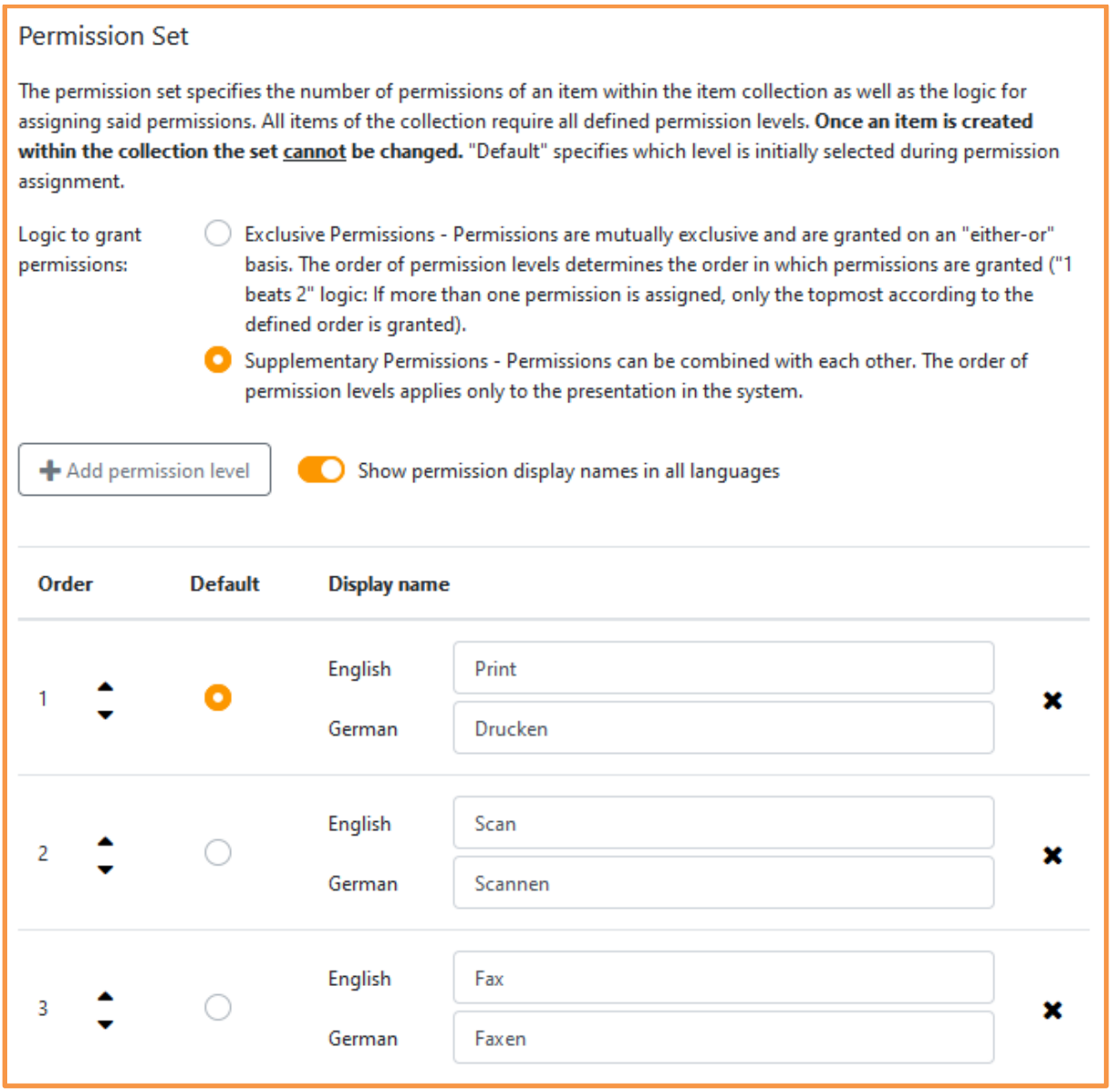


Here, the user needs to choose exactly one access permission on a database when he requests access. This logic can be compared to Read or Write access on filesystem folders.

8.2.3.2.2 Supplementary Permissions

Using Supplementary Permissions, multiple permissions of a set may be granted at the same time. Usually, this kind of logic is used if distinct permissions do not conflict with each other.

Example: Multifunctional Printer



Here, a user may request multiple permission at once as they target on independent functionality.

8.2.3.3 Item Collection Administrators

This tab lets you specify the persons who may manage exactly this single Item Collection, regardless of having the *3rd Party Administrator* role.

8.2.3.4 Data security

Similar to the function for folders, you can define a data protection class for a collection assigned by default to a newly created item.

8.2.4 SharePoint Collection (Modern Experience)

Important distinction: This area only deals with the SharePoint Modern Experience in the cloud ("Microsoft Entra SharePoint", "SharePoint online", "SharePoint Modern Experience").

Self-hosted SharePoint installations (on premise) and SharePoint Classic Experience in the cloud cannot be managed here.

You can find this in chapter 8.2.2. Due to the technical and administrative similarity to 3rd Party Item Collections, SharePoint Collections are also created in this workspace: select the *SharePoint Collection* entry from the drop-down list.

The input fields are very similar to those of the 3rd Party Item Collections. Instead of the AD OU for storing the AD groups, enter the Microsoft Entra Tenant in which your SharePoint Sites exist or can be created by Access Manager.

The logic of the permission assignment is always "Exclusive Permissions" (only one of the permissions can be granted), so there is no choice for this. The permission set is set by SharePoint itself (*Owner*, *Member*, *Visitor*). However, in addition to the labelling of these rights, you can specify here whether the right *Owner* and *Visitor* should be able to be requested at all.

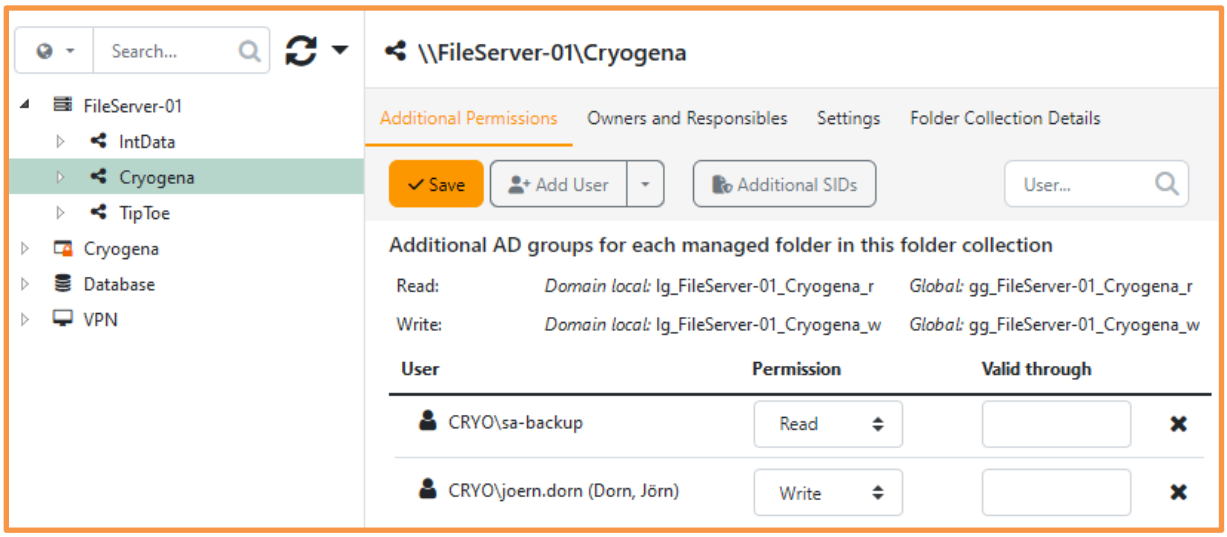
Although you will normally only have one Tenant and therefore probably only want to create one SharePoint collection (in which all sites are created), you can also use these collections to allow individual permission sets on certain sites – define one SharePoint collection for each desired set and then assign the sites accordingly.

8.2.5 MS Teams Collection

The same applies to Teams collections as to SharePoint Online collections (see previous chapter), Teams Collections are created in the very same way. The only difference is that a Permission Set in Teams only consists of the rights *Owner* and *Member* - there is no *Visitor* right.

8.3 Managing Special Permissions on Folder Collections

As an *Administrator* you have the same possibilities to manage permissions as a *Responsible*, meaning you can change user permissions on every resource. Additionally, at tab *Additional Permissions*, Read and Write permissions can be set on an entry point. The following description refers to page *Administrator/Permissions*:



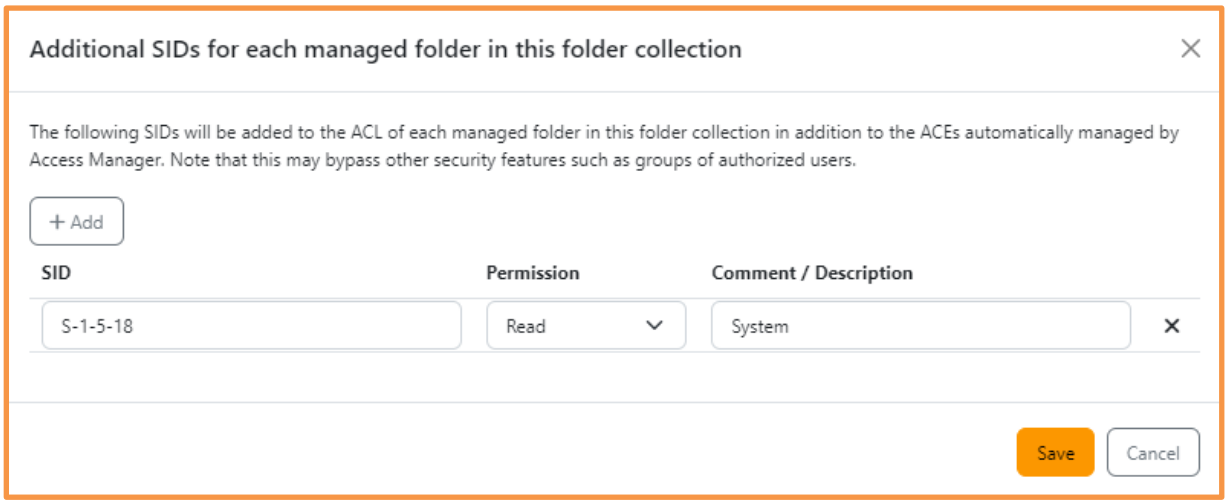
8.3.1 Additional Permissions (Special Permissions):

By default, Access Manager creates at least two additional AD groups (four, if Domain Mode *Multi Domain Optimized* is used) for every folder collection. These groups are not permitted on the folder collection root folder itself (except if it is also managed) but are set to *all* Rights Folders and their inheriting sub folders and files. Initially, these groups do not contain any members, but you can add users and, if enabled, AD groups at this tab with optionally setting an expiration date for the permission. The purpose of *Special Permissions* is to easily grant access i.e. to machine accounts for automated backup / restore software or to department heads for having general access to all folders. This saves a lot of effort as you do not need to grant access for every single managed folder. *Special Permissions* can only be set by an *Administrator* and they do not occur in *Reapproval* runs.

8.3.2 Additional SIDs

With the *Additional SIDs* button, you call up a dialog in which you can authorize any AD accounts or groups using their SID. These may explicitly be local accounts or so-called *well-known SIDs*, where the identifier is identical on all machines. This gives you the option, for example, to authorize the SYSTEM account of a file server if this is required for backup/restore purposes.

Microsoft provides a comprehensive overview of such well-known SIDs at https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/manage/understand-security-identifiers#well-known-sids



You can manage and view the SIDs only here. Entering a description is required in any case - ideally you would enter the name of the group/account here, as this is not recognized otherwise.

Because these SIDs must be written / removed on the complete folder collection, a change does not happen immediately but only with run of the next MAP job (see chapter 11.6.4.4).

The availability of the functionality is switched on / off by the administrative settings *ShowAdditionalManagedFolderSidsDialog* (see chapter 13.8.3.23).

8.4 Managing Resources

Users with the *Administrator, FM-Administrator, SharePoint-Administrator* or *3rd Party-Administrator* role are permitted to define resources or resources with explicit security and role settings. The following description refers to page *Administrator/Permissions*:

8.4.1 Level: Resource Group

If selecting a resource group, its Display name and description is shown in the details panel. This information is read-only.

8.4.2 Level: Folder Collection

If selecting a folder collection, the details pane displays all dedicated information separated into several tabs. Tab Special Permissions is described in previous chapter 8.3. Tab Owners and Responsibles lets you define all deciders (see following chapter 8.4.4.1). Setting Responsibles at this level is possible because the entry point of a folder collection can be set as a managed folder. Please pay attention to the following notice. Lastly, tab Folder Collection Details shows some non-editable technical information.

Entry Point of Folder Collection as managed folder:
Although possible, rights management on an entry point should be performed only under certain circumstances as removing the Permission Management at a later time may lead to severe difficulties on common user access.
See chapter 8.4.4.3.5 for more information and technical background.

8.4.3 Level: Item Collection

8.4.3.1 Tab: Item Collection Details

When selecting an *Item Collection*, the right pane displays the Item Collections´ descriptive text and the OU in AD, provided by the *AM-Administrator*. This information is for informational purpose only and cannot be changed here.

8.4.3.2 Tab: Settings

8.4.3.2.1 Public items

Here you can specify whether items of this collection shall be public by default. Being a public item, permission requests of user are automatically granted. This can be changed individually for every item. Furthermore, specify if Responsible shall also be informed by email about such a request (like for requests on non-public items).

8.4.3.2.2 Scripts

Here you may enter custom PowerShell Scripts that are executed on dedicated events – see chapter 8.4.4.3.7 for more information.

8.4.3.3 Tab: Create Item

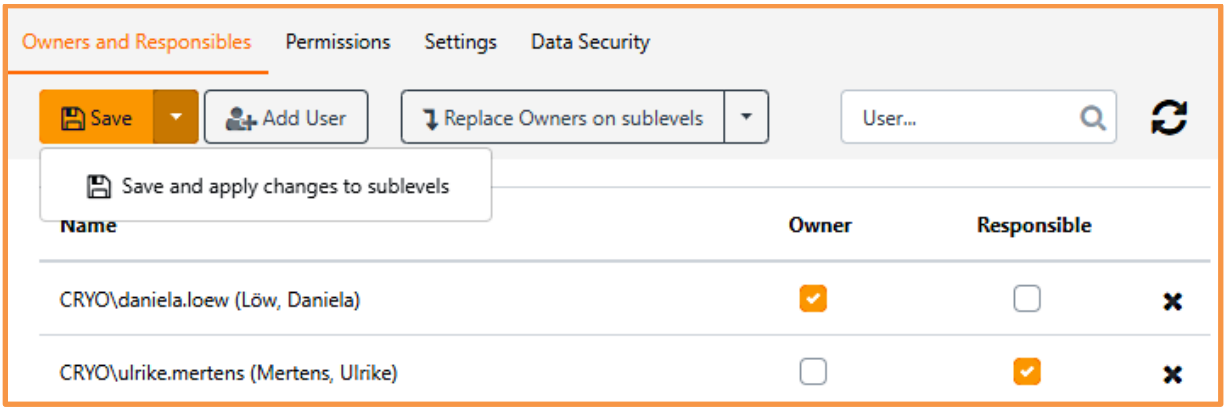
Options and conditions regarding the creation of a new item in a collection are explained in detail in chapter 8.5.

8.4.4 Level: Resource

The *level of resources* contains resources that belong to a Share, SharePoint Site Collection or Item Collection, thus these are managed / unmanaged Folders, SharePoint Sites and Items (3rd Party Resources).

Although all following functions are nearly identical for all resource types, there may be subtle differences resulting from the nature of the respective type.

8.4.4.1 Tab "Owners and Responsibles"



In this tab the *Owners* and *Responsibles* will be defined. Users to be added as Owner and / or Responsible will be added by first entering a user account name in the corresponding entry and then clicking the *Add User* button. The user then appears in the roles list below and roles can be granted to the user by selecting the corresponding checkbox for Owner or Responsible. All changes will take effect after the *Save* button has been clicked. All users where no checkbox is selected will be removed from the list.

In order not only to make role changes on individual managed addresses but also to be able to transfer these to child address structures without much further effort, Fileserver Management and SharePoint Management offer additional options:

8.4.4.1.1 Save and apply changes to sublevels

This option is used to apply exactly the change(s) you made to child items. Previously existing role assignments are not taken over.

8.4.4.1.2 Replace Owners / Responsibles on sublevels

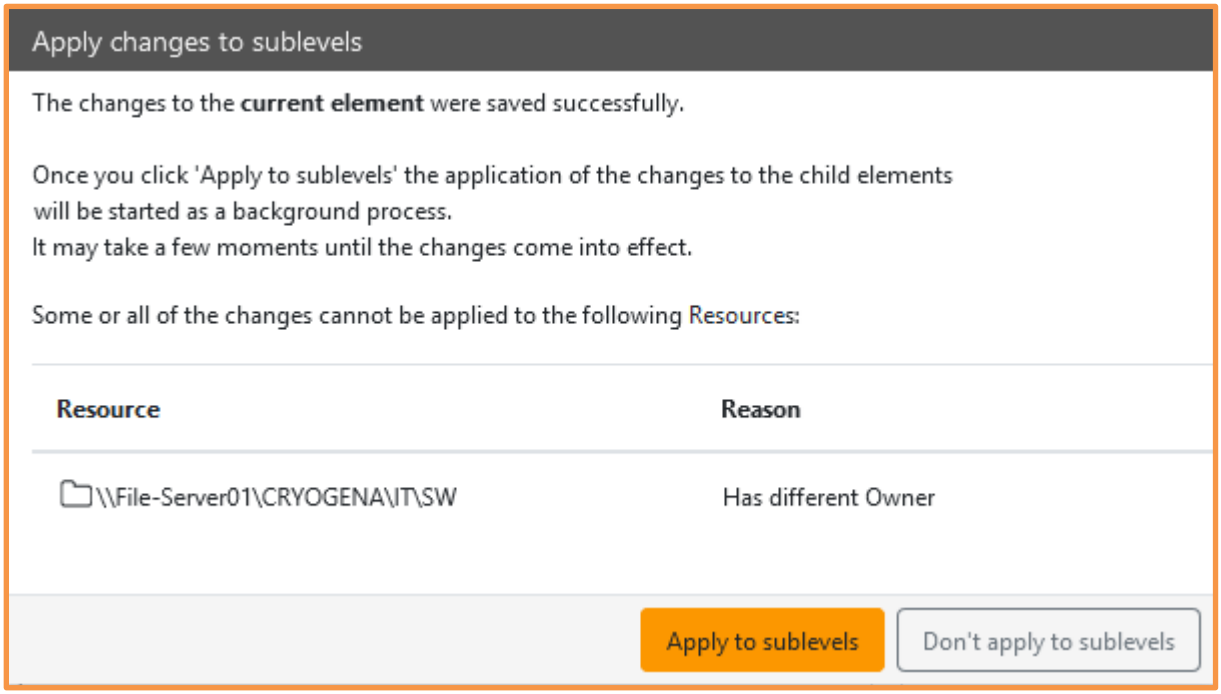
Unlike the first option, here the role assignment as it is set on the managed address is fully replicated to child addresses depending on the selection (*Replace Owner / Responsible on sublevels*), regardless of their actual state.

As with simple saving, there are some limitations resulting from the distinction between managed and unmanaged addresses in Access Manager. Only those changes are applied to the respective sub element that do not change its status, e.g. that would not turn a free folder into a managed folder or vice versa. For more information on the Operational Principle *Owner & Responsible*, see chapter 4.1 ff.

A short summary of the most important points:

- A free folder can have one owner but no Responsibles.
  → Added/changed owners are adopted, but no Responsibles
- A managed folder has exactly one owner and at least one responsible.
  → Owners are not removed or added without replacement. Responsibles will only be removed without replacement if at least one Responsible remains on the managed folder.
- A SharePoint site can have multiple owners and responsible.
  → Responsibles and Owners will only be removed without replacement if at least one Responsible and one Owner remain on the managed Site.

Access Manager checks for the above conditions and will list the managed addresses for which the saved changes cannot be accepted, along with a reason. Only after pressing the *Proceed* button, the action is triggered and processed by a job.



In this context, the difference between deleting a user and removing the role of a user must also be taken into account. If, for example, you remove the *Owner* role from a user for a managed address, the user also loses this role at lower levels. If, on the other hand, you delete an Owner of a managed address, this user is also deleted on sub-elements regardless of his role, even if he has the role *Responsible* on sub-elements.

A few case studies:

You remove the *Owner* Peter Schmitt from managed folder A and replace him by adding Ralf Müller.
What happens if:

- You select *Save and apply changes to sublevels*
  - Subfolder A1 has the Owner Peter Schmitt. He is replaced by the Owner Ralf Müller.
  - Subfolder A2 has the Owner Lisa Meier. She is not removed. Since managed folders can only have only one Owner, Ralf Müller is not added either (different from a SharePoint site, which can have more than one Owner).
- You save and select *Replace Owners / Responsibles on sublevels*
  - Ralf Müller is set as Owner on all subfolders. Other owners are removed.

You delete the *Owner* Peter Schmitt from managed folder A and replace him by adding Ralf Müller.
What happens if:

- You select *Save and apply changes to sublevels*
  - Subfolder A1 has two Responsibles: Lisa Meier and Peter Schmitt. Peter Schmitt is deleted as Responsible.

You remove the only *Responsible* Peter Schmitt from managed folder A and replace him by adding the Responsible Ralf Müller.
What happens if:

- You select *Save and apply changes to sublevels*
  - Subfolder A1 has the Responsible Peter Schmitt. He will be replaced by Ralf Müller as Responsible.
  - Subfolder A2 has the Responsible Lisa Meier. She is not removed. However, since a managed folder can have more than one Responsible, Ralf Müller is added as Responsible.
- You save and select *Replace Owners / Responsibles on sublevels*
  - Ralf Müller is set as Responsible on all subfolders. Other Responsibles will be removed.

You have two Responsibles on managed folder A, Peter Schmitt and Ralf Müller. You remove Peter Schmitt from the Responsible role.
What happens if:

- You select *Save and apply changes to sublevels*

- Subfolder A1 has only one Responsible Peter Schmitt. Since Peter Schmitt is the last Responsible, no action is triggered.
- Subfolder A2 has two Responsibles: Peter Schmitt and Lisa Meier. Peter Schmitt is removed as Responsible .

- You save and select *Replace Owners / Responsibles on sublevels*
  - Ralf Müller is set as Responsible on all subfolders. Other Responsibles will be removed.

8.4.4.2 Tab "Permissions"

As an *AM-Administrator*, you have the same possibilities for managing access permissions as a *Responsible*. These functions are described in detail in chapter 4.2.2.1.

You have extended options for permitting users. The DropDown-List *Add User* contains one more entry, *Add Special Group*:

Here, you can specify any existing AD group to be permitted on the selected folder. It is not possible to add a *Valid through* date or a comment. Please note that Special Groups do not count for the license management and are not audited, nor do they appear in the reports. Considering security aspects and traceability, Special Groups should be used with care.

Via button *Import* you allow user permissions to be read from an Excel file in the corresponding format (see below) and thereby assign them to the currently selected folder / site. To do this, the file must be selected. The user needs to decide if the user permissions will only apply to the current resource or should also apply for all managed resources below. In case of error during the import, error messages are listed and the file is not imported into AM. The following errors might be displayed:

- InvalidUser
- InvalidPermission
- InvalidValidThroughDate
- MissingColumns
- NothingToImport

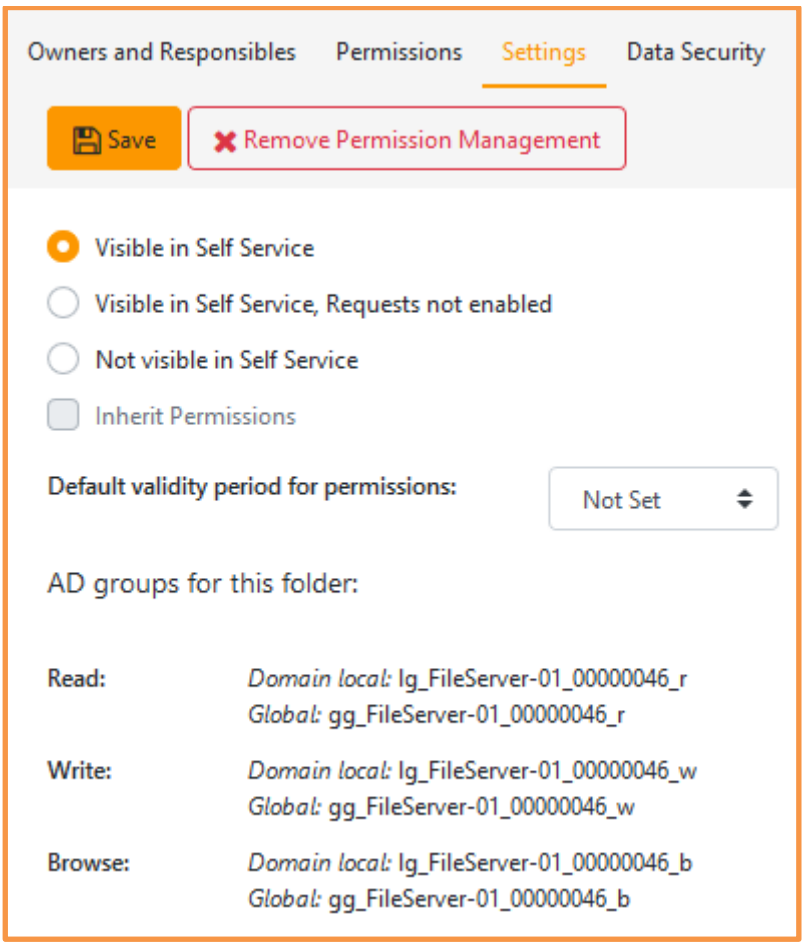
The Excel file must use a pre-defined format, which is described in the following. A template file can be downloaded from the *Import Permissions* dialog (using the *Download Excel Template file* link).

The first row in the Excel file must contain the column headings *USERID, READ, WRITE, DESIGN* and *EXPIRATIONDATE* (note the sequence of the headings). Each additional row in the file will contain the definition of the permission for one respective user:

- The *USERID* column contains the user IDs in the form of *domain\user* (SamAccountName).
- The *READ* column will contain an X if the user should have read permission. Otherwise, the column must be empty.
- The *WRITE* column will contain an X if the user should have write permission. Otherwise, the column must be empty.

- The *DESIGN* column will contain an X if the user should have design permission (only for SharePoint Sites). Otherwise, the column must be empty.
- The *EXPIRATIONDATE* column will contain an optional expiration date. If the permission should not expire, the column must be empty.

8.4.4.3 Tab "Settings"



This tab delivers features to define several settings for the selected resource. Depending on the resource type not all options may be available.

8.4.4.3.1 Visibility in Management Portal for Applicants:

The following options define the visibility of managed resources for requestors in the resource tree view:

Visible in Self Service shows the resource. A Requestor can submit any application.

Visible in Self Service, Requests not enabled also shows the resource but displays it as unmanaged, so users cannot file a request. This option is not available for 3rd Party Elements.

Not visible in Self Service fully hides the resource from users. This also applies to resources having managed child resources.

It is important to know that the visibility and the access options for the resource will not have any effect on the actual resource in the file system / site.

8.4.4.3.2 Inheritance of Permissions

The *Inherit Permissions* checkbox (only available for Rights Folders) determines if the user permissions of the parent rights folder will be inherited by the selected rights folder. This is a true inheritance regarding the NTFS permissions. The permissions will not be *copied* from above. The checkbox will be disabled if the current folder is the uppermost folder in the folder hierarchy. If the folder is a free folder (not a Rights Folder), inheritance cannot be disabled, because such folders always inherit their permissions from the parent folder.

8.4.4.3.3 Maximum validity period for Permissions

Maximum validity period for Permissions: If a user applies for a permission with an expiration date exceeding the maximum duration, it will automatically be shortened[5]. However, the *Responsible* may grant an even shorter duration when processing the request.

3rd-Party items allow for automatically granted access (public item). This function does also respect this setting and reduces the permission duration to the maximum validity period.

8.4.4.3.4 AD Groups used

AD Groups / *SharePoint Groups*: Displays the corresponding permission groups that have been assigned to the selected resource. Ultimately, this is only informational. AM will manage these group assignments itself – they cannot be changed manually.

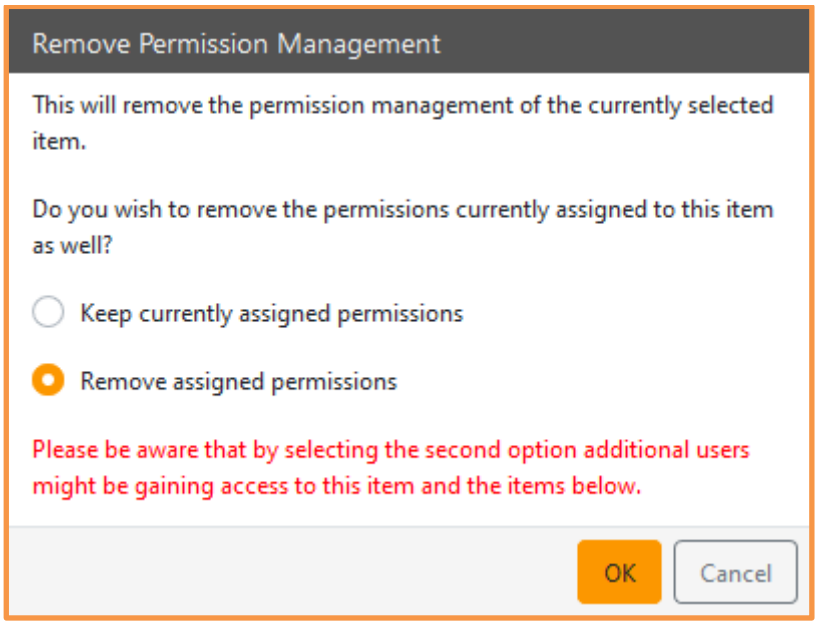
[5] The expiration date is then three months from the current date, for example.

8.4.4.3.5 Revoking Permission Management Status (Rights Folders & Sites)

The button *Remove Permission Management* is used to convert a managed resource into a free, unmanaged one. When doing this, the Administrator must make a decision regarding the permissions:

The user permissions set for this resource can either be removed completely or can be kept. If the current AM permissions are retained, the same people will continue to have access to the site. If the permissions are removed, the behavior differs slightly depending on the resource type:

In case of folders, inheritance is reactivated by AM and users permitted on the parent Rights Folder will get the same access permissions. SharePoint Sites, on the other hand, will remain accessible only to the users who were additionally permitted with SharePoint itself – all users permitted by AM will lose access.



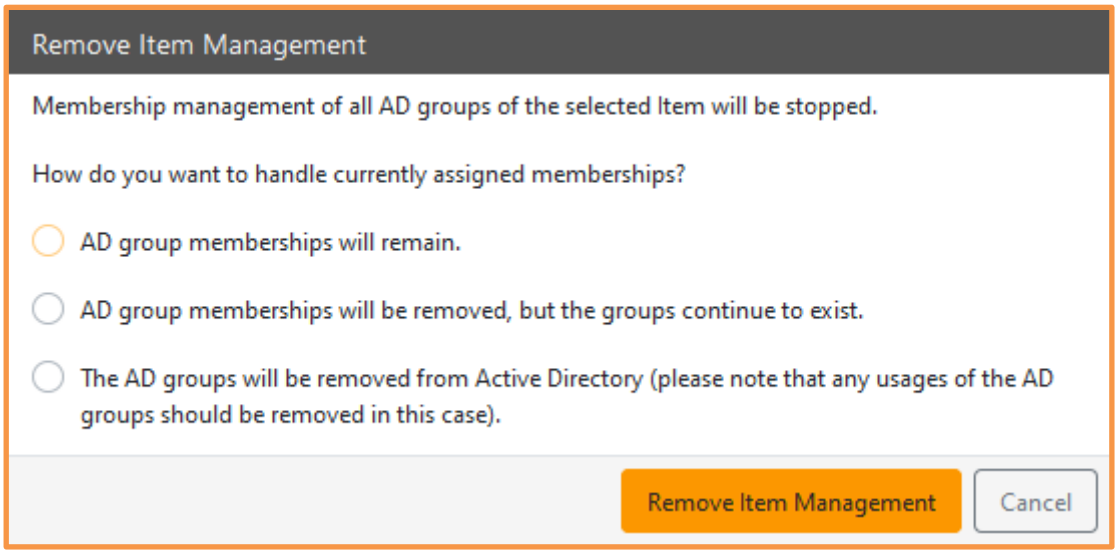
Warning! Important notice: Entry point of folder collection as managed folder

The combination of a folder collection entry point, technically being a Window Share, and defining it a managed folder, may lead to problems when the Permission Management Status shall be removed. The deletion of the technical permission groups and then switching on inheritance of parent permissions can make the share folder (and all its unmanaged child folders) inaccessible for every user account. MS Windows is not capable of correctly setting inheritance on a share, thus previous permissions are removed but inheritable permissions are not published. This can only be corrected locally on the file server with full access permission.

8.4.4.3.6 Revoking Permission Management Status (3rd Party Items)

The button *Remove Item Management* does not only remove the user permissions but also the Item itself. When doing this, the Administrator must make a decision regarding the affected AD groups:

The AD group is kept untouched, meaning that all currently assigned users will stay as members of this group. Alternatively, the group can be cleaned from all members but will kept in AD. This is the easiest way to remove an Item and its permissions but also keep full integrity of your infrastructure. If you are sure that the AD group is not used anywhere else in your company, you can select the 3rd option to also delete that group and have your system as clean as possible.



8.4.4.3.7 Execution of PowerShell Scripts (3rd Party Elements)

AM-Administrators have the option to bind PowerShell Scripts to *Items* and *Item Collections* that will be executed automatically when specific actions are performed like adding new items to an item collection or adding new members to an item. Please also note the PowerShell Script technical support guidelines in chapter 13.2.

Scripts for Item Collections:

Select an item collection and go to tab *Settings*. Scripts can be entered for different events:

1. A new item is added to the collection
2. An item is removed from the collection
3. A new member is added to an item of the collection
4. A member is removed from an item of the collection

Scripts that are stored for events 3 and 4 are effective for all items of this collection and automatically replace any script that may have been directly set on any item. AM provides different variables to be queried for the scripts, e.g. the name of the respective item and the underlying AD group.

Scripts for Item Permissions:

Select an item and go to tab *Settings*. Scripts can be entered *per permission* for these events:

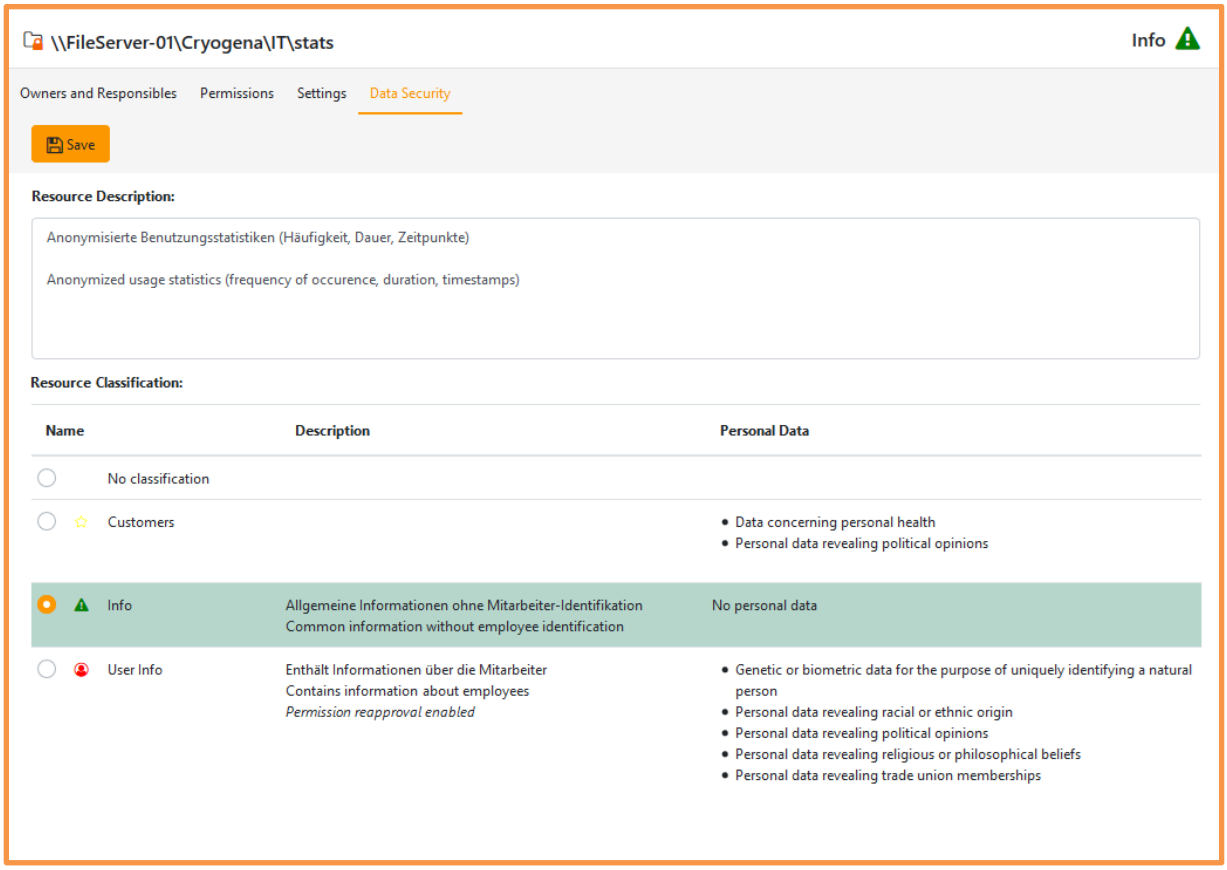
1. A new member is added to an item
2. A member is removed from an item

Scripts for items can only be entered if no scripts have been stored for the same event at their respective item collection. AM provides various variables to be queried.

A reserved variable *$custom* (type: string) is also provided for each element, which you can assign any individual value to. You can also query this variable in your scripts and thus create an individual treatment for each element.

Since AM version 2023.1 following variables are marked as deprecated and should not be used any longer:
- adGroupName (string)
- adGroupNames (string[])
- userName (string)

8.4.4.4 Tab "Data Security"

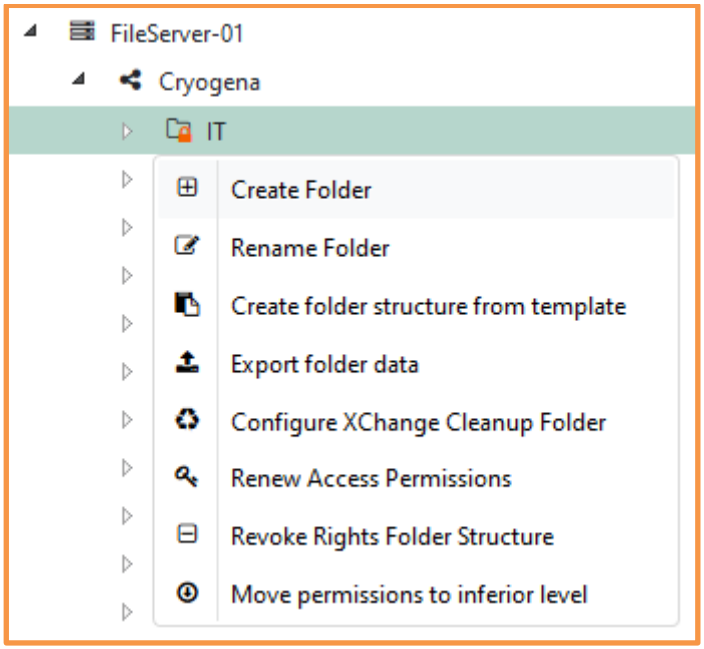


This page is only available for managed resources. A *Resource Description* may or must be entered. This depends on an administrative setting done by the *AM Administrator*. Further, as an Owner you can assign a given classification to the resource or switch to another one. Removing a classification from a resource is accomplished by selecting the option *No classification*.

Assigned EU-GPDR categories of each classification can only be set by a *Classification Administrator*.

Assigned classifications are not visible to normal users (applicants). The Responsible of a classified resource can tell the classification from the icon displayed on new permission applications. It is also displayed in resource details pane of a selected resource.

8.4.5 Resource Tree Context Menu



Right-clicking on a resource in the tree view will open the context menu. Various actions, which will be explained in the following sections, are available. The actions depend on the type of the selected node.

8.4.5.1 Create Site

Selecting the *Create Site* option will open a dialog where the desired name and SharePoint template for the new site can be entered. Which SharePoint templates for site creation are displayed depends on the "Page Layout and Site Template Settings" in SharePoint. For the new site name, validation rules apply as defined by the *AM Administrator*. The new site will be created under the site selected in the tree view and is selected automatically. Initially, the new site will not be a *Managed Site* because it has not yet been assigned a *Responsible*. The *Owner* will be taken from the site above the new site.

8.4.5.2 Rename Site

The selected site can be renamed using this action. All settings will be retained with only the name and URL of the site changed. For the new site name, validation rules apply as defined by the *AM Administrator*.

8.4.5.3 Rename Item

This option will rename an item. All other settings will be kept and only the name is altered if it does not yet exist in the containing item collection.

8.4.5.4 Create Folder

Clicking *Create Folder* opens a dialog window for entering the desired name of the new folder. For the new folder name, validation rules apply as defined by the *AM Administrator*. The new folder will be created below the selected folder and is automatically selected. Initially this folder is not a managed folder because no *Responsible* is defined yet. The *Owner* is taken over from the parent folder.

8.4.5.5 Create Folder Structure from Template

When choosing this menu item, you can select a folder structure template from a dialog window. Please click the button *Apply template* to let AM create the complete folder structure in the Folder Collection. Available Folder Templates are maintained in section *Folder Creation Templates*.

8.4.5.6 Rename Folder

The selected folder can be renamed using this action. All settings will be retained with only the name of the folder changed. For the new folder name, validation rules apply as defined by the *AM Administrator*.

8.4.5.7 Export Folder Data

This action will export the current user permissions of the selected Rights Folder and all its child Rights Folders into an Excel file. It can be imported back as a Folder Collection Import at any time by an *AM-Administrator* (see chapter 8.2.1.4.4).

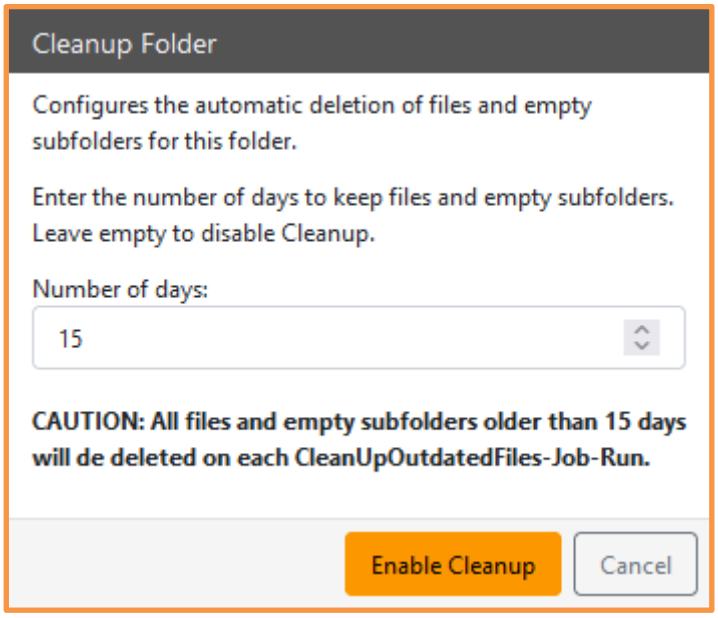
8.4.5.8 Revoke Rights Folder Structure

This action will remove all Rights Folder definitions of the selected folder **and all its child** rights folders. Afterwards, the folders will be treated as a common *Free Folders* and are not managed by AM anymore. Same rules apply as for single Rights Folder definition removal (chapter 8.4.4.3.5).

8.4.5.9 Renew Access Permissions

Selecting this option will start a job immediately in background and the user permissions and roles will be validated and updated in the AM database and in the SharePoint Site / AD & File Servers as needed.

8.4.5.10 Configure Cleanup Folder



The function *Cleanup* enables management of folders whose contents should be deleted automatically as soon as they have not been used for a certain period of time. These folders are called *Cleanup Folders*.

In the dialog window, enter the desired number of days where files have not been accessed. After confirmation, a new icon is added to the end of the folder name and all files are deleted once they reach the specified age. The same applies to empty folders and ones that contains only files being too old. To remove the cleanup status, empty the input field and save. The folder is not monitored any longer and files will not be deleted.

Please note that the job *CleanUpOutdatedFiles* must be scheduled for this feature to work.

8.5 Creating 3rd Party Items

Within one of your administered item collections you can create new items which will use their defined permission set and logic (see chapter 8.2.3.2).

Select the desired Item Collection first and navigate to Tab *Create Item*. Enter the desired name of the new item and, optionally, a descriptive text. The name must not be used yet within the current item collection. Furthermore, the item needs to be bound to an AD group. There are two options for this:

8.5.1 Use existing AD group

Enter the name of the desired AD group (autocomplete function is available here). The group must not yet be used by any other permission or item, even not by items in other item collections as this would lead to membership intersections and inconsistencies. Now choose the user accounts which shall stay as members of this group (only these will be permitted for this item); all other members will be removed by AM.

For correct functionality, make sure Access Manager has write access permission on this AD group.

***Never** use the same AD group twice,*
as this will lead to concurrent and contradicting permission management results.

8.5.2 Create new AD group

Enter the name of the AD group (without domain name) to be created. AM will warn you in case such a group already exists. Also specify group scope and type. The group will be created in the OU for the containing item collection defined by the *AM Administrator*. The OU / storage location cannot be altered.

8.5.3 Assign custom scripts

In this phase you cannot assign your own PowerShell scripts for events (grant / revoke permissions). This is not possible until the new item is fully created (see chapter 8.4.4.3.7).

8.6 Add SharePoint Site (Modern Experience)

Within a SharePoint Collection that you administrate, you can create new Sites or add existing ones that use the Collection's Permission Set and logic (see Chapter 8.2.4).

First select the desired SharePoint collection and there the *Create item* tab. You now have three options in the detail area (expandable areas):

- Create new Site
- Import existing Site
- Structure import

8.6.1 Create new Site

This option creates a new SharePoint Site in your Microsoft Entra Tenant. Provide the name of the site and a description if necessary. Although SharePoint allows multiple sites with the same name (internally, a unique ID is used for each), we do not recommend assigning two identical names since no difference is visible to the end user.

Now you have to choose the type of site. After clicking the *Create new Site* button, Access Manager creates a new site object in SharePoint for you. You are automatically assigned the roles of *Owner* and *Responsible* within Access Manager.

8.6.2 Import existing Site

With this function, existing sites, including permissions that have already been assigned, are transferred to Access Manager, and thus receive the status "private" (joining is only possible by request). If permissions available on the target site are not also managed by the SharePoint Collection used here, they are converted to the next lower right (e.g. *Owner* to *Member*) or removed if there is no lower right (e.g. *Visitor*).

Provide the name of the site to import and select it from the list of suggestions. Also specify whether users who already have the *Owner* role on the site should also have this role in Access Manager (then their corresponding AD account will get this AM role). If you say no, you yourself will automatically be given the roles of *Owner* and *Responsible* in the Access Manager. During the import, the current permissions of the users of the site are transferred to Access Manager.

8.6.3 Structure import

Similar to the structure import function for Folder Collections (Chapter 8.2.1.4.4), you can transfer existing sites, including permissions that have already been assigned, to the Access Manager and they are given the status "private" (joining is only possible by request). If rights available on the target sites are not also managed by the SharePoint collection used here, they are converted to the next lower right (e.g. *Owner* to *Member*) or removed if there is no lower right (e.g. *Visitor*).

Also specify whether users who already have the *Owner* role on the site should also have this role in Access Manager (then their corresponding AD account will get this AM role). If you say no, you yourself will automatically be given the roles of *Owner* and *Responsible* in the Access Manager. During the import, the current permissions of the users of the site are transferred to Access Manager.

You can first download a template file in Excel that contains the columns necessary for the import. Fill this out with the information you took from the CSV file that your Microsoft Entra administrator created for you as an export from the Microsoft Entra SharePoint administration. If you then load this Excel file into the Access Manager, it is first checked for syntactical and logical correctness and completeness (button: *Validate file*). If the validation does not find any errors, you can now actually load the data into the system with the *Start import* button.

8.7 Add MS Teams Team

Within a Teams Collection that you administrate, you can create new Teams or add existing ones that use the Collection's Permission Set and logic (see Chapter 8.2.5).

First select the desired Teams collection and there the *Create item* tab. You now have three options in the detail area (expandable areas):

- Create new Team
- Import existing Team
- Structure import

8.7.1 Create new Team

This option creates a new Team in your Microsoft Entra Tenant. Provide the name of the team and a description if necessary. Although Microsoft allows multiple teams with the same name (internally, a unique ID is used for each), we do not recommend assigning two identical names since no difference is visible to the end user.

After clicking the *Create new Team* button, Access Manager creates a new Team object in MS Teams for you. You are automatically assigned the roles of *Owner* and *Responsible* within Access Manager.

8.7.2 Import existing Team / Create Team from existing O 365 Group

With this function, existing Teams, including permissions that have already been assigned, are transferred to Access Manager and thus receive the status "private" (joining is only possible by request). If permissions available on the target Team are not also managed by the Teams Collection used here, they are converted to the next lower right (e.g. *Owner* to *Member*) or removed if there is no lower right (e.g. *Visitor*).

Another option is to specify an existing Office 365 (Microsoft Entra) group, which will be used as an identifier for a new team to be created. Ultimately, however, this makes no difference for you in terms of operation since the existing users are also taken over.

Enter the name of the group/team to be imported and select it from the suggestion list. You can tell from the preceding symbol whether it is a team or a group:

- : Team
- : O 365 Group

Provide the name of the group / Team to import and select it from the list of suggestions. Also specify whether users who already have the *Owner* role on the site should also have this role in Access Manager (then their corresponding AD account will get this AM role). If you say no, you yourself will automatically be given the roles of *Owner* and *Responsible* in the Access Manager. During the import, the current permissions of the users of the group / team are transferred to Access Manager.

8.7.3 Structure import

This Structure import for Teams is completely identical to the SharePoint Sites Import function (Chapter 8.6.3), even the Excel template file is the same.

9 Identity Management (IDM)

Menu:

Profiles & Organization → Requests
Profiles & Organization → Organization Chart

9.1 Approval Process

Personnel changes by personnel managers are normally not carried out automatically. Instead, an approval process is triggered that involves other personnel managers. After a dialog has been submitted, the associated workflow can be found in the workflow view with the status *Waiting for approval*.

The workflow remains until it is either approved or rejected, it will not be removed even if the recorded approvers all become unavailable. In this case, only administrators are still able to complete the approval process.

If you are entered as the person responsible in a corresponding position in the organization chart and are therefore assigned as the approver of a workflow, you will receive an E-Mail for new workflows that are waiting for your approval. After your decision, the applicant will receive an E-Mail about the new status of the workflow. If team leaders are configured as recipients of onboarding mails, they will receive a corresponding onboarding E-Mail for each successfully finished *Joining the Company* process. This E-Mail contains account data including the new employee's password and should therefore be handled with care.

To approve a workflow in your assigned organigram sector, first navigate to Personnel Changes under *Requests* in *Profiles & Organization* in your Access Manager interface. Here you will find a list of all your workflows.

Press the OK icon of the workflow you want to approve or reject to open the associated dialog. Here you can now check the applicant's entries and – especially in the event of a rejection – enter a reason. Press *Reject* to reject the request, after which the requestor will be informed, and no changes will be made to the system. A rejected workflow cannot be reopened, resubmitted, or subsequently accepted. If you press *Accept* instead, the applicant will also be informed, but the process will be scheduled and executed immediately. Regardless of your decision, you will be directed back to the overview of your approvals.

As an administrator, you have your own view of the approval workflows for personnel changes under *Requests* in the administrator area. Here you can view all approval processes, regardless of whether and where you are assigned as the responsible person in the organigram. You can accept or reject the active approval processes using the OK icon next to the relevant workflow. Note that even with the corresponding extension of the status filter, only approval workflows are displayed here. Administrator workflows that do not have to go through an approval process are only listed under *Logging*. The

approval workflows are also available there for you to view, but you can only approve or reject them here in the *Requests* area.

9.2 The Organigram

The organizational chart or organigram of the IDM module is used to model your company structure. Identities are assigned in two tree structures – for example department and location. This organigram position determines which configurations apply to this identity and who is responsible for approving workflows with this identity. The second tree is optional and separate from the first. Even with a second tree, identities do not have to have an assignment in it. Only an assignment in the first tree is mandatory.

The configurations, as described in the introduction to the *Moving within the Company* dialog, are done through an assignment in the Organigram. The configurations themselves are already assigned to the organizational chart by your superordinate AM administrators. Depending on the assignment of an identity within the organigram, the most suitable configurations are selected and used for the identity. The following fields can then automatically be adapted if they are assigned in the organigram:

- Home and Profile Folder
- Organizational Unit(OU) in the Active Directory
- Postal Address
- UserPrincipalName (especially the suffix)
- The Exchange Server used
- Access Manager Profile memberships

Note that data is not always simply migrated. The old home and profile directories remain in a renamed, rights deprived form, their content is neither deleted nor copied. The UPN and, if applicable, the SMTP address are also checked for uniqueness in the event of a change. If an address is already assigned, the identity receives a new value with a counter appended in the prefix. A new OU leads to a relocation of the Active Directory object. Access Manager profile memberships that were assigned to the identity because of their old position in the organigram are removed and new profiles added from the new position.

Please note that although you can use the IDM module to manage identities in different domains, it is not possible to switch between domains.
This rule applies regardless of the established trust factor between the domains.

The relevant configurations are determined by analyzing the tree structures from bottom to top. If a configuration has the exact same assignment as the identity, it will be chosen. Otherwise, a matching assignment is searched in the second tree structure for the selected node of the first tree structure. If no suitable configuration is assigned up to the root of the second tree, an assignment to only the node

in the first tree is searched for. If there is no assignment for this either, then the parent node of the assignment in the first tree is selected next. The search is now repeated with this new assignment until both trees have been searched to the root:

1. Check exact assignment
2. Check secondary tree towards its root
3. Check assignment without its secondary node
4. Start again at 1 with the first node's mother node

If there is no second tree, only 3. and 4. are alternated until a configuration is found.

9.2.1 The Organigram and its assignments

Menu:
Profiles & Organization → Organization Chart → Organization Structure → Settings
Profiles & Organization → Organization Chart → Resource Assignment

The organigram represents a projection of your organizational structure within the IDM module. It consists of two tree structures, the primary and the secondary organizational structure. Only the primary structure is necessary, the complexity of your organigram will depend on your needs. If all of your identities are to be created and handled identically, the root node of the primary structure would be sufficient. To modify the organigram or its assignments you need the system role *Organigram Administrator*.

Since "primary organizational structure" is a rather complex term in the long run, and is also not practicable for the end users, you can determine it yourself. To do this, navigate to the organizational structure and then to *Settings*. You can now specify the official designations of the two structure trees in the two lower fields. We can recommend a division into *business units* and *locations*.

Now it is time to fill your freshly named trees. Open the dialogs by selecting the corresponding tab with the name you have just chosen above *Settings*. Here you can now create and expand your structure node by node. Note that only one secondary tree is recommended, so you should not create more than one root node per tree.

Before the next step, check your organizational chart for completeness and correctness. Once resources and identities are assigned to your organigram, further modifications are associated with considerable effort. This does not apply to renaming and extensions: New nodes can be added at any time without any further effort.

Next you can assign the configurations previously made in the organization chart. To do this, navigate to the *Resource Assignment*. Under *+ New resource assignment*, select one of the relevant sub-items. The dialog that then opens is largely identical. In the first field, select the configuration you created and in the other two fields select the nodes in the organizational structure for which the configuration should apply. The assignment then applies to the selected nodes and all those below them, until a

more precise assignment if any replaces them. To prevent mistakes when handling, we always recommend an assignment in the root node of the primary organizational structure.

At this point, it is also possible to assign Access Manager profiles. The profiles assigned here must first be defined in the Access Manager and future new identities will automatically be assigned to the corresponding profiles when they receive their organigram assignment. However, profile assignments are not required for the correct functionality of the IDM module.

Now the identity dialogs of the IDM module are functional. For the moment, however, this only applies to the administrator dialogs. Approval processes are triggered for requests via self-service, which requires that there are approvers. Navigate to the *Employees* menu item in the *Identities* tab in the *Administrator* area to start creating new identities. If future managers already have AD accounts, you can skip this step. However, an identity not created in the IDM module is also not managed by the IDM. Although the account can be assigned as an approver in the organigram, it does not itself have an assignment in the organigram. It therefore does not benefit from any of the configurations made in the IDM module.

The next step is to assign these identities or accounts as (team) Responsibles. Return to Resource Assignment and select Team Owner. Here you can now select identities or accounts and assign them in the organizational chart. Note that this only involves an assignment of responsibility and does not affect the actual org chart assignment. An identity in the exemplary sub-node *Human Resources* remains there, including all configurations there, even if it is assigned here as the responsible person in the root node above. Accounts without an IDM identity can then also carry out their work as responsible persons, but none of the configurations in the organizational chart apply to them.

Note that while the search for identities and accounts uses the same field, they work slightly differently. Identities are found by search term by first name, last name, or SamAccountName; accounts by last name and account name (including domain). You can differentiate the results by their color coding: Accounts from the AD are orange, synchronized identities are green and identities that have not yet been imported into the AM are cyan.

Finally, it is still necessary to authorize all users and organigram administrators of the IDM module as such in the system roles. Administrators use the same role as in the Access Manager. They have access to all dialogs mentioned in this chapter. The *Human Resources (HR)* role must be distributed to everyone who should be able to work with the identity dialogs. This also includes all team responsibles, since they are supposed to approve these dialogues. The *Organigram Administrator* role must be distributed to everyone who should be able to edit the Organization Chart and its assignments. The configurations to be assigned can only be created and edited by administrators.

The IDM module is now fully configured and ready for productive operation. If you haven't already, try creating an identity. If there are problems with the installation, the configuration or the infrastructure, the process will show errors in the *Staff Changes History* under *Logging*.

9.2.2 Adjustments to the Configuration

If you want to adjust the IDM configuration during operation, there are a few things to consider.

The administrative data usually cannot be modified or deleted if they are assigned in the organizational chart. Furthermore, an OU cannot be modified if there are identities assigned to it, but a postal address can. However, if the latter is changed, identities with existing addresses are **not** updated. They keep their old information until it is touched by an identity process.

Organigram nodes are also subject to these guidelines: The position of a node in the organization chart cannot be changed, only the naming. If it contains identities or has a daughter node, it cannot be deleted. To still see them in the selection of the dialog, you can deselect the checkbox "Hide invalid records and records assigned in the organigram".

9.3 Workflow Views

In addition to the view of your own workflows, there is also one for the approvers. To see this, navigate to *Profiles & Organization*. There you will find the workflow view mentioned under *Requests*. Here you can see all workflows for which you have been identified as an approver. For this reason, only workflows that are waiting for approval are displayed by default. However, you can also see past workflows after they have been approved by expanding the filter selection of the status column accordingly.

For administrators there is a similar view called *Staff Changes History* in the *Logging* tab. All workflows are displayed here, regardless of the applicant, only workflows in the approval process are filtered out by default.

There is again a separate view of the approval workflows for administrators under the *Requests* tab in the administrator area. All workflows that are in the approval process are also displayed here, regardless of whether you are entered as an approver.

10 Fileserver Accounting

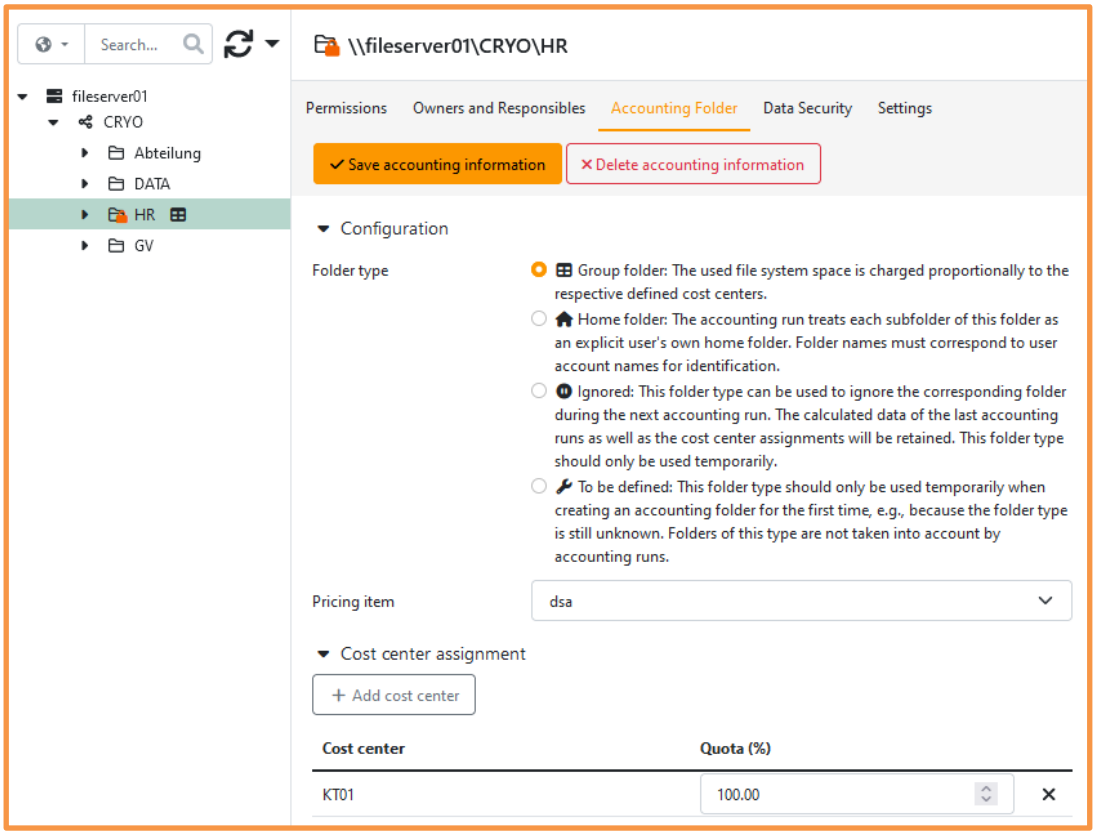
10.1 Operation Principle: Cost Center-based collection of used Storage space

The optional *Fileserver Accounting* module provides features for the determination and depiction of cost information at the directory level. Access Manager uses two types of accounting through which folders can be defined as accounting folders: *Group* and *Home*. A *cost unit* determines the estimated costs per gigabytes of storage space used (unit price).

An accounting folder that has been defined as a *Group* will be invoiced by its size and the resulting costs will be proportionally distributed to one or more cost centers.

With an accounting folder with the *Home* definition, each sub-folder will be treated as a so-called “home directory” for a specific user, in which case the costs determined will be invoiced to the respectively defined user.

10.2 Defining Accounting Folders



Define a selected folder as an accounting folder. It is defined by the type of folder and an assigned cost center, which specifies the pricing for a gigabyte of used storage space. Additionally, assign one or more cost centers to that the calculated costs are billed.

10.2.1 Types of Folders

There are four types of folders that can be defined for an accounting folder:

Type of Folder	Description
Home	This folder is defined as a Home directory. The accounting process treats each sub-folder in this folder as an individual home directory for an explicit user. These folders are identified by the folder names, which must correspond to the user account.
Group	This folder is defined as a Group directory. The storage space used will be invoiced proportionally to the respectively determined cost center.
Ignore	This type of folder can be used to ignore the corresponding directory for the next accounting process. The data determined, such as for assignment to a cost center, will be retained from the last accounting process. This type of folder should only be used temporarily.
To Be Defined	This type of folder should only be used temporarily for the creation of an accounting folder, because the type of folder is not yet known for example. Directories with this folder type will not be considered for accounting.

10.2.2 Manual entering of Accounting Data

Detailed information about the selected accounting folder will be displayed in the right pane. Adjustments can also be made to the accounting values.

Cost centers to which the used storage space can be invoiced must be setup for a *Group folder*. The type of folder can be saved only if the corresponding cost distribution key (quota) has been totally assigned to the responsible cost centers. Cost centers and their quotas can be added as an administrator to the accounting folder using the *Assigned Cost Centers* section. The cost centers available will be managed from the *Cost Centers* page (see chapter 13.8.5.6).

Once the changes to the accounting folder settings have been saved (using the *Save* button on the status bar at the bottom of the window), the *Accounting Scan* job should be scheduled in a timely manner in order to assure the determination of the correct data for the accounting (see chapter 11.6.8.2).

To set a Folder as an Accounting Folder, select it in the tree view and enter values in the given fields:

Folder Type: Select the type from the DropDown List.
Pricing Item: Select the pricing item from the DropDown List.
Assigned Cost Centers: If Folder Type *Group* was selected, enter the concerned Cost Centers and their proportional payment amount.

10.2.3 Accounting Details

A specific accounting process can be selected in the *Accounting Detail* section of the lower pane. Since several accounting processes may have occurred at the same day, including various agent groups, you need to select Year, Month and the combination of Date, Time, and Agent Group separately. Once these have been selected, a summary of the selected process will be displayed below the selection controls.

The *Existing Conflicts* section at the bottom of the page will list problems determined during account processing. If errors, such as *No Cost Center Assignment Available*, arise or a Share was not available, the check can be repeated using the *Rescan* button. As long as conflicts exist, the data to be exported will not reflect the actual accounting situation.

10.2.4 Importing Data

The contents of previously exported or manually created Excel files can be imported using the context menu of a Folder Collection. Please note that all cost centers, pricing items etc. already need to be already stored in the AM system.

A pre-formatted Excel template, which will include all the required data columns for creating independent content, can be downloaded also from the *Import* dialog. Once an existing file has been selected and uploaded, it must be validated, and a success message is displayed. The *Start import* button is activated if there are no errors.

An import file will replace all data for accounting folders for the selected share. Existing data will be deleted entirely during the import process and re-created if the data exists in the import file.

10.2.5 Exporting Data

The data of all Accounting Folders of a Folder Collection can be exported via the context menu. You can manually alter the Excel file and import it back as needed. Exporting data of a single Accounting Folder is also possible.

10.2.6 Structure of the Excel File

The import file must be an Excel file (an XLSX file created using Office 2007 or later) that includes all the columns in a precise sequence and whose contents match the requirements for successful import. This will be assured by exporting the existing data for an accounting folder.

The name of the worksheet must be "AccountData" for successful detection during import process.

Column A: **FOLDER**	Mandatory: **Yes**
Format	**Description**
\\Server\Share\Directory	The SMB path specification for the accounting folder to be imported consists of the name of the server, the share and the directory.

Column B: **COSTCENTER1**	Mandatory: **see description**
Format	**Description**
Text	The name of the first cost center. Required if the type folder is *Group* (see Column V, TYPE_NAME).

Column C: **PERCENTAGE1**	Mandatory: **see description**
Format	**Description**
A whole number between 1 and 100	The quota for the COSTCENTER 1 column. The total of the quotas for all cost centers used must equal 100 precisely. Required when COSTCENTER1 has been specified.

Columns D-U: **COSTCENTER2-10 & PERCENTAGE2-10**	Mandatory: **No**
Format	**Description**
As per COSTCENTER1 / PERCENTAGE1	As per COSTCENTER1/PERCENTAGE1 The columns are optional, however PERCENTAGEx must always be specified in combination with a COSTCENTERx.

Column V: **TYPE_NAME**	Mandatory: **Yes**
Format	**Description**
One of the following words: Home, Group, Ignore, ToBeDefined	The type designation for the accounting folder. Be sure to use the correct upper / lower case!

Column W: **PRICING ITEM ID**	Mandatory: **No**
Format	**Description**
Text	The ID of the pricing item for the accounting folder. The column is only valid when the folder type is HOME, GROUP or IGNORE. If the ID has not been set, the default value for the pricing item will be used (set from the Administration Module, see the corresponding manual).

10.2.7 Possible Validation Errors

In case file validation fails, the error log lists all errors occurred containing row number, type of error and the erroneous data. You cannot import the file until the errors are fixed within in the file. Following errors are discovered:

Error Type	**InvalidServerOrShare**
Description	The server and share selected for importing the data does not correspond to the server and share indicated in the import file.
Correction	Make sure that the complete UNC path in the import file corresponds to the proper server and share.

Error Type	**InvalidFolder**
Description	The folder specified in the import file does not yet exist in the file system.
Correction	Create the directory from the *Folder Management* module and import the file again.

Error Type	**NestedAccountingFolders**
Description	Nested accounting folders were detected. For example: \\Server\Share\c\d, where directories c and d are both accounting folders.
Correction	To avoid multiple invoicing, accounting folders is not possible in the AM system.

Error Type	**InvalidCostCenterPercentageFormat**
Description	An incorrect decimal format was found in a percentage column.
Correction	Correct the entry to use a correct decimal number.

Error Type	**InvalidCostCenterPercentageSum**
Description	The total of all specified percentages is not 100.
Correction	Correct the individual percentages so that they total 100.

Error Type	**SameCostCenterSingleFolder**
Description	The same cost center has been specified multiple times on the same row for an accounting folder.
Correction	Only specify different cost centers for one accounting folder.

Error Type	**CostCenterMissing**
Description	A percentage was specified, but the associated cost center was not.
Correction	For each percentage specified, define an associated cost center.

Error Type	**CostCenterUnknown**
Description	The specified cost center is unknown.
Correction	Create the cost center from the *Cost Center* window and import the file again.

Error Type	**InvalidCostCenterPercentageValue**
Description	The percentage value of a cost center is outside the valid range.
Correction	Correct the percentage for the associated cost center.

Error Type	**InvalidPricingItemId**
Description	An unknown ID was specified for the pricing item.
Correction	Concerning the pricing item, use a truly existing pricing item ID from the *Pricing Items Window*.

Error Type	**InvalidPricingItemTypeNameCombination**
Description	The combination of the defined pricing item and type of accounting folder is not valid.
Correction	Pricing items can only be associated with the HOME, GROUP and IGNORE folder types.

Error Type	**InvalidOrMissingTypeName**
Description	Either the type of the accounting folder is unknown, or a type was not assigned.
Correction	Specify one of the following types of accounting folder: HOME, GROUP, IGNORE, TOBEDEFINED.

Error Type	**InvalidCostCenterTypeNameCombination**
Description	The combination of the defined cost center and type of accounting folder is not valid.
Correction	Cost centers can only be assigned for the GROUP and IGNORE types of accounting folders.

Error Type	**DuplicateFolder**
Description	The same name was assigned multiple times to the accounting folder.
Correction	The names of accounting folders must be unique.

10.3 Accounting Reports

Menu:

Reports → Fileserver Accounting

This page enables the generation of various reports with a variety of topical statements. General reports and those that are based on a concrete accounting process are differentiated. Since several accounting processes may have occurred each day, including various agent groups, you need to select Year, Month and the combination of Date, Time and Agent Group separately. Once they have been selected, the buttons for the creation of process-dependent reports will become active.

Using the respective buttons will open a new tab in the browser and the report will display. The report can be downloaded in various formats using the *Export* button. The following section will explain the available reports.

10.3.1 Cost Center Report

This report will list all cost centers that have been used and display the accounting folders used with them at which cost percentages.

10.3.2 Folder Report

This report will list all accounting directories and display the cost centers used with them at their proportional costs.

10.3.3 Conflicts Report

This report displays the problems that arose during an accounting process. This involves the same data that is displayed on the *Data* window in the *Existing Conflicts* section.

10.3.4 Overall Accounting Summary Report

This report displays a historical list of the payment data (storage consumed and invoiced and nominal & calculated prices) grouped by year and month.

10.3.5 Folders without Accounting Report

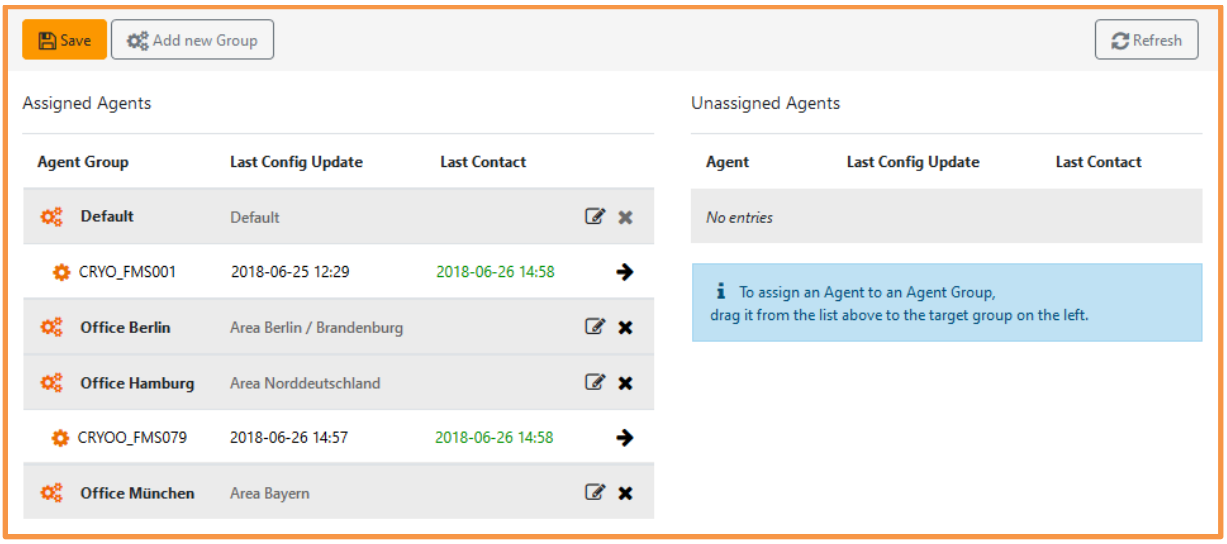
This report will list all rights folders that have not also been defined as accounting folders and therefore do not have the *Home* or *Group* folder types.

11 Job Scheduling

11.1 Operation Principle: Job Execution by Agents

All tasks that need to be executed outside of the Access Manager application itself (e.g. accessing AD, File Server, SharePoint Sites, 3rd Party Elements) are performed by so-called *Agents* that are installed on at least one other computer. Multiple Agents are combined in *Agent Groups* and do autonomously distribute several subtasks among their members for better performance. Jobs are distinguished in terms of types, i.e. for synchronizing AD with the AM database or maintaining access rights on the file system. Usually, jobs are planned for continuous repetition by the AM Administrator to guarantee a flawless operation.

11.2 Agent Groups



This page allows for maintaining AM agents and agent groups. A group may contain numerous agents but each agent can only be a member of one group at a time. Agent groups specified here will be assigned to the managed folder collection (see chapter 8.2.1.3). By this assignment AM will control the proper agents for each file server.

Agent group *Default* does always exist and must contain at least one agent. Only agents in this specific group will handle AD jobs (i.e. AdUserImport) and should therefore be installed on a machine with a fast network connection to the Active Directory server. Usually, additional agents are installed at remote resources to benefit from fast connections to file servers located at the respective site.

The page is divided into two areas. The left side lists existing groups with their assigned agents, the right table shows the installed but currently unused agents. The agent name displayed corresponds to the name given to an agent at the time of installation; it usually follows the naming schema

<DOMAIN>_<SERVERNAME> which helps the administrator to tell the installation location of the agent.

Each agent group has a unique name and an optional description. While the name cannot be altered once set, the description is editable via icon *Edit*.

Below every agent group record, the assigned agents are listed, displaying agent name, timestamp of last configuration change and last contact between agent and AM control server. Deleting an agent group (icon *Delete Group* ✖) is only possible if it does not include any agent and is not assigned to a file server. Group *Default* cannot be deleted anyway.

Creating a new agent group using button *Add new Group*, a new record is added at the bottom of the list where name and description is to be entered.

To remove an agent from a group, click the icon *Unassign Agent* ➔. The agent is displayed at the right table of unassigned agents.

Unassigned agents are assigned to a specific group by simply dragging them to the left and dropped onto the desired group record.

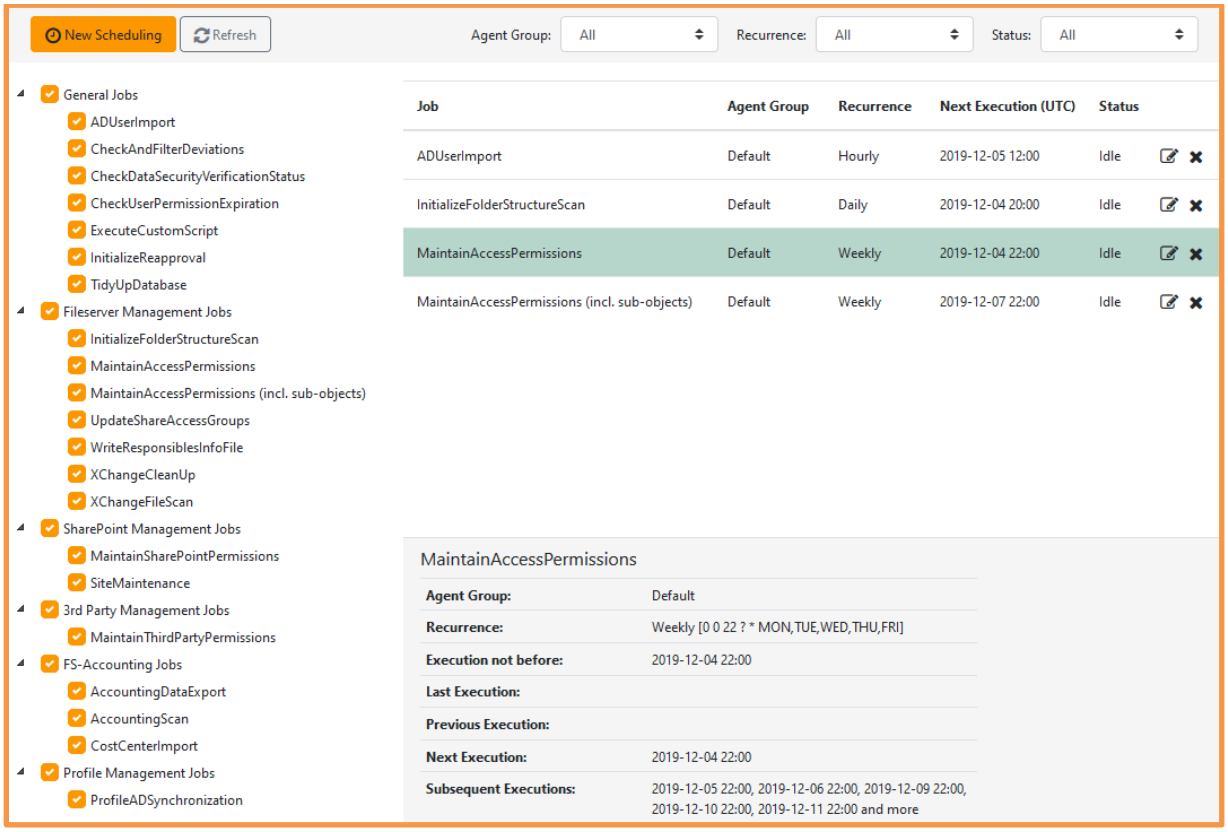
Unassigned agents can be removed using the icon ✖. The purpose of this function is solely to delete agents from the AM database that are no longer installed. Agents that are still installed but removed by using this function will reconnect to AM and automatically be listed as free agents again.

All changes are saved when the button *Save* is clicked.

11.3 Overview of planned jobs

Menu:

Administrator → Settings → Job Scheduling

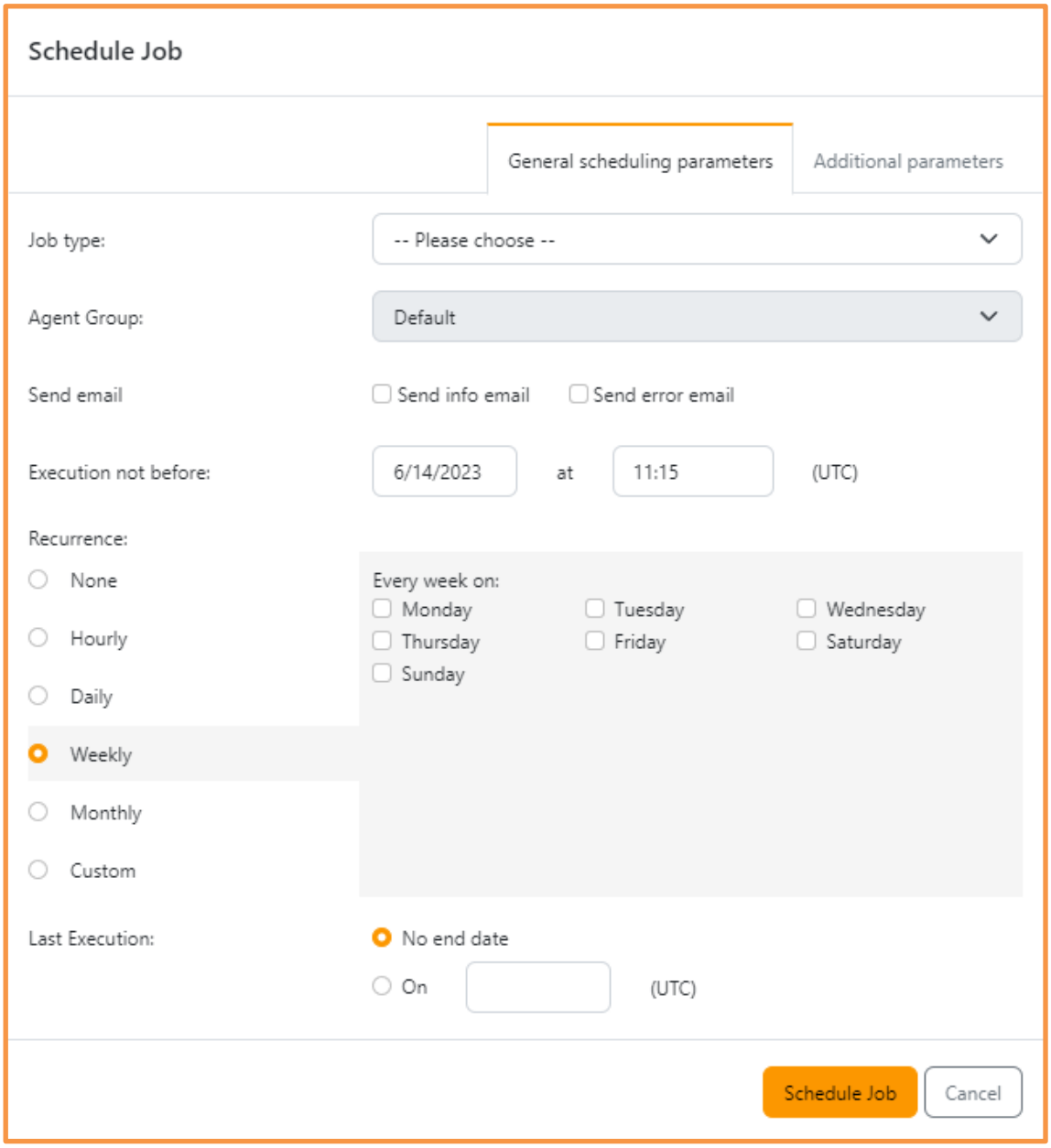


Job Scheduling represents periodically repeating jobs for an agent group. Depending on your role, available jobs (grouped by module) are displayed in the left view. For an organized view in the job list each job can be selected or deselected here. By default, all available jobs are selected.

The job list provides information about the scheduled jobs. This information can be filtered by agent group, recurrence and status. By selecting a job in the list, further details like recurrence interval, last execution, next execution etc. are displayed below the job list.

11.4 Scheduling jobs

A click on *New Scheduling* or a right click on a job in the job list (on the left) opens an overlay window where configurations can be set for a job. If a job is selected on the *Edit* button the input fields are already pre-filled with the configuration data of the currently selected job.



Job Type: Select the necessary job type.

Agent Group: In case multiple Agent Groups exist and the Job Type is compatible, you can select the desired Group here. This also has impact on the agents processing a specific (file) server. For multiple file servers with different agent groups, please create the job for each one with the correct agent group.

Send email: Select whether you and all other AM administrators would like to receive a corresponding email after completing the task (*Send info email*) and if the task was carried out incorrectly (*Send error email*). The default is derived from the default values set in the administrative settings (chapter 13.8.1.28).

Execution not before: By default, the current timestamp is pre-filled in UTC form (Universal Time Consolidated, not your local time zone). Alter the timestamp as desired, especially for repeating jobs.

Recurrence: Select the desired recurrence interval and enter necessary values.

Last Execution: You can optionally limit job execution until a specified date and time.

After all values are given, save the new job by Schedule Job button which will take it over to the job list and execute it as specified.

11.4.1 Custom recurrence

A recurrence is defined by using cron-expressions. In case the available recurrence intervals do not fit to your needs, you can enter your own cron-expression in the *Custom* section.

The structure consists of six parts separated by a blank character. Specifying the parts in the following order have this meaning:

A B C D E F

A: Seconds (unused, set to 0 always)
B: Minutes (0-59)
C: Hours (0-23)
D: Day of month (1-31)
E: Month (1-12)
F: command to execute (if not needed, set ? as wildcard)

Examples:

- Yearly recurrence on Feb the 1st at 9:05 am:
  0 5 9 1 2 ?
- Half-yearly on March the 15th & September the 15th at 9:05 am:
  0 5 9 15 3/6 ?
  → The part 3/6 (without any blanks!) means: starting at month 3 and repeat every 6 months
- Hourly execution from Monday to Friday between 7 am and 9 pm:
  0 0 7-21 ? * MON-FRI

11.5 Best Practice: Recommended recurrence intervals for Maintenance jobs

To accomplish a reliable functioning of the Access Manager system, you need to correctly specify a list of jobs that fit your company´s conditions. This chapter gives some general hints to plan most commonly needed jobs. You will need to adapt start times and intervals to your specific IT requirements (i.e. file server backup schedules or Update timeframes).

11.5.1 Mandatory Jobs

The following jobs are required in any case, dependent of your licensed modules. For a function description see chapter 11.6.

11.5.1.1 FetchMicrosoftEntraUsers

This task must run before the ADUserImport, as the latter builds on the results of this task. The shortest repetition interval should not be less than 30 minutes - not for technical reasons, but because Microsoft Entra may no longer allow the connection for security reasons.

11.5.1.2 ADUserImport

To rapidly reflect changes to AD user accounts and groups in AM, set a high recurrence rate for this job. Recommended values are 30 or 60 minutes. This has no negative impact as the job only needs a few minutes at maximum even for several thousands of records.

11.5.1.3 TidyUpDatabase

Schedule this job once a day. For a better load balancing, we recommend early morning hours.

11.5.1.4 (Fileserver Management) InitializeFolderStructureScan

Schedule this job once a day, preferably in the evening hours outside of main working times. The job uses Read Access on File Servers, thus it should run outside their maintenance times. If processing several hundreds of Rights Folders on one server, the job may need a considerable time (up to hours), therefore you should not plan it with short intervals.

*In any case, schedule this job **before** a MaintainAccessPermissions job.*

11.5.1.5 (Fileserver Management) MaintainAccessPermissions

Schedule this job once a day at working days (Mo-Fr), preferably in the evening hours outside of main working times. The job uses Read and Write Access on File Servers, thus it should run outside their maintenance times. If processing several hundreds of Rights Folders on one server, the job may need a considerable time (up to hours), therefore you should not plan it with short intervals.

*In any case, schedule this job **after** an InitializeFolderStructureScan job.*

11.5.1.6 (Fileserver Management) MaintainAccessPermissions (incl. sub-objects)

This job is functional identical to the previously mentioned one but processes much more file system objects (sub folders and files). Therefore, it should be scheduled complementary, i.e. once a week. As the time needed may take more than 24 hours (depending on you amount of objects and file server performance), we recommend to start the job on Friday evenings / Saturday mornings.

*In any case, schedule this job **after** an InitializeFolderStructureScan job.*

11.5.1.7 (SharePoint Management) SiteMaintenance

Schedule this job once a day, preferably in the evening hours outside of main working times. The job uses Read Access on SharePoint Servers, thus it should run outside their maintenance times.

*In any case, schedule this job **before** a MaintainSharePointPermissions job.*

11.5.1.8 (SharePoint Management) MaintainSharePointPermissions

Schedule this job once a day, preferably in the evening hours outside of main working times. The job uses Read and Write Access on SharePoint Servers, thus it should run outside their maintenance times.

*In any case, schedule this job **after** a SiteMaintenance job.*

11.5.1.9 (3rd Party Management) MaintainThirdPartyPermissions

It is sufficient to schedule this job once a day. As it accesses only the AD (Read and Write Access), execution times a usually quite short and you may schedule even shorter intervals if required.

11.5.1.10 (Fileserver Accounting) AccountingScan

Schedule this job once a day, preferably in the evening hours outside of main working times. The job uses Read Access on File Servers, thus it should run outside their maintenance times.

11.5.2 Recommended Jobs

The following jobs are not needed in any case but should be scheduled anyway. They are needed for some optional functionalities of the AM system. If such functions are not used, the jobs will be executed anyway but terminated immediately (as they have nothing to do) and do not stress the system.

11.5.2.1 CheckUserPermissionExpiration

Schedule this job once a day, preferably in the early morning hours. Users will then receive a mail with the correct number of days left right off.

11.5.2.2 ProfileADSynchronization

To rapidly reflect changes to AD user accounts and groups in AM, set a high recurrence rate for this job. Recommended values are 30 or 60 minutes.

This has no negative impact as the job only needs a few minutes at maximum even for several thousands of records.

11.5.2.3 (Fileserver Management) UpdateShareAccessGroups

To rapidly reflect changes to permitted user accounts and groups in the Share Access Group, set a high recurrence rate for this job. Recommended values are 30 or 60 minutes.

11.5.2.4 (Fileserver Management) CleanUpOutdatedFiles

Schedule this job once a day, preferably in the evening hours outside of main working times. The job uses Read and Write Access on file servers, thus it should run outside their maintenance times. Depending on the amount of file objects on one server, the job may need a considerable time (up to hours).

11.6 Available Job Types

Job Types are grouped by functional modules / competencies. Depending on your license, not all jobs may be available to you.

11.6.1 General Jobs

11.6.1.1 CheckDataSecurityVerificationStatus

This job sends information mails to classification administrators with classified addresses that do not have a checked and confirmed status. A mail contains the first 100 resources found which status have changed since the last check run.

11.6.1.2 CheckPermittedButUnauthorizedUsers

Evaluates if a user was permitted on a resource he is not authorized for, according to a classification. Two administrative options specify if administrators and / or responsibles shall be notified by email (see chapters 13.8.1.16 and 13.8.1.18).

11.6.1.3 CheckUnprocessedRequests

Checks all user requests, whether their creation date is at least X days ago and cancels such requests (configuration see chapter 13.8.1.7) or sends a reminder (configuration see chapter 13.8.1.46).

11.6.1.4 CheckUserPermissionExpiration

Notifies users by email whose access rights for a specific address will expire in a configured period.

11.6.1.5 DeleteOldAuditData

Deletes over-aged audit information from the database which must not be accessible any longer, i.e. because of data protection rules. To decide if a record is over-aged, administrative settings (see chapter 13.8.1.37ff) are considered.

11.6.1.6 ExecuteCustomScript

The job executes self-defined PowerShell Scripts that are chosen from the Script Management pool.

11.6.1.7 NotifyUserRoleChanges

If a user is given a resource-related role (Owner, Responsible, Profile Responsible, Substitute), they will be informed when this task is scheduled. All new roles accumulated until the next execution of this task are then sent in a single email – so an email is not sent immediately with every new assignment.

11.6.1.8 PerformReapproval

This task checks for all existing reapproval definitions (as part of the data protection classifications) whether they should be started (i.e. beginning of a reapproval cycle) or whether, for example, reminder emails should be sent within an ongoing cycle. It is advisable to plan the job daily.

11.6.1.9 SendDeviationMail

Sends email messages with lists of deviations between the configuration of the file system and AM settings with regards to the permissions for the AM Administrators, Owners, Responsibles and their substitutes. Only the deviations that have arisen since the last execution of the job will be taken into consideration.

11.6.1.10 TidyUpDatabase

Temporary permissions will be removed from the file system at their expiration date, but the information remains as database entries. This job maintains said entries for temporary permissions as well as for substitute roles. After expiration, these entries are kept in the AM database - also visible in the AM interface with expiration date - until they will be removed by the next job run. Additionally, after expiration of a substitute role, an information mail is triggered to inform the respective substitute.

Furthermore, the job deletes access permissions, roles, profile memberships etc. of user accounts not found in AD if the respective option is set (see chapter 13.8.1.7). It is therefore recommended to plan the job on a daily basis.

11.6.2 Active Directory Jobs

11.6.2.1 ImportGroupsAndGroupMembers

Imports AD user groups into the AM database and updates existing records.

11.6.2.2 ImportUsers

Imports AD user accounts into the AM database and updates existing records. Afterwards, automatically executes job ADGroupImport (see above) and CheckPermittedButUnauthorizedUsers (see below).

11.6.3 Microsoft Entra ID Jobs

11.6.3.1 FetchMicrosoftEntraUsers

Imports Microsoft Entra user accounts into the AM database and updates existing records.

11.6.4 Fileserver Management Jobs

11.6.4.1 CleanUpOutdatedFiles

Deletes outdated files / folders in the Cleanup folders based on the date of last access or the creation date, respectively. This distinction comes from the administrative setting *CleanUpOutdatedFilesUseCreationTime*.

11.6.4.2 InitializeDesktopClassificationIcons

In every classified folder, an icon file is created (on the file server) and the hidden file “desktop.ini” is modified to make client machines display this icon in the Windows Explorer. If a folder is not classified any more, the icon is deleted. If another classification is selected for a folder or the icon of a classification changes, the icon is also changed on the file system. See also chapter 0.

Please note: Because of various caching mechanisms of Windows, it may happen that after changing the icon in Access Manager, Windows still displays the old icon.

11.6.4.3 InitializeFolderStructureScan

Synchronizes the folder structure in the AM database with that of the file system. Multiple child jobs are automatically scheduled to check parallel folder structures simultaneously. Also, these jobs are created for the respective agent group that is dedicated to a file server. Moreover, the job also deletes expired substitutes of Owners and Responsibles.

11.6.4.4 MaintainAccessPermissions

Maintains the access permissions for the rights folders in the file system corresponding to the settings made in AM. Superfluous permissions will also be deleted by this job as needed.

11.6.4.5 MaintainAccessPermissions (incl. sub-objects)

Sets the access permissions for the rights folders in the file system corresponding to the settings made in AM and also overwrites the access permissions for all sub-folders and files contained in the rights folder.

11.6.4.6 UpdateShareAccessGroups

Ensures the existence of AD groups for share access and their proper members. Members are all user accounts that have at least one folder permission on the respective share.

11.6.4.7 WriteResponsiblesInfoFile

Creates or updates the admin information file for a rights folder. This file will include information about the Responsibles for the corresponding folders.

11.6.5 SharePoint Management Jobs

11.6.5.1 MaintainSharePointModernPermissions

Same as the *MaintainSharePointPermissions* job but for sites in “Modern” mode.

11.6.5.2 MaintainSharePointPermissions

Maintains the access permissions for the managed sites in SharePoint corresponding to the settings made in AM. Superfluous permissions will also be deleted by this job as needed.

11.6.5.3 SiteMaintenance

Synchronizes the site structure in the AM database with that of SharePoint site collections. It also notifies the Owner about any missing Responsibles.

11.6.6 AD Management Jobs

11.6.6.1 MaintainAdManagementPermissions

Like the *MaintainAccessPermissions* job (see chapter 11.6.4.4), this job checks and corrects the user memberships of items.

11.6.7 MS Teams Jobs

11.6.7.1 MaintainMsTeamsPermissions

Like the *MaintainAccessPermissions* job (see chapter 11.6.4.4), this job checks and corrects the user memberships of Teams objects.

11.6.8 FS-Accounting Jobs

11.6.8.1 AccountingDataExport

Exports the data determined for the last accounting process for the selected agent group into the directory as determined by the settings in the Administration module.

11.6.8.2 AccountingScan

Starts the accounting process for all defined accounting folders for the selected agent group. The size of each folder will be calculated from the assigned user or cost center(s).

11.6.8.3 CostCenterImport

Imports the cost centers stored in AD. The exact storage location will be determined by the settings in the Administration module. Cost centers that have been imported using this job will be flagged with *IMP*, in contrast to cost centers created manually or by the manual import of an Excel file (*MAN* flag).

11.6.9 Profile Management Jobs

11.6.9.1 ProfileADSynchronization

In Profile management / User Profile, if a *Profile Administrator* has assigned an AD group instead of a Profile Responsible, this job is needed for taking over all user accounts being a member of that AD group. Here, also nested AD groups are resolved except for built-in Windows groups. User accounts that have been members in the last job run yet but are removed since then will also be removed from the User Profile (full sync).

If AM has no access to an account or group within the assigned AD group (e.g. because of missing permission in AD or an external group of an untrusted domain), the affected accounts cannot be included.

11.7 Job Queue

Menu:

Administrator → Settings → Job Queue

The *Job Queue* page provides an overview of all running and scheduled jobs. Here, also jobs are listed that are automatically scheduled by AM.

Job Name: Shows the type of job and may contain not only manually scheduled jobs (see chapter 11.5 and 11.4) but also ones of the AM system (i.e. *RemoveDirectAcl*, *MaintainADPermission*) as well as jobs of the Report Mailing (*SendReports*, see chapter 5.3).

Agent Group: Shows the group of the job to be executed – only servers this group is dedicated to will be processed (see chapter 11.2).

Agent: The agent being member of the group named above that executes the current job.

Status: Contains one of three values: *Not Running*, *Running* or *Blocked*. If two jobs of the same type have been started at the same time, *Blocked* will be displayed as the status for one of the two jobs, because simultaneous execution is not possible. The blocked job will execute after the completion of the currently running job.

Job information will not be updated automatically. The *Refresh* button must be clicked to renew the job status display.

When the *Agent Group Reset* button is clicked, a dialog will appear and help with the selection of agent groups for which all non-repetitious and erroneous jobs can be removed.

Resetting an Agent Group will stop the currently running job, which may affect the operation of the AM system, such as interrupting jobs that are currently setting access rights and should therefore be used with care.

---

12 User Management

12.1 Operation Principle: AD User Provisioning

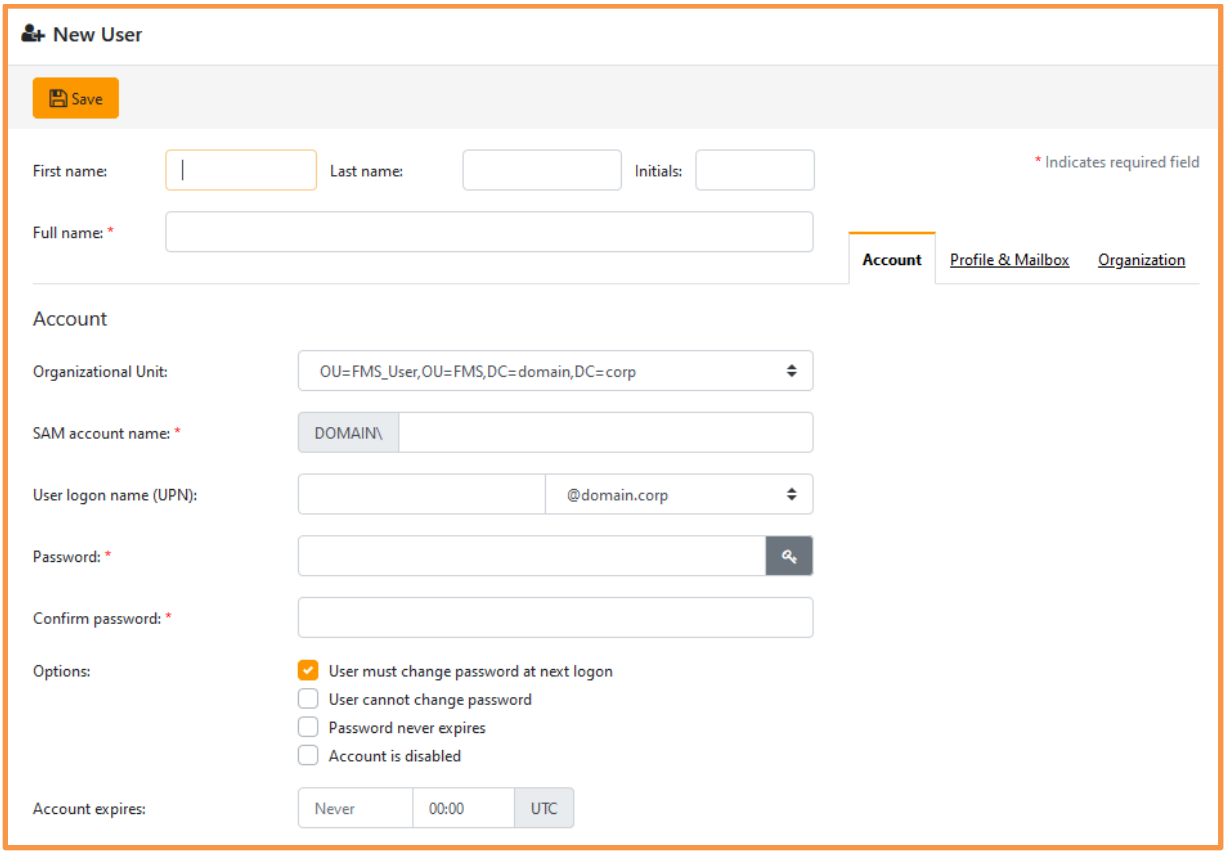
As an AM Administrator, Access Manager provides you functions to create new AD user accounts and manage existing ones, even if your account does not have permissions to AD. Advantages are not only a single point of access to several aspects of user provisioning but also a higher security level as AD access can be limited for many (administrative) accounts; user provisioning is logically performed by order of your account but physically through the AM service account. Furthermore, all such actions are logged by AM, so it is available in the audit trail later on (see chapter 13.9).

Menu:

Administrator → Identities

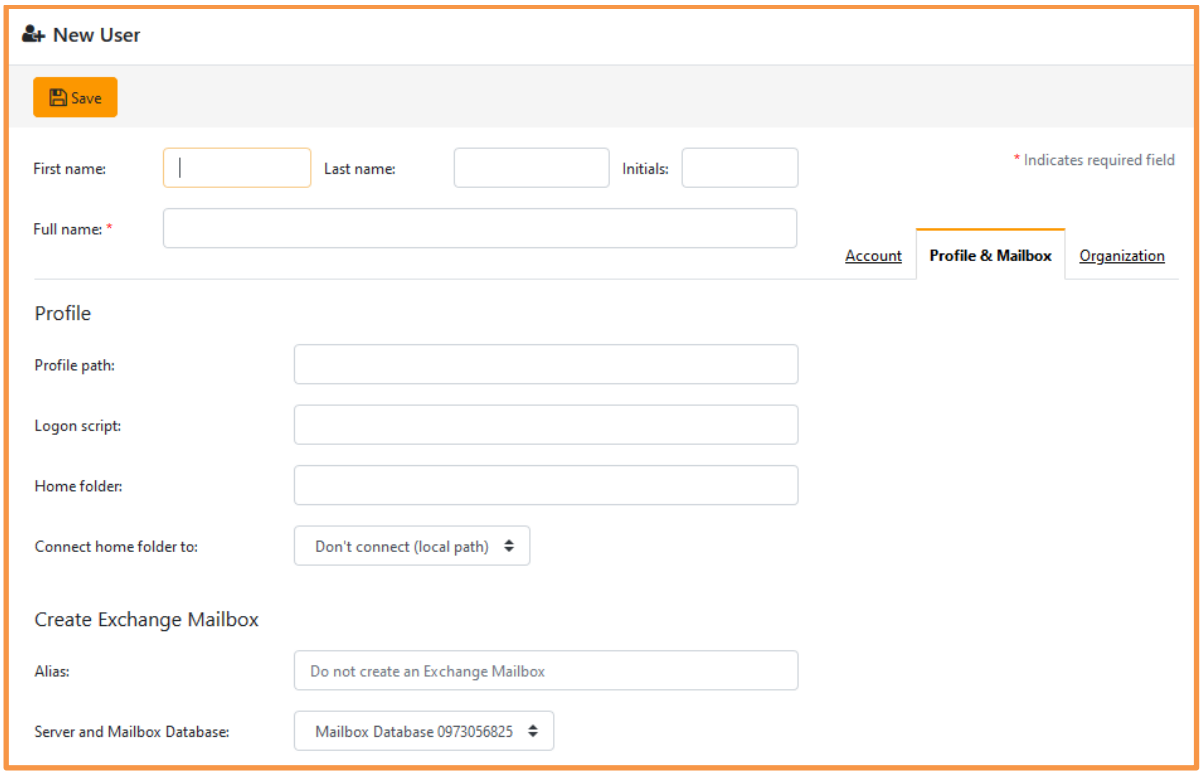
12.2 Creating AD User Accounts

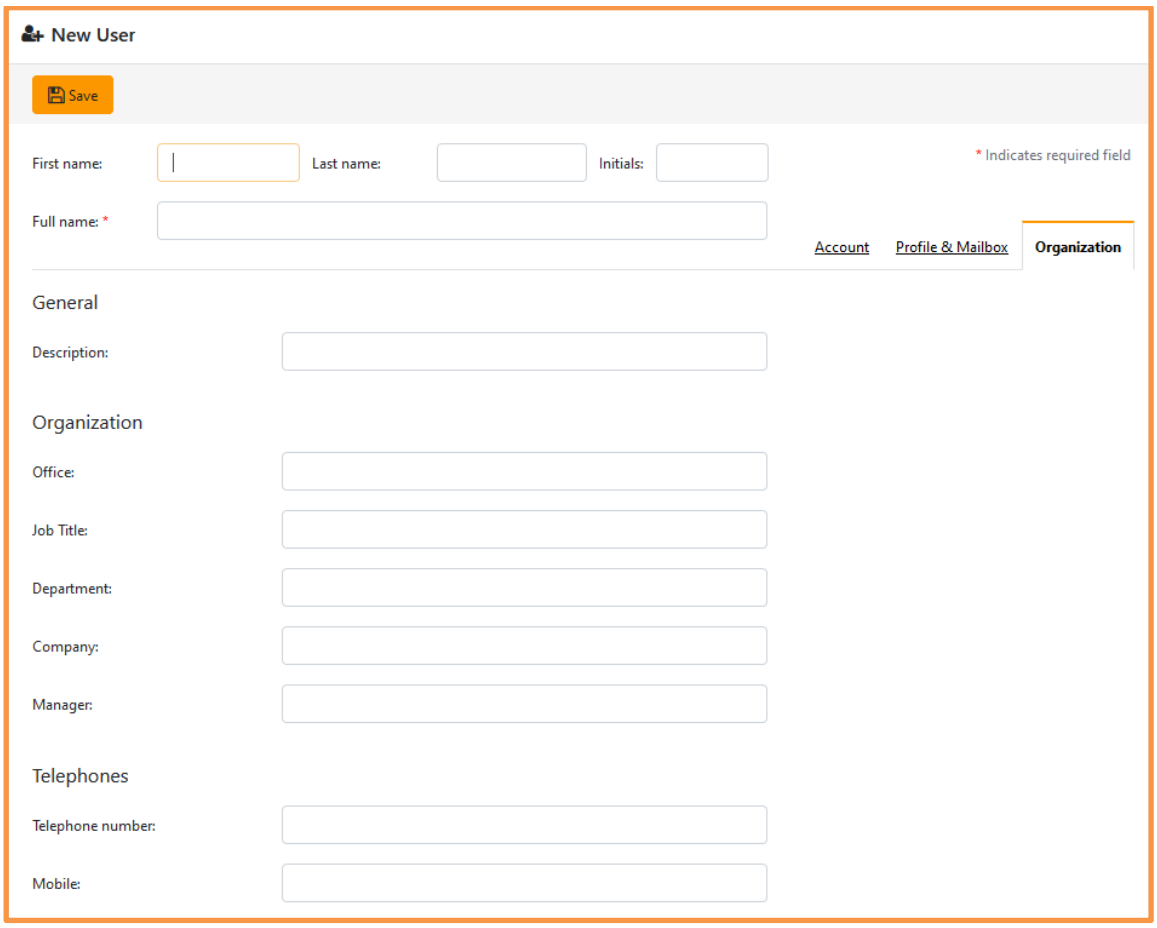
Via button New User you can create a new AD user account, optionally including an Exchange Mail Account. The clock icon button is used to immediately schedule an AD User Import job to synchronize the AD against Access Manager. The whole functionality is only available if configured correctly in the administrative settings.



Depending on administrative settings, one or more Organizational Units are available for saving the account. Available UPN suffixes are also predefined by the AM Administrator. Passwords can be entered directly or can be generated by AM if clicking the key icon. New passwords must respect the complexity rules as defined by your Active Directory. When created by AM, the password is displayed only once (popup window) and shall be jot down right now as it is not possible to look it up later on for security reasons. Password changes are logged in the *Audit* tab.

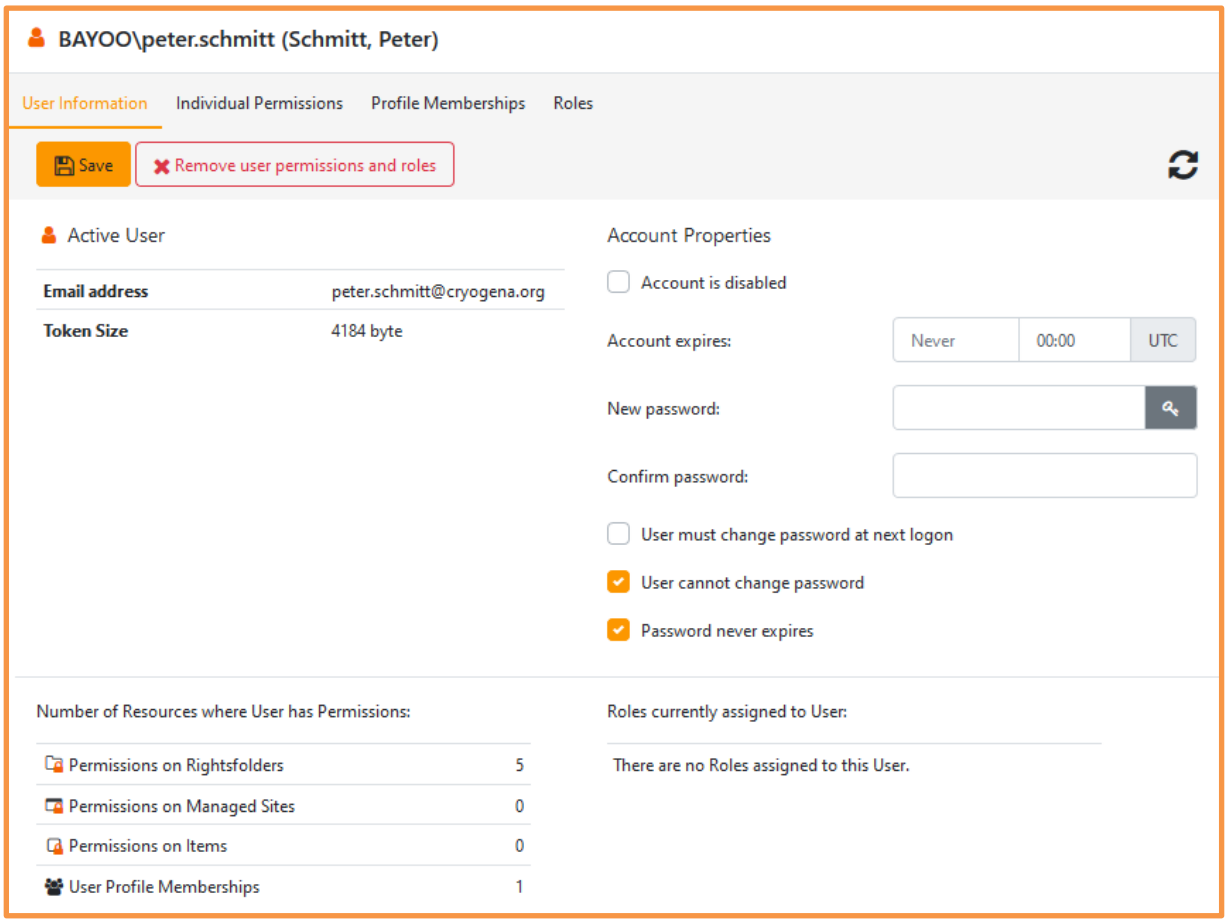
Password options, profile and organization attributes are derived from Active Directory. Depending on administrative settings, an Exchange Mailbox can be created for the user. In this case, the tab “Profile” will change its name to “Profile & Mailbox”.


New User
Save
First name:
Last name:
Initials:
* Indicates required field
Full name: *
Account
Profile & Mailbox
Organization
Profile
Profile path:
Logon script:
Home folder:
Connect home folder to:
Don't connect (local path)
Create Exchange Mailbox
Alias:
Do not create an Exchange Mailbox
Server and Mailbox Database:
Mailbox Database 0973056825


New User
Save
First name:
Last name:
Initials:
* Indicates required field
Full name: *
Account
Profile & Mailbox
Organization
General
Description:
Organization
Office:
Job Title:
Department:
Company:
Manager:
Telephones
Telephone number:
Mobile:

12.3 User Information

After selecting any known user account (and, if option was enabled, also AD groups) from the left side, you get a huge amount of information at the right. For better overview, information is separated into several tabs with general *User Information* displayed first by default:



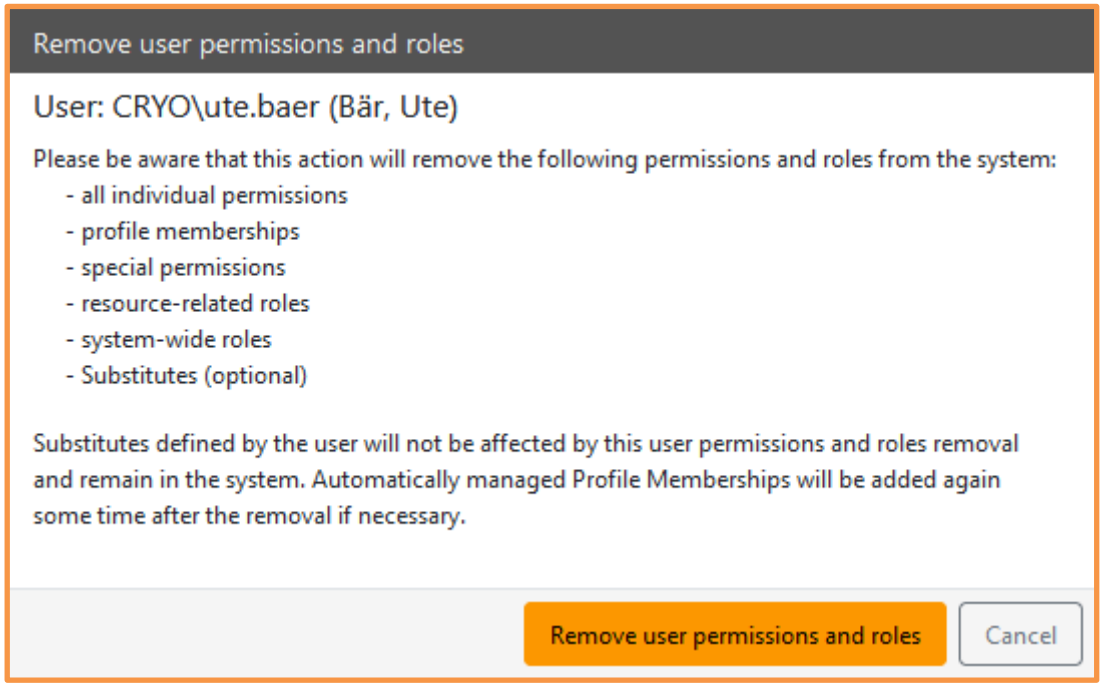
Besides the basic data, a summary of the permitted resources and assigned roles for the selected user is displayed.

The section *Account Properties* lets you de- or reactivate an account or set an expiry date directly in the AD: The Save button will write the information directly to the AD user account.

Using the password option, you may reset a users´ password by either entering it manually or by having AM generate it using the key icon. In both cases, AM and AD password policies apply. When created by AM, the password is displayed only once (popup window) and shall be jot down right now as it is not possible to look it up later on for security reasons. Password changes are logged in the *Audit* tab.

12.3.1 Removing all permissions

Additionally, you have the option to remove all permissions and roles for the selected user (button: *Remove user permissions and roles*) and the following dialog appears:

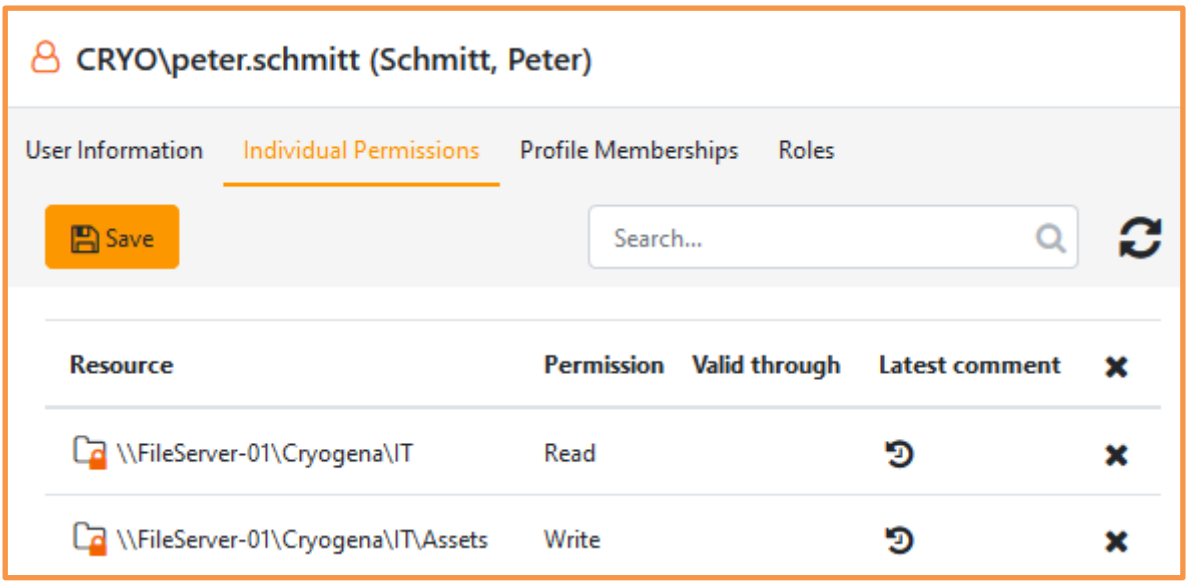


This way, permissions will be removed completely. However, roles often are not simply removed since the roles of a user are of special importance. For roles, another user must be selected as replacement to take over this role in the future. It is possible to select a different replacement for every role. Furthermore, special permissions and system-wide roles are removed.

With this functionality everything can be removed at once. If only permissions or roles shall be removed, this is possible on the following tabs.

12.4 Individual Permissions

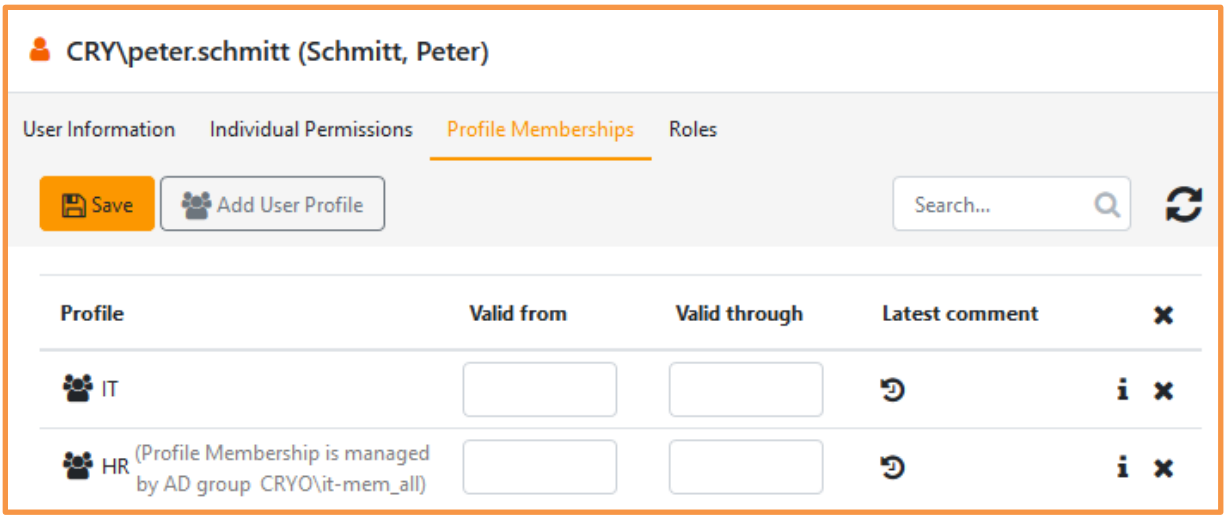
The tab *Individual Permissions* lists all resources of the user including the according permissions and, if available, the date of expiry is shown. In contrast to the view of a *Responsible*, you as an *AM Administrator* get a list of all resources, not only the ones you are responsible for.



For every resource the access permission can be changed (Drop Down Menu), a date of expiry can be set, comments can be viewed and added, and the permission can be removed entirely (X icon). Via the X icon in the table header it is possible to remove all permissions for the selected user at once. Permissions for additional resources can be added via the *Add Folder* / *Add Site* button. All changes are delayed, and the changed row is shown in a different color until the *Save* button is clicked. No automatic emails are sent to the affected parties, since for all these actions no requests are needed.

12.5 Profile Memberships

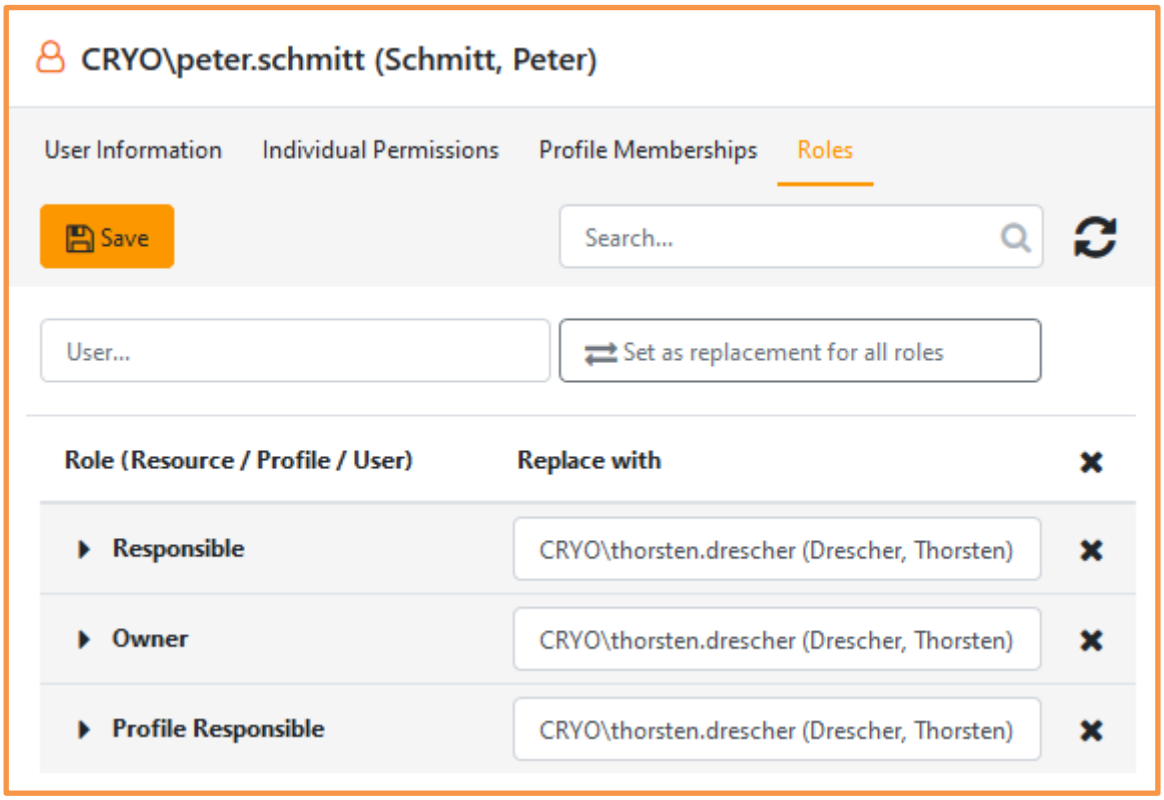
The tab *Profile Memberships* lists all Profiles, including Start and End dates that the user is a member of. The list also includes memberships which will start in the future and are not yet active. In contrast to the view of a *Profile Responsible*, you as an *AM Administrator* get a list of all resources, not only the ones you are responsible for.



Changes to the validity period for a membership can also be done on this page. Via the Info icon it is possible to discover folders that are permitted by the according profile. A profile can be removed for the selected user by clicking the X icon next to the profile, which will result in the user losing all permissions granted by the according profile. It is also possible to remove all profiles at once for the selected user by clicking the X icon in the table header. Vice versa, by clicking the *Add User Profile* button it is possible to add the selected user to other profiles, granting him the according permissions.

12.6 User Roles

The tab *Roles* informs you as an *AM Administrator* about additional resource related roles of the selected user e.g. *Responsible Substitute*, *Profile Responsible* and *Site-*, *Server-* and *Share-Administrator*. Similar to *Responsible* roles, *Owner* roles cannot be removed if there is only one owner for the respective resource. A user can be set as a replacement for all roles of the selected user by entering his name in the according field and clicking the *Set as replacement for all roles* button:



12.7 Managing User Substitutes

As an administrator, after selecting a user account, you will see an overview of his substitution situation in the *Substitutions* tab. The view is divided into the two areas *Is substituted by* and *Is substituting for*, which in turn differentiate according to role type (*Owner*, *Responsible*). You can change/delete all entries here and add new Substitutes. New Substitutes will not automatically be informed via email.

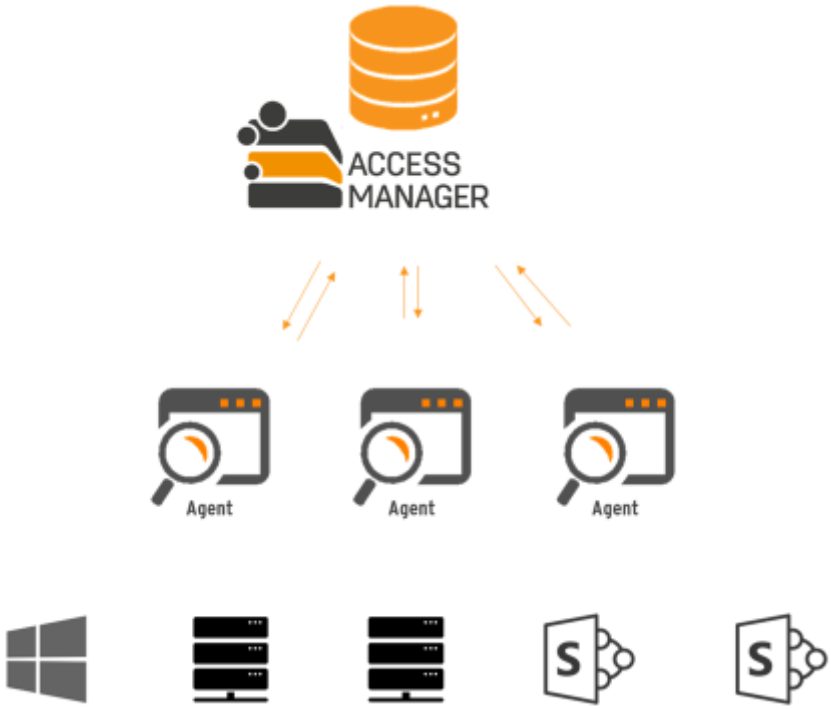
13 System Administration

13.1 Architecture and Operation principle

Access Manager follows the classic distributed client-server architecture and, in following those principles, relies on an agent concept for the parallel execution of multiple tasks in large, distributed environments.

The actual AM Server application runs as a web service under IIS on a dedicated server and provides the Management Portal as the interface to the users. The AM database (an MS SQL Server instance), where all management and log data will be stored, may run on the same or a different machine. Similarly, the AM Agent, which takes care of the execution of jobs, will be installed on that server or other servers. The AM components have read and write access as well as access to AD (for the creation and population of permission groups) as well as the associated file server (for recording the NTFS permissions).

One or more AM Agents may be installed:



An Agent is implemented as a Windows Service and must run on at least one server (usually on the same server where AM has been installed but may also be a file server). Commonly, a Job is a repetitive planned task for an Agent, e.g. for maintaining access permission on a file system. This way, all permissions set via Access Manager are automatically made permanent without any manual processing. To perform its jobs, the agent will access the AM database and read the required data. Vice versa, it will write the result values (such as error messages from AD and the file server, execution time stamps and so on) back to the database. Even though an agent can process multiple file servers, installing multiple agents and distributing their jobs is only reasonable in large infrastructures with multiple and/or widely distributed file and AD servers for technical IT reasons. This minimizes the network load and latency of communications with the central AM Server.

13.2 Technical Concept: User-created PowerShell Scripts

On different resources, Access Manager offers to execute your own created PowerShell Scripts.

Execute user-defined scripts at your own risk. BAYOOSOFT GmbH cannot be held responsible for any errors, defects or loss of data resulting from using such scripts.

Access Manager supports execution of scripts under PowerShell Script Version 4 and 5. Scripts are always executed as a job, hence by an agent. This means they are running locally on the machine that hosts the executing agent. Although it is possible to type the full source code into the text fields, it is recommended to just enter the path to a ready-made script file. The file must be accessible from the agent machine. As script jobs are executed within their assigned agent group containing an arbitrary number of agents, make sure that any agent can execute the script file. This can be achieved by either install the script at the very same location on every agent machine or, preferably, save it on a central share location accessible by all agents. This makes script updates easier and more reliable.

In your scripts please do **not** use commands `Write-Host` and `Write-Information` as these are not suitable for automation and prone to producing error messages. Use `Write-Output` instead.

Errors produced by a script are stored by AM and can be found at *Administrator → Logging → System Log*.

Please find examples about functionality and calling of scripts in chapter 15.

13.2.1 Calling scripts

In the text input field "Script", you can either enter the source code of the PowerShell script or a PowerShell file (*.ps1), which is processed.

Please note that when using multiple AM agents, it is not possible to specify which agent will run the script. Therefore, all machines on which agents are installed must have identical PowerShell versions, permissions, additional PowerShell modules that may be required, and access permissions to third-party systems (if needed by the scripts). **Scripts will always run under the AM Agent user account.**

Since visual feedback is not possible, you should always use a log file via `Write-Output` or similar for the output (but never use `Write-Host` or `Write-Information`).

13.2.1.1 Input: Source Code

If you enter source code, it is executed directly on the target machine as if you were executing every single line on the command line. This means that relative directory paths are not possible because the current execution directory is not known. A log file must therefore be specified with an absolute path:

```
$logFile = "C:\tmp\Example_ComputerInfo_AM-Agent.txt"
$computerName = [system.environment]::MachineName
$pshellVersion = [string]$PSVersionTable.PSVersion.Major + "." + [string]$PSVersionTable.PSVersion.Minor

Write-Output "$(Get-Date): --- ExecuteCustomScript Job: started" | Out-File $logFile -append
Write-Output "$(Get-Date):     PowerShell Version: $pshellVersion" | Out-File $logFile -append
Write-Output "$(Get-Date):     Host: $computerName" | Out-File $logFile -append
Write-Output "$(Get-Date):     Log File=$logFile" | Out-File $logFile -append
Write-Output "$(Get-Date): --- ExecuteCustomScript Job: ended" | Out-File $logFile -append
```

When this script is executed by Access Manager, you will find the output file in the C:\tmp\ directory on the machine where the AM Agent that executed the task is installed.

13.2.1.2 Input: Name of a script file

In most cases, it makes more sense to use an existing script file (*.ps1) that is executed by the AM agent. The agent executes the file locally. Especially if more than one agent is installed in the assigned agent group, it is uncertain which agent will run the script. Therefore, the identical script file must be stored at the very same location on all machines that have an agent running. A script would be called like this (content of text input field *Script*):

```
C:\tmp\Example_ComputerInfo_AM-Agent.ps1
```

A better alternative would be to centralize the script on one share that is accessible for every computer that runs an agent and for the AM Agent user account, as this makes maintenance and distribution of the script much easier. In that scenario a script could be called like this:

```
\\SERVER\SHARE\tmp\Example_ComputerInfo_AM-Agent.ps1
```

In both cases, always use an absolute path to avoid ambiguities and never put any quotation marks around the complete path (i.e. not as the first character), since this syntax is not understood. It is sufficient to put the quotation marks only around the parts of the path that contain spaces. This syntax is valid:

```
C:\"tmp 6\Example ComputerInfo AM-Agent.ps1"
```

```
\\SERVER\SHARE\"tmp 6\Example ComputerInfo AM-Agent.ps1"
```

13.3 Technical Concept: Profile Permissions via dedicated AD Groups

Besides the classic technique to permit users on distinct folders, Access Manager offers an alternative technical approach on setting user permissions by *Profiles* on file systems.

The classic approach always puts members of user profiles in the AD groups corresponding to the permitted Rights Folder (=Folder AD group) as this is done for direct permissions. Looking at the file system there is no difference, and it cannot be told whether permissions were set by direct or (user-) profile permission.

The new approach creates one distinct AD group for every AM user profile (=Profile AD group) and manages its member in this group only. The new Profile AD group is granted Read or Write access on the permitted Rights Folder (depending on the selection in the profile), meaning that the same AD group is used multiple times on a variety of file system folders. While Folder AD groups are still used for direct permissions, they are not filled with members of user profiles any longer.

Both methods can be used simultaneously in AM. It is possible to switch from one method to the other during operation without any data loss.

13.3.1 Comparison of technical approaches

The classic method causes a user to have a fast-growing Kerberos token if he is authorized on many folders, due to the fact that he becomes a member in all folder AD groups. With the new method, on the other hand, he is a member of fewer profile AD groups, but can still be authorized on many folders. The realization of added or deleted profile members in the file system speeds up significantly (especially with many folders in a profile), since the respective directory AD groups no longer need to be edited, but only the affected profile AD group.

The use of profile AD groups does not result in fewer AD groups overall and thus does not improve the transparency of the permissions in the file system. It is also not possible to use already existing customer-defined AD groups as profile AD groups, as this could lead to incalculable malfunctions due to missing access rights and incorrect validity areas (global / local AD groups).

13.4 Assigning System Roles

Menu:
Administrator → Settings → System Roles

The *System Roles* page manages users who are allowed to execute certain administrative functions and features. Roles are assigned to each user, which will be the basis for the rights to access the licensed modules. They can be combined as desired.

Existing AD users can be added using the *Add User* button. The Roles checkboxes can be used to assign roles to users or change their assignments. The *Delete* button will remove users from the list, whereby they will lose all role assignments. It will not delete AD user accounts.

DropDown button besides *Add User*: Additionally, you have the possibility to add multiple users at once by selecting an AD group and choosing the desired members (option: *Add users from AD group*). Also, you may select an AD group to add directly. The difference between these options is as follows: with the first option you will grant roles to multiple individual user accounts, while the second option will grant the roles to a potentially unknown bunch of users who may change over time, depending on the content of the group.

More information about the available roles and their areas of applicability can be found in chapter 2.3.2.

Please be aware that the first role, Administrator, does not automatically include all other roles. Hence, you should additionally activate them if you want to grant widespread system rights.

Using the search field, you can not only filter for user account names but also for roles: If, for example, you would like to list all users / groups having the “Profile Administrator” role, just enter this name.

13.4.1 Password Reset System Roles (AMPR Role Management)

Menu:
Administrator → Settings → Password Reset System Roles

This function is available only if application AMPR is present and if you own the *AMPR role Administrator*. Here, you can manage user roles existing in AMPR.

This menu item provides the functionality of the AMPR application.
Please find a more detailed description in the corresponding manual.

13.5 Script Management

Menu:
Administrator → Settings → Script Management

Access Manager supports using your own PowerShell scripts. These are maintained centrally by the *Script Management Administrator*.

Similar to profile management, individual scripts are organized in clusters, although scripts with the same name can be created in different clusters. Scripts also cannot be moved between clusters; once created, this is their permanent location.

A script can be deleted if it is not used. The button *Show script usages* will list all the relevant positions. Deactivation is also possible; a script can remain assigned but will not be executed.

Since the places where scripts can be used (e.g. AD group management, user creation) offer different internal variables, you can display these variables in the built-in script editor, divided into the respective areas.

With the option *Use Windows PowerShell* you can specify that scripts are not executed in AM's own PowerShell instance, but that the executing agent uses the normal Windows environment for PowerShell. Use this option if you have compatibility problems, as it is less performant and the environments could differ from one agent to another depending on the computer configuration, which can make troubleshooting extremely difficult.

Please note that for these reasons, BAYOOSOFT GmbH does not provide support for problems that may arise when using the Windows PowerShell option.

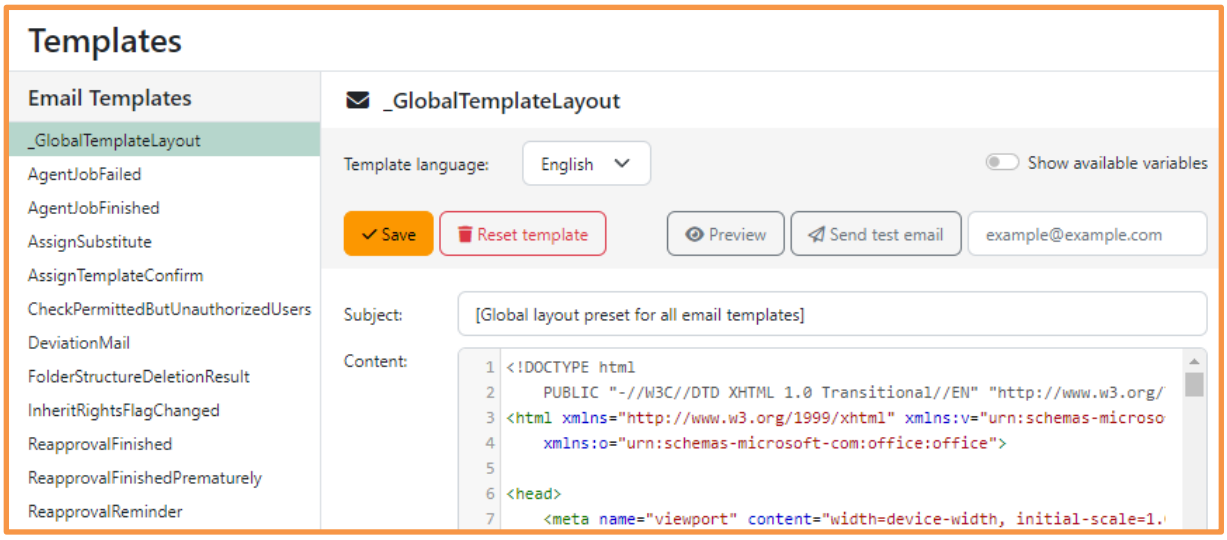
Using the script editor, you can enter the script source code yourself or simply call an external PowerShell file. Please note the instructions for use in Chapter 13.2.

13.6 Configuring Mailing

Menu:
Administrator → Settings → Templates

The page *Templates* provides management of structure and visuals of notification emails. The left column lists available templates, divided in two areas (Email Templates, Other Templates). After selecting one, you can edit the template at the right area.

13.6.1 Email Templates



Initially, the source code of the e-mail is displayed and can be edited there - knowledge of HTML, CSS and XSLT is an advantage. Use the key combination Ctrl-F to search for any character string within the source code of a template; all occurrences are highlighted in yellow. The *Save* button saves your changes, with *Reset* all changes to the template (including previously saved ones) are discarded and the factory settings are restored. The *Preview* button shows you how your template will look using demo data, even if you have not yet saved the changes. If you enter an e-mail address, you can also send this sample e-mail to yourself by clicking the *Send test email* button for real testing. This allows you to see, for example, whether images are being loaded correctly – most mail clients initially block the download of external graphics, so you may have to define an exception here.

You can use the drop-down list *Template language* to create different texts for German and English (and, if desired, also different layouts) – this also includes the subject of the mail.

You can use variables offered by Access Manager both in the subject and in the mail body. You can display which these are in a window using the *Show available variables* button.

Users will receive mails always in their chosen language,
so there is no need to write bi-lingual templates.

13.6.1.1 Exceptional case "_GlobalTemplateLayout"

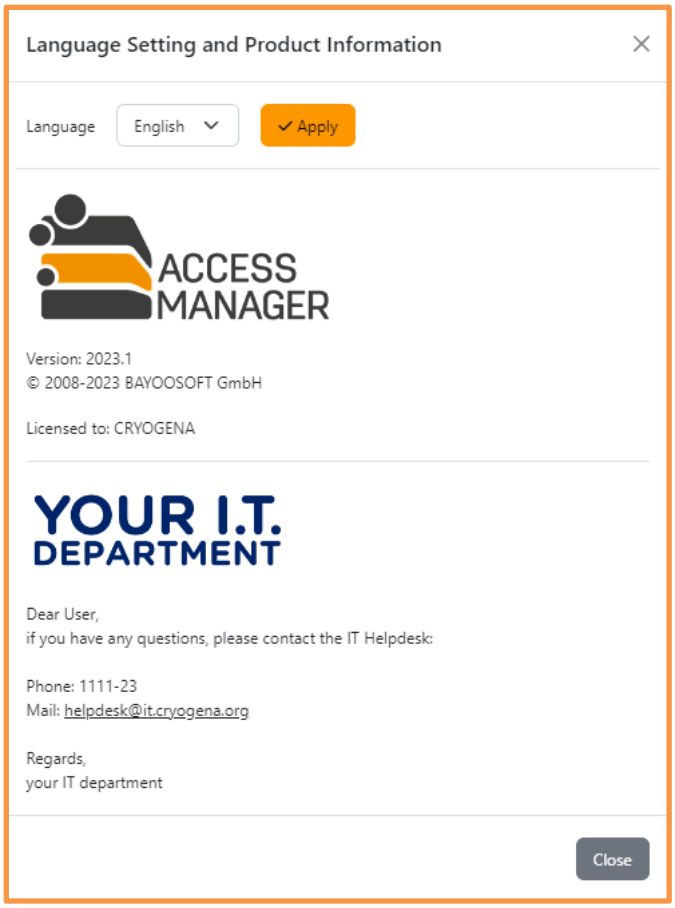
The top entry *_GlobalTemplateLayout* exists to simplify a uniform layout across all email types. Only here do you define (for each language) the appearance and basic content (e.g. greetings, standard links to support team, etc.). All other mail templates integrate this layout (see first line in the source text) and only add their specific content.

13.6.2 Other Templates

Besides email templates, there are other informational templates that are used on various occasions. Naturally, there are neither test mails nor internal variables usable here.

13.6.2.1 CompanyInformation

The information displayed to you in the information and settings window (burger menu at the top right next to your login name) is set to BAYOOSOFT for administrators. For end users (all non-administrators) you can enter your company's own information here:



13.6.2.2 ResponsiblesInfoFile

The job *WriteResponsiblesInfoFile* (chapter 11.6.4.7) creates files in the file system. Here you can determine their content and appearance yourself. Please note that the language selection has no effect here – the **English** template version is always used. You should make the content multilingual right away.

13.6.3 Overwriting & Retention of Templates on Program Updates

If AM is updated to a newer version, the templates delivered will also be updated. However, templates that have been customized by you will be retained and will not be changed in any manner. Only the *Reset Template* button (on every Template) will cause the default template to overwrite custom changes, so they get lost.

Caution: When updating from an AM version 2022.1 or earlier, all custom changes get lost because version 2023.1 introduced a completely new templating engine.

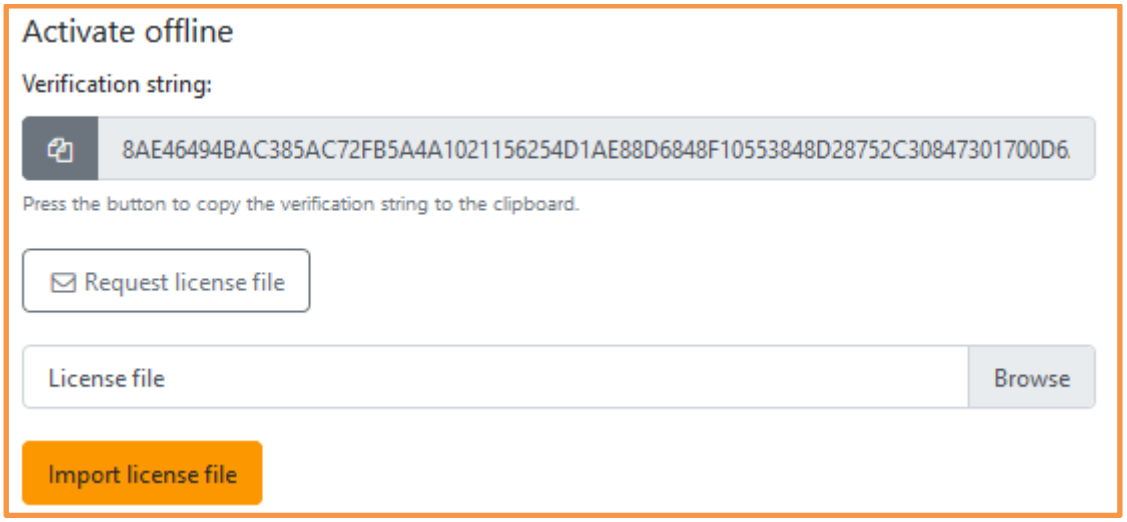
13.7 License Management

Menu:
Administrator → Settings → License Management

The *License Management* window is used to license and activate various modules for use.

13.7.1 Entering / Updating License

To license a module or raise the number of licensed users, enter the License Key provided when the module license was purchased for the first time and click button *Activate online*. Now, the necessary licenses are transferred via Internet from the BAYOONET AG license server. If an Internet connection is not available, use function *Activate offline* instead. Further input fields are available:



Click button Request license file. This will generate an email in your default mail client, containing all necessary information. As an alternative, copy the Verification string into a new email. Send the email to the service department of BAYOONET AG (*support@accessmanager.net*). The support team will send a license file by email that you can save locally and import it with the *Import license file* button. The licensed modules and the user limits are immediately displayed like shown in the above screenshot.

Note: Updated license information may take up to 10 minutes to become effective.

13.7.2 Upgrading License

If you need to raise your currently licensed user limits, you may send an email to the sales department of BAYOONET AG (*sales@accessmanager.net*) via button *Request upgrade*. Please be sure to enter your desired license amount and provide additional recipients if applicable. The sales team will send your customized offer soon.

13.8 System Settings

Menu:

Administrator → Settings → System Settings

On this page, the global AM settings are managed. Each setting has a name and a value that can be modified. A description is displayed when hovering the mouse over a setting. Additionally, the AM module is listed which the setting belongs to. By default, the list will be grouped by module.

To change a setting, simply alter the old value. The button *Undo* will reset your changed parameter to the original value. The new values will be valid after the *Save* button has been clicked and become immediately effective.

The upper area offers filter checkboxes to hide settings of modules to provide a better overview.

All global settings for the currently available modules will be explained in the following chapters.

13.8.1 Module "Administration"

13.8.1.1 AdditionalAdData

By this setting a list of fields of the AD user object can be created. The fields specified in this list will be read from each user account at every user import and displayed in the Management Portal as additional information for each user. Depending on the selected interface language, the English or German description is prefixed. The following should be kept in mind:

- The additional data can be viewed by any user of the Management Portal, including users without any administrative roles. Therefore, no sensitive or confidential data (e.g. accountExpires, lastLogonTimestamp, ...) should be used in this setting.
- Some predefined fields in the user object are not stored in the AD GlobalCatalog and are therefore not replicated across multiple domain controllers. The display of such a field therefore depends on the connected DC and is not consistent. Use only replicated fields; replication should usually be active for user-defined fields.
- Some fields (e.g. displayName) are already used by AM internally and are therefore not displayed additionally.

13.8.1.2 AllowRenewAccessSettingsByOwners

With this option activated, *Owners* can force AM to update access permissions on managed resources. A new context menu item, *Renew Access Permissions*, appears.

13.8.1.3 AllowRetiredUserImport

Allows disabled or expired AD user accounts to be imported or prevents import. This option refers to the import of folder collection permissions: import validation will fail if deactivated accounts are to be imported and this option is set to false.

13.8.1.4 AllowRevocationOfOwnOwnership

If activated, you are allowed to revoke your own *Owner* role on a resource. Note that you will lose all associated management options - in particular, you will not be able to give the role back to yourself.

13.8.1.5 ApproverCommentsAreMandatory

If this option has been enabled, people processing user requests (Owners or administrators) will be forced to provide a comment during processing.

13.8.1.6 CalculateTokenSizeOnADUserImport

Enables determination of the approximate size of Kerberos tokens during the ADUserImport job or disables it.

13.8.1.7 CancelUnprocessedRequestsAfterXDays

If a user request has not been processed within X days, it will be automatically cancelled. The applicant will not be informed of this by email, but the cancellation will be audited with a corresponding comment.

Enter nothing to turn off the feature. Entering 0 cancels the next day, 1 cancels the day after that, and so on.

This function is performed by the *CheckUnprocessedRequests* task (chapter 11.6.1.3) and therefore needs to be scheduled.

13.8.1.8 CleanUpPermissionsOfDeletedAdUsers

Activating this option, Access Manager will remove access permissions from its database of user accounts that are not found in AD anymore. “Not found in AD” means that either an account was truly deleted in AD or was moved to another place (OU) where Access Manager has no access permission. For this to work, the job *TidyUpDatabase* (chapter 11.6.1.7) must be scheduled.

Following data is deleted from the AM database:

- Individual Permissions
- Membership of Profiles, hence the permissions of related resources
- Substitutes of Responsibles and Owners
- Role Responsible, Owner – if there is at least one more person having the respective role. If the account to delete is the last one, it will keep the role and the administrator is requested by email to manually assign another person in charge. Only after that, the role can be removed from the account.
- Special permissions (i.e. on folder collection level)
- Roles not concerning a resource (System Roles)

13.8.1.9 CommentsAreMandatoryDuringImport

If this option is enabled and you perform a Folder Collection Data Import (chapter 8.2.1.4.4), you must fill out every row of column COMMENT in the Excel file with a reason text for the permission, otherwise the import will fail.

13.8.1.10 Database

This read-only value shows the currently used Access Manager database.

13.8.1.11 DefaultAccessDuration

Default value for newly created (Folder) Collections. This presets the duration (in days) of granted permissions but can be changed afterwards individually for every Collection (chapter 8.2.1.4.2).

13.8.1.12 DefaultLanguage

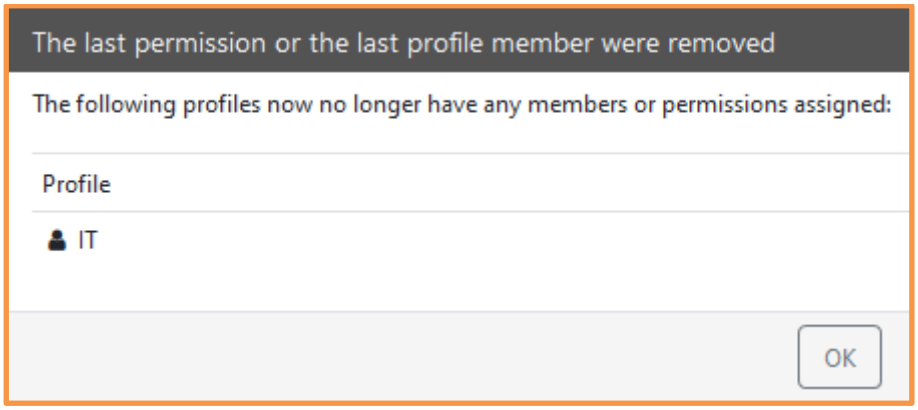
As long as a user has not adjusted the language setting himself, all texts (interface, e-mails, etc.) will be displayed in the default language set here.

13.8.1.13 DeviationFilterLimit

Use this setting to specify the number of encountered but irrelevant permission deviations are filtered out in one pass. If the value is too high, filtering may last very long, blocking processing of other jobs.

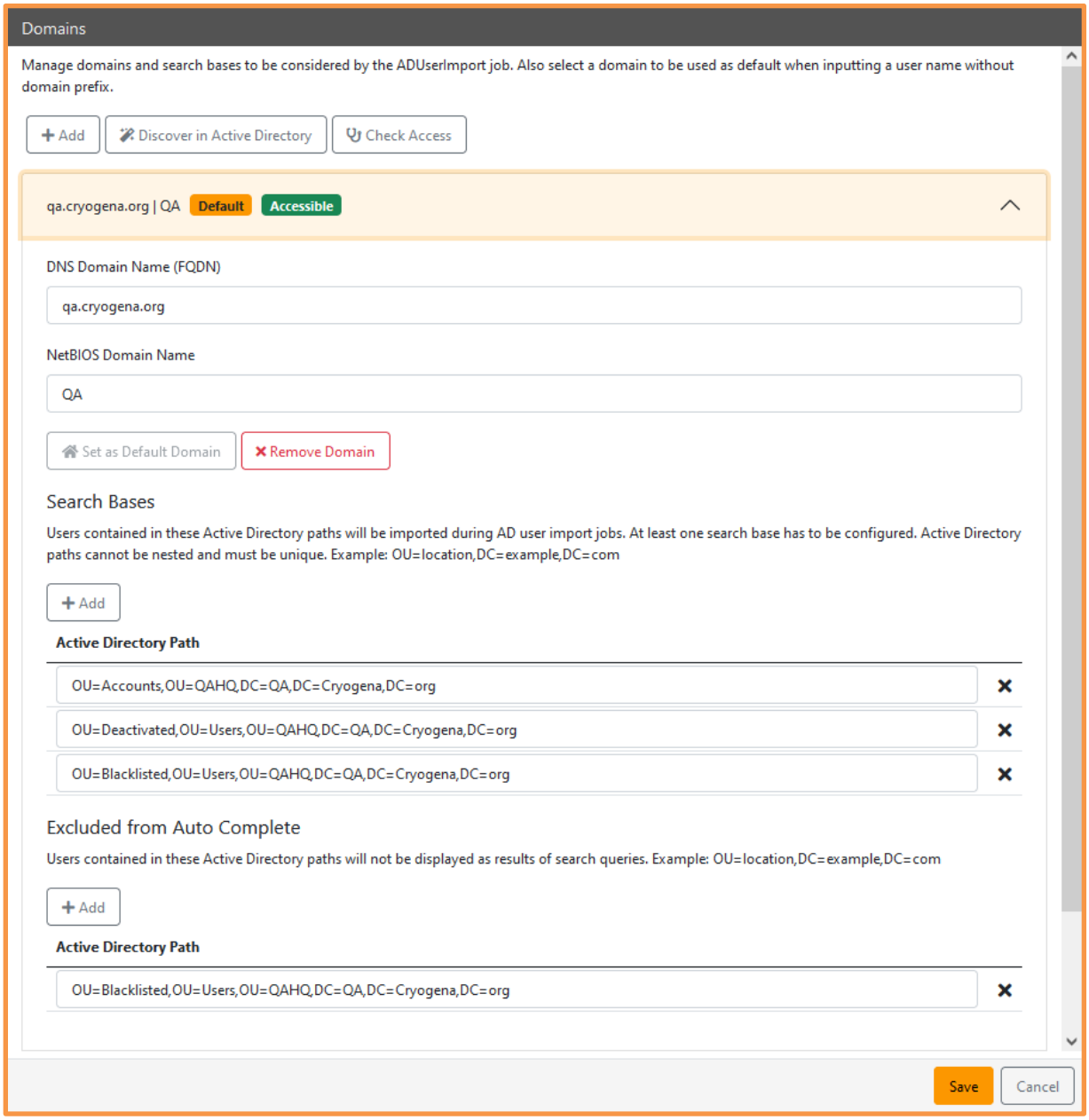
This option should only be used in very special cases concerning the processing time of permission managing jobs.

13.8.1.14 DisplayLastPermissionOrMemberRemovedWarning



Setting for displaying a warning message to a decider if he removes the last permission of a resource. For example, the message is presented if a folder permission is removed from a profile and it was the last permission the folder had. As a result, no-one is able to access the folder any longer. Vice versa, if permissions of a folder are changed and a profile permission is removed from this folder, it may happen that the profile has no more permissions on any resource which means that the profile is useless now.

13.8.1.15 Domains



This dialog provide means to enter Domains, Subdomains and (external) Trusts to be included when *ADUserImport* job (chapter 11.6.2.1) is executed. In turn, all domains not listed here remain ignored.

Button *Discover in Active Directory* will automatically insert all publicly available domains, while button *Add* lets you enter further domains manually. Use button *Check Access* to ensure that the domains can be accessed. If not, you can remove the respective record if you are sure it is not a temporary outage that is to be corrected.

In case the job ADUserImport cannot query one of the listed domains, none of the other domains will be synchronized either and an error email will be sent. Therefore, check and correct this domain list as soon as possible and / or correct the cause of the connectivity issue.

The button *Set as Default Domain* denotes the domain that will be the first suggestion if you enter a user account name existing in multiple domains.

Search Bases

Within each given domain, at least one Search Base (OU) must exist, from which user accounts are searched for import, and all paths below are searched recursively. By default, the topmost level is preconfigured, but you can alter this to a specific entry point on lower levels. Moreover, you may enter multiple Search Bases.

---

*The technical accounts used by Access Manager itself **must** reside in a Search Base.*
*Search Bases **must not** be nested.*
User not found in one of the Search Bases cannot log in to the Access Manager Website – they are not able to use it.

Excluded from Auto Complete

Enter one or more AD paths with contained user accounts that shall not be displayed when entering an account, i.e. while giving personal access rights. The automatic list of matching accounts will not contain such accounts, reducing the risk of providing access to unwanted accounts.

---

*Hereby entered paths **must** be included in the above-mentioned Search Bases.*

13.8.1.16 EmailAdministratorIfPermittedUserIsNotInAuthorizedGroup

If activated, all Administrators receive an email with a list of users who were permitted for a resource they are not authorized for, according to a classification. This indicates an erroneous permission granting by a decider and should be checked.

13.8.1.17 EmailIfPermissionExpiresInXDays

Number of days in advance to notify a user that their file system permissions will be removed.

13.8.1.18 EmailResponsibleIfPermittedUserIsNotInAuthorizedGroup

If activated, all assigned Responsibles receive an email with a list of users who were permitted for a resource they are not authorized for, according to a classification. This indicates an erroneous permission granting by a decider and should be checked.

13.8.1.19 EnableProfileMembershipRequests

With this setting activated, users may apply for membership of User Profiles. Requests work in the same way as for all other resource types (Folders, SharePoint Sites, 3rd Party Elements…). A User Profile is only available for application if it is managed manually by *Profile Responsibles* but not if managed automatically by a synchronization group.

13.8.1.20 ExchangeMailServers

Configures Exchange servers and credentials for Exchange mailbox creation for AD users. By clicking the - button, the connection configuration can be tested before saving.

13.8.1.21 GlobalAssistantAllUsers

Use this setting to make all users having the *Assistant* role. In effect, every single user may file a request for other users.

13.8.1.22 GrafanaLokiLogMinimumLevel

Only log entries with the configured level (and above) will be sent to Loki. Enter one of the following values: Verbose, Debug, Information, Warning, Error, Fatal

13.8.1.23 GrafanaLokiQueryLimit

With this value you determine how many log entries should be read and displayed from Loki by default in the system log. It should not be higher than the limit set in Loki itself. Although you can change this value in the system log at any time (chapter 13.10.1), this default value is always used each time the page is opened again.

13.8.1.24 GrafanaLokiQueryPreset

This value is created automatically by the system and only needs to be changed in the rarest of cases (e.g., if you have another AM instance logged into the same Loki instance).

13.8.1.25 GrafanaLokiQueryTimeMs

The timespan to wait before a request querying log entries from Loki times out (in milliseconds).

13.8.1.26 GrafanaLokiUrl

Access Manager will look for your Loki instance at this address. Only if you enter a value here, Access Manager will display the logging from the Loki instance instead of from its own database. Displaying both sources at the same time is neither possible nor useful.

13.8.1.27 ImportAdGroupsAsUsers

This option activates treatment of AD groups (type: Security group) in the same way as user accounts when managing access permissions. This means that only those groups can be used that are available in the configured domain-specific search bases. Permission management will not resolve the group members but will simply grant permission to the group object itself. This may lead to security breaches as members are not checked. For this reason, AD groups are not permitted anyway if the resource is additionally secured by sabotage prevention function.

13.8.1.28 JobNotificationMails

Here you can define default values that determines the cases in which AM Administrators and users with specific roles will be notified about events by email after the execution of a job. The cases are identified as either informational messages or error notifications. You can individually alter these values on every job creation.

Informational mails will be sent after a job has completed successfully. For this purpose, the associated Info Template *AgentJobFinished* will be used. The information contained in the message will depend on the type of job. For example, the information may include the start and stop times for the job as well as the access permissions.

Error mails will only be sent when an error occurs during a job, and an informational message will also be sent. The *AgentJobFailed* error template is used for all error notifications regardless of the type of job.

The checkboxes (*Info* or *Error*) next to each template are used to enable (checked) or disable (unchecked) transmission of the corresponding mails to AM Administrators. The *All* checkboxes will enable or disable transmission of all notifications to AM Administrators. The changes will take effect after the *Save* button is clicked.

If an email template does not have an *Info* checkbox, the job has its own mail template because necessary information includes a broader range than the common template can bear and must be sent depending on other cases than just for information. For example, this applies to the jobs *CheckAndFilterDeviations*, *InitializeReapproval* und *FinishReapproval*.

The *ExecuteCustomScriptInternal* job is an exception to this. That job is frequently used by AM itself and it does not make sense to steadily inform about its successful execution.

13.8.1.29 LinkToExternalLogPage

Set a link to an external logging system. If a link is set, it replaces the System Log page. For example, this is important when using Splunk logging (see following chapters) to easily point to your Splunk web page.

13.8.1.30 MailServer

SMTP settings for the transmission of email messages. Clicking this setting will open a popup dialog with additional settings. Activate the checkbox *Send test mail to verify the settings* to send a test mail to the account that you are currently logged in with; this account must be able to receive emails.

13.8.1.31 ManagedLocationDescriptionIsMandatory

For every managed resource a descriptive text can be entered. This setting enforces the input.

13.8.1.32 ManualsPath

The path to the user manuals that will be linked in the Management Portal. The path may be either a local, or an SMB path; URLs may not be used. Note that AM will only display the *Manual* menu item

on the Portal's main menu if the specified folder contains at least one file (in PDF format). All PDF files will then automatically be listed by file name and linked for downloading.

13.8.1.33 MicrosoftEntraTenants

Similar to the settings dialog *Domains* (Chapter 13.8.1.15), here you set connection data for your Microsoft Entra tenant. Please refer to your Microsoft Entra configuration for the values to be entered or ask your cloud administrator. Also, you can find further information in document "Installation_EN.pdf" which is part of the Access Manager package.

Parameter *Service Account Object ID*: This means an Entra User object that owns the necessary licenses for MS Teams and SharePoint, respectively. This user object is also set as the fallback owner on SharePoint and Teams groups.

Parameter *Allow guest invitations*: This enables you to authorize so-called "guest users" in your tenant. This gives users the option of requesting access to a Microsoft Entra resource by providing an e-mail address without a Microsoft Entra account already having to exist for them.

13.8.1.34 PermissionCommentsAreMandatory

If activated, a comment must be entered by the decider (Responsible, Administrator) when altering access permissions in any way. This includes all kinds of changes: add, remove and change permissions and durations as well as adding / removing a user to / from a profile. This setting does not affect changes to profile settings.

13.8.1.35 ProcessingActivitiesGeneralDescription

The English and German text that will appear in the general description of the technical and organizational measures of the report *Processing Activities of a resource*:

13.8.1.36 RequestsCommentsAreMandatory

If this option has been enabled, users will be forced to enter a comment when they make requests through the Management Portal.

13.8.1.37 RetentionPeriodAudits

All following RetentionPeriod settings refer to the duration of keeping audit records. These values (in months) define how long a record will be kept in the system after its creation. When the period is reached, the record is deleted irrevocably from the database. If the value is 0 (default), records are never deleted. Please note that for this functionality to perform, the job DeleteOldAuditData must be scheduled (see chapter 11.6.1.5).

This option is meant to remove all records ***not*** covered by the following settings. Hence, it is not a "delete everything" but "delete remaining" function.

13.8.1.38 RetentionPeriodClosedRequests

To remove closed user requests.

13.8.1.39 RetentionPeriodDeviations

To remove permission deviations discovered by the automatic maintenance jobs.

13.8.1.40 RetentionPeriodImportData

To remove information about folder data imports. This means permission data that were created using the Structure import (see chapter 8.2.1.4.4) of a Folder Collection.

13.8.1.41 RetentionPeriodOwnershipAudits

To remove information about ownership takeovers in the file system. For more information about Ownership Takeover, see chapters 13.8.3.14ff.

13.8.1.42 RetentionPeriodPermissionAudits

To remove information about permission management.

13.8.1.43 RetentionPeriodPermissionComments

To remove comments of permission management.

13.8.1.44 RetentionPeriodReapprovals

To remove information about reapproval runs.

13.8.1.45 SelfServicePortalUrl

The URL for the Management Portal. The URL must be terminated with a slash (/). We recommend using https.

13.8.1.46 SendEmailForUnprocessedRequestsAfterXDays

Decision-makers (Owners and Responsibles) receive a reminder email if they have not processed an application for at least X days.

This function is performed by the *CheckUnprocessedRequests* task (chapter 11.6.1.3) and therefore needs to be scheduled.

13.8.1.47 ShowAllProfilesInSelfServicePermissions

If the option is activated that users can view their profile memberships (see next option), this setting can be used to determine whether they can only see those which can also be requested in the Self Service Portal or also all others in which they were made a member.

13.8.1.48 ShowProfileMembershipsTabInSelfService

This setting enables the tab *Self Service → My Permissions → My Permissions → Profile Memberships*.

13.8.1.49 ShowResourceProfilesOnRequestPages

If this option and option *EnableProfileMembershipRequests* is enabled, the page for requesting access rights (see chapter 3.2.1) will incorporate a drop down list, showing all user profiles that also give permission onto this resource. As an exception, user profiles for which the profile administrator has disabled the option *Visible in Self Service*, will be omitted in the list.

13.8.1.50 SplunkLogEventCollectorToken

A valid and enabled (status: “Enabled”) Splunk HTTP Event Collector Token Value.

13.8.1.51 SplunkLogMinimumLevel

Only log entries with the configured level (and above) will be sent to Splunk. Enter one of the following values: Verbose, Debug, Information, Warning, Error, Fatal

13.8.1.52 SplunkLogUrl

URL of Splunk HTTP Event Collector. Must end with /services/collector/event.

13.8.1.53 ThirdPartyDefaultSelfServiceEnabled

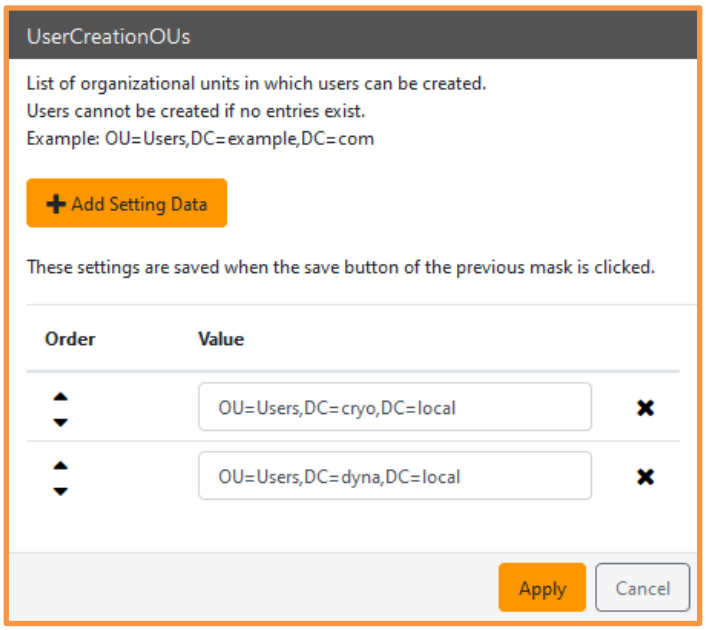
The default setting that will be used for the visibility of newly created elements.

13.8.1.54 UserCreationJobScheduleTime

Newly created user accounts do initially have the status “Newly created User”. The job *FinalizeUserCreation* will check if this account was granted access permissions by AM, processes them and then switches account status to “Active”. This setting defines the waiting time in minutes from account creation to job start. Also, the *UserCreationScript* job is started after this waiting time. This way it is ensured that the synchronization over several DCs is completed before further actions are executed by AM on the AD.

13.8.1.55 UserCreationOUs

When creating a new user account, it is possible to select the OU where the account shall be created. This setting allows for managing the list of selectable OUs by clicking the icon .



If no OU is specified it is not possible to create an account, hence the button *New User* is hidden in Management Portal.

---

*Hereby entered OUs **must** reside within a domain-specific Search Base (see chapter 13.8.1.15).*

13.8.1.56 UserCreationPasswordLength

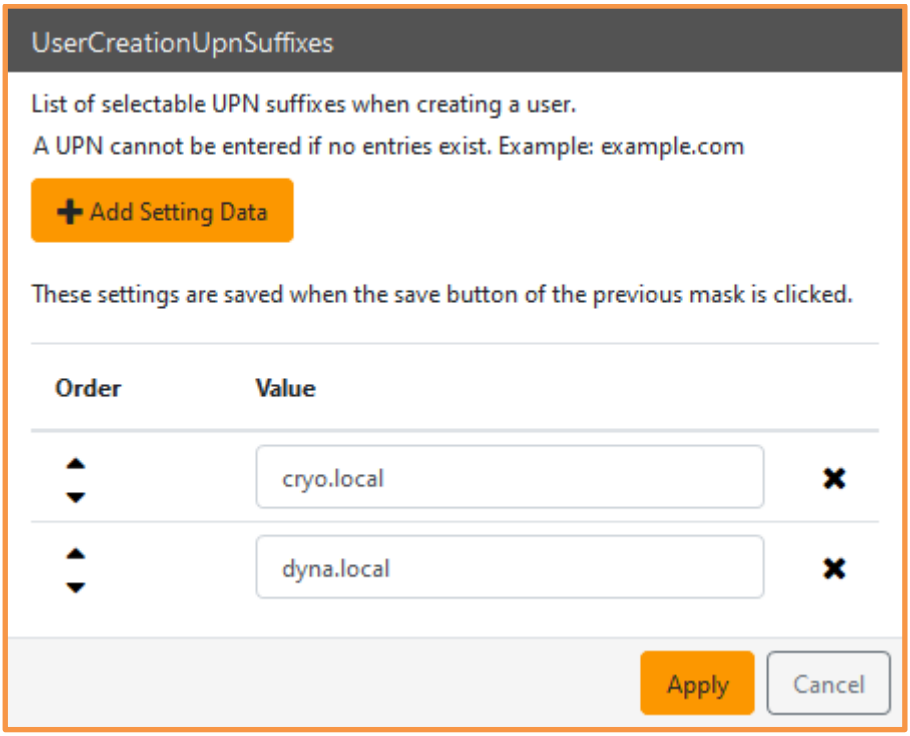
Access Manager can create a random password for new accounts of the hereby specified character length.

13.8.1.57 UserCreationScriptId

After a new user account has been created, a PowerShell script can be executed. Here you can select a script from the Script Management. Please also refer to the PowerShell script technical support notes in chapter 13.2.

13.8.1.58 UserCreationUpnSuffixes

This option offers an editable list of suffixes to add to new user account names (UPN, User Principal Name) by clicking the icon .



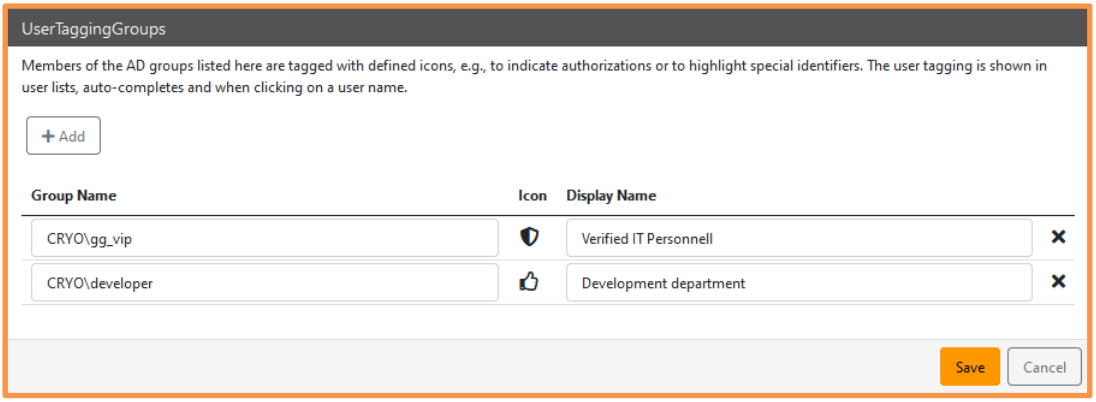
If no suffix is specified, the corresponding dropdown list is hidden in Management Portal.

13.8.1.59 UserProfilesDefaultSelfServiceEnabled

Analogous to options for folders and SharePoint Sites, this setting specifies if newly created User Profiles shall be available for application by default.

13.8.1.60 UserTaggingGroups

Define a list of AD groups and assign an icon and a short description. All users being member of such an AD group will be displayed along with the respective icon. In case a user is member of multiple groups, their icons are displayed also.



13.8.2 Module "AD Group Management"

13.8.2.1 AdGrouItemNameRegex

Analogous to the validation rules for folders and SharePoint site names, you use this option to specify the permitted or prohibited characters for AD group names and, if applicable, the maximum length. This will prevent problems with automatic group creation in AD.

13.8.2.2 ThirdPartyItemAdGroupDescription

Template for the description field of AD groups created by AM. This description is not used for existing AD groups connected to an Item but only when AM creates a new AD group.

13.8.3 Module "Fileserver Management"

13.8.3.1 AdGroupDescription

Template for the description of AD groups generated by AM. The {0} placeholder will be replaced by the complete UNC path. The {1} placeholder will be replaced by the rights granted to this group for the indicated file system.

13.8.3.2 AllowMissingFolderRenamingInDatabaseByOwners

If the job InitializeFolderStructureScan cannot find a managed folder, it will be marked with the respective icon in the tree view and the administrator may either remove it from Access Managers´ database (if he is sure the folder was removed) or – if the folder was simply renamed – select another folder which he knows it is the missing one. With this option, the latter possibility can be given to folder owners also (see chapter 4.3.2.6).

13.8.3.3 CleanUpOutdatedFilesUseCreationTime

If activated, the job *CleanUpOutdatedFiles* will use the file creation date instead of the last access date for determining the age of a file.

13.8.3.4 DefaultAdGroupNamingPatternGlobal

Default value for naming global AD groups of managed folders for newly created Folder Collections, can be individually changed afterwards (chapter 8.2.1.3).

13.8.3.5 DefaultAdGroupNamingPatternLocal

Default value for naming local AD groups of managed folders for newly created Folder Collections, can be individually changed afterwards (chapter 8.2.1.3).

13.8.3.6 DefaultBrowseGroupForShares

Suggests a browse group when a new folder collection is created.

13.8.3.7 DefaultCleanUpPeriodInDays

The default setting for the number of days that a file can remain unused before it will be deleted by the CleanUpOutdatedFiles job.

13.8.3.8 DefaultInheritRights

The default setting for the Inherit Rights option when creating new rights folders.

13.8.3.9 DefaultSelfServiceEnabled

The default setting that will be used for the visibility of newly created Rights Folders in Management Portal when creating new rights folders.

13.8.3.10 FileserverDefaultPermissionIsWrite

If this option is enabled, the write permission is the default setting when manually assigning file system permissions, otherwise it is the read permission.

13.8.3.11 FolderNameBlacklist

This list holds any number of full folder paths (UNC path notation) or partial paths that are ignored and hidden in AM tree view when a folder scan job is executed (see chapter 11.6.4.1). If a full folder path is specified (i.e. \\filer01\share\folder-01\), only this distinct folder with its subfolders is excluded. If only part of a folder name is given (i.e. \folder-02\), all paths are excluded that contain it, like \\filer01\share\folder-02\, \\filer01\share\folders\folder-02\, \\filer02\sharename\folder-02\.

Please note:

- A leading and trailing backslash (\) is mandatory.
- All path entries are case-sensitive, meaning that \folder\ will only affect path names with "folder" but not "Folder".
- This function only works for unmanaged folders. Rights Folders cannot be ignored as well as unmanaged folders that contain further Rights Folders.

13.8.3.12 MaxNestedFolderDepthSSP

The maximum number of folder levels that rights folders can be nested for queries or creation using the Management Portal. Set this value to 0 to prevent nesting. A value greater than 99 will disable this check. For example, a value of 1 means that a new rights folder may only be nested one level below an existing rights folder and no deeper.

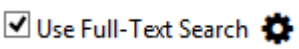
13.8.3.13 MaxTokenSize

The maximum size allowed for a Kerberos user token. This setting is only used within AM to avoid conflicts using the MovePermissionsToInferiorLevel job. The value should be a little lower than the current maximum token size defined in AD.

13.8.3.14 OwnershipTakeoverAuditOnNewShares

Default value for option *Ownership mode* (chapter 8.2.1.4.2) in conjunction with option *OwnershipTakeoverOnNewShares* (chapter 13.8.3.16). This activates logging in the database of taking over ownership in the file system.

13.8.3.15 OwnershipTakeoverAuditUseFullTextSearch

This option will activate the internal use of a full text search algorithm on the database when the report *Assumption of Ownership of resources by folder* is used and a specific folder path is searched by clicking button *Search resource*. Using this option is advised only if a large number of files (more than a billion) was audited. After activation, a search index must initially be generated on the database. Use the gear icon to start the generation: 

Due to technical limitations, behavior of the folder search algorithm is different: the full text search will only find entered search strings at the beginning of a folder name whereas the normal search will find strings also within folder names. This will lead to different amounts of result records.

As the technical precondition for using full text search the optional package for full text search must be installed on the database server.

13.8.3.16 OwnershipTakeoverOnNewShares

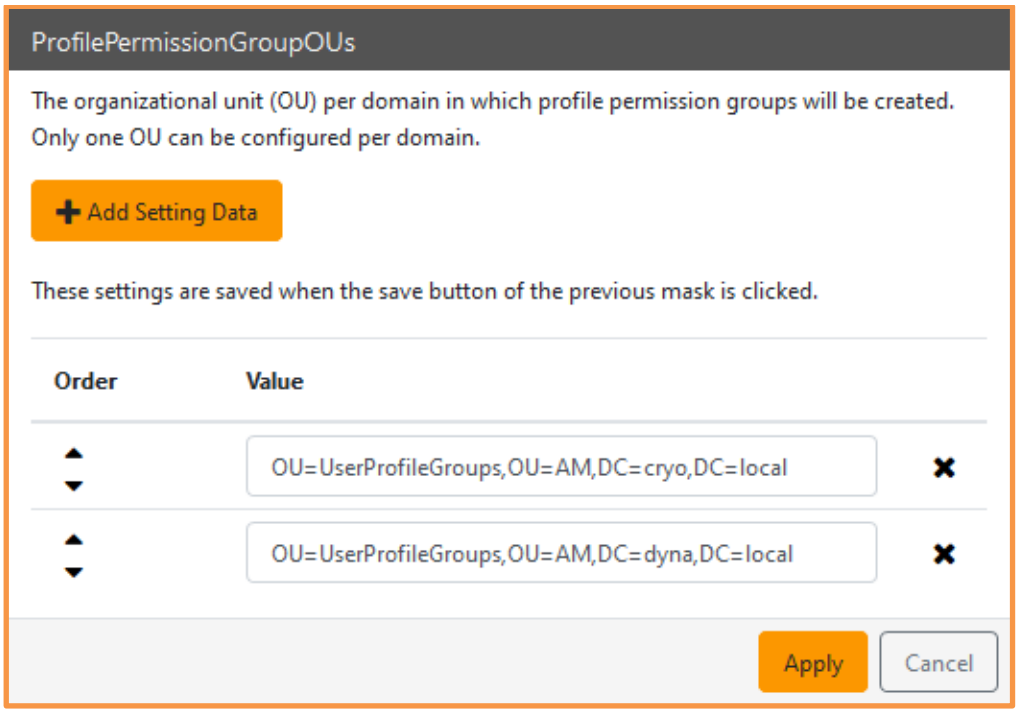
Default value for option *Ownership mode* (chapter 8.2.1.4.2) in conjunction with option *OwnershipTakeoverAuditOnNewShares* (chapter 13.8.3.14). This activates taking over ownership in the file system.

13.8.3.17 ProfilePermissionGroupNamingPatternGlobal, ProfilePermissionGroupNamingPatternLocal

If profile groups are used (see setting below), these settings define the naming scheme used for creating the AD groups. Parameter {0} is replaced by the domain of the file server holding the permitted folder. Parameter {1} is a counter AM increases for every distinct user profile. To ensure unique AD group names, both parameters are mandatory for the naming pattern.

13.8.3.18 ProfilePermissionGroupOUs

If profile groups are used (see previous setting), this setting is used to define the AD storage location (OU). Specify exactly one OU per file server domain managed by AM.



When the Profile Administrator permits a user profile on a folder of a server located in domain CRYO, AM will create the corresponding AD groups within the OU of that domain. If another folder is added of server in domain DYNA, further AD groups are created within the respective OU. Profile members (user accounts) are added to the local or global groups with respect to their domain membership.

13.8.3.19 ProfilePermissionGroupsEnabled

This option toggles permission management by using specially created AD groups for user profiles as the standard technique. Technical implications of this approach are described in chapter 13.3.

All user profiles that created after changing this option follow the set technical approach. Previously created user profiles are still functioning using the former technique and will show a hint concerning this matter. They may be switched to use the currently set technology manually by the Profile Administrator, thus AM supports usage of both techniques at the same time. The profile administrator can tell from the color of the profile symbols which technique a profile uses:

- Orange: the profile uses directory groups
- Black: the profile uses its own profile group

Internal settings for the new Profile AD groups are described above, including naming pattern and storage location. Profile AD groups are created once a user profile is permitted on at least one folder.

When a user profile is deleted by a Profile Administrator, the associated profile AD groups are removed from file system and are deleted automatically without further notice.

Do not use profile AD groups outside AM for your own purposes.

Special case when using a classification with set option *Group of authorized users*:

As described at the end of chapter 7.2, with profile groups the user permissions are different compared to not using profile groups, if a profile contains at least one folder that reduces the possible permittable users based on a classification having an authorized user group defined.

13.8.3.20 RegexFolderNameValidation

Validation rule for new folder names. Knowledge about regular expressions is recommended for changing this setting to meet internal needs. Also, enter the English and German text that will be displayed if validation of a folder name fails.

If, for example, also a whitespace character and German Umlauts shall be allowed, having a length between 2 and 30 characters, use this expression:

```
^[A-Za-zÄÖÜäöüß0-9-_]([ ]?[A-Za-zÄÖÜäöüß0-9-_]){1,29}$
```

13.8.3.21 ResponsiblesInfoFileName

The name of the info file that contains the list of Responsibles who can assign permissions and that is stored in the parent directory of a rights folder. If the parent folder contains more than one rights folder (meaning there are several rights folders at the same level), the respective folder information will be stored in the specified file.
The structure and layout of the file can be adjusted using the Agent Template section of the Mail Templates window.

13.8.3.22 RetainADGroupsAfterRightsFolderRevocation

If this option has been enabled, the AD groups assigned in the file system will be retained when the Management Portal is used to revoke the rights folder status for a folder.

13.8.3.23 ShowAdditionalManagedFolderSidsDialog

This setting enables you to switch on / off the option of being able to authorize additional SIDs as an administrator at the level of a folder collection (see chapter 8.3.2).

13.8.3.24 SkipDirectoriesWithReparsePoints

Activating this option keeps the job MaintainAccessPermissions (incl. sub-objects) (see chapter 11.6.4.5) from following so-called Junctions / ReparsePoints which are pointing to another folder. This avoids problems with unintended endless loops where Junctions are accidently referencing in circle on themselves.

13.8.4 Module "SharePoint Management"

13.8.4.1 SharePointDefaultPermission

With this option you can specify the permission that set by default when manually assigning SharePoint permissions, i.e. *write*.

13.8.4.2 SharePointDefaultSelfServiceEnabled

Default setting for the *Self Service Enabled* flag when defining a new managed site.

13.8.4.3 SharePointGroupDescription

Template for description of SharePoint groups created by AM. Placeholder {0} is replaced with full URL, {1} is replaced with the SharePoint permission granted to this group.

13.8.4.4 SharePointOnlineDomainMap

Maps NETBIOS names to DNS names to translate user ids to a SharePoint Online compatible format, e.g. configure DOMAIN:mydomain.onmicrosoft.com so DOMAIN\user.name becomes user.name@mydomain.onmicrosoft.com. Multiple NETBIOS:DNS pairs can be configured, separated by ";". Please note that only 1:1 mapping are allowed, meaning you cannot map the same NETBIOS name to several different DNS names or vice versa.

13.8.4.5 SharePointSiteNameValidationRegEx

Validation rule for names of new / renamed SharePoint sites.

13.8.5 Module "Fileserver Accounting"

13.8.5.1 CostCenterLdapFilter

LDAP filter expression to determine the relevant entries from the folder.

13.8.5.2 CostCenterLdapPass

Password for LDAP access.

13.8.5.3 CostCenterLdapProperty

LDAP property that contains the name of the cost center.

13.8.5.4 CostCenterLdapString

The LDAP server for importing cost centers. The format is LDAP://server:portnumber

13.8.5.5 CostCenterLdapUser

User account for LDAP access.

13.8.5.6 CostCenters

Cost centers are displayed and managed in this dialog. In addition to the IDs for the cost centers (column *Cost Center*) and the descriptions, the table also displays the manner in which they entered the AM system (*Source* column) and a counter indicating by how many accounting folders they have already been used.

Cost centers cannot be edited. They can be re-created (*Add* button) or deleted (Cross icon) if they have been manually added to the system (source is *manual*) and have not currently been assigned (the *Assignment Count* is 0).

The cost centers known through the company can be periodically imported and updated from Active Directory through a scheduled *CostCenterImport* job. AD connectivity data will be entered in the administrative settings (see previous *CostCenter** items). Such costs centers will have the *imported* identifier as their source and cannot be manually deleted.

13.8.5.7 DefaultPricingItemId

Default ID for calculating pricing items for new accounting folders.

13.8.5.8 ExportPath

Path for storing accounting data after a successful accounting process.

13.8.5.9 GroupExportData

The template for the export file for group-related accounting data. Variables provided by AM will start with a dollar sign ($). Use semicolons (;) to separate the columns.

13.8.5.10 NoChargeBelow

Costs will not be invoiced when the amount calculated is less than this value (in €).

13.8.5.11 PricingItems

Pricing Items are displayed and managed from this window. In addition to the IDs for an item, the table also displays the name, the price per unit (1 gigabyte of storage space) and a counter indicating by how many accounting folders it has already been used.

Pricing items can only be deleted if they have not been assigned (the *Assignment Count* is 0). However, they can be edited at any time except for the ID because it is used for the unique assignment.

13.8.5.12 UserExportData

Template for the export file for group-related accounting data. Variables provided by AM will start with a dollar sign ($). Use semicolons (;) to separate the columns.

13.8.5.13 UserWhitelist

The users that should be excluded from accounting for Home directories are managed from this window. Storage space in the Home directory that is used by the user accounts listed here will not be used in accounting process. Users can be added and deleted from this list at any time.

13.8.6 Module "Password Reset"

As this module can also be purchased and used independently of Access Manager, its functionality is described in a separate document. For configuration within AM, following parameters exist:

13.8.6.1 PasswordResetApiKey

This is the authorization key Access Manager uses to legitimate itself against the AMPR interface. The key is provided by AMPR.

13.8.6.2 PasswordResetApiTimeoutMs

Waiting period for requests against the AMPR interface in milliseconds.

13.8.6.3 PasswordResetUrl

Address to contact the AMPR service. At least AMPR version 7 must be installed.

13.8.7 Module "Easy Desktop"

This module extends permission application ability onto a user´s client machine and needs to be installed on all such computers. The functionality is described in a separate document. For configuration within AM, following parameters exist:

13.8.7.1 EasyDesktopEnabled

This option will switch on or off the function of applying for access permissions and new folders on the ED client installations.

13.8.7.2 EasyDesktopManualPath

The context menu item "Help" will open the resource specified here. The resource may be of any type (web link, text document, video tutorial etc.). Please make sure the linked resource is available from the client computer.

13.8.8 Module "Identity Management"

To create the AD accounts associated with the identities, the IDM module requires a specification for the form of some entries, such as the login name or e-mail address.

Basically, there are two options for this: A fixed pattern, according to which the IDM module creates the respective entries, or a free text field in which the appropriate entries must already be made when creating the identity in the system.

To set a pattern, navigate to the system settings in your access manager. Of interest here are only the settings in the "Identity Management" section that start with the prefix *IdmPattern*.

Menu:
Administrator → Settings → System Settings → Identity Management

13.8.8.1 Method „Free text"

If you choose to use the free text method, leave the input field of the respective entry empty. In this case, you will find free text fields for the corresponding entries in the affected identity dialogues. Future personnel managers will have to manually choose and input those AD account entries here.

The IDM module will provide support to the extend, that your input will be validated on syntactical correctness and uniqueness within the Active Directory when pressing the "Verify"-button. If an entry, which must be unique, has already been assigned, you will be informed of this. If there are any problems with the syntax or if the input has too many characters, the IDM module will try to fix it on its own. All invalid characters will be removed or replaces with underscores.

Note, however, that the home directory, mail nickname, and SMTP address entries cannot be entered as free text fields but **require** a pattern instead.

13.8.8.2 Method „Pattern"

If you decide to use the pattern method instead, you can specify an expression for any fields here. These fields are later automatically filled with the appropriate content and cannot be changed by the personnel manager.

Each expression must use at least one variable and result in a character string at the end. The syntax for this corresponds to PowerShell code with a series of variables that are read from the associated identity. Several methods are available for processing these character strings:

- **ToString** – Conversion of non-character strings (e.g., a number or a date) for use in the pattern expression
- **ToLower** – Converts all letters in a string to lowercase
- **ToUpper** – Converts all letters in a string to uppercase
- **Substring(a,b)** – Extracts a b-characters-long substring starting at position a
- **Replace(a,b)** – Replaces each occurrence of a with b in a string
- **Length** – Determines the length of a character string
- **IndexOf(a)** – Finds the position of the first occurrence of a in a string
- **LastIndexOf(a)** – Like IndexOf(a), however, finds the last occurence
- **Min(a,b)** – Math-Method: Returns the smaller number of a and b

The use of other, unauthorized methods leads to an error message which prevents access to the IDM dialogs!

The IDM module also supports you here insofar as syntax errors that can occur here due to the variables are substituted as described above. However, it is necessary that the length restrictions are adhered to here. Otherwise, the result will be truncated to the maximum length. Entries that must be unique are adjusted by the IDM module if a calculated value is already assigned. The IDM module always appends a globally incremented number to the value.

The following variables are available to you when selecting the pattern expressions:

- **$gn** – The first name of the identity
- **$sn** – The last name of the identity
- **$ti** – The title of the identity
- **$sam** – The calculated or free-text-entered login name
- **$cn** – The calculated or free-text-entered common name
- **$disp** – The calculated or free-text-entered display name
- **$upn** – The calculated or free-text-entered user principal name
- **$uid** – The globally incremented number mentioned above, hereby mandatory

When choosing the expressions, only the variables of known, i.e., already calculated, values are available.

In addition, the variable **$tmp** is always available to you. You can fill and process this variable like a normal variable in PowerShell. Note, however, that the expression itself must still result in a character

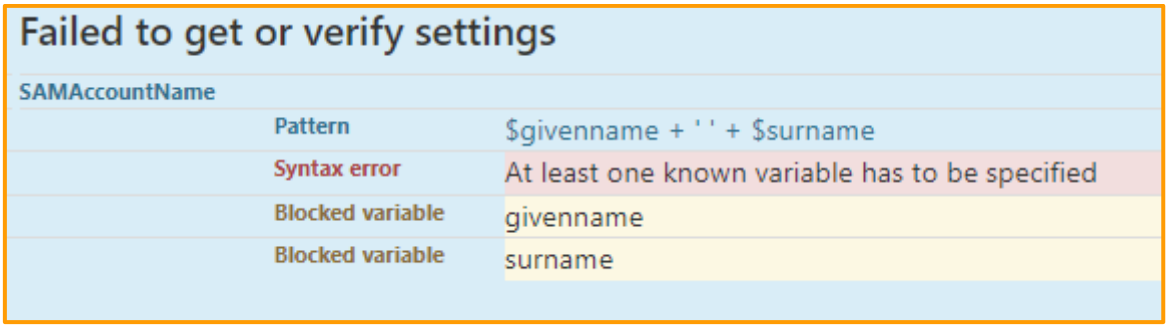
string. If you calculate the value inside the variable, you still have to eventually print it out. The globally incremented number **($uid** variable) can also be used anywhere.

13.8.8.3 Updating the Patterns

If you want to update the patterns, you should make sure that the update takes place outside of active working hours. Active sessions with the IDM module are not aborted, but dialogs that were started before the update could lead to errors when sending.

In particular, this applies to switching between the patterns and free text field methods. A workflow created with an active pattern method will not have the necessary information after switching to the free text field method. This means that when implementing such a change, no more IDM workflows may be active, i.e., in progress or still in the approval process.

After setting or updating a pattern, wait a moment for the Access Manager Agent to propagate the information and be sure to verify that you can still access the IDM dialogs. If you try, you may be shown errors in the new patterns instead of the usual dialogs, but so will anyone else attempting to access an IDM dialog.



13.8.8.4 Example Entries

13.8.8.4.1 IdmPatternCommonName

The common name is the second calculated value and may only be 64 characters long at most. Additional to the variables for the login name, here you can use the latter as a variable, too.

Instead of variable processing of character strings as in the previous example, you can also specify the latter directly. The following pattern is a simple example of an expression that consists of only one character string. As shown, double or single quotation marks can be used for this:

```
"$gn $sn"
```

13.8.8.4.2 IdmPatternDisplayName

The display name can be a maximum of 100 characters long. Additional to the variables for the common name, you can use the latter as a variable here, too.

In the following pattern, PowerShell syntax is integrated into the string. For this it is necessary to put the code part in brackets and to put a $ sign in front of the opening brackets. It is thus possible to only integrate the title and an associated space if the title field is actually filled:

```
"$(if ($ti.Length -gt 0 ) {$ti + ' '})$gn $sn"
```

13.8.8.4.3 IdmPatternHomeFolderName

The name for the home folder is limited to 100 characters. This pattern, as well as all the following except for the SMTP address, can use the display name itself in addition to variables. This means that all variables except the UserPrincipalName can be used.

If a profile folder has been set, it receives the same name as the home folder.

For the home directory pattern, it's best to use an already computed entry, such as display name or login name, which gives the pattern a simple form of, say, $disp. To further establish the possible syntax, here is an example pattern that reduces the display name to lowercase and removes any trailing dots:

```
$tmp = $disp.ToLower(); while ($tmp.LastIndexOf('.') -eq $tmp.Length
- 1) {$tmp = $tmp.Substring(0, $tmp.Length - 1)}; $tmp
```

13.8.8.4.4 IdmPatternMailNickName

The mail nickname (also: alias) and the following SMTP address are only relevant for identities for which an Exchange mailbox is also created. It is limited to 64 characters. All variables except for the user principal name can also be used here.

Usually, using the login name directly or a *$gn + $sn* composition makes sense here. The following example uses the globally incremented number, which is otherwise only added to the end of the value in the case of duplication, and always appends it in the middle instead:

```
$gn + $uid + $sn
```

13.8.8.4.5 IdmPatternSamAccountName

The login name is the first calculated value and can be a maximum of 20 characters long. Only the first and last name and the title of the identity are available as variables. Only a few special characters and no accents or umlauts are permitted in the login name. If there are such illegal characters in the variables, they are automatically substituted. Here and in the following calculated values, LDAP-search-control-characters like **) * (&** should be omitted.

The following pattern forms the login name in the form "firstname.lastname" but reduces the number of characters for the two names to 8, leaving at least 3 characters for an appended number if there are duplicates:

```
$gn.ToLower().Substring(0, [System.Math]::Min(8, $gn.Length)) + '.' +
$sn.ToLower().Substring(0, [System.Math]::Min(8, $sn.Length))
```

13.8.8.4.6 IdmPatternSMTPAddress

For the SMTP address, only the UserPrincipalName is available, and we recommend that you restrict the pattern to exactly that:

```
$upn
```

13.8.8.4.7 IdmPatternUPN

The user principal name is limited to 64 characters in the prefix (before the @ sign) and 48 characters in the suffix. The pattern specified here only affects the prefix, the suffix depends on the assignment in the respective organigram position. All variables can still be used here, except for the UserPrincipalName itself.

Often the login name *$sam* is simply used here, in the following example we are bothered by potential dots in this, which is why we remove them without replacement:

```
$sam.Replace('.', '')
```

13.8.8.5 Configuration

The IDM module needs to be configured after installation before you can start using its functions.

You have two options here: an import of existing data in an infrastructure and a manual configuration.

13.8.8.5.1 Configuration via Import

The import is used for the automatic configuration of the IDM module. With its help, it is possible to automatically read out most of the configurations that the IDM manages within the organization chart and the identities in it and to integrate them into the IDM module. All identities within the selected AD OUs are also imported, including their Exchange mailboxes, if any.

The IDM import requires a complete installation of the Access Manager and the Identity Management module. You need the login data of your AM/IDM service account and your Exchange server remoting account to carry out the process. You also need some information about your infrastructure:

- The AD OUs relevant for identity management including Relative Distinguished Name (RDN)
- A plan for building the organizational chart
- The names of the domains in which identities, exchange servers, or shares to be managed by the IDM are located

The import is carried out on the IDM server under the service account. The next step to address is preparing your organization chart and your OU-RDNs in cooperation with our qualified service engineers and implementing the import.

Subsequently, you should check the created configurations. Have the correct file system roots been created, and do you want to create additional ones? What about additional OUs for identity management or a new Exchange Server? You can find out how to create these configurations in the following chapter, but our service engineers will be happy to help you here as well.

Once the import has finished, the configuration still needs to be completed. More precisely, you are still missing UPN suffixes, company addresses and calculation patterns. Once all configurations have been created, they still must be assigned in the organizational chart. Before you do this, however, you should check the organizational chart again for correctness and completeness.

13.8.8.5.2 Manual Configuration

The manual configuration consists of two core aspects: the administrative data and the organigram. The former includes providing the necessary information for using the required infrastructure, in particular the Active Directory, the relevant file system directories, and the Exchange Server. The organigram, on the other hand, models your organizational structure. Here identities are assigned and adjusted according to the configuration, authorized and more.

The configuration of the administrative data takes place entirely in the system settings. Open the Identity Management tab here. First check the above settings with the prefix *IdmConfiguration* for correctness.

You can then start configuring the administrative data. The relevant dialogs begin with the prefix *IdmDialog*. Note that all configurations made here require a match in your infrastructure. A configured Exchange Server that does not actually exist will cause errors in operation.

The configuration of home and profile folders as well as postal addresses are optional. If you do not configure those, created identities will not receive user directories and the corresponding fields in their AD accounts will not be populated.

Description and IDM-internal name fields do not require any content representation in the infrastructure. They only serve for identification in the dialogs of the IDM module.

Configuration Dialogs (bold) and their input fields:

Label	Explanation and Example
IdmDialogDomain	Domains in which identities are to be created or Exchange Server or file system roots are to be managed
DNS Name	DNS name of the domain: *companydomain.org*
Base DN	Distinguished name of the domain: *dc=companydomain,dc=org*
NetBios Name	Domain NetBIOS name: *companydomain*
Description	An IDM module internal description of the domain. Cannot be viewed by end users and is only relevant in configuration dialogs
Parent Domain	If you want to integrate nested domain structures, you can select a higher-level domain here. If not, leave this field blank
IdmDialogAdOu	Organizational units in Active Directory in which identities are to be created
Name	IDM internal designation of this configuration
Domain	Selection of the domain previously configured in IDM in which this OU is located: *companydomain*
Area	Choose between normal user OU and tombstone OU. Identities that have been permanently deactivated are stored in the latter
Display Name	Name of the OU: *Users*
RDN	Relative distinguished name of the OU. Enter the OU fragment without DC part here: *ou=Sales,ou=Users,ou=HQ*
Description	An IDM module internal description of the OU. Can be viewed by administrators and organizational chart management and is only relevant in configuration dialogs
IdmDialogExchangeServer	Exchange Servers in which mailboxes are to be created for new identities
Display Name	Name of the Exchange Server: *Exchange*
Description	An IDM module internal description of the Exchange Server. Cannot be viewed by end users and is only relevant in configuration dialogs

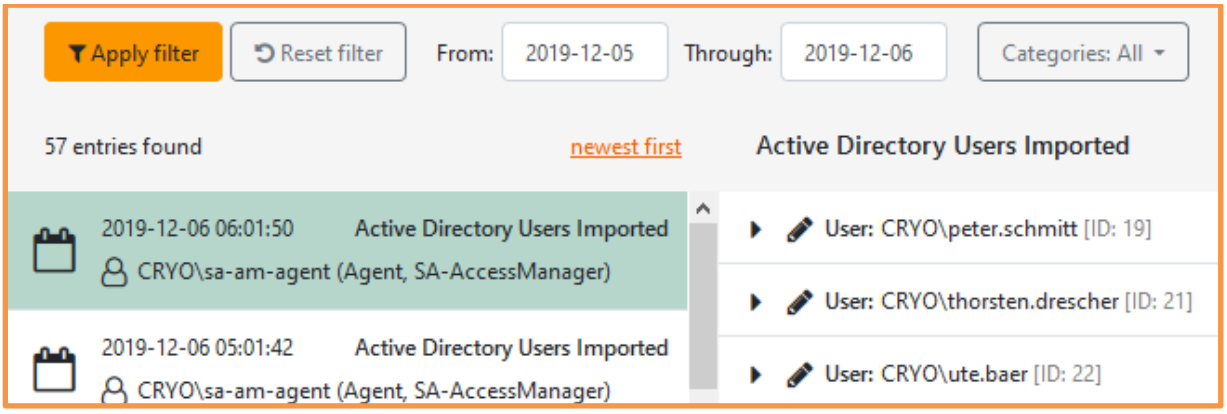
Server NetBios Name	NetBIOS name of the Exchange Server: *exchange.companydomain.org*
Domain	Selection of the domain previously configured in IDM in which this Exchange Server is located: *companydomain*
Authentication Type	Choice of authentication type. Must be supported by the Exchange Server
Login	Login name of a privileged Exchange Server account as described in the Setup Prerequisites manual
Password	Unencrypted password of the privileged account
IdmDialogFileServiceRoot	File system directories (shares) in which managed identities can have a home or profile directory
Domain	Selection of the domain previously configured in IDM in which this file system directory is located: *companydomain*
Name	IDM internal designation of this configuration
Description	IDM module internal description of the file system directory. Cannot be viewed by end users and is only relevant in configuration dialogs
File Server	The server where this file system directory resides: *dataapp.companydomain.org*
Admin Path	Path to the directory under which the user directories should be created. Requires appropriate authorizations for creating and editing in the share: *adminshare01\Userdir\home*
User Path	Path to the directory under which the user directories should be created. If there are no special share permissions, this can be identical to the administrative path: *share01\Userdir\home*
Area	Here you can choose between home and profile directories. If both are configured, new identities will also get both directories
IdmDialogPostalAddress	Postal addresses of branches to which relevant identities are to be assigned
Name	IDM internal designation of this configuration
IdmDialogUPN	UserPrincipalName suffix to be assigned to the managed identities AD account

Name	IDM internal designation of this configuration
Policy Values	The desired UPN suffix without '@' - Pay attention to the maximum length of 48 characters!

Before you start configuring the organigram, you can now configure the patterns. The fields relevant for this are located directly under the dialogs in the system settings and have the prefix *IdmPattern*. You can also carry out this configuration at a different time, but all settings should be made before you start productive operation of the IDM module. You can find more information about the templates in chapter 13.8.8.2. You can also specify the recipients of the onboarding emails here. You can choose from the team Responsibles assigned in the organization chart and the requestor. Finally, you need the *Organigram Administrator* system role before you can proceed to the next step.

13.9 Audit

Menu:
Administrator → Logging → Audit



The *Audit* page provides a multi-level list of all actions that have been performed in AM. Here you can see in detail which activities were carried out at which time, who initiated them and which objects were affected. For a better overview and to quickly find certain information, a filter and a sorting can be applied.

The structure of the page is divided into three sections:

- Top: filter settings
- Left: List of activities
- Right: Details of a selected activity

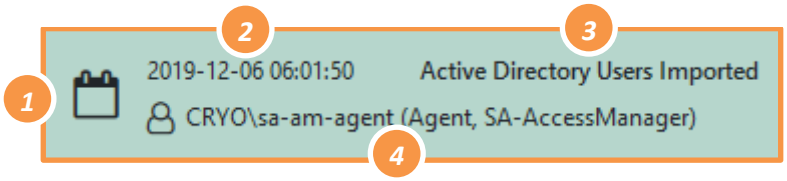
13.9.1 Filter Settings

The filter area allows to restrict the time for the activities to be displayed (specified by the criteria "from" - "through"). Since all activities are assigned to a specific category, the individual categories can be selected and deselected. When filtering by clicking the *Apply* button, only activities of the selected categories are displayed.

The *Reset* button resets all filter settings to their default values, i.e. the period covers only yesterday, and all categories are activated.

13.9.2 List of Activities

All activities that meet the filter criteria are listed in this area. Each entry displays the following information:



1) The icon indicates if the activity was triggered manually by a user or automatically by a scheduled task.
2) Date and time of the activity (UTC)
3) The activities category
4) The user account that triggered the activity

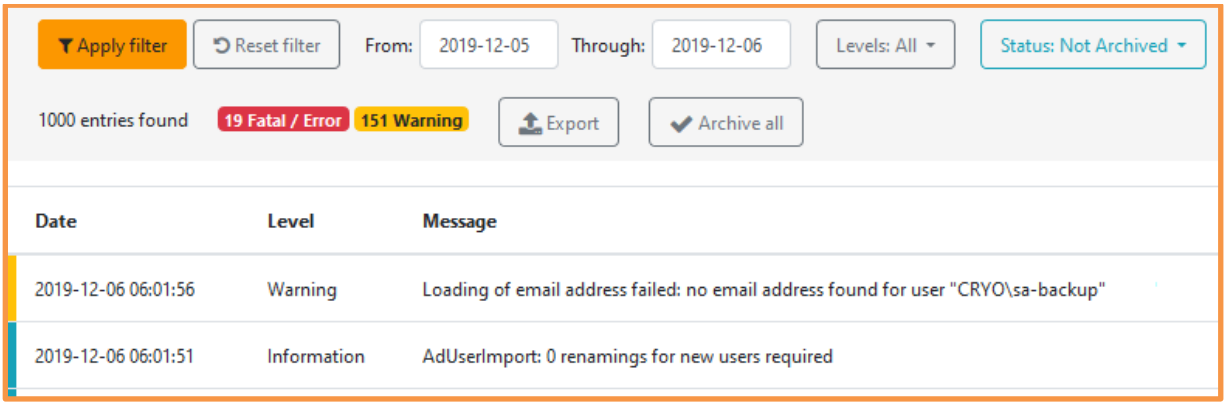
13.9.3 Details of Activities

This area contains a list of all objects affected by the selected activity. Each object can be clicked and then expands its view by a table which contains the new and old value for the altered object properties.

13.10 Error Logging

Menu:

Administrator → Logging → System Log



The *System Log* shows all messages that arise, stating date, severity and description.

A message may be flagged as *Archived* by clicking its checkbox. It immediately disappears from the list but can be reviewed again by selecting *Status: Archived*. Upon your confirmation, the *Archive All* button will flag all messages that apply to the current filter settings.

The *Export* button creates a CSV file, containing all messages that apply to the current filter settings. In case of issues with your installation, you can hand over this file to a BAYOONET AG Service Engineers.

Please note that the Error File may contain sensible data of your company.

13.10.1 Alternative logging to Grafana Loki

If the Access Manager database is no longer used for logging (new standard for version 2023.1), you can not only have the agents write to local files, but also to the OpenSource product **Loki** of **Grafana**.

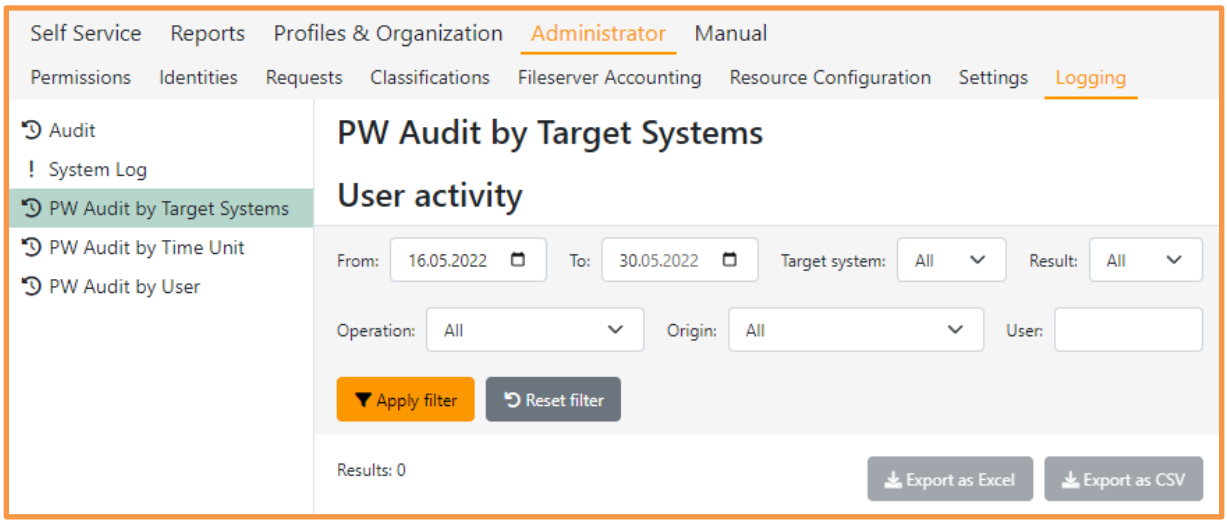
After you have configured the connection to Loki (see Chapter 13.8.1.22 ff), Access Manager reads the entries from there and displays them without replicating them in its own database.

Except for the archiving option, all filter options are still available, and you can also limit the number of entries displayed (*Max. results to display*). The *Grafana Loki Query* input field contains the limitation to Access Manager log entries and usually does not need to be adjusted unless you are using multiple AM instances (e.g. an additional TEST system) that all log to the same Loki instance.

13.11 Password Audit

This function is available only if application AMPR is present and if you own the *AMPR role Administrator*. In the Administrator area *Logging*, some more auditing options are available. You may display reports about all password related user activities for a distinct timeframe. Audit reports focus on the following:

- Password Audit by Target Systems
- Password Audit by Time Unit
- Password Audit by User



These menu items provide the functionality of the AMPR application.
Please find a more detailed description in the corresponding manual.

14 GUI Customization Options

Access Manager provides the ability to customize the user interface to suit the customer(s).

The user interface design has been implemented using established web technologies like HTML, CSS and JavaScript and provides the ability to overwrite the existing styles. Knowledge about working with the indicated technologies is required. Upon request, BAYOONET AG can be contacted to make such adjustments or provide support for their implementation.

Please note that user customizations are not supported and are applied at your own responsibility. It cannot be guaranteed that current customizations will still work flawlessly after an Access Manager update. In case, please check your codes for possible adaptions.

14.1 Files and Storage Locations

The user interface for the Management Portal is modified on the AM server in the respective IIS directory. If the default installation directory was used when installing AM, the local directory on the server will be

`C:\inetpub\wwwroot\AccessManager\ssp\wwwroot`

Here, a folder named `Customization` exists and in it the text file `custom.css` for graphical changes and `custom.js` for functional changes via JavaScript Code. You may edit these files using a simple text editor.

An additional sub-directory, `Images`, is available under the `Customization` directory for internal resources, such as company logos.

The following sections will provide several examples of what can be entered in the `custom.css` file such as for replacing the AM logo with an internal company logo or for hiding certain screens.

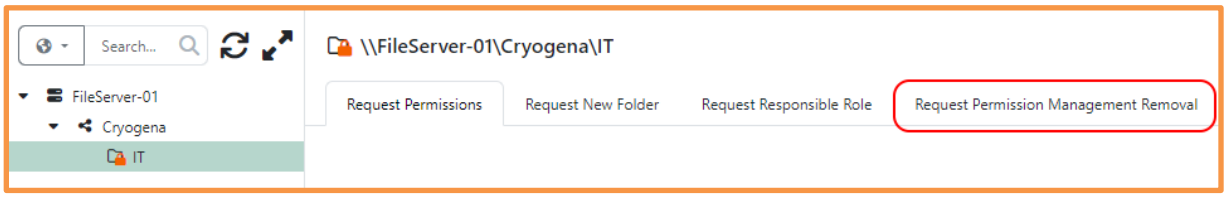
14.2 Company Logo

The logo is always depicted using a height of 22 pixels. The width will be scaled to this in relation to the window. In order to keep the file size as small as possible, and thereby allow web pages to be loaded as quickly as possible, the image file should be scaled to this height in advance using a graphics editor. Note the width resulting from the scaling operation. Copy the image file (in PNG format) to the Images directory with the name, `company_header_logo.png`, and make the following entries in `custom.css`:

```
.main-header-logo {
  background-image:url(/Customization/Images/company_header_logo.png)
!important;
  width: 77px !important;
  background-repeat: no-repeat;
  background-size: contain;
}
```

Replace the number highlighted in red (77) using the previously determined image width; please note that the “px” literal is mandatory and is required to directly follow the image width.

14.3 Hiding individual Elements



The *Request Permission Management Removal* option usually appears when selecting a managed location. The following code will hide the option.

This code hides the option for managed **folders**:

```
/* Hide "Self Service/Requests/[Folder]/Request Permission Management Removal" */
body.controller-filesystemrequest ul.nav-tabs>li.nav-item:nth-last-child(1) {
  display:none !important;
}
```

14.4 Extended Functionality with JavaScript

While using `custom.css` to alter the visual representation of the GUI, `custom.js` offers the possibility to extend and change functionality of the Access Manager User Interface (surprisingly, this includes simple alterations of text strings). The file already contains several commonly needed default functions you may use for your own purposes.

AM supports plain JavaScript / ECMA-Script (version support is browser-dependent) and jQuery Version 3.6.0.

For reliable separation of custom functions, the scope "custom" is defined. All functions and variables must make use of it. The factory-provided file defines the scope. Add your own functions in this scheme.

Call your functions within the `document.ready()` function.

14.5 Customizing Reports

14.5.1 Custom Logo

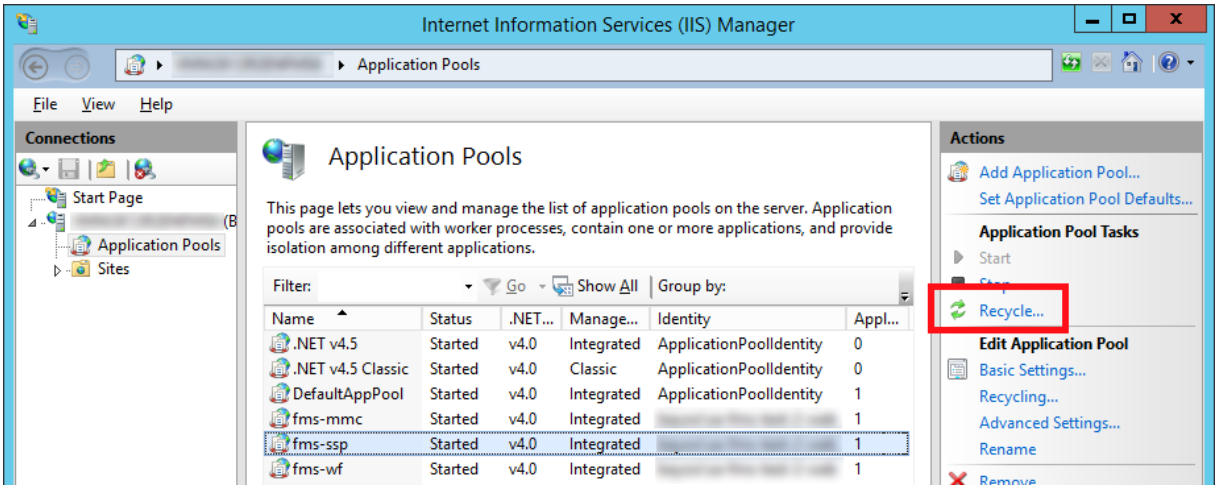
Reports may use your own company logo in the upper right corner, substituting the default BAYOOSOFT logo. The AM logo in the lower left corner **cannot** be exchanged.

You will need a graphics file in PNG format named exactly `report-header-logo.png`. Best display quality is accomplished with an aspect ratio of 4:1 (Width:Height). Images having any other form factor will be scaled appropriately, keeping the image´s aspect ratio.

Please copy your graphics file on the AM server into this folder:

`C:\inetpub\wwwroot\AccessManager\ssp\wwwroot\Customization\Images`

The new logo is available for all types of report once you have clicked *Recycle* on the Application Pool *fms-ssp* in IIS of the AM server:



14.5.2 Changing colors, fonts, layout

At the moment, customer changes of the visual representation are not supported. If you need customization, please contact our sales team.

14.6 Multi-Language support

By default, Access Manager supports the languages German and English. If you require additional languages, please contact our sales team. A simple import of additional language packs is not yet possible.

15 Examples of user-defined PowerShell Scripts

PowerShell scripts can fulfil many different tasks and their specific purpose depends on customer requirements. If your script accesses external systems using a different user account, for obvious security reasons you should store only encrypted user credentials in the script file (if stored in the file at all).

Please be aware that user-defined scripts are not supported. Use such scripts at your own risk. It cannot be guaranteed that your scripts will still work correctly after application updates, please check and adapt your code if necessary.

Execute user-defined scripts at your own risk. BAYOONET AG cannot be held responsible for any errors, defects or loss of data resulting from using such scripts.

15.1 Executing script after creating new AD user account

The following example shows only a debug output in a log file with a check of the variables passed by AM, after you have created a new user account. Save the script as a file (e.g. named `Create-AD-User-Logging.ps1`) on the agent server (Agent Group: *Default*) and call the file in the administrative settings (see chapter 13.8.1.57).

```
$scriptDir = $PSScriptRoot
$logFile = $scriptDir + "\" +
   $(([io.fileinfo]$MyInvocation.MyCommand.Definition).BaseName) + ".txt"
$computerName = [system.environment]::MachineName
$pshellVersion = [string]$PSVersionTable.PSVersion.Major + "." +
   [string]$PSVersionTable.PSVersion.Minor

$notset = "!!!NOT SET!!!"

# for debugging purposes: check which AM-provided variables are set
if ([string]::IsNullOrEmpty($firstName)) { $firstName = $notset }
if ([string]::IsNullOrEmpty($lastName)) { $lastName = $notset }
if ([string]::IsNullOrEmpty($initials)) { $initials = $notset }
if ([string]::IsNullOrEmpty($organizationalUnit)) { $organizationalUnit = $notset }
if ([string]::IsNullOrEmpty($samAccountName)) { $samAccountName = $notset }
if ([string]::IsNullOrEmpty($userPrincipalName)) { $userPrincipalName = $notset }
if ($(Test-Path variable:global:$userMustChangePasswordAtNextLogon)) {
   $isSetUserMustChangePasswordAtNextLogon = $userMustChangePasswordAtNextLogon
} Else {
   $isSetUserMustChangePasswordAtNextLogon = $notset
}
if ($(Test-Path variable:global:$userCannotChangePassword)) {
   $isSetUserCannotChangePassword = $userCannotChangePassword
} Else {
   $isSetUserCannotChangePassword = $notset
```

```
}
if ($(Test-Path variable:global:$passwordNeverExpires)) {
   $isSetPasswordNeverExpires = $passwordNeverExpires
} Else {
   $isSetPasswordNeverExpires = $notset
}
if ($(Test-Path variable:global:$accountIsDisabled)) {
   $isSetAccountIsDisabled = $accountIsDisabled
} Else {
   $isSetAccountIsDisabled = $notset
}
if ($accountExpirationUtc) {
   $isSetAccountExpirationUtc = $accountExpirationUtc.ToString()
} Else {
   $isSetAccountExpirationUtc = $notset
}

Write-Output "$(Get-Date): --- Create AD User : started" | Out-File $logFile -
   append
Write-Output "$(Get-Date):     PowerShell Version: $pshellVersion" | Out-File
   $logFile -append
Write-Output "$(Get-Date):     Host: $computerName" | Out-File $logFile -append
Write-Output "$(Get-Date):     Log File=$logFile" | Out-File $logFile -append
Write-Output "$(Get-Date):   firstName: $firstName" | Out-File $logFile -append
Write-Output "$(Get-Date):   lastName: $lastName" | Out-File $logFile -append
Write-Output "$(Get-Date):   initials: $initials" | Out-File $logFile -append
Write-Output "$(Get-Date):   organizationalUnit: $organizationalUnit" | Out-File
   $logFile -append
Write-Output "$(Get-Date):   samAccountName: $samAccountName" | Out-File $logFile -
   append
Write-Output "$(Get-Date):   userPrincipalName: $userPrincipalName" | Out-File
   $logFile -append
Write-Output "$(Get-Date):   userMustChangePasswordAtNextLogon:
   $isSetUserMustChangePasswordAtNextLogon" | Out-File $logFile -append
Write-Output "$(Get-Date):   userCannotChangePassword:
   $isSetUserCannotChangePassword" | Out-File $logFile -append
Write-Output "$(Get-Date):   passwordNeverExpires: $isSetPasswordNeverExpires" |
   Out-File $logFile -append
Write-Output "$(Get-Date):   accountIsDisabled: $isSetAccountIsDisabled" | Out-File
   $logFile -append
Write-Output "$(Get-Date):   accountExpirationUtc: $isSetAccountExpirationUtc" |
   Out-File $logFile -append
Write-Output "$(Get-Date): --- Create AD User : ended" | Out-File $logFile -append
```

16 Programming Interface (REST API)

If there is already a Service Management System in place and you want to provide your employees their familiar interface for permission requests, the *REST API extension module* offers you the possibility to provide a technical interface to the proven solution for automated access management. Implement your individual connection or rely on our available connectors.

Interface documentation is available if you assign yourself the additional system role *API User*. In main menu *Manual*, a new sub menu *API Documentation* is displayed.