
# Benutzerhandbuch

**Management Portal**

**Access Manager 2021.2**

**Handbuch für Endanwender und Administratoren**

BAYOOSOFT
MANAGEMENT SOFTWARE

# Inhalt

# 1 Glossar

| Begriff | Bedeutung |
|---|---|
| AM | BAYOOSOFT Access Manager |
| AMPR | Access Manager Password Reset – Modul zum Rücksetzen von Passwörtern |
| Ressource | Allgemeiner Begriff, welcher sowohl Berechtigungsordner als auch Berechtigungssites und Dritt-Elemente beinhaltet. |
| (Dritt-)Element | Eine logische Ressource wie z.B. ein Drucker, eine Web-Applikation oder ähnliches, auf die der Zugriff über eine AD-Gruppenmitgliedschaft geregelt wird (3rd-Party Management Modul). |
| Berechtigungs-verzeichnis | Ein Dateiordner, dessen Zugriffsrechte durch Access Manager verwaltet und überwacht wird. |
| Berechtigungssite | Eine SharePoint Seite, deren Zugriffsrechte durch Access Manager verwaltet und überwacht wird. |
| Freies Verzeichnis | Ein Dateiordner, welcher *nicht* durch Access Manager verwaltet wird. |
| Workflow | Der Ablauf einer Anfrage eines Benutzers, von seiner Anfrage bis hin zur Bearbeitung der Zugriffsberechtigung durch den Verantwortlichen. |
| AM-Agent | Ein Windows-Dienst, der die verschiedenen Arbeitsaufträge vom AM-Server entgegennimmt und abarbeitet. |
| AD | Active Directory |
| DFS | Distributed File System |
| ABE | Access Based Enumeration: Funktion des Fileservers, die einem Anwender nur die Objekte anzeigt, für die er Zugriffsrechte hat. |
| Share, Freigabe | Freigegebenes Verzeichnis auf dem Dateisystem |
| Site Collection | Sammlung von SharePoint Sites |
| Site | Eine SharePoint Site |
| Elementesammlung | Eine Gruppe von Elementen (3rd Party Management Modul) |
| NTFS | New Technology File System |
| ACL | Access Control List |
| API | Application Programming Interface, Programmier-Schnittstelle |
| IIS | Internet Information Server |
| MS SQL Server | Microsoft SQL Datenbank Server |
| EU-DSGVO | Europäische Datenschutzgrundverordnung |

# 2 Der Access Manager

## 2.1 Willkommen im automatisierten Berechtigungsmanagement

Das Management Portal dient dazu, Ihnen als Benutzer auf einfache Weise den Zugriff auf verschiedene Arten von Ressourcen zu geben. Hierunter fallen Verzeichnisse im Netzwerk und – bei Nutzung des jeweiligen Zusatzmoduls – Sites in SharePoint Site Collections bzw. Elemente von Elementesammlungen. Je nachdem welche Benutzerrolle Sie haben, können Sie bestimmte Zugriffsrechte und neue Verzeichnisse bzw. Sites beantragen oder sie können Ihnen auch ohne Antrag gewährt oder entzogen werden. Verschiedene Zusatzfunktionen runden die Unterstützung der notwendigen Verwaltungsaufgaben ab. Nicht alle der hier beschriebenen Seiten sind daher für alle Benutzer verfügbar; ihre Sichtbarkeit hängt von der jeweiligen Rolle des angemeldeten Benutzers ab.

## 2.2 Generelle Benutzungshinweise

Der Access Manager ist eine technisch hochentwickelte Client-Server Lösung, die modernste Software-Technologie einsetzt. Die Anforderungen an die Infrastruktur, speziell für das Management Portal, bleiben dabei dennoch moderat. Als Web-Anwendung benötigt das SSP lediglich einen aktuellen Web-Browser, keine zusätzlichen Plug-ins wie Adobe Flash Player, Microsoft Silverlight oder PDF Viewer. Unterstützt werden derzeit folgende Browser:

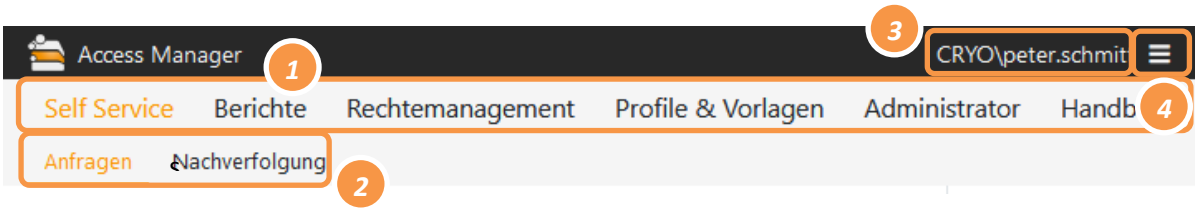
- Microsoft Edge
- Mozilla Firefox 70 oder neuer
- Google Chrome 78 oder neuer

Für andere und ältere Browser als die oben genannten kann eine korrekte Darstellung / Ausführung nicht garantiert werden.

*Sofern Sie einen Werbeblocker verwenden, stellen Sie bitte sicher, dass die Webadresse des Management Portals von einer Behandlung ausgenommen ist (Whitelisting), da sonst manche Funktionen nicht zur Verfügung stehen.*

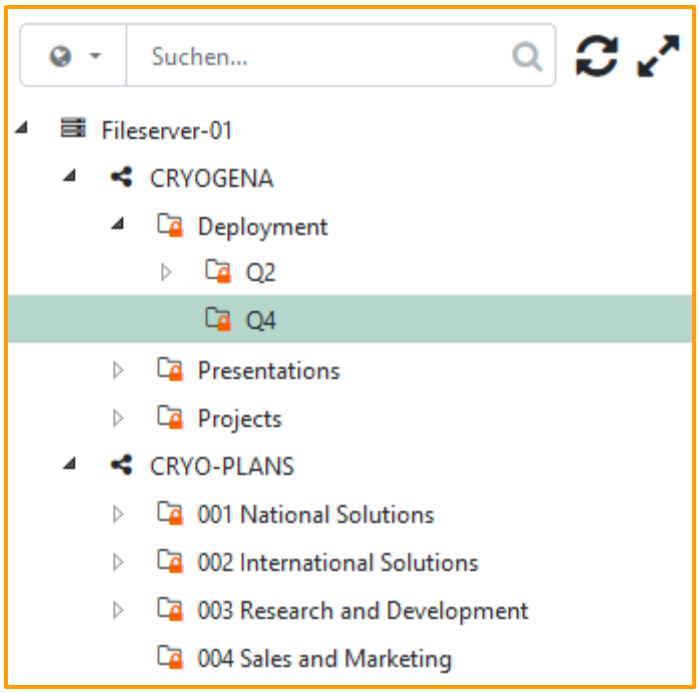
### 2.2.1 Die Benutzungsoberfläche

Das Self Service Portal hat einen grundsätzlichen Aufbau, der die Navigation innerhalb der Anwendung vereinfacht:




1) Das Hauptmenü – Über diese Menüpunkte gelangen Sie in den jeweiligen Arbeitsbereich. Es sind nur die für Sie freigeschalteten Einträge sichtbar, d.h. als reiner Endanwender ohne weitere Rollen werden Ihnen z.B. die Menüpunkte *Rechtemanagement* oder *Berichte* nicht angezeigt.
2) Das Untermenü – Hier erscheinen abhängig von Hauptmenü untergeordnete Menüpunkte, die auf weitere Seiten verweisen.
3) Der Kontoname (Windows) des angemeldeten Benutzers.
4) Das Burger-Symbol (drei Striche) öffnet ein Informationsfenster mit Versions- und Lizenzhinweisen. Hier stellen Sie auch die Oberflächensprache ein.

### 2.2.2 Der Ressourcen-Baum




Ein Ressourcen-Baum zeigt – ähnlich wie der Windows Dateimanager – eine hierarchische Ansicht der verfügbaren Verzeichnisse, SharePoint Sites, Berechtigungselemente usw. an. Ein Klick auf das kleine Dreieck-Symbol klappt die darunter liegende Ebene auf bzw. ein. Existiert kein Dreieck, enthält der Eintrag keine untergeordneten Elemente.

Zusätzliche Symbole zeigen an um welche Art von Ressource es sich handelt:

- Server
- Server (DFS)
- Share
- Berechtigungsordner
- Normaler Ordner (ohne Rechteverwaltung)
- Berechtigungssite
- Normale Site (ohne Rechteverwaltung)
- Elementesammlung (Icon kann frei gewählt werden)
- Berechtigungselement
- Benutzerprofil

#### 2.2.2.1 Multifunktionsleiste


Die Multifunktionsleiste über dem Ressourcen-Baum dient mehreren Zwecken:

Über die DropDown-Liste mit dem Globus-Symbol können Sie den Suchbereich bestimmen: Standardmäßig wird die komplette Ressourcen-Liste durchsucht. Haben Sie bereits einen Eintrag in der Liste angewählt (z.B. einen Server, ein Share oder ein Verzeichnis), so können Sie auch nur innerhalb dieser Ressource suchen.

Im Textfeld lässt sich ein Teil des Namens einer gesuchten Ressource eingeben. Sobald Sie beginnen Text einzugeben, wird die Liste der gefundenen Einträge angepasst, indem alle Einträge fett kursiv markiert werden, die diesen Namensteil enthalten.

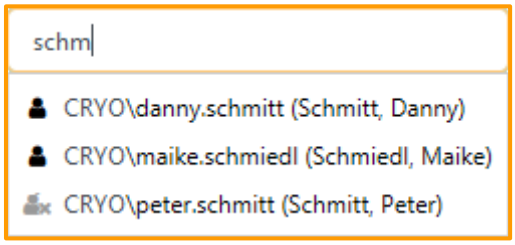
Darüber hinaus stehen Ihnen diese Funktionen zur Verfügung:

*Aktualisieren*: Ein Klick auf dieses Symbol aktualisiert den gesamten Ressourcen-Baum, wodurch eventuell neu erstellte oder gelöschte Ressourcen angezeigt bzw. entfernt werden.

*Aufklappen*: Dieses Symbol blendet von allen Ressource-Containern die erste Ebene ein und dient der schnellen Übersicht der enthaltenen Ressourcen.

### 2.2.3 Suche nach Benutzern

#### 2.2.3.1 Einzelne Benutzer

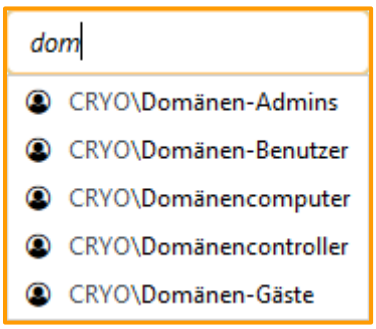



In Fällen, in denen ein bestimmtes Benutzerkonto bearbeitet werden soll – etwa um als Verantwortlicher jemandem zusätzliche Rechte zu geben – hilft die Benutzersuche beim schnellen Finden des korrekten Kontos.

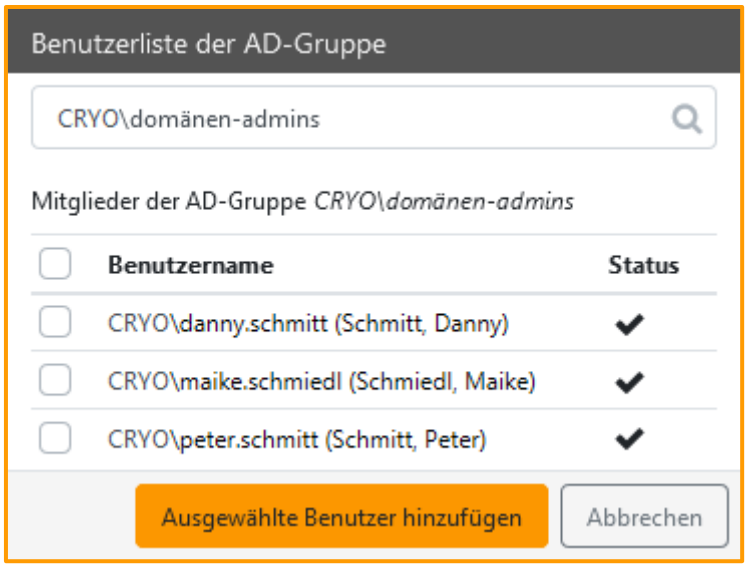
Im Textfeld geben Sie dazu einfach einen Teil des Namens ein (sowohl Anmeldenamen als auch Nachnamen werden durchsucht) und ab dem zweiten Zeichen zeigt der Access Manager eine Auswahl der dazu passenden Benutzerkonten. Durch weitere Buchstaben lässt sich die Auswahl einschränken. Wird das passende Konto bereits angezeigt, kann es auch direkt mit Maus oder Tastatur selektiert und übernommen werden.

#### 2.2.3.2 Mehrere Benutzer (Gruppensuche)

Möchten Sie mehrere Benutzer auf einmal hinzufügen, bietet sich das Gruppen-Feature an. Im ersten Schritt funktioniert die Suche identisch zur Einzelbenutzersuche mit dem Unterschied, dass Sie keinen Benutzernamen eingeben, sondern den Namen einer AD-Gruppe (die die gewünschten Benutzer enthält):




Die Gruppe wird zunächst wie ein einzelner Benutzer der Liste hinzufügt. Erst wenn Sie den Button *Speichern* drücken, werden die in der Gruppe enthaltenen Benutzer ermittelt und in einem Dialog zur Auswahl angezeigt:




In der Kopfzeile bietet eine Checkbox die Möglichkeit, alle Benutzer auf einmal an- oder abzuwählen um dann für einzelne Einträge gezielt diese Auswahl umzukehren. Es lassen sich jedoch nur solche Benutzer anwählen, deren Checkbox aktiviert ist (abhängig vom Status).

Die Statussymbole der Benutzerkonten haben folgende Bedeutung:

✔ Der Benutzer kann hinzugefügt werden.

Der Benutzer ist im Active Directory deaktiviert und kann nicht hinzugefügt werden.

### 2.2.4 Anzeige zusätzlicher Benutzerdaten

Je nach Verfügbarkeit können zu einem Benutzerkonto zusätzliche Informationen zu dieser Person anzeigt werden. Fahren Sie mit dem Mauszeiger über dem Benutzernamen. Wenn sich der Mauszeiger verändert, klicken Sie auf den Namen und es erscheint darunter ein Tooltip mit den Zusatzdaten:


Die angezeigten Informationen werden von der Administration bereitgestellt und können variieren. Zum Beispiel wird der Eintrag Telefon nicht angezeigt, wenn diese nicht hinterlegt ist. Zusatzinformationen sind nicht vertraulich und können von jedem Anwender gesehen werden.

## 2.3 Rollenkonzept

Jeder Benutzer des Management Portals erfüllt eine bestimmte Aufgabe und erhält dafür spezifischen Zugriff auf die erforderlichen Seiten gemäß der ihm zugewiesenen Rolle(n).

### 2.3.1 Rollenbeschreibung

Prinzipiell kennt der Access Manager drei grundsätzlich verschiedene Rollen:

- *Benutzer*: Ein reiner Anwender, der für seine Tätigkeit Zugriff auf verschiedene Ressourcen im Unternehmensnetzwerk benötigt. Er beantragt die gewünschten Zugriffsrechte oder stellt einen Antrag für eine neue Ressource über das Management Portal.
- *Besitzer*: Ihm obliegt die Verwaltung einer Ressource. Dazu gehört neben der Entscheidung über die Neu-Anlage oder die Entfernung von verwalteten Ressourcen vor allem die Bestimmung von Verantwortlichen (s.u.), das Reporting sowie ggf. (bei Einsatz des optionalen Moduls *Accounting*) die Spezifizierung der beteiligten Kostenstellen. Der Besitzer entscheidet explizit nicht über die Vergabe von Zugriffsrechten.
- *Verantwortlicher*: Er wird vom Besitzer damit beauftragt, Nutzeranfragen zur Vergabe von Zugriffsrechten auf den jeweiligen verwalteten Ressourcen zu bearbeiten (gewähren, ablehnen). Er kann auch ohne Anfrage Rechte vergeben / entziehen sowie Berichte erstellen. Der Verantwortliche hat explizit nicht die Möglichkeit neue Ressourcen anzulegen oder zu entfernen.

Darüber hinaus gibt es zusätzliche Rollen, die nur im Zusammenhang mit den oben genannten funktionieren. Diese beinhalten u.a. Möglichkeiten zur Bearbeitung und Verwendung von *Profilen* für das Berechtigungsmanagement (*Profiladministrator*, *Profilverantwortlicher*) sowie zur Beantragung von Zugriffsrechten für andere Mitarbeiter (*Assistent*).

### 2.3.2 Rollenübersicht

Die folgende Tabelle listet alle Rollen mit ihren Rechten und Pflichten im Self Service Portal auf. *Hat ein Benutzer mehrere Rollen, addieren sich seine Rechte,* um alle Aufgaben erfüllen zu können.

| Rolle | Aufgaben & Rechte |
|---|---|
| *Benutzer* | - Beantragt Lese-/Schreibrechte auf bestehende Ressourcen<br>- Beantragt Änderung / Entfernung von Rechten auf Ressourcen<br>- Beantragt die Erstellung einer neuen Ressource<br>- Beantragt die Entfernung der Rechteverwaltung auf einer Ressource<br>- Kann seine aktuellen und früheren Beantragungen nachverfolgen |
| *Assistent* | Gleiche Rechte wie ein Benutzer, kann Anträge aber auch für andere Anwender stellen |
| *Benutzer globaler Berichte* | Gleiche Rechte wie ein Benutzer, kann zusätzlich alle Berichte einsehen (personenübergreifend) |
| *Verantwortlicher* | - Bearbeitet offene Anfragen für alle seine Ressourcen (zulassen, abweisen)<br>- Fügt hinzu, entfernt oder ändert Benutzerrechte auf allen seinen Ressourcen<br>- Erstellt Berichte über seine Ressourcen, Vorlagen und Benutzer<br>- Benennt und entfernt Vertreter für sich<br>- Erstellt, löscht und ändert Rechtevorlagen zu seinen Verzeichnissen |
| *Verantwortlicher (Vertreter)* | Gleiche Rechte wie der Verantwortliche, den er vertritt, jedoch ohne das Recht einen Vertreter zu benennen |
| *Besitzer* | - Bearbeitet offene Anfragen zur Erstellung neuer Ressourcen und zur Entfernung des Berechtigungsstatus, die in seinem Verantwortungsbereich liegen<br>- Vergibt und entzieht Verantwortlichenrechte für Ressourcen in seinem Verantwortungsbereich<br>- Erstellt verschiedene Berichte über seine Ressourcen<br>Benennt und entfernt Vertreter für sich |
| *Besitzer (Vertreter)* | - Gleiche Rechte wie der Besitzer, den er vertritt, jedoch ohne das Recht einen Vertreter zu benennen |
| *Administrator* | - Eine Kombination der Rechte von Besitzer und Verantwortlichem. Der Administrator kann keine Vertreter benennen, aber Anfragen zu allen Ressourcen bearbeiten |
| *Vorlagen-administrator* | - Erstellt und editiert Globale Vorlagen<br>- Bestimmt andere Benutzer, die die Globalen Vorlagen weiterverwenden können<br>- Verwendet Globale Vorlagen |

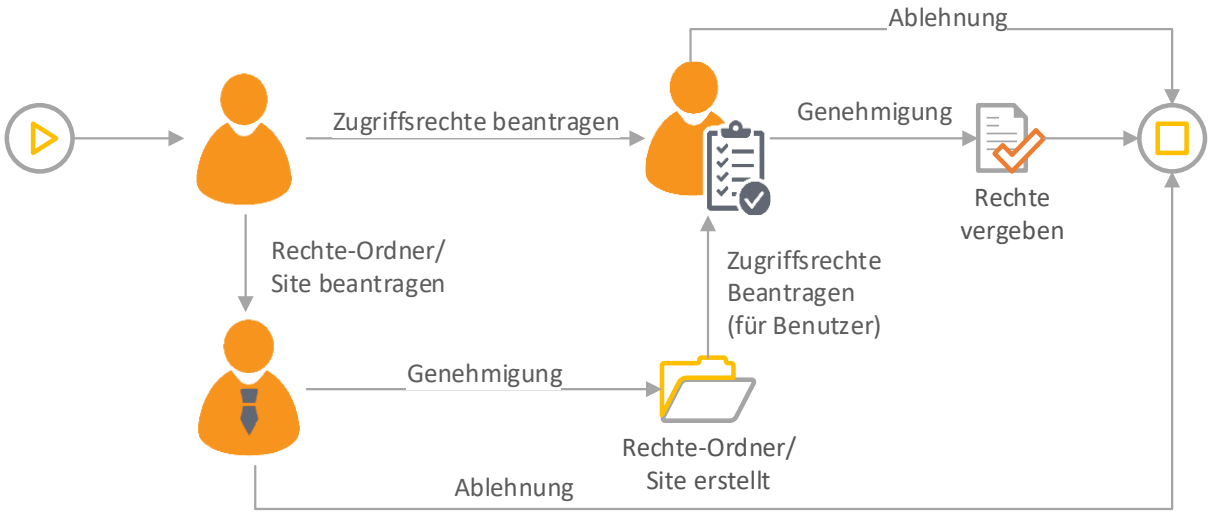
| Rolle | Aufgaben & Rechte |
|---|---|
| *Globaler Vorlagenbenutzer* | - Verwendet vom Vorlagenadministrator zugewiesene Globale Vorlagen |
| *Profiladministrator* | - Erstellt und editiert Profile<br>- Vergibt und entzieht Verantwortlichenrechte für Profile |
| *Profilverantwortlicher* | - Fügt hinzu, entfernt oder ändert Mitgliedschaften auf all seinen Profilen |
| *Klassifizierungs-administrator* | - Erstellt und editiert Klassifizierungen, die Kategorien gemäß der EU-DSGVO enthalten können |

# 3 Self Service für Endanwender

## 3.1 Arbeitsprinzip: Berechtigungsanfragen

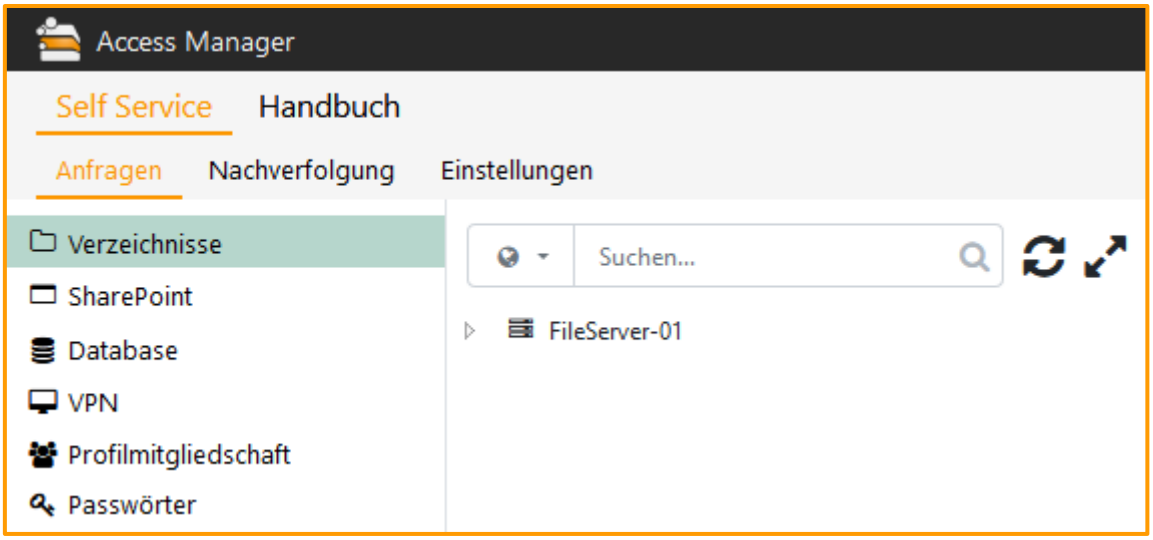
Wenn Sie Zugriff auf eine bestimmte Ressource benötigen, wählen Sie diese aus einer Liste aus und beantragen über eine einfache Eingabemaske das gewünschte Recht. Die für diese Ressource verantwortliche Person – der *Verantwortliche* – wird sofort informiert. Sobald er die Anfrage bearbeitet hat (zugelassen, mit Einschränkungen zugelassen, abgelehnt) werden Sie per Email informiert. Im Idealfall kann der Zugriff so innerhalb von Minuten zur Verfügung stehen.

Wenn Sie die Bereitstellung einer bisher nicht bestehenden Ressource beantragen (z.B. ein neues Verzeichnis), wird zunächst der *Besitzer* der übergeordneten Ressource informiert. Stimmt dieser dem Antrag zu, erledigt er die dafür notwendigen Verwaltungsaufgaben innerhalb der Access Manager Webseite. Die gewünschte Ressource wird automatisch angelegt und das Rechtemanagement eingerichtet – ein tiefes IT-Verständnis ist hierfür nicht erforderlich. Nachdem die neue Ressource erstellt wurde, erhält der hierfür vom Besitzer festgelegte Verantwortliche automatisch eine Anfrage zur Einrichtung Ihrer Zugriffsrechte (siehe vorigen Absatz), die Sie zusammen mit der Beantragung der neuen Ressource angegeben hat.



## 3.2 Anfragen stellen

Jeder Benutzer hat Zugriff auf diese Seite, denn hierüber werden Anfragen zur Erstellung neuer Ressourcen, zur Vergabe von Zugriffsrechten usw. gestellt. Je nach der lizenzierten Ausbaustufe des Access Manager finden sich im Untermenü neben Verzeichnissen auch Antragsmöglichkeiten für SharePoint Sites, Dritt-Elemente usw.:



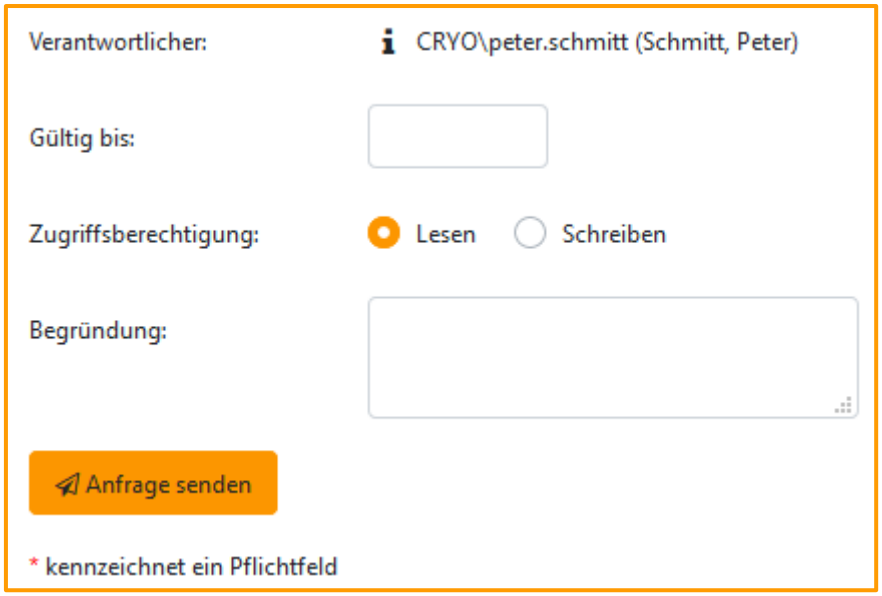

Wählen Sie zunächst den gewünschten Ressourcen-Typ aus und dann den gewünschten Eintrag im Ressourcen-Baum. Rechts sehen Sie nun eine Menüleiste mit den Tabs für mögliche Aktionen. Diese sind abhängig vom gewählten Ressourcen-Typ ggf. nicht alle verfügbar:


Die Darstellung der Antragsformulare ist für alle Ressourcen-Typen identisch. In den folgenden Kapiteln werden die Antragsmöglichkeiten daher beispielhaft anhand des Ressourcen-Typs „Verzeichnisse“ erläutert.

Detailunterschiede betreffen beispielsweise die möglichen Berechtigungen, die sich je nach Ressourcen-Typ unterscheiden:

- **Verzeichnisse**: Mögliche Rechte: Lesen / Schreiben
- **SharePoint Sites**: Mögliche Rechte: Lesen / Schreiben / Gestalten
- **Dritt-Elemente**: Mögliche Rechte: Variabel, durch Kunde definiert
- **Benutzerprofile**: Mögliche Rechte: Mitgliedschaft
- **Passwörter**: Verschiedene Möglichkeiten, um Ihr Passwort ändern zu lassen

### 3.2.1 Zugriffsberechtigungen beantragen (Verzeichnisse)




Mit diesem Formular können Sie Lese- oder Schreibrechte für sich selbst auf das angegebene Verzeichnis beantragen. Zur Information wird die verantwortliche Person angezeigt (*Verantwortlicher*). Wenn dem Benutzernamen das Info-Symbol vorangestellt ist, gibt es noch weitere Verantwortliche, die aufgelistet werden, wenn Sie mit der Maus über das Symbol fahren. Jeder dieser Verantwortlichen kann Ihren Antrag bearbeiten.

Eine optionale Angabe bei *Gültig bis* gewährt das benötigte Zugriffsrecht nur bis zu dem gewählten Datum, danach wird das Recht automatisch entfernt.

Bei der *Zugriffsberechtigung* wird zwischen „Lesen“ und „Schreiben“ unterschieden. „Schreiben“ umfasst dabei neben „Lesen“ zusätzlich das Anlegen, Löschen und Verändern von Dateien und Unterverzeichnissen.

Sofern Sie bereits Zugriffsrechte auf dem Verzeichnis besitzen, wird Ihnen dies durch eine Notiz angezeigt und es erscheint eine zusätzliche Option zum Entfernen der Berechtigung.

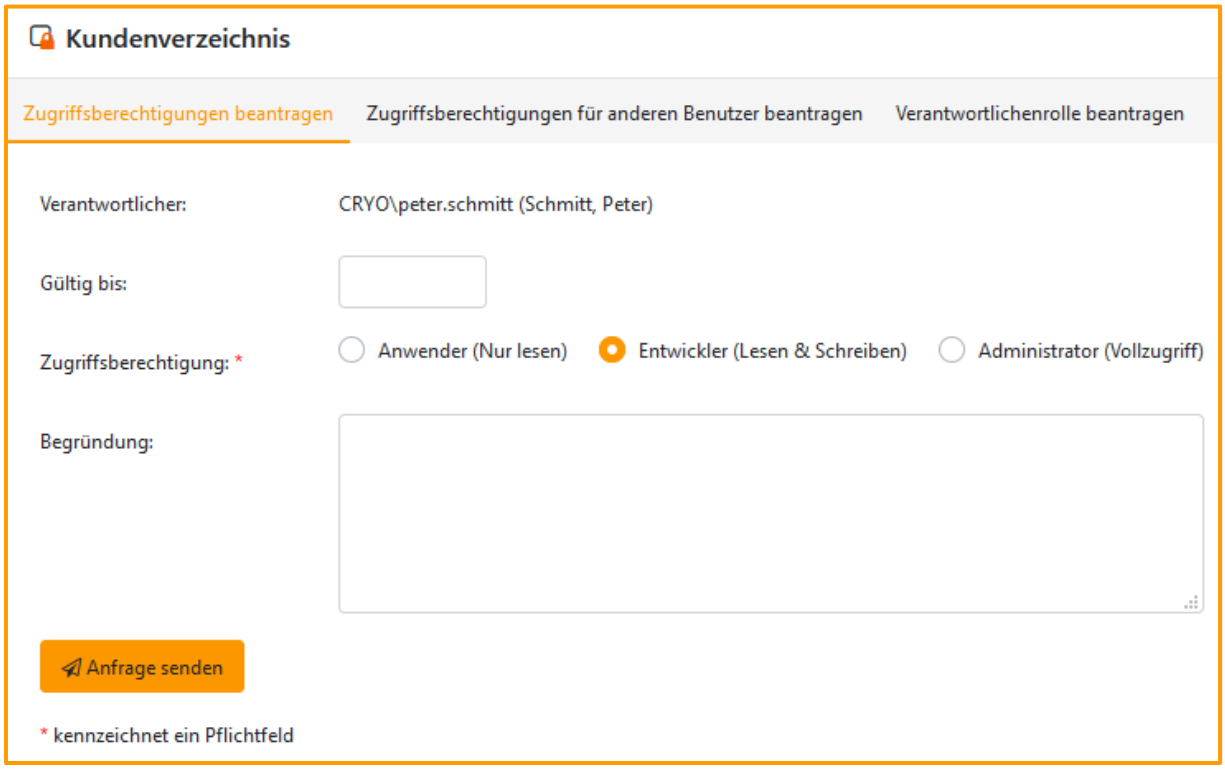
Ggf. ist eine Angabe im Feld *Begründung* zwingend und sollte eine formlose Nachricht an den Verantwortlichen enthalten.

### 3.2.2 Zugriffsberechtigungen beantragen (Dritt-Elemente)

Die Beantragung von Rechten auf Dritt-Elemente nimmt eine Sonderstellung ein, da es hierbei zwei verschiedene Logiken bei der Rechtevergabe geben kann.

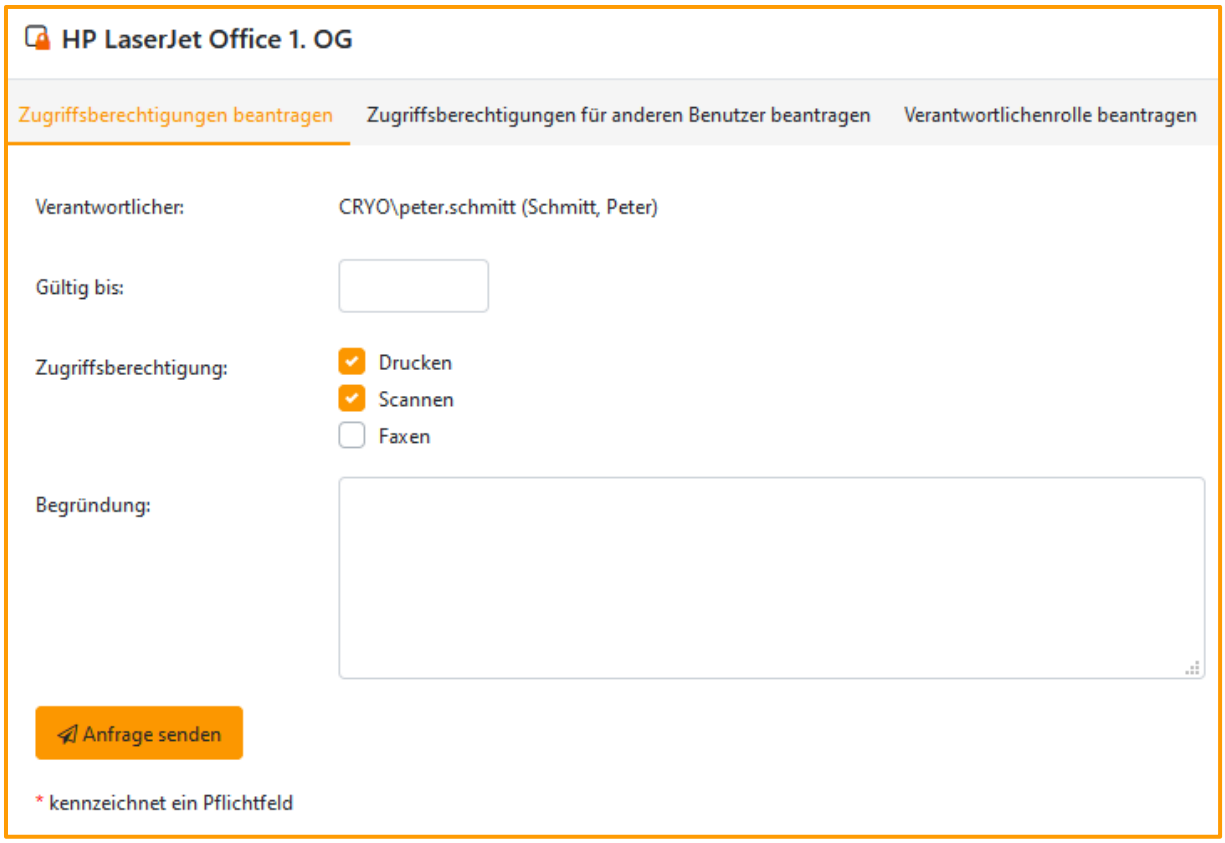
#### 3.2.2.1 Alternative Berechtigungen

Die Logik der alternativen Berechtigungen ist genauso wie bei Verzeichnissen und SharePoint Sites: Sie können aus mehreren möglichen Rechten genau eines auswählen (z.B. haben Sie bei Verzeichnissen die Wahl zwischen Lese- und Schreibrechten, können aber nicht beides gleichzeitig auswählen – auch wenn Schreibrechte natürlich die Leserechte implizieren). Im folgenden Beispiel wurden unterschiedlich weitreichende Rechte für den Zugriff auf die Datenbank „Kundenverzeichnis“ angegeben. Sie können genau eine Zugriffsberechtigung auswählen:



### 3.2.2.2 Ergänzende Berechtigungen

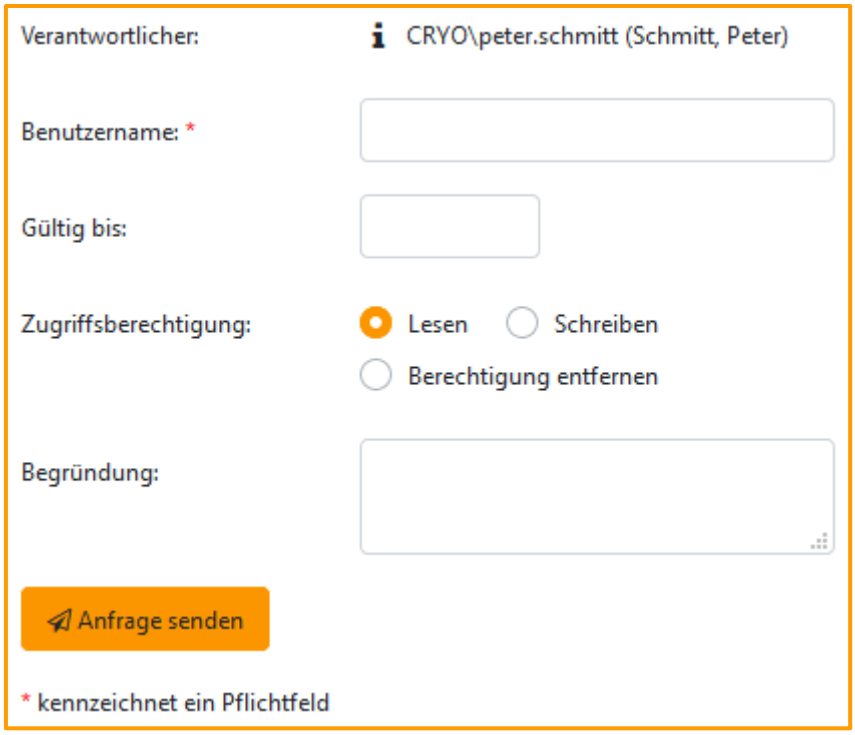
Bei ergänzenden Berechtigungen stehen oft ebenfalls mehrere Berechtigungen zur Auswahl, diese sind jedoch kumulativ, d.h. Sie können mehrere Rechte gleichzeitig erhalten. Diese Variante wird häufig eingesetzt, wenn es sich um voneinander unabhängige, also sich nicht gegenseitig widersprechende Rechte handelt. Im folgenden Beispiel können Sie gezielt verschiedene Nutzungsmöglichkeiten eines Multifunktionsdruckers beantragen:




**Bitte beachten Sie:** Haben Sie bereits bestimmte Berechtigungen für ein Element und möchten bei einer erneuten Beantragung die Auswahl ändern, werden Ihnen zunächst die bereits gewährten Rechte vorausgewählt. Sofern Sie solche Rechte abwählen, werden Ihnen diese später entzogen.

*Sie erhalten immer nur die Rechte, die Sie in der Rechte-Liste ausgewählt haben.*

### 3.2.3 Zugriffsberechtigungen für eine andere Person beantragen




Mit diesem Formular lassen sich Zugriffsrechte für eine andere Person beantragen. Bis auf die zusätzliche notwendige Angabe des gewünschten Benutzerkontos (Feld *Benutzername*) ist dieses Formular identisch mit dem zur eigenen Berechtigungsbeantragung (siehe voriges Kapitel).

### 3.2.4 Neues Verzeichnis beantragen


Mit diesem Formular beantragen Sie die Erstellung eines neuen Verzeichnisses. Die Bearbeitung erfolgt durch den angegebenen *Besitzer*.

Zwingend erforderlich ist die Angabe des *Verzeichnisnamens*, wobei gewisse Namensregeln zu beachten sind. Bei Nichteinhaltung werden Sie darauf hingewiesen, wenn Sie versuchen die Anfrage abzuschicken.

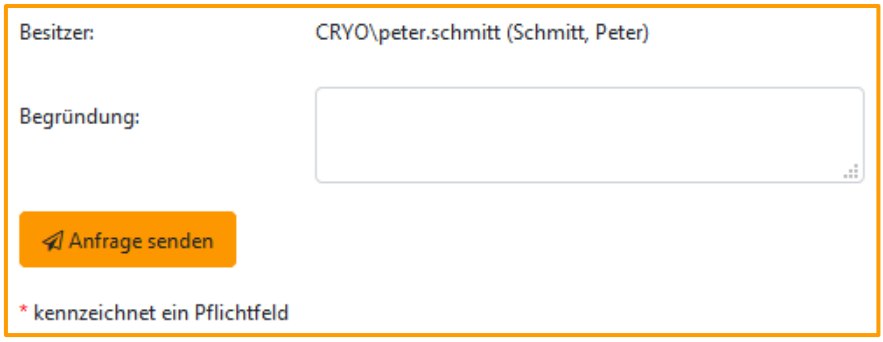
Die *Zugriffsberechtigung* unterscheidet zwischen Lesen, Schreiben und Keine (nur geerbte): Letzteres Recht hängt davon ab, wie der Verzeichnis-Besitzer die sog. Rechte-Vererbung geregelt hat: Wenn das neue Verzeichnis dieselben Rechte erhalten soll wie sein Elternverzeichnis, erhalten Sie dieselben Rechte wie dort. Andernfalls, wenn auf dem neuen Verzeichnis eigenständige Rechte verwaltet werden, erhalten Sie keine Zugriffsrechte. Sie können nicht steuern, welche Regelung der Besitzer treffen wird.

Bei Einsatz des Zusatzmoduls SharePoint besteht auf dieser Seite keine Möglichkeit vererbte Rechte zu beantragen.

Ggf. ist eine Angabe im Feld *Begründung* zwingend und sollte eine formlose Nachricht an den Besitzer enthalten.

Da jedem Berechtigungsordner außer dem *Besitzer* auch mindestens ein *Verantwortlicher* zugeordnet sein muss und dieser durch den Besitzer ernannt wird, kann es sinnvoll sein, dass diese Rolle Ihnen als dem Antragsteller selbst zugewiesen wird – notieren Sie dies am besten im Begründungsfeld.

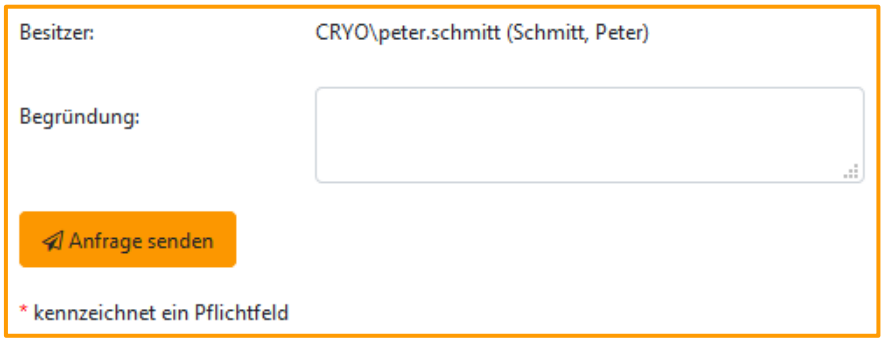
### 3.2.5 Die Rolle des Verantwortlichen beantragen




Mit diesem Formular können Sie die Rolle *Verantwortlicher* für das gewählte Berechtigungsverzeichnis beantragen, um somit künftig selbst Zugriffsrechte für andere Personen zu vergeben.

Dieser Antrag wird vom zuständigen *Besitzer* bearbeitet. Ggf. ist eine Angabe im Feld *Begründung* zwingend und sollte eine formlose Nachricht enthalten.

### 3.2.6 Entfernen der Zugriffsverwaltung beantragen




Über dieses Formular können Sie beantragen, dass ein Verzeichnis seinen Status als verwalteter Ordner verliert. Damit sind einige Konsequenzen verbunden (u.a. Verlust der Kontrolle über Zugriffsberechtigungen anderer Benutzer, ggf. Verlust der Abrechnungskontrolle etc.), die der *Besitzer* bei seiner Entscheidung über den Antrag besonders berücksichtigen sollte. Dies gilt insbesondere für die bestehenden Zugriffsrechte: Wird ein Ordner nicht mehr separat vom AM verwaltet, erbt er automatisch die Zugriffsrechte seines Elternverzeichnisses.

Dieser Antrag wird vom zuständigen *Besitzer* bearbeitet. Ggf. ist eine Angabe im Feld *Begründung* zwingend und sollte eine formlose Nachricht enthalten.

### 3.2.7 Profilmitgliedschaft beantragen

Profile beinhalten unterschiedliche Berechtigungen auf mehrere Ressourcen, daher kann bei diesem Typ kein explizites Recht angefordert werden. Stattdessen können Sie die Mitgliedschaft in einem Profil beantragen, wodurch Sie entsprechende Berechtigungen auf den hinterlegten Ressourcen

erhalten. Es ist für Sie als Antragsteller nicht erkennbar, um welche Ressourcen und Berechtigungen es sich handelt.

### 3.2.8 Passwort-Verwaltung

Hier haben Sie die Möglichkeit, Ihr Passwort für ein bestimmtes Programm oder eine bestimmte Umgebung zu verändern, zurücksetzen oder entsperren zu lassen. Geben Sie zunächst an, welches Ihrer Konten betroffen ist und authentifizieren Sie sich dann mittels einer der zuvor konfigurierten Möglichkeiten (siehe Kapitel. 3.4).

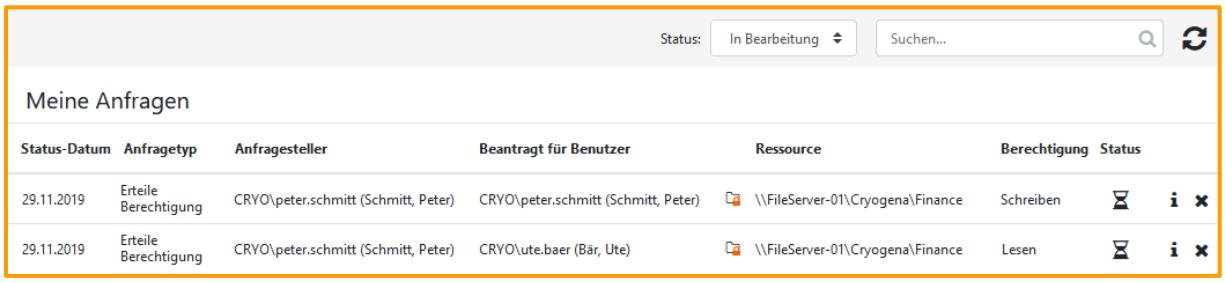
Haben Sie innerhalb des AMPR die *Service Desk*-Rolle erhalten, können Sie hier auch ohne zusätzliche Legitimation das Passwort für einen anderen Benutzer zurücksetzen (Menüpunkt *Passwort für anderen Benutzer zurücksetzen*).

---

*Dieser Menüpunkt stellt die Funktionen des Programms AMPR zur Verfügung.*
*Eine Beschreibung aller Funktionen finden Sie im zugehörigen AMPR-Handbuch.*

---

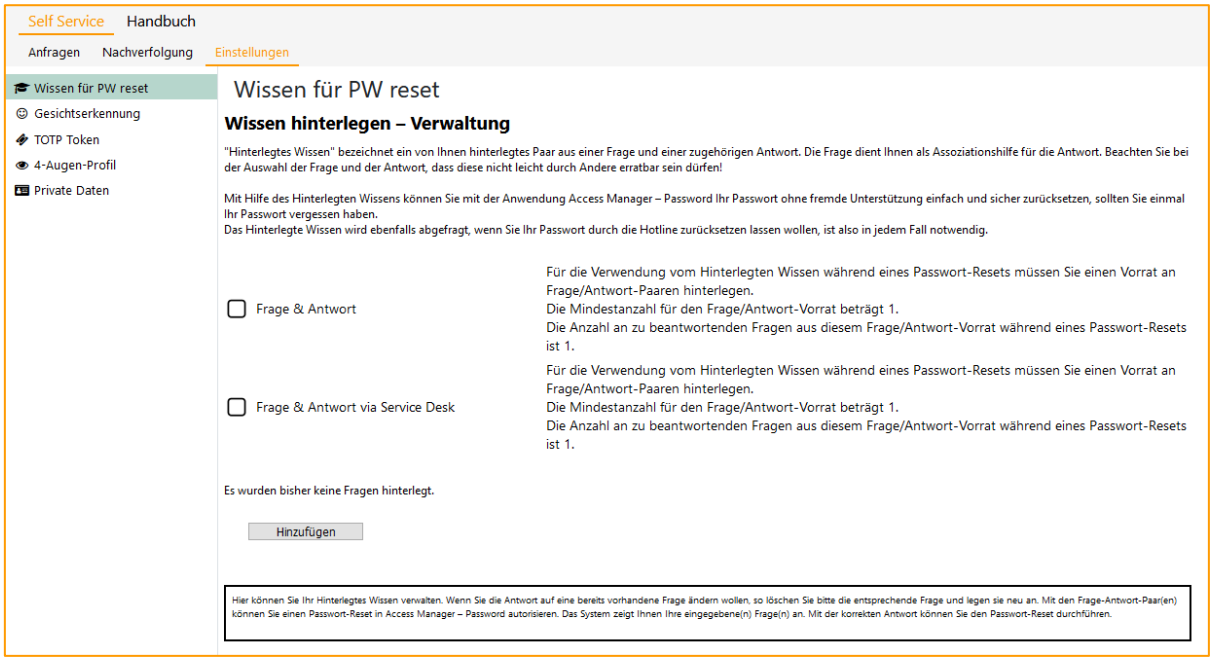
## 3.3 Anfragen nachverfolgen




Über die Seite *Nachverfolgung* können Sie sich Ihre laufenden und abgeschlossenen Beantragungen anzeigen lassen, die Sie auch durchsuchen und nach ihrem Status filtern können. Die einzelnen Spalten geben Aufschluss über verschiedene Details der einzelnen Anträge. Bei noch offenen Anträgen (Status *In Bearbeitung*) wird der Button *Abbrechen* ✖ angeboten um einen Antrag zurückziehen zu können.

Für die Übersichtlichkeit sind einige Informationen der Anträge in ein separates Fenster ausgelagert, welches durch Anklicken des Button *Details* ℹ erreichbar ist. In diesem Fenster werden die verschiedenen Informationen von Anfrage und Genehmigung gegenübergestellt. Handelt es sich um eine offene Anfrage, ist die Spalte *Genehmigung* entsprechend leer. Zusätzlich erhalten Sie hier eine Information über die Entscheider dieser Anfrage.

## 3.4 Einstellungen für die Passwort-Verwaltung




Diese Funktionen stehen nur bei aktiviertem AMPR Programm zur Verfügung und erlauben Ihnen, verschiedene Authentifizierungsmöglichkeiten für die Passwort-Verwaltung (siehe Kapitel 3.2.8) einzurichten, z.B. geheime Sicherheitsfragen, Einmal-Token oder auch ein Kollegenkonto für das Vier-Augen-Prinzip.

---

*Dieser Menüpunkt stellt die Funktionen des Programms AMPR zur Verfügung.*
*Eine Beschreibung aller Funktionen finden Sie im zugehörigen AMPR-Handbuch.*

---

# 4 Berechtigungsmanagement für Datenverantwortliche

## 4.1 Arbeitsprinzip: Verantwortliche & Besitzer

Neben der Rolle *Anwender*, die jeder Benutzer des Access Manager automatisch erhält, existieren zwei weitere Basisrollen, der *Verantwortliche* und der *Besitzer*. Mit diesen Rollen werden Aufgaben der Datenverantwortlichen in Ihrem Unternehmen abgebildet, die zur Durchführung innerhalb des Access Manager berechtigt sind. Diese zwei strikt getrennten Rollen unterstützen die Gewaltenteilung der Ressourcenverwaltung:

Der *Verantwortliche* entscheidet über Zugriffsberechtigungen der Anwender auf den ihm zugewiesenen Ressourcen. Er bearbeitet Benutzeranträge und pflegt auch antragsunabhängig die aktuellen Berechtigungen. Ggf. ist er auch für eine zyklische Überprüfung der gültigen Benutzerrechte zuständig (siehe nächstes Kapitel).

Der *Besitzer* ist für die grundlegende Verwaltung „seiner“ Ressourcen zuständig. Er entscheidet bspw. darüber, wenn neue Verzeichnisse erstellt werden sollen, ob und wie sie durch den Access Manager verwaltet werden und wer der Verantwortliche einer Ressource sein soll. Er entscheidet auch über die besondere Schutzbedürftigkeit einer Ressource im Sinne der EU-DSGVO und darüber, ob und welche Ressourcen von den Verantwortlichen zyklisch überprüft werden müssen (siehe nächstes Kapitel).

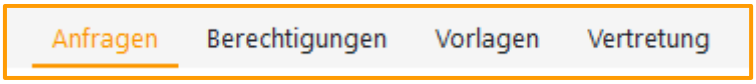
Ein *Administrator* hat immer die Möglichkeit, alle Aufgaben der *Verantwortlichen* und *Besitzer* selbst auszuführen. Er kann jederzeit alle Workflow-Anträge einsehen und bearbeiten sowie Zugriffsrechte und Ressource-Einstellungen verändern.

## 4.2 Aufgabenbereich des Verantwortlichen

Als Verantwortlicher erhalten Sie Zugriff auf den Hauptmenüpunkt *Rechtemanagement*, der Ihnen in weiterer thematischer Unterteilung die Rechteverwaltung Ihrer Ressourcen ermöglicht.

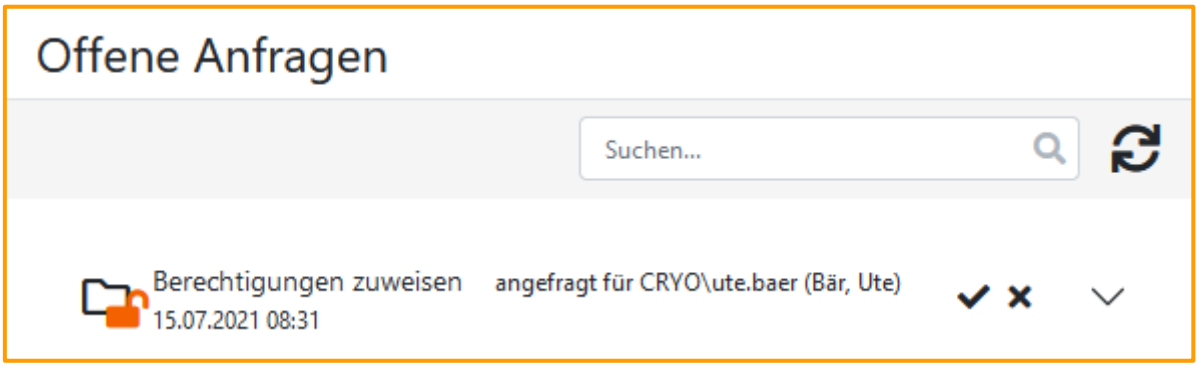

Mit dieser Übersichts- und Bearbeitungsseite können Sie als Verantwortlicher bzw. dessen Vertreter in allen in Ihrer Verantwortung liegenden Ressourcen die Zugriffsrechte anderer Benutzer einsehen und verändern, ohne dass ein Benutzer einen entsprechenden Antrag gestellt hat. Dies ist ein wichtiger Unterschied zur normalen Bearbeitung von Benutzeranfragen, da alle hier vorgenommenen Änderungen ohne automatische Email-Benachrichtigungen an die beteiligten Personen stattfinden – der üblicherweise vorgesehene Workflow findet nicht statt.

### 4.2.1 Anfragen bearbeiten




In diesem Bereich finden Sie die Anfragen der Benutzer für Zugriffsrechte. Wählen Sie zunächst links aus, ob Sie offene (also noch nicht bearbeitete) oder bereits abgeschlossene Anträge einsehen wollen. Diese werden dann rechts aufgelistet und lassen sich nach verschiedenen Kriterien filtern bzw. durchsuchen.

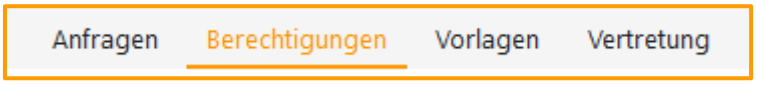
Bei der Bearbeitung von Anträgen können Sie die Anfragen in (un-)veränderter Form gewähren oder auch komplett ablehnen. Ihre Entscheidung wird sofort vom System ausgeführt und eine Informationsmail an den betroffenen Anwender und den Antragsteller geschickt.




Bei der Bearbeitung von Anfragen sind ggf. zwingende Angaben zu machen, z.B. muss u.U. bei der Entscheidung ein Kommentar zur Begründung angegeben werden.

Klappen Sie einen Antrag zur Überprüfung und Bearbeitung über das DropDown-Symbol ⌄ auf. Sind alle erforderlichen Angaben bereits vorhanden, können Sie den Antrag über die Symbole ✔ (Genehmigen) und ✖ (Ablehnen) sofort und ohne Bestätigungsnachfrage abschließen.

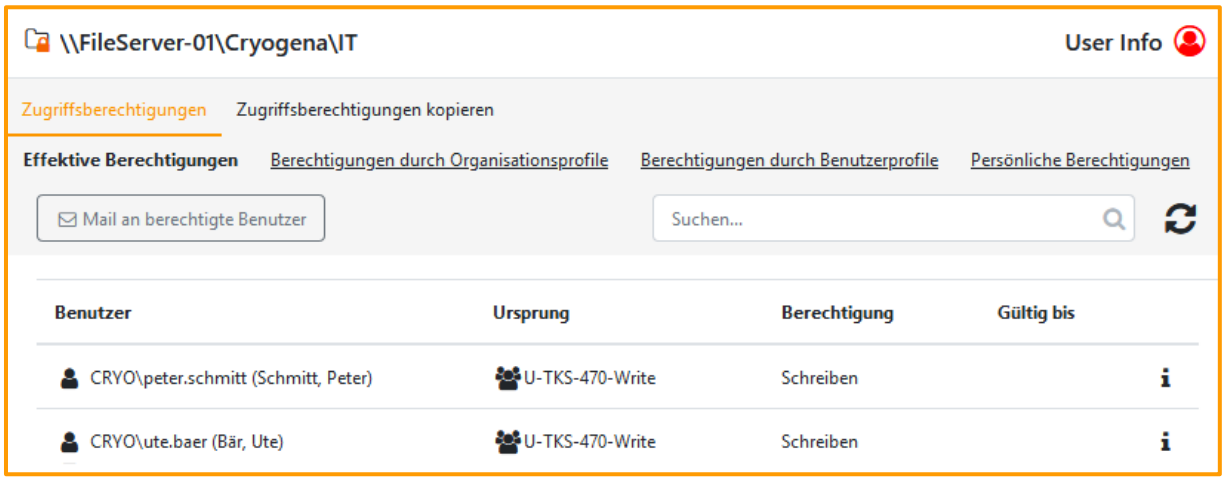
### 4.2.2 Berechtigungen von Ressourcen verwalten




Wählen Sie in der linken Liste den Eintrag *Nach Ressource* aus. Der Ressourcen-Baum zeigt nun Ihre verantworteten Ressourcen an, aus denen Sie die für die weitere Bearbeitung gewünschte Ressource auswählen.

Der rechte Detailbereich zeigt in der Kopfzeile außer der Ressourcen-Angabe auch eine eventuell gesetzte Klassifizierung an. Im Detailbereich stehen Ihnen wiederum zwei Tabs zur Verfügung, „Zugriffsberechtigungen“ und „Zugriffsberechtigungen kopieren“:

#### 4.2.2.1 Detailbereich „Zugriffsberechtigungen“




Dieser Arbeitsbereich zeigt die bestehenden Zugriffsrechte der gewählten Ressource an, wobei jeder Benutzer mit seinen Kerndaten in einer eigenen Zeile steht.

Bei ergänzenden Rechten (siehe Kapitel 3.2.2.2) steht außerdem jedes Recht eines Benutzers ebenfalls in einer eigenen Zeile. Dies ist erforderlich, da verschiedene Rechte unterschiedlichen Ursprungs sein können:


Durch die Möglichkeit der Berechtigung über *Profile* gibt es mehrere Wege, auf denen ein Benutzer Zugriffsrechte auf die ausgewählte Ressource erhalten kann. Daher unterteilt sich dieser Bereich in vier Ansichten:

- Effektive Berechtigungen
- Berechtigungen durch Organisationsprofile
- Berechtigungen durch Benutzerprofile
- Persönliche Berechtigungen

#### *4.2.2.1.1 Effektive Berechtigungen*

Die effektiven Berechtigungen setzen sich aus den jeweiligen Rechtevergabemöglichkeiten (*Profile*, *Persönliche Berechtigung*) zum aktuellen Zeitpunkt zusammen, wobei sich das höhere Recht durchsetzt. Wurde bspw. einem Benutzer per *Persönlicher Berechtigung* Lesezugriff auf eine Ressource gewährt, ein *Benutzerprofil* definiert aber gleichzeitig für diese Ressource Schreibrechte (und der Benutzer ist zum aktuellen Zeitpunkt Mitglied dieses Profils), erhält der Benutzer effektiv Schreibrechte.

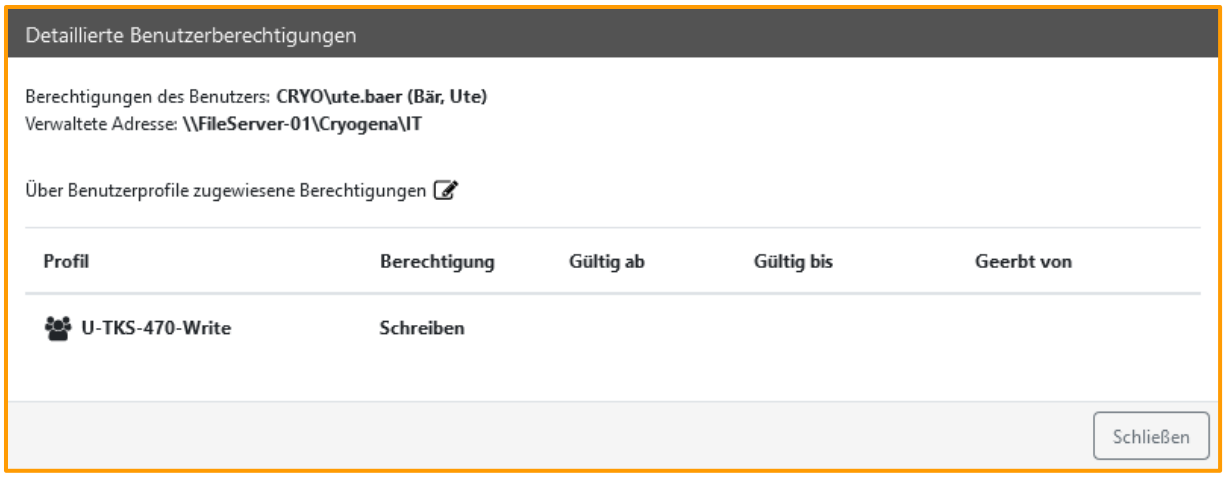
Naturgemäß ist diese Ansicht eine rein informative Listenansicht ohne Editierfunktion, die jeden Benutzer genau einmal anzeigt und dabei neben dem effektiven Recht auch den Ursprung des angezeigten Rechts angibt.

Der Ursprung des effektiven Rechts kann hierbei einer der folgenden sein:

- **Persönliche Berechtigung** – Diese Berechtigung wurde einem Benutzer explizit auf der gewählten Ressource gewährt.
- **Benutzerprofil** – Diese Berechtigung wurde einem Benutzerprofil gewährt, in welchem der angezeigte Benutzer Mitglied ist.
- **Organisationsprofil** – Diese Berechtigung wurde einem Organisationsprofil gewährt. Der angezeigte Benutzer ist Mitglied in einem, diesem Organisationsprofil zugewiesenen, Benutzerprofil.
- **Sonderberechtigungsgruppe** – Diese Berechtigung wurde explizit durch den *Folder Management Administrator* gewährt und liegt außerhalb der Verantwortung und der Zuständigkeit des Verantwortlichen. Sie kann auf dieser Seite nicht geändert werden.

Rechte, die auf einem übergeordneten Berechtigungsordner vergeben wurden (nicht zwangsläufig auf dem direkten Elternverzeichnis, sondern ggf. noch höher), werden in einer gesonderten aufklappbaren Liste aufgeführt und sind hier nicht bearbeitbar (sondern nur in dem Ordner, in dem sie gesetzt wurden).

Weitere Informationen zu den Berechtigungen lassen sich über das zugehörige Info-Symbol anzeigen. Hier erhalten Sie eine detaillierte Übersicht über alle gewährten Berechtigungen, wobei das effektive Recht hervorgehoben wird. Über das Icon haben Sie die Möglichkeit direkt in die Bearbeitungsansicht der jeweiligen Berechtigungsherkunft (Organisationsprofile, Benutzerprofile oder Persönliche Berechtigungen) zu springen und dort Änderungen an der Berechtigung vorzunehmen.

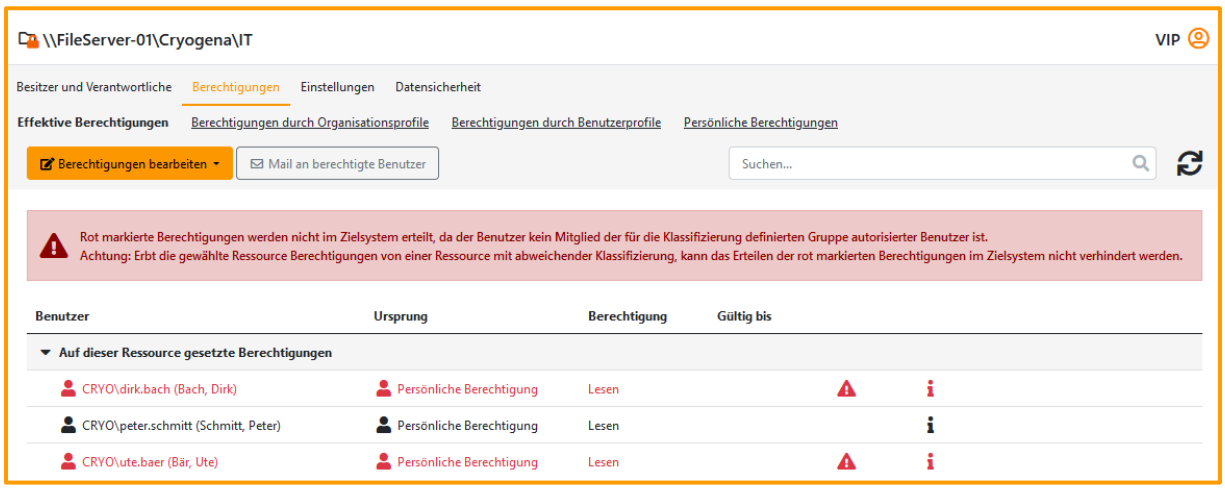



*Mail an berechtigte Benutzer:*

Mit diesem Button versenden Sie eine Rundmail an alle Personen, die auf dieser Ressource Zugriffsrechte bzw. eine Mitgliedschaft haben. In dem Dialogfenster können Sie den vorgegebenen Mail-Betreff anpassen und im Textbereich Ihre Nachricht eingeben. Die Anwender erhalten die Email zwar von der für den Access Manager konfigurierten Absenderadresse; wenn sie antworten, geht die Mail aber an Ihre eigene Adresse.

**Anmerkung: Sonderfälle bei der Verwendung mit einer Klassifizierung mit autorisierten Benutzern**

Ist eine Ressource mit einer Klassifizierung versehen, in der eine Gruppe autorisierter Benutzer definiert wurde (siehe Kapitel 7.2), so kann es vorkommen, dass auf dieser Ressource Personen berechtigt werden, die nicht Mitglied der Gruppe und damit nicht für den Berechtigungserhalt autorisiert sind. Solche Benutzer werden – ausschließlich in dieser Übersicht der effektiven Rechte – mit einem Warnhinweis dargestellt:



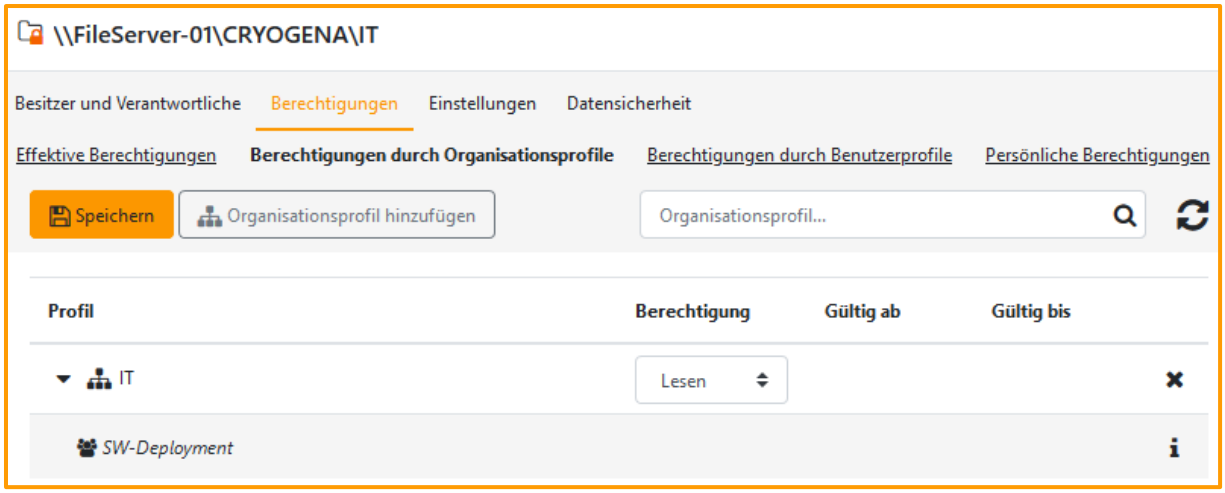

Access Manager merkt sich die Berechtigungsvergabe, teilt den Benutzern im Zielsystem (AD-Gruppe bzw. Dateisystem, abhängig vom Ressourcen-Typ) jedoch kein Zugriffsrecht zu.

Dieser Hinweis sollte Sie veranlassen zu überprüfen, ob entweder der Benutzer fälschlich berechtigt wurde oder ob er noch in die Gruppe autorisierter Personen aufgenommen werden muss.

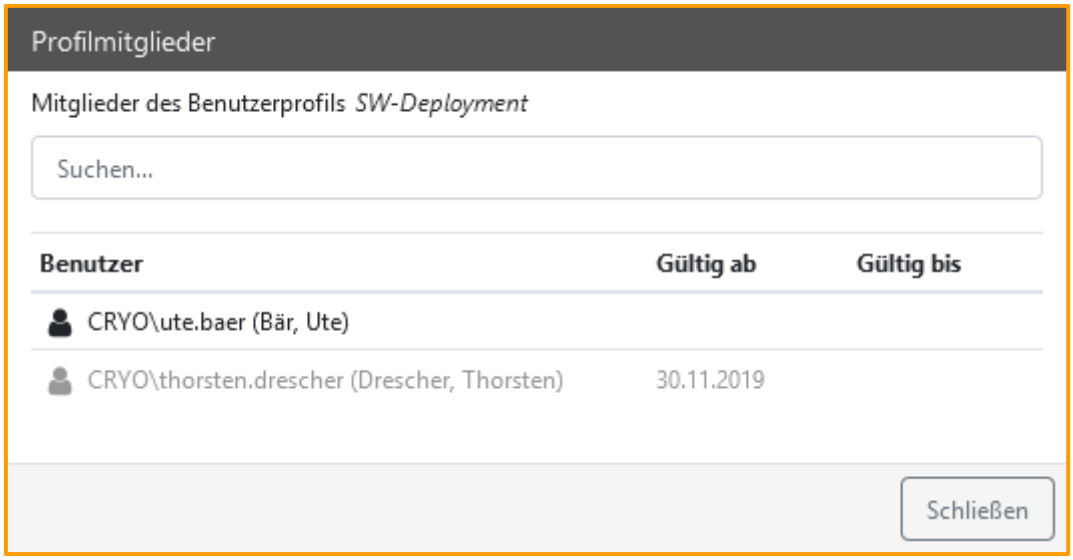
#### *4.2.2.1.2 Berechtigungen durch Organisationsprofile*

Diese Ansicht zeigt die *Organisationsprofile*, die auf der gewählten Ressource berechtigt wurden, mit ihrem Zugriffsrecht. Zu jedem Organisationsprofil werden zusätzlich die Mitglieder (*Benutzerprofile*) mit möglichen Start- und Ablaufdaten der Mitgliedschaft angezeigt, wenn das Profil über das Expander-Icon aufgeklappt wird.

Näheres über die Funktionsweise von Profilen finden Sie im Kapitel 6.1.




Ein Klick auf das Info-Symbol eines Benutzerprofils zeigt wiederum dessen Mitglieder (Benutzerkonten) in einem zusätzlichen Fenster an.

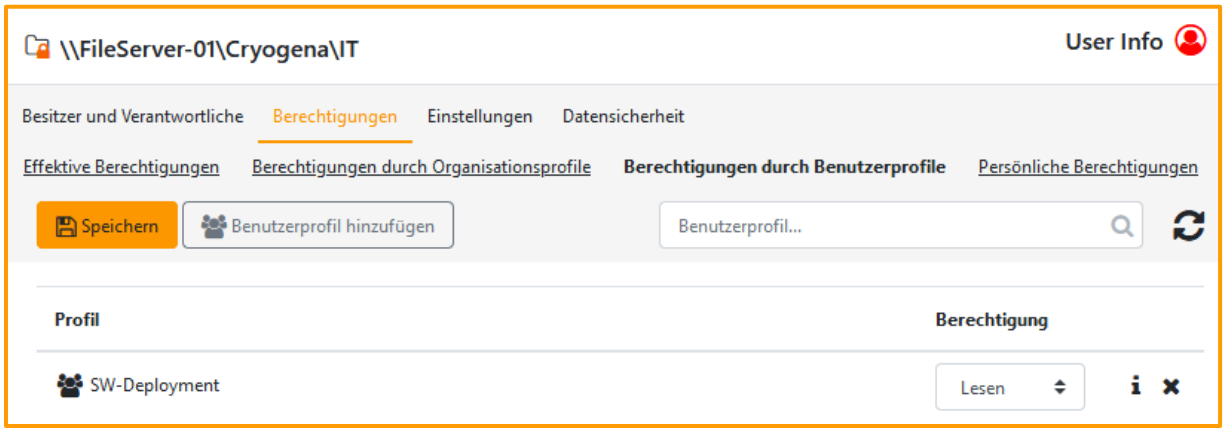



Zusätzlich zu den bereits berechtigten Organisationsprofilen können Sie auch weiteren Organisationsprofilen Zugriff gewähren (Button *Organisationsprofil hinzufügen*). Sie haben die

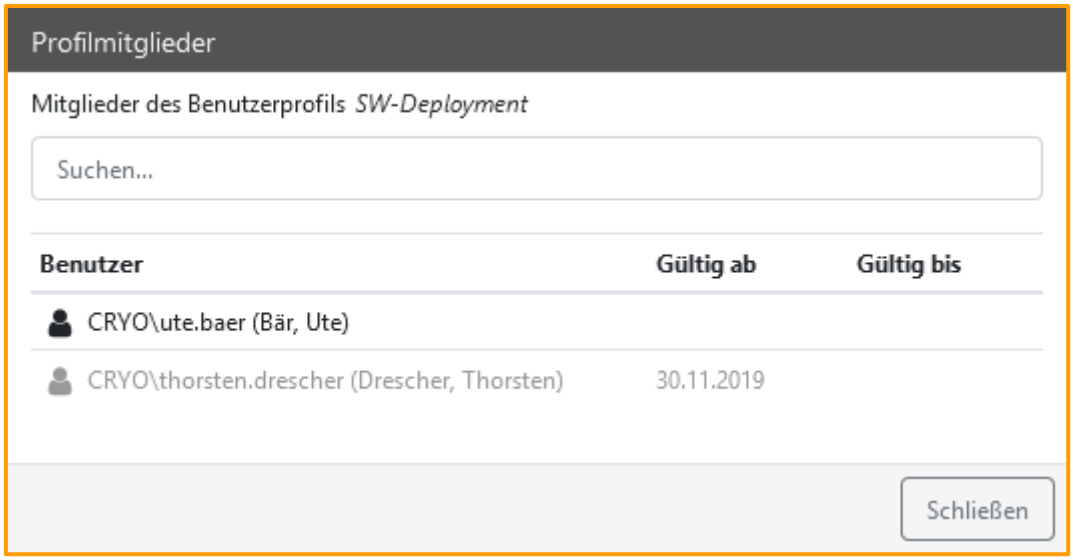
Möglichkeit, alle angezeigten Berechtigungen zu ändern oder zu löschen. Durch jede Änderung der Profile werden den zugehörigen Benutzern die Zugriffsrechte gewährt oder entzogen.

#### *4.2.2.1.3 Berechtigungen durch Benutzerprofile*

Diese Ansicht zeigt die auf der gewählten Ressource berechtigten Benutzerprofile mit ihrem Zugriffsrecht. Näheres über die Funktionsweise von Profilen finden Sie im Kapitel 6.1.



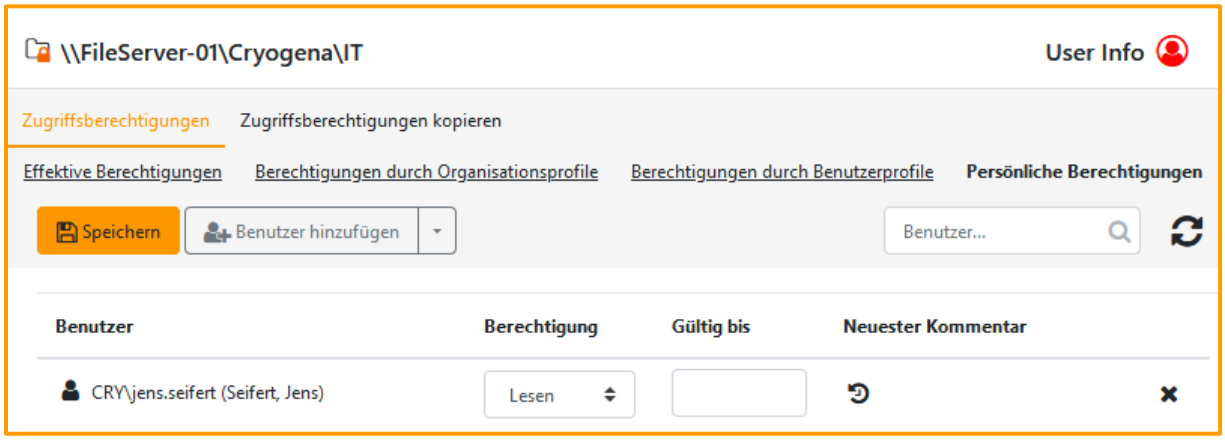

Ein Klick auf das Info-Symbol zeigt dessen Mitglieder (Benutzerkonten) mit möglichen Start- und Ablaufdaten der Mitgliedschaft in einem separaten Fenster an.



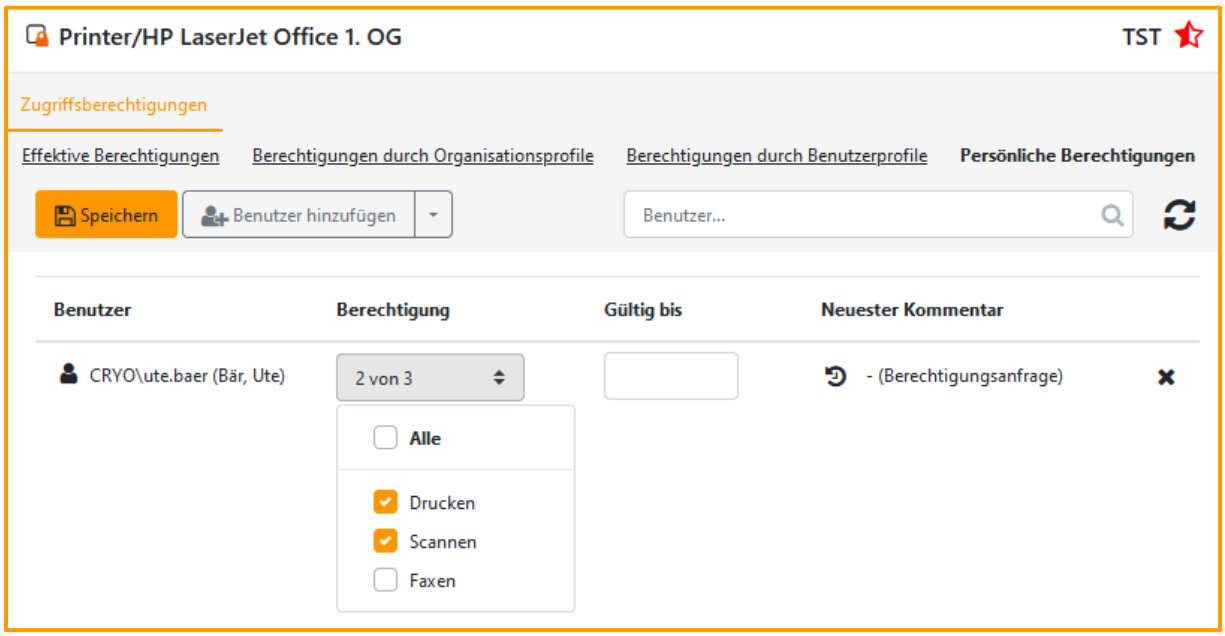

Zusätzlich zu den bereits berechtigten Benutzerprofilen können Sie auch weiteren Benutzerprofilen Zugriff gewähren (Button *Benutzerprofil hinzufügen*). Sie haben die Möglichkeit, alle angezeigten Berechtigungen zu ändern oder zu löschen. Durch jede Änderung der Profile werden den zugehörigen Benutzern die Zugriffsrechte gewährt oder entzogen.

#### *4.2.2.1.4 Persönliche Berechtigungen*

Dieser Arbeitsbereich zeigt die bestehenden Zugriffsrechte mit optionalem Ablaufdatum und Kommentar an, welche einem Benutzer explizit auf der gewählten Ressource gewährt wurden.




Ergänzende Berechtigungen von Dritt-Elementen werden individuell abhängig von ihrer Anzahl („Alle“, manche („2 von 3“)) angezeigt:



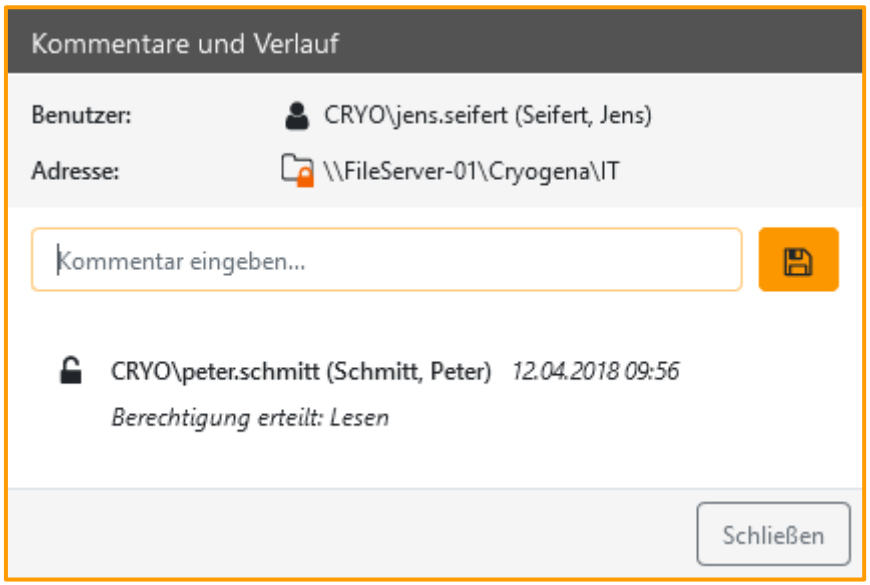

Sie haben die Möglichkeit, alle angezeigten Berechtigungen zu ändern oder zu löschen. Zusätzlich zu den bereits berechtigten Benutzern können Sie auch weiteren Benutzern Zugriff gewähren. Dies wird über die folgenden Buttons ermöglicht:

*Benutzer hinzufügen*: Gewähren Sie einem weiteren Benutzer eine Zugriffsberechtigung durch Angabe des Benutzerkontos, dem zu gewährenden Recht und optional einem Ablaufdatum sowie Kommentar.

*Benutzer aus AD-Gruppe hinzufügen*: Hiermit lässt sich eine AD-Gruppe angeben, dessen Mitglieder im folgenden Schritt aufgelistet werden. Von diesen können Sie beliebig viele auswählen und zur

Berechtigung übernehmen. Dadurch wird nicht die Gruppe selbst berechtigt, sondern nur ihre Mitglieder.

Wurde vom Administrator eingestellt, dass Kommentare verpflichtend sind, müssen Sie für jede Berechtigungsänderung einen erklärenden Kommentar eingeben. Dies betrifft sowohl das Hinzufügen / Entfernen eines Benutzerkontos als auch das Verändern eines bestehenden Rechtes (z.B. Umstellung von Lesen auf Schreiben, Anpassen des Ablaufdatums). Kommentare können aber auch ohne Veränderung jederzeit eingegeben werden. Über das Icon öffnet sich ein Dialog, in dem alle bisherigen Kommentare und Berechtigungsänderungen (auch ohne Kommentar) eingesehen und neue Kommentare eingegeben werden können:

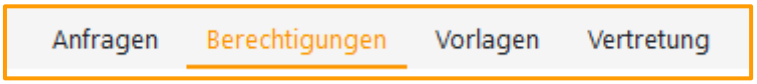



Alle vorhandenen Kommentare werden auch in den Berichten angezeigt, mit Ausnahme der Historischen Berichte.

#### 4.2.2.2 Detailbereich „Zugriffsrechte kopieren“:


Dieser Bereich ermöglicht das einfache Berechtigen mehrerer Benutzer auf ein Verzeichnis (derzeit nicht verfügbar für Dritt-Elemente und SharePoint Sites) mit wenigen Mausklicks. Mittels der Auswahlliste *Quell-Verzeichnis* bestimmt man die Ressource[1], von der die Benutzer in die aktuelle Ressource kopiert werden sollen. Mit den Checkboxen *Einbeziehen* selektieren Sie diejenigen Benutzer, die Lese- und / oder Schreibrechte besitzen. Prinzipiell werden jedoch nur die Benutzer berücksichtigt, welchen die Zugriffsrechte in der Quell-Ressource explizit zugewiesen wurden, d.h. Benutzer mit geerbten Rechten sowie spezielle Berechtigungsgruppen werden ignoriert. Mit dem Button *Kopieren* werden die Benutzer mit ihrem jeweiligen Recht sofort in den aktuellen Berechtigungsordner übernommen.

### 4.2.3 Berechtigungen von Benutzern verwalten




Während die Unterseite *Nach Ressource* eine Rechte-Übersicht ausgehend von einem Verzeichnis liefert, beantwortet diese Seite die Frage, welche Berechtigungen ein einzelner Benutzer hat.

Wählen Sie in der linken Liste den Eintrag *Nach Benutzer* aus. Die Personenliste listet alle Benutzerkonten auf und bietet verschiedene Möglichkeiten der Filterung an. Neben der Möglichkeit, über die Sucheingabe einen bestimmten User zu finden, können Sie mit der Checkbox *Nur Berechtigungsbenutzer* nur die Konten anzeigen lassen, die bereits auf einem Ihrer Verzeichnisse berechtigt wurden. Zusätzlich kann über die Dropdown-Liste *Benutzerstatus* bestimmt werden, ob (de-)aktivierte Nutzerkonten angezeigt werden sollen. In jeder Filterung werden zunächst nur die ersten 100 Treffer angezeigt – daher gibt es am Ende der Liste die Möglichkeit auch die restlichen Konten anzuzeigen. Je nach Anzahl kann dies mehrere Sekunden dauern.

[1] Auch hier werden nur Ordner angezeigt, für die Sie als Verantwortlicher zuständig sind.

Benutzerkonten ist ein Symbol vorangestellt, das Auskunft über ihren aktuellen Status im Access Manager gibt:

- Aktiver Benutzer mit Berechtigungen / Rollen
- Aktiver Benutzer ohne Berechtigungen / Rollen
- Inaktiver Benutzer mit Berechtigungen / Rollen
- Inaktiver Benutzer ohne Berechtigungen / Rollen
- Blacklisted Benutzer mit Berechtigungen / Rollen
- Im AD gelöschter Benutzer mit Berechtigungen / Rollen (kann auch mit „***“ markiert sein)

Bei sogenannten *Blacklisted Benutzern* handelt es sich um normale Benutzerkonten, die vom Administrator auf eine „Schwarze Liste“ gesetzt wurden. Damit werden sie in den üblichen Suchmasken und Eingabevervollständigungen nicht mehr berücksichtigt und nur angezeigt, falls sie bereits über Berechtigungen oder Rollen verfügen. Ohne Antrag lassen sich keine neuen Berechtigungen vergeben, es können lediglich bestehende Berechtigungen entfernt werden. Vorhandene Rechte werden vom Access Manager weiterhin überprüft und gepflegt. Außerdem sind die betreffenden Anwender weiterhin in der Lage Anträge im Management Portal zu stellen.

#### 4.2.3.1 Detail-Tab „Benutzerinformationen“


Im Tab *Benutzerinformationen* werden zunächst allgemeine Informationen über das Benutzerkonto gezeigt. Diese umfassen z.B. die E-Mail-Adresse und das Benutzerverzeichnis (sofern verfügbar) und weitere technische Angaben.

#### 4.2.3.2 Detail-Tab „Persönliche Berechtigungen"

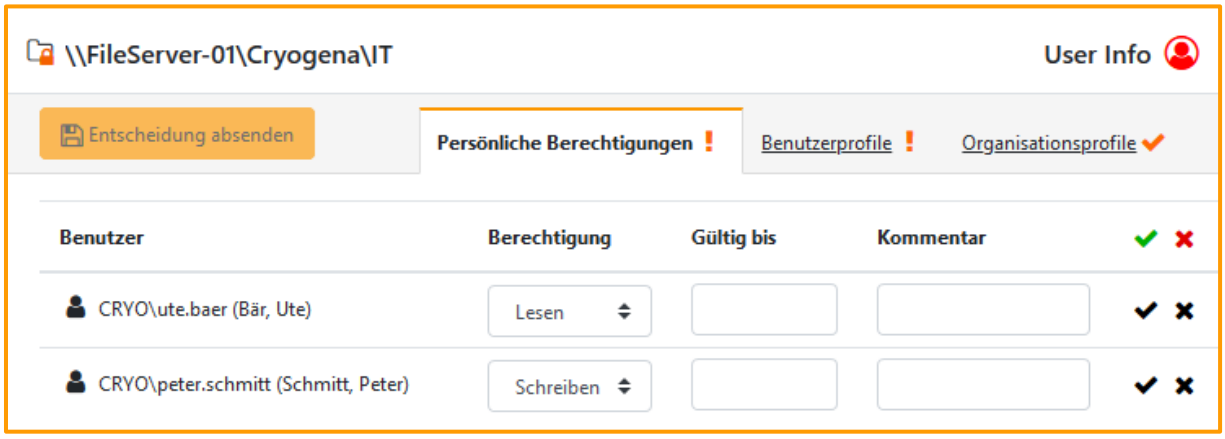
Im Tab *Persönliche Berechtigungen* werden die von Ihnen verantworteten Ressourcen mit dem jeweils vergebenen Recht und dem ggf. gesetzten Ablaufdatum aufgeführt.


Für jede Ressource können Sie die Zugriffsberechtigung ändern (Dropdown-Liste), ein Ablaufdatum setzen, Kommentare einsehen / hinzufügen sowie die Berechtigung ganz entfernen (Kreuz-Symbol). Über das Kreuz-Symbol im Tabellenkopf können auch alle Berechtigungen auf einmal entfernt werden. Darüber hinaus können auch Berechtigungen auf weitere Verzeichnisse vergeben werden (Button *Ordner hinzufügen*). Alle Änderungen werden nicht sofort durchgeführt, sondern es wird die geänderte Zeile zunächst farblich markiert und erst beim Klick auf *Speichern* übernommen. Da für alle diese Aktionen keine Beantragung erforderlich ist, werden auch keine automatischen Benachrichtigungsemails an die Betroffenen versendet.

### 4.2.4 Reapproval durchführen

Wählen Sie in der linken Liste den Eintrag *Berechtigungsreapproval* aus.

Das Konzept der erneuten Berechtigungsvergabe (siehe Kapitel 4.4) sieht vor, dass in zyklischen Abständen die aktuellen Zugriffsrechte von Benutzern und Profilen auf die verwalteten Ressourcen überprüft und bestätigt werden müssen. Ob und welche Ressourcen überprüft werden müssen, bestimmt dabei der *Besitzer* über eine Klassifizierungszuordnung. Sie als Verantwortlicher können sich auf dieser Seite die aktuell zu prüfenden Ressourcen anzeigen lassen, diese werden im Ressourcen-Baum mit einem Ausrufzeichen hinter dem Namen markiert.




Nach Auswahl einer Ressource werden rechts die zurzeit vergebenen Berechtigungen aufgeführt, gruppiert nach persönlichen und Profilrechten. Um ein Reapproval für eine Ressource durchzuführen, müssen Sie die einzelnen Rechte auf jedem der drei Reiter (Persönliche Berechtigungen, Benutzerprofile, Organisationsprofile) bestätigen, erst dann wird der Button *Entscheidung absenden* freigegeben und damit die erfolgte Prüfung gespeichert. „Bestätigung einer Berechtigung“ bedeutet in diesem Kontext, dass Sie eine Entscheidung über jede vorhandene Berechtigung fällen müssen – ob hierbei das vorhandene Recht beibehalten, verändert oder entfernt wird, ist irrelevant; wichtig ist nur, *dass* eine Entscheidung getroffen wurde. Sobald innerhalb eines Reiters alle Berechtigungen bestätigt wurden, ändert sich das Ausrufzeichen in einen Haken. Erst wenn alle Reiter einen Haken haben, ist das Reapproval für diese Ressource abgeschlossen und kann gespeichert werden – eine Teilbearbeitung ist nicht möglich.

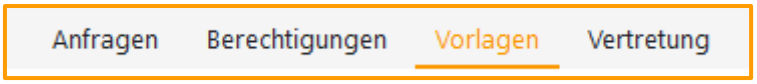
Mit der Option *Alle Ressourcen anzeigen* werden auch bereits bestätigten Ressourcen aufgeführt; diese sind mit einem Haken versehen.

---

*Abhängig von der Entscheidung Ihres Unternehmens werden ggf. alle nicht von Ihnen bestätigten Berechtigungen mit Ende eines Reapproval-Laufs automatisch entfernt.*

---

### 4.2.5 Vorlagenmanagement & -zuweisung




#### 4.2.5.1 Erstellen von Vorlagen

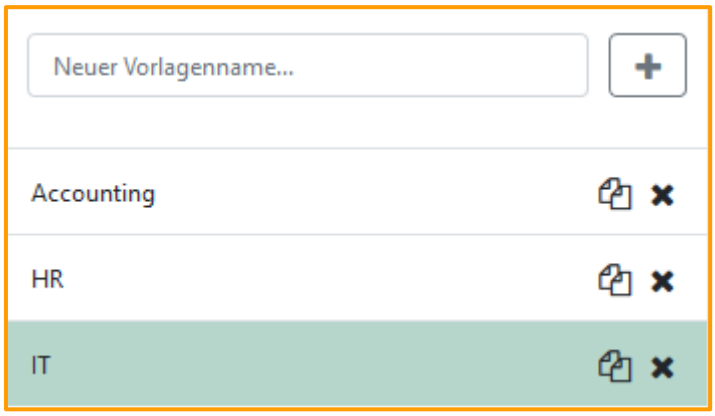
Mit *Vorlagen* können Sie Schablonen erstellen, durch die Sie und Ihre Vertreter künftig auf einfache Weise eine große Anzahl an immer gleichen Berechtigungen und Berechtigungsordnern mit wenigen Mausklicks verschiedenen Benutzer zuweisen. Diese Vorlagen sind explizit privat, d.h. nur für Sie als Verantwortlicher sicht- und nutzbar; Sie können außerdem nur Verzeichnisse verwenden, für die Sie auch der Verantwortlicher sind. Um eine Vorlage für mehrere Bearbeiter nutzbar zu machen und auch Verzeichnisse anderer Verantwortlicher zu nutzen, existieren die *Globalen Vorlagen* (siehe Kapitel 6.4ff).

---

*Vorlagen können nur auf Berechtigungsverzeichnisse angewendet werden, SharePoint Sites und Dritt-Elemente werden nicht unterstützt. Verwenden Sie Profile, welche alle Ressourcen-Typen unterstützen.*

---

Wählen Sie in der linken Liste den Eintrag *Vorlagenmanagement* aus. Im Bereich daneben gibt es ein Eingabefeld, um eine neue Vorlage zu erstellen sowie eine Liste mit den bereits angelegten Vorlagen:

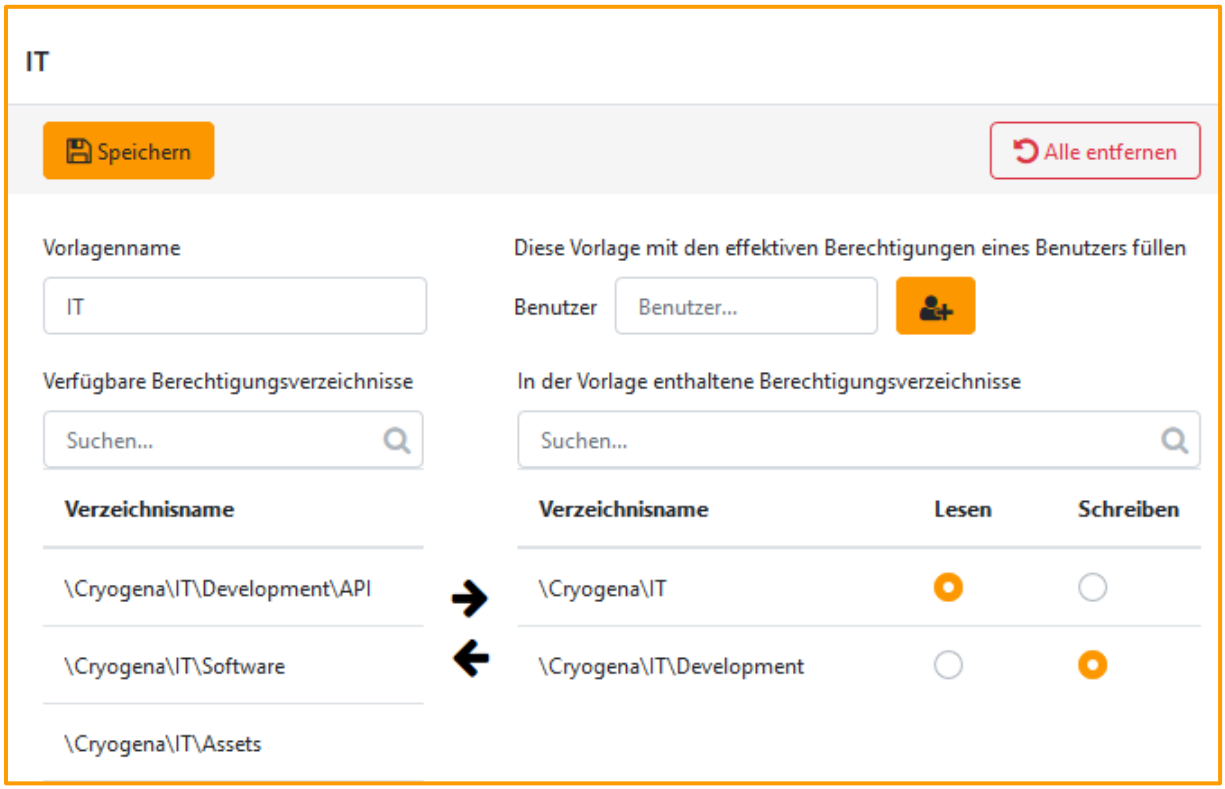



Für jede Vorlage lassen sich Aktionen per Klick auf das jeweilige Symbol durchführen:

- *Duplizieren*: Eine Kopie der Vorlage wird unter einem neuen Namen gespeichert. Dabei werden alle gesetzten Berechtigungsordner mit ihren Zugriffsrechten übernommen.
- *Entfernen*: Die Vorlage wird gelöscht, eine Wiederherstellung ist nicht möglich.

Nach Auswahl einer Vorlage sehen Sie im rechten Detailbereich alle Einstellungsmöglichkeiten. Sie können etwa den Namen ändern und die Verzeichnisse mit den gewünschten Berechtigungen

bestimmen. Diese können Sie entweder manuell aus der linken Liste nach rechts übernehmen oder einen Benutzer angeben, dessen Verzeichnisse (inklusive seiner Berechtigungen) eingesetzt werden. Bitte beachten Sie, dass dadurch keine vollständige Übernahme aller Benutzer-Rechte möglich ist, da Sie nur auf die von Ihnen selbst verwalteten Verzeichnisse zugreifen können.




### 4.2.5.2 Zuweisen von Vorlagen

Wählen Sie in der linken Liste den Eintrag *Vorlagenzuweisung* aus. Die zuvor erstellten Vorlagen können auf dieser Seite verwendet werden. Diese Aufteilung in Vorlagenerstellung und -verwendung begründet sich dadurch, dass Sie nur als vollwertiger Verantwortlicher Vorlagen erstellen können, während Sie als Vertreter diese nur benutzen dürfen.

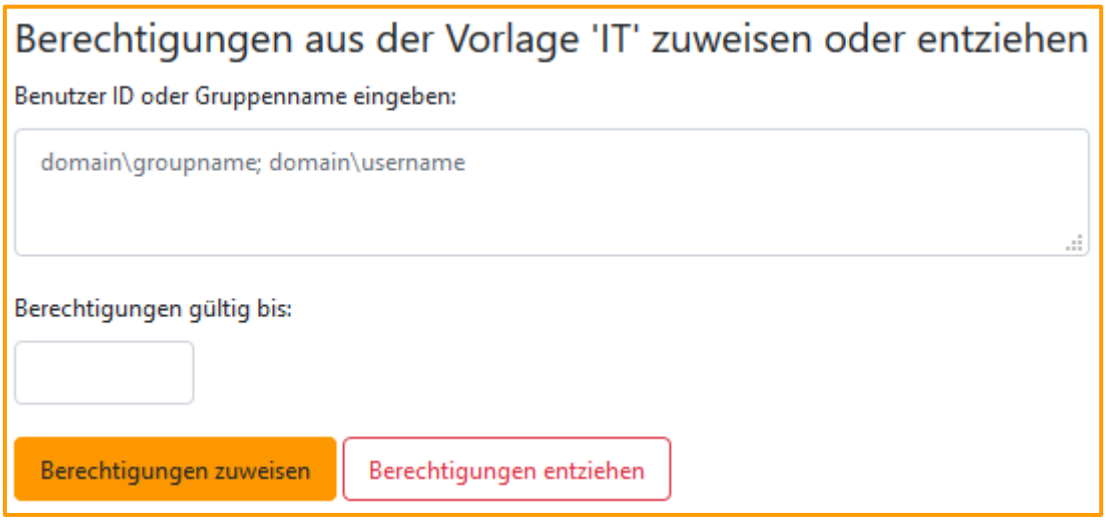
Die Seite unterteilt sich grob in drei Bereiche:

- Vorlagenauswahl
- Festlegung der betroffenen Benutzer und der Gültigkeitsdauer
- Anzeige der enthaltenen Verzeichnisse & Rechte

#### 4.2.5.2.1 Vorlagenauswahl


Das obige Beispiel zeigt die möglichen Sichtbarkeiten von Vorlagen: Die Vorlage *HR* wurde von Ihnen als tatsächlicher Verantwortlicher erstellt. Die Vorlage *IT* wurde von einem anderen Verantwortlichen (Peter Schmitt) erstellt und ist hier nur sichtbar, weil Sie zusätzlich auch Vertreter für Peter Schmitt sind. Leere Vorlagen, also solche ohne berechtigte Verzeichnisse, werden in dieser Liste nicht angezeigt, da sie nicht sinnvoll einsetzbar sind.

#### 4.2.5.2.2 Benutzer & Gültigkeitsdauer festlegen




In diesem Abschnitt werden die Benutzerkonten angegeben, auf die die Vorlage angewendet werden soll. Mehrere Konten werden durch Semikola getrennt. Auch die Angabe einer oder mehrerer Benutzergruppen ist möglich – die enthaltenen Mitglieder werden abschließend in einer Auswahlliste zusammengefasst dargestellt. Die Angabe eines Ablaufdatums der Rechte ist zusätzlich möglich.

Buttons *Berechtigungen zuweisen* / *Berechtigungen entziehen*:

Da es vorkommen kann, dass ein von der Rechte-Zuweisung per Vorlage betroffener Benutzer bereits Zugriffsrechte auf einem der enthaltenen Verzeichnisse hat, ist es wichtig zu wissen, dass grundsätzlich keine Reduzierung vorhandener Rechte erfolgt – bestehende höherwertige Rechte haben immer Vorrang[2].

[2] D.h. hat ein Benutzer bereits Schreibrecht auf ein Verzeichnis, behält er dieses, auch wenn die Vorlage ein Leserecht vergibt.

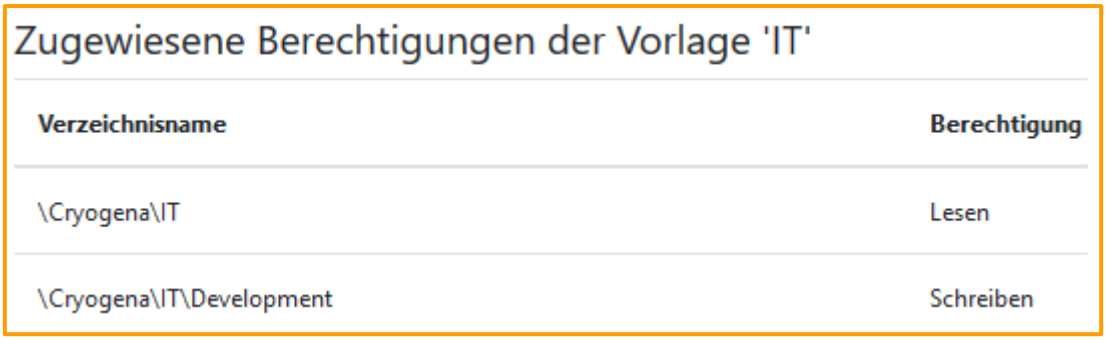
Wurde kein Enddatum angegeben, erfolgt die Berechtigungsänderung unter Berücksichtigung obiger Regel sofort und dauerhaft; andernfalls gilt:

- *Berechtigungen zuweisen*: Allen angegebenen Benutzern und Gruppen werden die jeweiligen Zugriffsrechte auf die Verzeichnisse sofort zugewiesen und das Ablaufdatum wird gesetzt (unter Berücksichtigung obiger Regel). Dadurch kann sich das zuvor ggf. vorhandene Ablaufdatum verlängern.

- *Berechtigungen entziehen*: Es werden keine neuen Rechte gesetzt, jedoch werden bereits bestehende Rechte der Benutzer und Gruppen mit dem Ablaufdatum versehen, sofern es sich um das gleiche Recht wie in der Vorlage handelt (d.h. nur bei Lesen/Lesen bzw. Schreiben/Schreiben) und ein ggf. schon bestehendes Ablaufdatum erst später greifen würde. Das bedeutet, dass sich ein Berechtigungszeitraum höchstens verkürzen, jedoch nie verlängern kann.

Klicken Sie abschließend auf *Berechtigungen zuweisen* bzw. *Berechtigungen entziehen*, werden die Berechtigungen für alle angegebenen Benutzer durchgesetzt und sie – sowie Sie als Verantwortlicher – werden darüber per Email informiert.

#### *4.2.5.2.3 Anzeige der Verzeichnisse einer Vorlage*




Zur Kontrolle werden nach der Auswahl einer Vorlage die darin definierten Verzeichnisse und ihre Zugriffsrechte angezeigt – eine Änderung ist nicht möglich.

### 4.2.6 Eigene Vertreter bestimmen


Diese Seite dient dazu, für einen (un-)begrenzten Zeitraum (z.B. während Ihres Urlaubs) eine oder mehrere andere Personen zu Ihrem Vertreter zu ernennen. Da es nicht vorgesehen ist, dass diese Vertreter wiederum weitere Vertreter benennen können, steht Ihnen diese Seite nur zur Verfügung, wenn Sie die Rolle *Verantwortlicher* innehaben. Ein Vertreter hat Zugriff auf fast alle verantworteten Seiten (siehe vorangegangene Kapitel) und erhält alle Möglichkeiten des Verantwortlichen zur Ressource- und Benutzerrechteverwaltung. Die Benennung eines Vertreters bedeutet nicht, dass Sie als Verantwortlicher Ihre administrativen Möglichkeiten verlieren – Sie können auch weiterhin alle Aufgaben durchführen.

Für die Vertretung lässt sich wahlweise ein Gültigkeitszeitraum angeben, wobei sowohl der Beginn als auch das Ende optional sind. Wird kein Startdatum eingetragen, beginnt die Vertretung sofort; fehlt eine Angabe zum Ende, läuft die Vertretung solange, bis Sie den Vertreter entfernen.

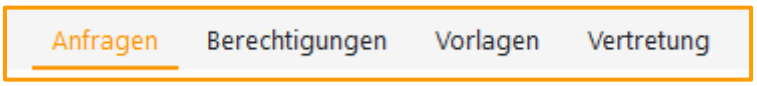
Über den Button *Entfernen* ✖ können einzelne Vertreter entfernt werden; mit *Bearbeiten* ändern Sie bspw. den Gültigkeitszeitraum der Vertretung.

## 4.3 Aufgabenbereich des Besitzers

Als Besitzer erhalten Sie Zugriff auf den Hauptmenüpunkt *Rechtemanagement*, der Ihnen in weiterer thematischer Unterteilung die Verwaltung Ihrer Ressourcen ermöglicht.

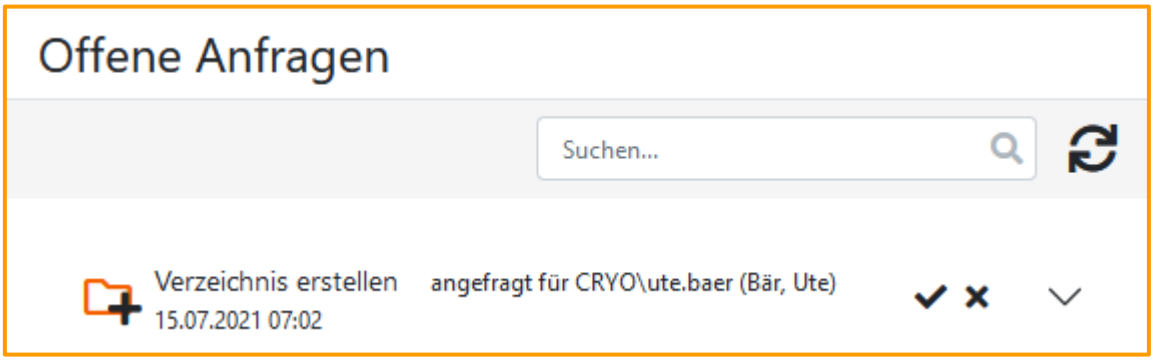

Die Rolle *Besitzer* erhält ein Benutzer nur durch explizite Zuweisung durch einen *Administrator*. Üblicherweise werden Sie durch eine organisatorische Entscheidung zum Besitzer für eine auf oberster Ebene liegende Ressource bestimmt. Sie sind dann zunächst automatisch auch für alle darunter liegenden Ressourcen der Besitzer. Erst wenn für eine Ressource (und deren Unter-Ressourcen) in tieferer Ebene eine andere Person den Besitz übernehmen soll, wird diese wiederum vom *Administrator* gesetzt.

### 4.3.1 Anfragen bearbeiten




In diesem Bereich finden Sie die Anfragen der Benutzer. Dazu gehören etwa die Erstellung neuer Berechtigungsordner/-sites, die Entfernung ihres Verwaltungsstatus´ sowie das Beantragen von *Verantwortlicher*-Rollen. Wählen Sie zunächst links aus, ob Sie offene (also noch nicht bearbeitete) oder bereits abgeschlossene Anträge einsehen wollen. Diese werden dann rechts aufgelistet und lassen sich nach verschiedenen Kriterien filtern bzw. durchsuchen.

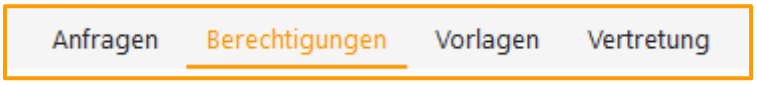
Bei der Bearbeitung von Anträgen können Sie die Anfragen in (un-)veränderter Form gewähren oder auch komplett ablehnen. Ihre Entscheidung wird sofort vom System ausgeführt und eine Informationsmail an den betroffenen Anwender und den Antragsteller geschickt.




Bei der Bearbeitung von Anfragen sind je nach Typ der Anfrage mehr oder weniger Angaben zu machen, z.B. muss bei der Erstellung einer neuen Ressource als Berechtigungsressource neben der Entscheidung über den tatsächlichen Namen auch ein *Verantwortlicher* festgelegt werden.

Klappen Sie einen Antrag zur Überprüfung und Bearbeitung über das DropDown-Symbol ⌄ auf. Sind alle erforderlichen Angaben bereits vorhanden, können Sie den Antrag über die Symbole ✔ (Genehmigen) und ✖ (Ablehnen) sofort und ohne Bestätigungsnachfrage abschließen.

### 4.3.2 Strukturmanagement

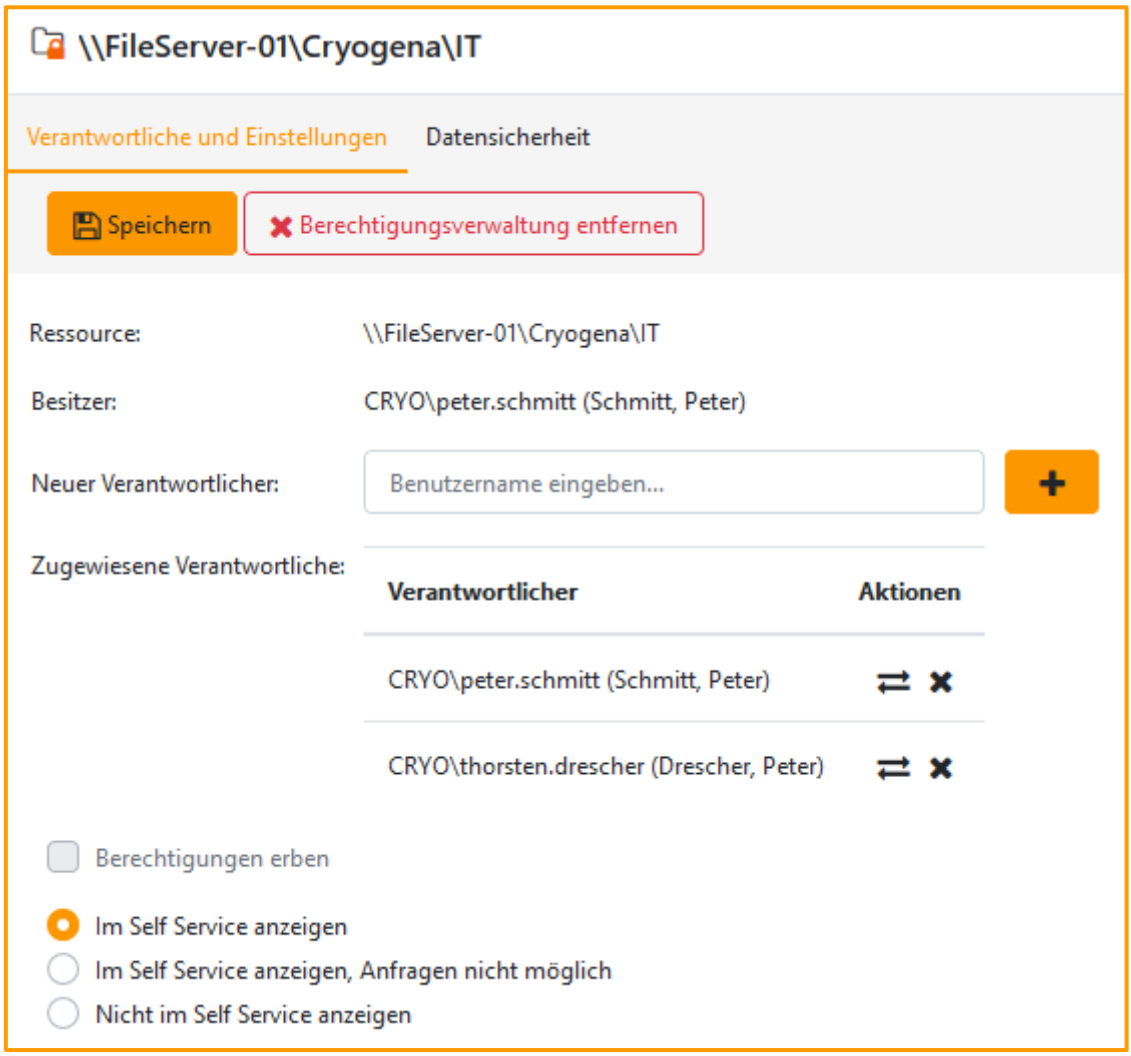



Wählen Sie in der linken Liste den Eintrag *Strukturmanagement* aus. Der Ressourcen-Baum zeigt nun Ihre eigenen Ressourcen[3] an, aus denen Sie die für die weitere Bearbeitung gewünschte Ressource auswählen.

Der rechte Detailbereich zeigt in der Kopfzeile außer der Ressource-Angabe auch eine eventuell gesetzte Klassifizierung an, die Sie anpassen können.

[3] Im Gegensatz zu den anderen Adressbäumen werden hier nicht nur die *verwalteten* Adressen angezeigt, sondern auch solche ohne bestehenden Verwaltungsstatus.

#### 4.3.2.1 Detail-Tab „Verantwortliche und Einstellungen“

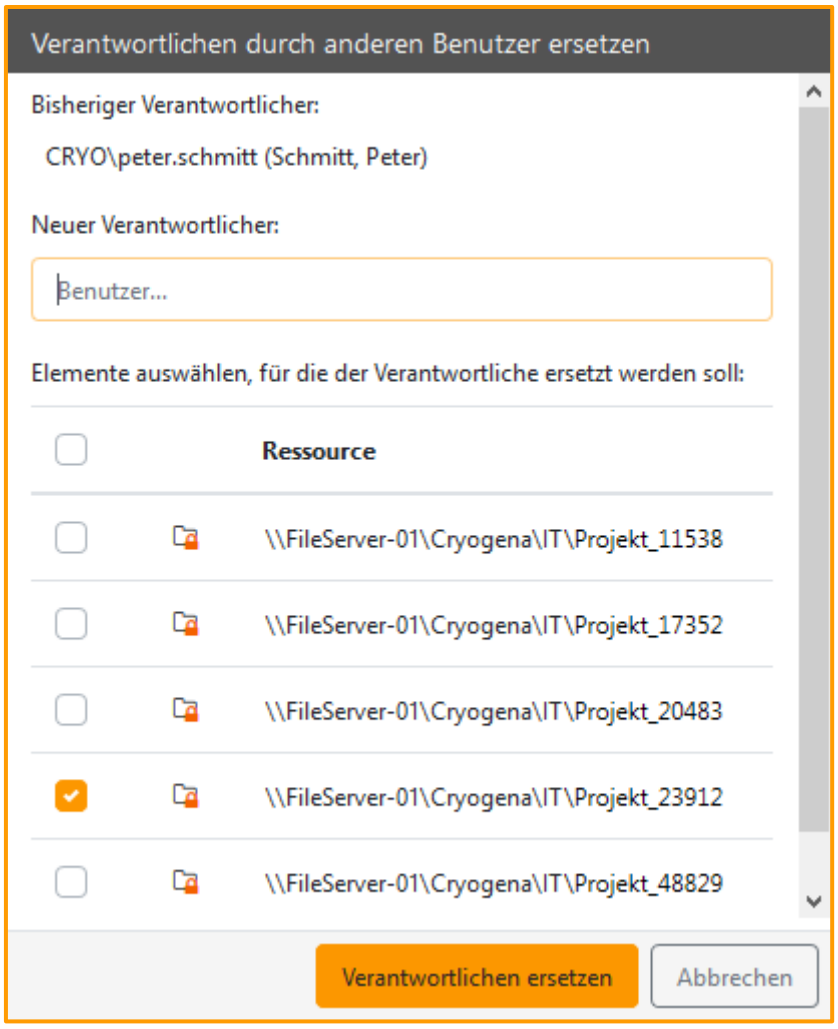



Im rechten Bereich werden Details zur gewählten Ressource angezeigt. Abhängig davon, ob es sich um eine verwaltete Ressource handelt, werden einige der oben gezeigten Elemente aktiviert oder deaktiviert. Nur im Falle einer verwalteten Ressource ist außerdem die Liste *Zugewiesene Verantwortliche* mit mindestens einem Eintrag befüllt.

Für jede Ressource wird der aktuelle Besitzer angezeigt, sofern dieser zuvor durch den *Administrator* gesetzt wurde – ansonsten bleibt die Anzeige leer (in diesem Fall kann es sich nicht um eine verwaltete Ressource handeln).

Mit dem Eingabefeld *Neuer Verantwortlicher* lässt sich ein (weiterer) Verantwortlicher angeben; mit dem Button *Hinzufügen* wird er in die Liste *Zugewiesene Verantwortliche* übernommen.

In der Liste ist es außerdem möglich, einen Verantwortlichen durch eine andere Person zu ersetzen, wofür der Button *Ersetzen* ⇄ verwendet wird. Hierbei bietet der AM eine besondere Vereinfachung:




In der sich öffnenden Dialogbox können Sie nicht nur der neue Verantwortliche eintragen, sondern auch wählen, für welche seiner Ressourcen die Ersetzung gelten soll. Mit zwei Klicks lässt sich damit ein Verantwortlicher komplett durch einen anderen ersetzen.

Mit der Checkbox *Berechtigungen erben* (nur bei Verzeichnissen verfügbar, nicht bei SharePoint Sites) lässt sich für diesen Berechtigungsordner einstellen, dass die Benutzerberechtigungen des übergeordneten Berechtigungsordners auf diesen Ordner vererbt werden. Es handelt sich hierbei – auch in den NTFS-Berechtigungen – tatsächlich um eine Vererbung: Die Rechte werden nicht von oben kopiert. Diese Checkbox ist deaktiviert, wenn der aktuelle Ordner der erste in der Berechtigungshierarchie ist, da er von niemandem erben kann. Im Falle eines normalen Ordners (kein Berechtigungsordner) kann die Vererbung nicht ausgeschaltet werden, da solche Ordner ihre Berechtigungen in jedem Fall vom Eltern-Verzeichnis erben.

#### *4.3.2.1.1 Sichtbarkeit im Self Service Portal für Antragsteller*

Über die folgenden Optionen legen Sie fest, ob und wie die Ressource den Anwendern (Antragstellern) im Ressourcen-Baum angezeigt werden soll:

*Im Self Service anzeigen* blendet die Ressource ein. Der Anwender kann die üblichen Anträge stellen.

*Im Self Service anzeigen, Anfragen nicht möglich* blendet die Ressource ebenfalls ein, erlaubt aber keine Anträge durch die Anwender – die Ressource wird dargestellt, als sei sie nicht verwaltet. Diese Option steht nur Verzeichnisse und SharePoint Sites zur Verfügung, für Dritt-Elemente jedoch nicht.

*Nicht im Self Service anzeigen* blendet diese Ressource sowie alle darunter liegenden aus – dies gilt auch, wenn es sich bei den Kind-Ressourcen um verwaltete handeln sollte.

---

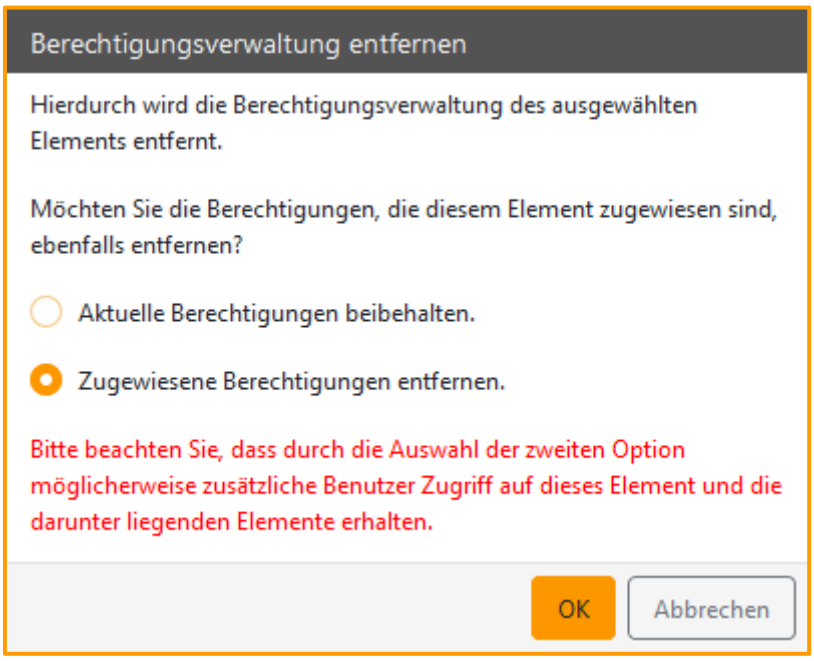
*Durch diese Einstellung wird keinerlei Einfluss auf die Sichtbarkeit und die Zugriffsmöglichkeiten der Ressource auf dem realen Verzeichnis bzw. SharePoint Site genommen.*

---

Nachdem alle gewünschten Änderungen vorgenommen wurden, werden diese mit dem Button *Speichern* in den Access Manager übernommen. Wenn es sich anfangs um eine nicht verwaltete Ressource handelte, dem Sie nun mindestens einen Verantwortlichen zugewiesen haben, wird die Ressource beim Speichern automatisch in eine Berechtigungsressource umgewandelt (erkennbar an dem entsprechenden Icon vor dem Namen im Ressourcen-Baum).

#### *4.3.2.1.2 Berechtigungsverwaltung eines Verzeichnisses entfernen*

Alternativ lässt sich die Ressource mit dem Button *Berechtigungsverwaltung entfernen* in eine normale, d.h. nicht verwaltete Ressource umwandeln. Treffen Sie hierbei eine Entscheidung bzgl. des Rechtemanagements:



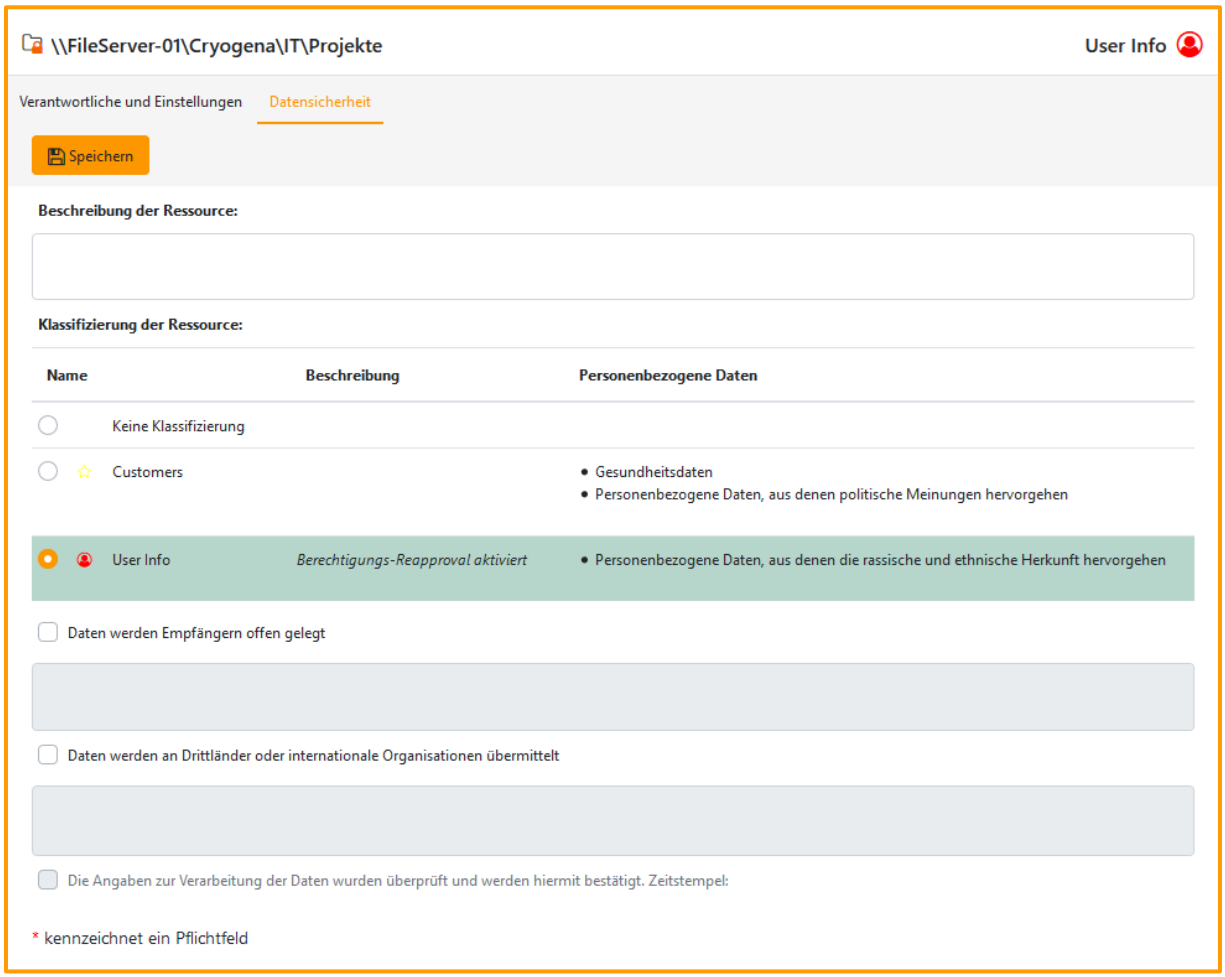

Die bisher auf diesem Verzeichnis durch den Access Manager gesetzten Benutzerrechte können entweder entfernt (empfohlen) oder beibehalten werden. Bei einer Entfernung der Rechte bleibt das Verzeichnis dennoch für Benutzer zugreifbar (allerdings ggf. für andere als vorher), da es dann automatisch die Rechte des Eltern-Verzeichnisses erbt. Behält man die aktuellen Rechte bei, tritt die Vererbung dagegen nicht in Kraft, so dass weiterhin dieselben Personen Zugriff haben wie zuvor.

---

*Wir empfehlen das Entfernen der bisherigen Rechte, da dadurch eine konsistente Behandlung der Berechtigungen im Vergleich zu anderen unverwalteten Ressourcen sichergestellt ist.*

---

#### 4.3.2.2 Detail-Tab „Datensicherheit"




*Beschreibung der Ressource:* Abhängig von der Einstellung des *Administrators* kann oder muss ein beschreibender Text für diese Ressource eingegeben werden.

*Klassifizierung der Ressource:* Sie können die Ressource mit einer der vorgegebenen Klassifizierungen markieren und auch nachträglich ändern. Das Entfernen einer Klassifizierung von einer Ressource erfolgt durch die Auswahl des Eintrags „Keine Klassifizierung". Die verfügbaren EU-DSGVO Kategorien einer Klassifizierung lassen sich nur von einem *Klassifizierungsadministrator* setzen. Details zu *Klassifizierungen* finden Sie im Kapitel 7.1.

Über die Optionen *Daten werden Empfängern offen gelegt* und *Daten werden an Drittländer oder internationale Organisationen übermittelt* werden diese DSGVO-Informationen, ggf. mit einer Beschreibung im Textfeld, an der Ressource gespeichert. Sie können außer von Ihnen auch von einem *Klassifizierungsadministrator* geändert werden.

Die Checkbox *Die Angaben zur Verarbeitung der Daten wurden überprüft und werden hiermit bestätigt.* dient Ihnen als Information, dass die oben gemachten Angaben von dritter Seite validiert wurden. Sie können diese Information und insbesondere den Zeitstempel nicht selbst setzen, doch durch eine

Anpassung der anderen Werte wird der Überprüfungsstatus entfernt – die Ressource ist dann nicht mehr validiert. Dies kann nur durch den *Klassifizierungsadministrator* erfolgen.

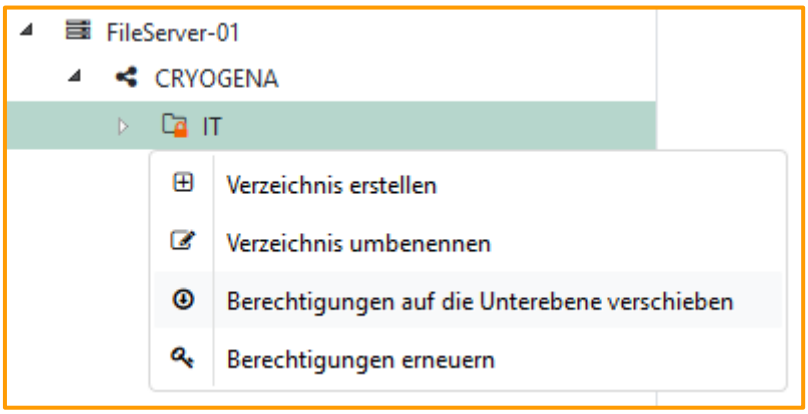
Zur Übernahme aller Änderungen klicken Sie den Button *Speichern*.

Die eingestellte Klassifizierung ist für normale Anwender (Antragsteller) nicht sichtbar. Der Verantwortliche einer klassifizierten Ressource erkennt diese am Symbol bei neuen Anträgen. Sie wird außerdem im Detailbereich einer ausgewählten Ressource im Tab *Berechtigungen* angezeigt.

**Bezüglich Reapproval:**
Sofern der *Administrator* für eine Klassifizierung die Option *Erneute Genehmigung aktivieren* gesetzt hat, werden Ressourcen, die Sie mit dieser Klassifizierung versehen haben, automatisch den Verantwortlichen zum *Reapproval* (siehe Kapitel 4.2.4) vorgelegt. Ob eine Klassifizierung für ein Reapproval vorgesehen ist, erkennen Sie an der entsprechenden Information innerhalb der Auswahlliste der Klassifizierungen.

#### 4.3.2.3 Kontextmenü

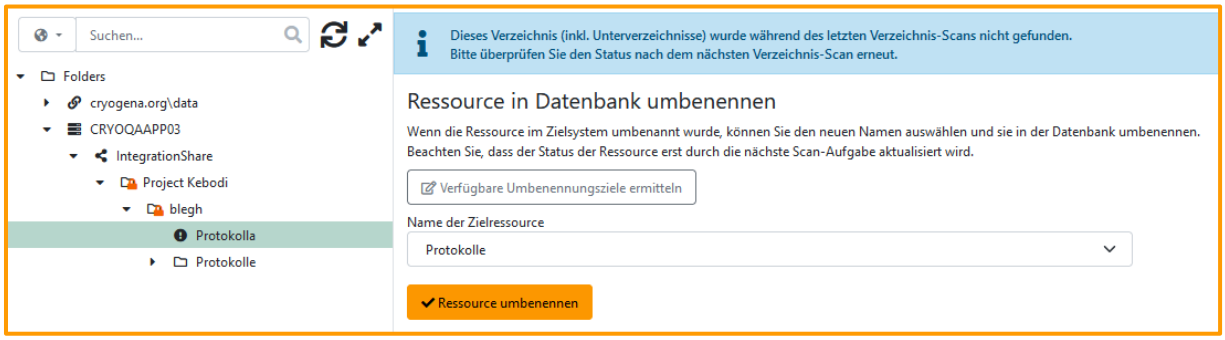
Zusätzlich zum Detailbereich haben Sie im Ressourcen-Baum die Möglichkeit per Rechts-Klick auf eine Ressource ein Kontextmenü zu öffnen, welches – abhängig von Ebenentiefe und Ressourcen-Typ – folgende Optionen bietet:




- *Verzeichnis erstellen:* Hiermit wird unterhalb des Ordners ein neues, zunächst nicht verwaltetes Verzeichnis im Dateisystem angelegt. Per Definition erbt dieses alle Zugriffsrechte des nächsthöheren Berechtigungsordners. Bei der Namensvergabe werden die vom Administrator global eingestellten Namensregeln beachtet. Diese Funktion ist analog für Sites des SharePoint Moduls verfügbar.
- *Verzeichnis umbenennen:* Die Namensänderung wird auch im Dateisystem durchgeführt. Es werden die vom Administrator global eingestellten Namensregeln beachtet. Diese Funktion ist analog für Sites des SharePoint Moduls verfügbar.
- *Berechtigungen auf die Unterebene verschieben:* Wenn es sich um einen Berechtigungsordner handelt, kann hiermit der Berechtigungsordner-Status auf alle direkt darunter liegenden Ordner übertragen und vom aktuellen Ordner entfernt werden. Ist ein darunter liegender Ordner ein bisher nicht verwalteter Ordner, erhält er nun den Status eines Berechtigungsordners mit denselben Einstellungen (zugewiesene Verantwortliche, Zugriffsrechte der Benutzer usw.). War der Unterordner bereits ebenfalls ein Berechtigungsordner, behält er seine bisherigen Einstellungen bei und erhält zusätzlich die Einstellungen des Elternordners (logische Zusammenführung).
- *Berechtigungen erneuern:* Diese Option steht standardmäßig nur den Administratoren zur Verfügung. Wurde diese Option vom Administrator auch für Besitzer freigegeben, können Sie damit eine sofortige Überprüfung / Korrektur der Berechtigungen auf der gewählten Ressource erzwingen.

#### 4.3.2.4 Nicht gefundene verwaltete Verzeichnisse reparieren

Es kommt vor, dass verwaltete Verzeichnisse ohne Wissen des Access Manager umbenannt, verschoben oder gelöscht werden. Bei den zyklischen Konsistenzprüfungen wird dies erkannt und mit einem entsprechenden Symbol am Verzeichnis angezeigt. Da eine automatische Behandlung dieses Fehlerfalls nicht möglich ist, kann der Administrator Ihnen die Möglichkeit geben, darauf zu reagieren. Sofern Sie sicher sind, dass der Ordner hier noch existiert und lediglich umbenannt wurde, können Sie eines der anderen (nicht verwalteten) Verzeichnisse auswählen und damit dem Access Manager mitteilen, dass es sich dabei um den vermissten Ordner handelt. Ihre Auswahl wird erst mit dem nächsten zyklisch geplanten Lauf des Verzeichnis-Scans umgesetzt.




Für die Behandlung aller anderen Fehlerfälle wenden Sie sich bitte an Ihren Administrator.

### 4.3.3 Verantwortliche verwalten

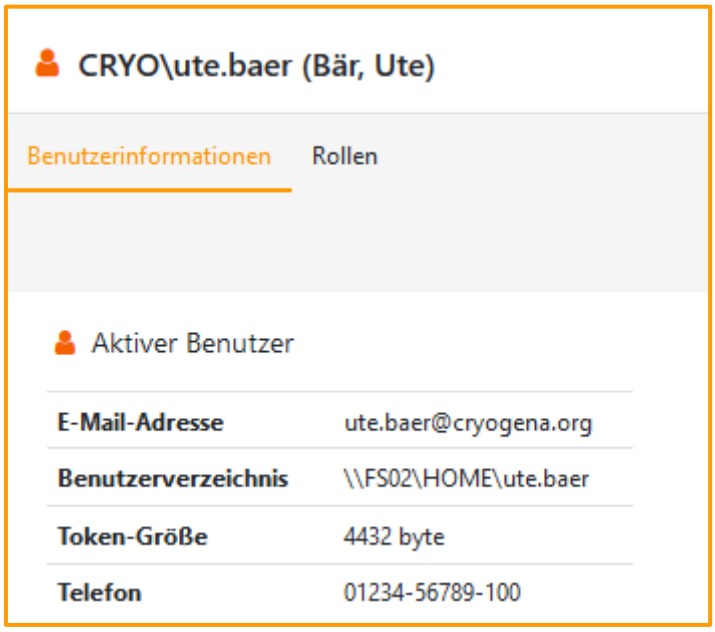

Wählen Sie in der linken Liste den Eintrag *Nach Benutzer* aus. Die Personenliste listet alle Verantwortlichen Ihrer Ressourcen auf und bietet verschiedene Möglichkeiten der Filterung an. Neben der Möglichkeit, über die Sucheingabe einen bestimmten Benutzer zu finden, kann über die Dropdown-Liste *Benutzerstatus* bestimmt werden, ob (de-)aktivierte Nutzerkonten angezeigt werden sollen. In jeder Filterung werden zunächst nur die ersten 100 Treffer angezeigt – daher gibt es am Ende der Liste die Möglichkeit auch die restlichen Konten anzuzeigen. Je nach Anzahl kann dies mehrere Sekunden dauern.

Benutzerkonten ist ein Symbol vorangestellt, das Auskunft über ihren aktuellen Status im Access Manager gibt:

- Aktiver Benutzer mit Berechtigungen / Rollen
- Aktiver Benutzer ohne Berechtigungen / Rollen
- Inaktiver Benutzer mit Berechtigungen / Rollen
- Inaktiver Benutzer ohne Berechtigungen / Rollen
- Blacklisted Benutzer mit Berechtigungen / Rollen

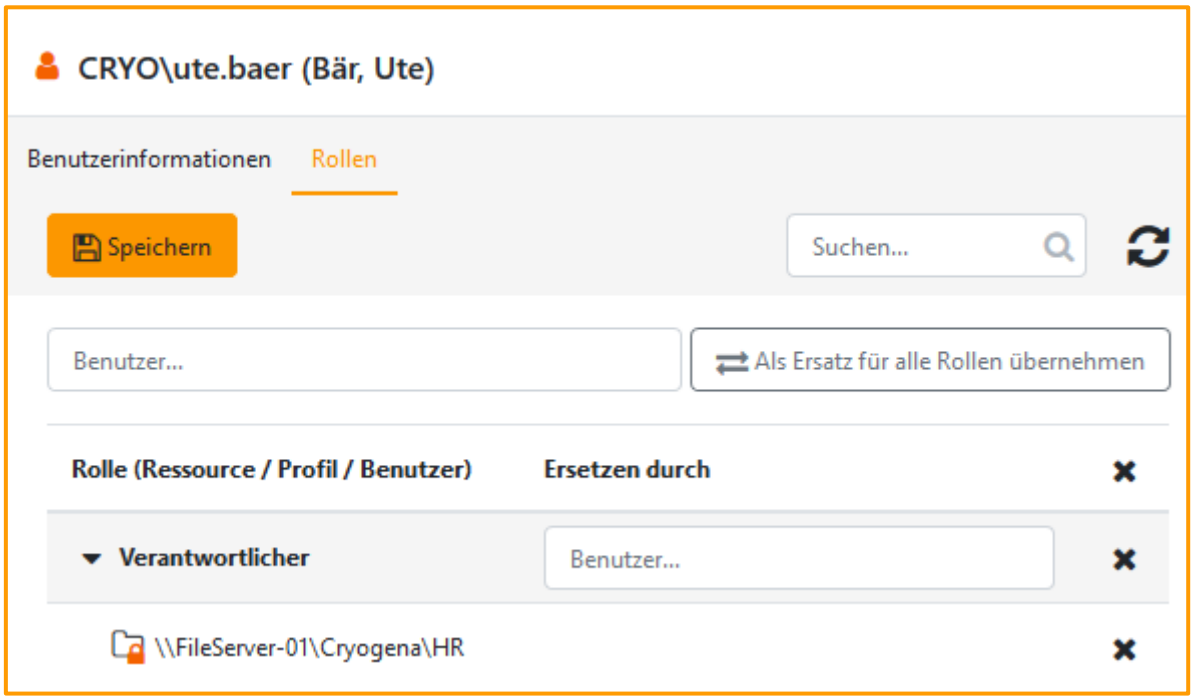
Bei sogenannten *Blacklisted Benutzern* handelt es sich um normale Benutzerkonten, die vom Administrator auf eine „Schwarze Liste“ gesetzt wurden. Damit werden sie in den üblichen Suchmasken und Eingabevervollständigungen nicht mehr berücksichtigt und nur angezeigt, falls sie bereits über Berechtigungen oder Rollen verfügen. Ohne Antrag lassen sich keine neuen Rollen vergeben, nur entfernen. Vorhandene Rechte werden aber vom Access Manager weiterhin überprüft und gepflegt, auch sind diese Anwender weiterhin in der Lage Anträge im Management Portal zu stellen.

#### 4.3.3.1 Detail-Tab „Benutzerinformationen“



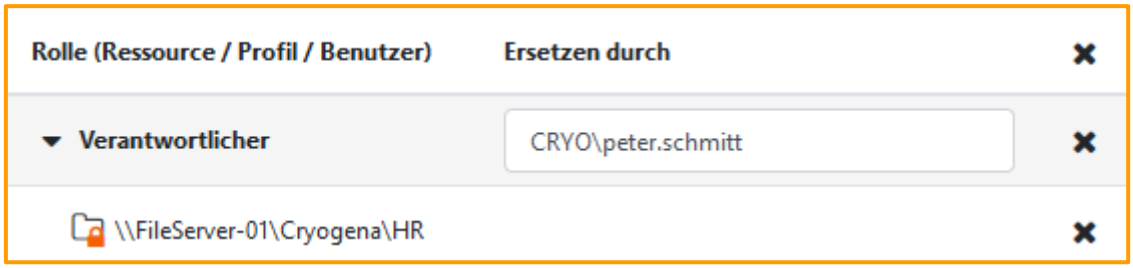

Im Tab *Benutzerinformationen* werden zunächst allgemeine Informationen über das Benutzerkonto gezeigt. Diese umfassen z.B. die E-Mail-Adresse und das Benutzerverzeichnis (sofern verfügbar) und weitere technische Angaben.

#### 4.3.3.2 Detail-Tab „Rollen"




Im Tab *Rollen* werden unter dem Eintrag *Verantwortlicher* alle Ressourcen der ausgewählten Person aufgeführt, die von Ihnen verwaltet werden. Über das Kreuz-Symbol neben jedem Verzeichnis kann der Person die Verantwortlichen-Rolle selektiv entzogen werden. Dies ist nicht möglich (Kreuz ist grau / deaktiviert), wenn es sich um die einzige Person mit dieser Rolle auf dem Verzeichnis handelt. Änderungen werden erst nach einem Klick auf den *Speichern* Button übernommen.

Alternativ können Sie den Verantwortlichen durch einen anderen ersetzen:




Die Ersetzung geschieht erst nach einem Klick auf den *Speichern* Button – dabei werden die betroffenen Personen per Email informiert.

Diese Funktion ist insbesondere sinnvoll, um deaktivierte Benutzer ausfindig zu machen und ihre Verwaltungsrollen auf andere Personen zu übertragen, damit z.B. die Rechtevergabe auf verwaltete Ressourcen weiterhin gewährleistet ist.

### 4.3.4 Eigene Vertreter bestimmen


Diese Seite dient dazu, für einen (un-)begrenzten Zeitraum (z.B. während Ihres Urlaubs) eine oder mehrere andere Personen zu Ihrem Vertreter zu ernennen. Da es nicht vorgesehen ist, dass diese Vertreter wiederum weitere Vertreter benennen können, steht Ihnen diese Seite nur zur Verfügung, wenn Sie die Rolle *Besitzer* innehaben. Ein Besitzer-Vertreter hat Zugriff auf fast alle verantworteten Seiten (siehe vorangegangene Kapitel) und erhält alle Möglichkeiten des Besitzers zur Ressource- und Verantwortlichenverwaltung. Die Benennung eines Vertreters bedeutet nicht, dass Sie als Besitzer Ihre administrativen Möglichkeiten verlieren – Sie können auch weiterhin alle Aufgaben durchführen.

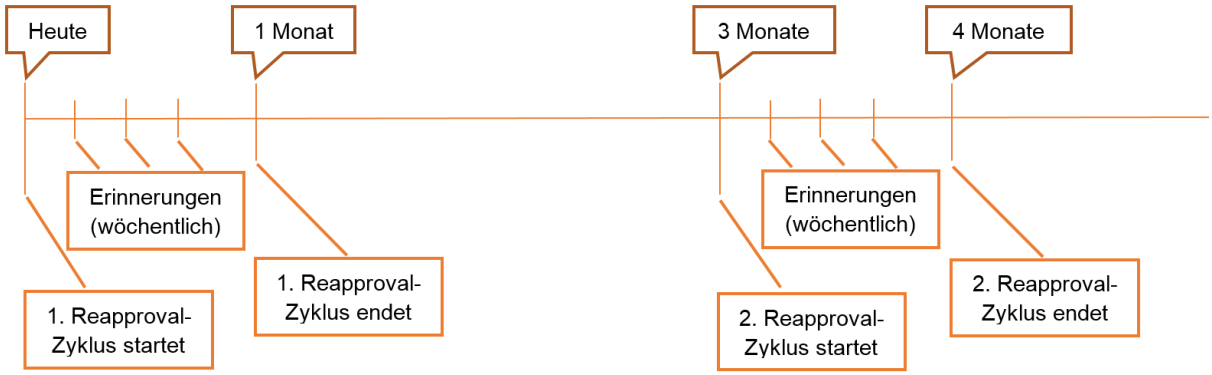
Für die Vertretung lässt sich wahlweise ein Gültigkeitszeitraum angeben, wobei sowohl der Beginn als auch das Ende optional sind. Wird kein Startdatum eingetragen, beginnt die Vertretung sofort; fehlt eine Angabe zum Ende, läuft die Vertretung solange, bis Sie den Vertreter entfernen.

Über den Button *Entfernen* ✖ können einzelne Vertreter entfernt werden; mit *Bearbeiten* ändern Sie bspw. den Gültigkeitszeitraum der Vertretung.

## 4.4 Reapproval – Workflow zur erneuten Genehmigung

Beim Reapproval sollen bestimmte Ressourcen (Verzeichnisse, SharePoint Sites, Dritt-Elemente) in regelmäßigen Abständen darauf überprüft werden, ob die in der Vergangenheit vergebenen Zugriffsberechtigungen noch immer erforderlich bzw. gewünscht sind.

Ein Reapproval-Zyklus wird vom *Administrator* nach Unternehmensvorgaben definiert. Er startet in regelmäßigen Intervallen (z.B. alle drei Monate) und hat eine feste Laufzeit (z.B. 4 Wochen). Innerhalb dieser Zeit werden die zuständigen Ressource-Verantwortlichen mehrmals per Mail an die notwendige Überprüfung erinnert, sofern sie diese noch nicht abgeschlossen haben.




Eine Überprüfung wird immer pro Ressource vorgenommen und beinhaltet eine Bestätigung / Aktualisierung oder auch eine Löschung der vorhandenen Berechtigungen von Benutzern und Profilen. Sobald ein Verantwortlicher alle seine Ressourcen überprüft hat, ist seine Aufgabe für diesen Reapproval-Zyklus abgeschlossen.

Über Berichte lässt sich während eines Zyklus jederzeit der aktuelle Zustand der zu überprüfenden Ressourcen ausgeben. Wurden mit Ende eines Zyklus noch nicht alle Ressourcen geprüft, können, abhängig von Ihrer Unternehmensentscheidung, alle unbestätigten Berechtigungen entfernt werden.

### 4.4.1 Zuständigkeiten

Während die Reapproval-Intervalle und -Laufzeiten vom *Administrator* bestimmt werden, legt der *Besitzer* fest, welche seiner Ressourcen im Rahmen des Reapprovals von den *Verantwortlichen* behandelt werden sollen.

### 4.4.2 Reapproval-Zuweisung

Ein *Klassifizierungsadministrator* legt zunächst Klassifizierungen an mit der Option des Reapprovals. Der Besitzer weist eine solche Klassifizierung den zu überprüfenden Ressourcen zu. Der Verantwortliche erhält dann automatisch die Aufforderung zum Reapproval und führt dies durch.

### 4.4.3 Interner Ablauf (für Administratoren)

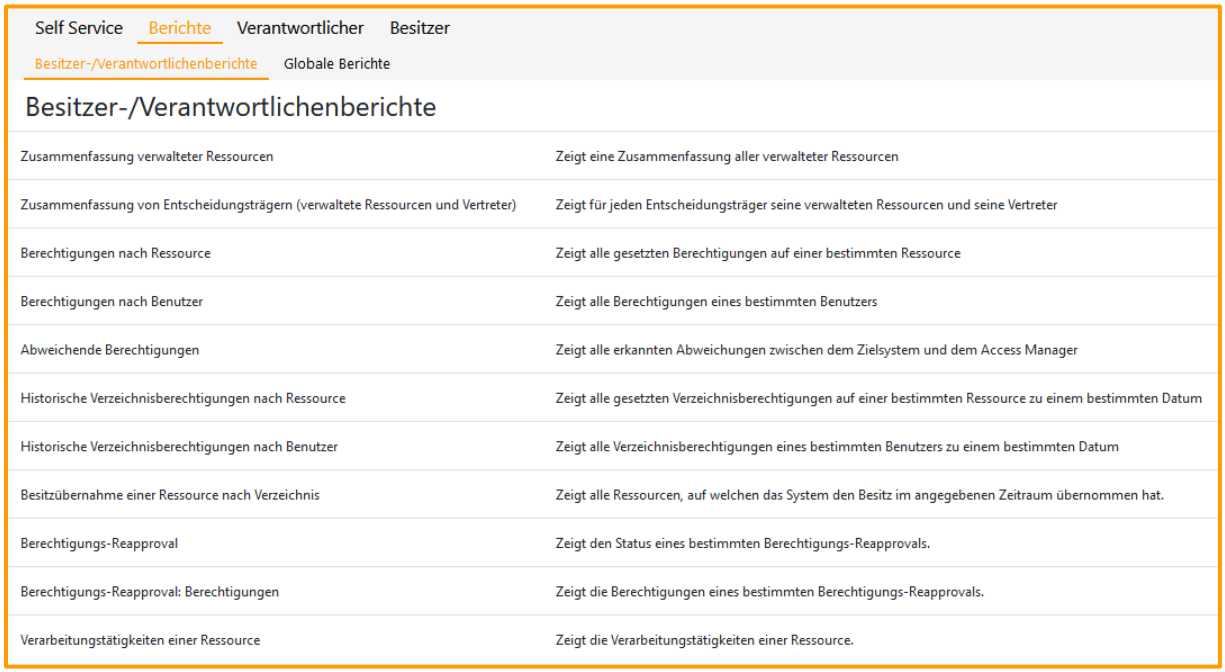
Mit dem Start eines neuen Reapproval-Lauf (durch die Aufgabe *InitializeReapproval* geplant) erhalten die Administratoren sowie alle vom Reapproval betroffenen Verantwortlichen eine Mail, die sie über die zyklische Überprüfung der vorhandenen Berechtigungen informiert. Die Aufgabe *InitializeReapproval* erstellt automatisch vier weitere Aufgaben: 3x *ReapprovalReminder* mit der Ausführungszeit, die sich aus der administrativen Einstellung *ReapprovalReminderInterval* ergibt, sowie der Aufgabe *FinishReapproval*, deren Ausführungszeit sich aus der Einstellung *ReapprovalMaxDurationInDays* ergibt (Startzeit des *InitializeReapproval* plus Anzahl der Tage). Sollte ein neuer Reapproval-Lauf gestartet werden, während der vorhergehende Lauf noch nicht abgeschlossen ist, wird mit dem neuen Lauf automatisch sofort ein *FinishReapproval* (s.u.), durchgeführt, um den vorherigen Lauf abzuschließen. Bereits geplante Aufgaben *ReapprovalReminder* und *FinishReapproval* werden dabei nicht aus der Aufgabenwarteschlange gelöscht, lösen aber für den abgeschlossenen Lauf keinen E-Mail-Versand mehr aus.

Zweck der *ReapprovalReminder* Aufgaben ist es, diejenigen Verantwortlichen zu erinnern, die die Überprüfung ihrer zugewiesenen Ressourcen noch nicht vollständig abgeschlossen haben. Die ersten beiden Erinnerungsmails werden nur den Verantwortlichen geschickt, die dritte Mail geht zusätzlich an die Besitzer, um ggf. steuernd eingreifen zu können, bevor die Überprüfungsphase beendet ist.

Die Aufgabe *FinishReapproval* beendet den Lauf, indem alle noch ungeprüften Ressourcen mit dem Status *Abgeschlossen ohne Bearbeitung* versehen und für eine weitere Bearbeitung gesperrt werden. Abschließend wird eine Informationsmail über das Ende des Reapproval-Laufs an die Administratoren, Besitzer und Verantwortlichen geschickt. Abhängig von der administrativen Einstellung *RevokeOpenPermissionsOnFinishReapproval* (siehe Kapitel 12.7.1.29) können in diesem Schritt alle nicht bestätigten Berechtigungen automatisch gelöscht werden, d.h. die betroffenen Personen verlieren ihre Zugriffsrechte auf die entsprechenden Ressourcen.

Im Audit erscheinen im Rahmen des Reapprovals nur solche Berechtigungen, welche durch den prüfenden Verantwortlichen verändert wurden (Recht entzogen, von Lesen nach Schreiben geändert bzw. umgekehrt, Ablaufdatum angepasst, …). Bei einer reinen Bestätigung erscheint die Berechtigung zwar im Bericht, nicht jedoch im Audit.

# 5 Berichte zur Berechtigungssituation




Berichte geben Auskunft über verschiedene Aspekte der verwalteten Ressourcen. So lassen sich bspw. Übersichtstabellen zusammenstellen, die alle Verzeichnisse und Sites auflisten, für die ein Verantwortlicher aktuell zuständig ist. Die zur Verfügung stehenden Berichtstypen sind in ihrer Beschreibung selbsterklärend, ihre Daten beziehen sich immer auf den aktuellen Zeitpunkt des Aufrufs.

Durch Auswahl eines verfügbaren Berichts in der Übersicht öffnet sich unterhalb der Liste ein Bereich zur Filterung der Daten. Hier haben Sie die Möglichkeit nach verschiedenen Kategorien oder einer verfügbaren Rolle zu filtern. So können Sie entscheiden, ob Sie z.B. nur die Ressourcen angezeigt bekommen möchten, welche Sie besitzen oder verantworten. Im Falle einer Benutzerrechte-Abfrage ist es erforderlich, den Anmeldenamen (*Benutzer-ID*) des gewünschten Benutzers einzugeben.

## 5.1 Berichte für Datenverantwortliche

Dateneigner, die die Rolle *Besitzer* und / oder *Verantwortlicher* besitzen, haben über die Berichte nur Einsicht auf die von ihnen verwalteten Ressourcen (persönliche Berichte), alle Fremd-Ressourcen bleiben ihnen verborgen.

Haben Sie sowohl die Rolle *Administrator / Berichtebenutzer* Rolle, können Sie im Untermenü zwischen den beiden Berichtstypen *Besitzer-/Verantwortlichenberichte* und *Globale Berichte* wählen. Die Berichte sind identisch, nur die Datenmenge unterscheidet sich.

Darüber hinaus haben Sie als Administrator zusätzlich die Möglichkeit, Berichte per Mail zu versenden – auch automatisch wiederholend.

## 5.2 Globale Berichte

Benutzer mit der Rolle *Administrator* oder *Berichtebenutzer* erhalten personenübergreifende – globale – Berichte, die die Situation aller Ressourcen umfassen.

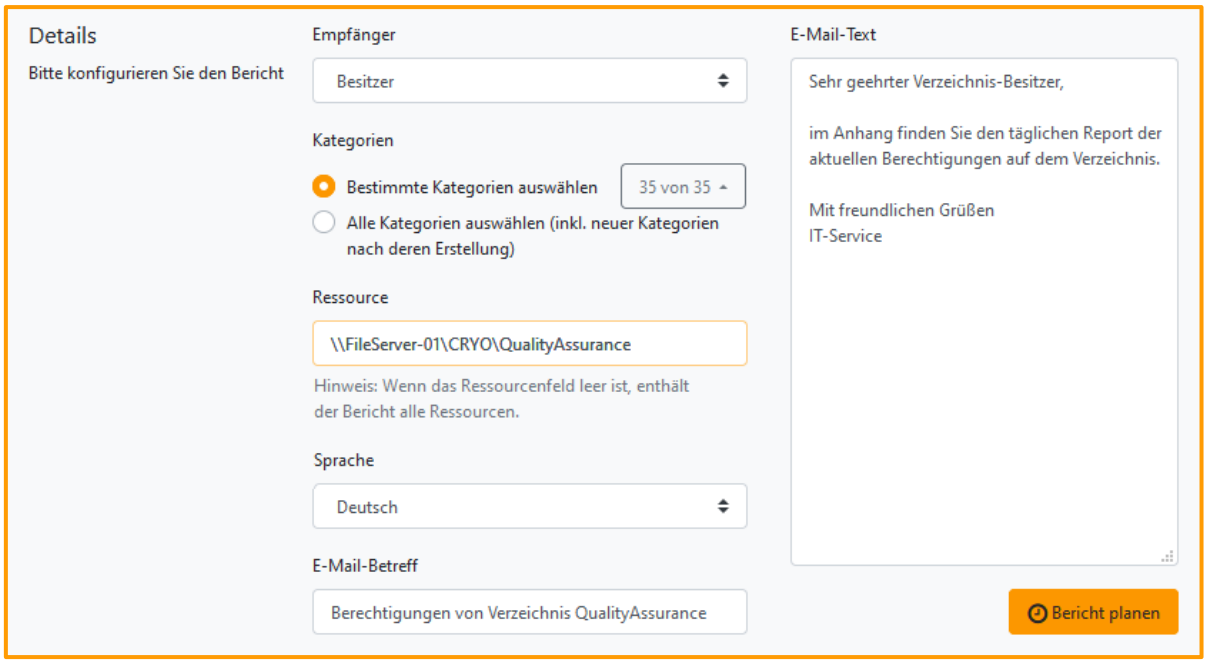
Haben Sie sowohl die *Verantwortlicher / Besitzer* Rolle als auch die *Administrator / Berichtebenutzer* Rolle, können Sie im Untermenü zwischen beiden Berichtstypen wählen. Die Berichte sind identisch, nur die Datenmenge unterscheidet sich.

## 5.3 Berichtversand

Als *Administrator* steht Ihnen ein weiterer Untermenüpunkt zur Verfügung, der *Berichtversand*. Hierüber haben Sie die Möglichkeit, den Bericht *Berechtigungen nach Ressource* einem bestimmten Anwenderkreis **im PDF-Format** per Mail zu senden, wahlweise einmalig oder auch wiederkehrend auf Basis eines Zeitplans. Bereits erstellte Versandpläne werden Ihnen in der Übersichtstabelle angezeigt:

### 5.3.1 Berichtversand erstellen

Zum Erstellen eines Berichtversands klicken Sie zunächst den Button *Neuen Bericht planen*. Im unteren Bildschirmbereich können Sie nun die Versandoptionen eingeben:




#### 5.3.1.1 Empfänger

Wählen Sie aus, welche Personengruppe den Bericht erhalten soll. Wenn Sie *Besitzer* oder *Verantwortlicher* auswählen, erhalten nur die von den jeweiligen Ressourcen betroffenen Personen den Bericht, nicht per se alle Anwender mit dieser Rolle.

#### 5.3.1.2 Kategorien

Bestimmen Sie, welchen Ressourcen-Typ Sie im Bericht einschließen wollen.

Mit der ersten Option wählen Sie gezielt bestimmte Kategorien (Ressourcen-Typen) aus, nur diese werden im Bericht berücksichtigt. Diese Auswahl ist statisch, d.h. sie verändert sich auch zukünftig nicht, wenn Sie weitere Ressourcen-Typen im Access Manager anlegen. Demgegenüber arbeitet die zweite Option dynamisch, d.h. bei der Berichterstellung werden alle zu diesem Zeitpunkt verfügbaren Kategorien mit einbezogen.

#### 5.3.1.3 Ressource

Wenn Sie dieses Feld leer lassen, werden alle verwalteten Ressourcen der o.a. Kategorien berichtet. Alternativ geben Sie hier genau eine Ressource an. Erstellen Sie dafür ggf. mehrere Berichtspläne.

#### 5.3.1.4 Sprache

Geben Sie hier an, in welcher Sprache (deutsch oder englisch) der Bericht erstellt werden soll. Diese Auswahl hat keinen Einfluss auf den im Folgenden angegebenen Betreff und Text der Email.

#### 5.3.1.5 E-Mail-Betreff

Tragen Sie hier den Betreff der Bericht-Mail ein.

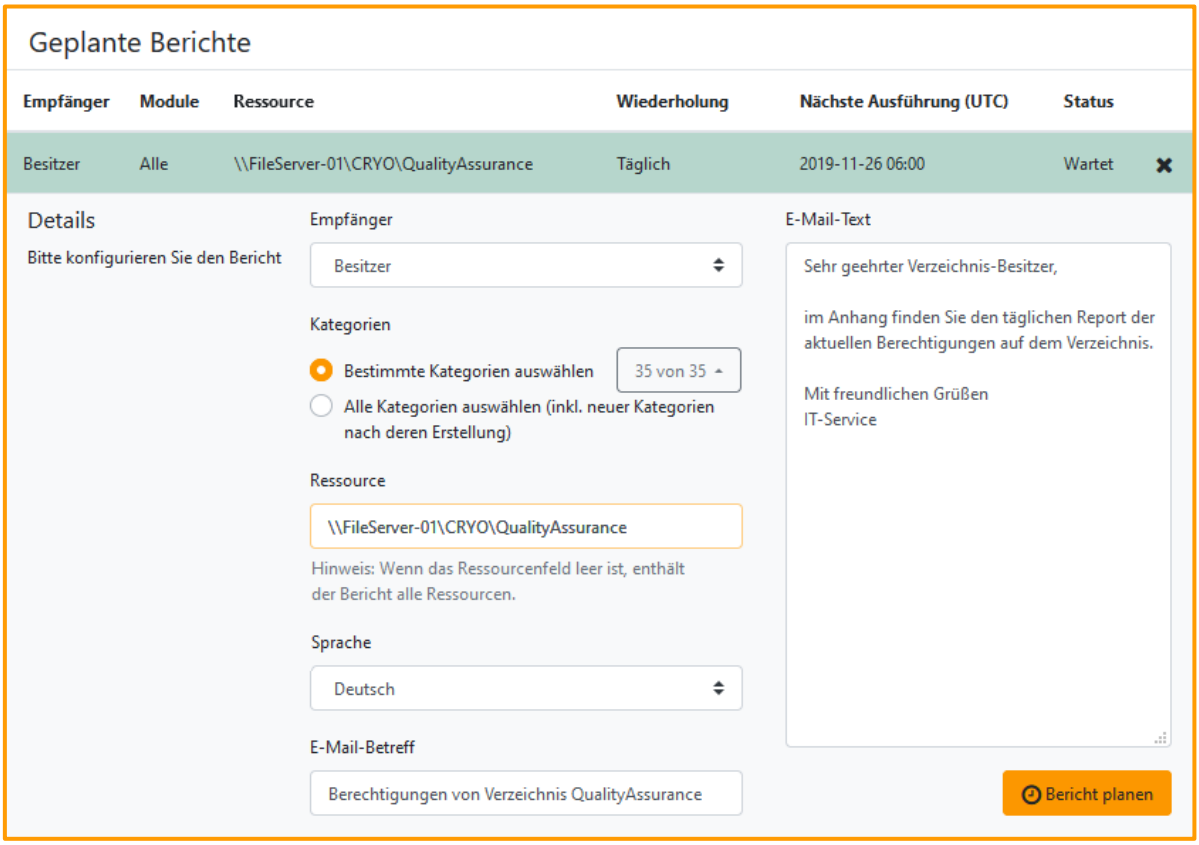
#### 5.3.1.6 E-Mail-Text

Tragen Sie hier den begleitenden Text der Bericht-Mail ein. Es werden derzeit keine Platzhalter oder Formatierungsoptionen unterstützt.

### 5.3.2 Zeitplan hinzufügen / ändern

Nach dem Erstellen der Inhalte und Empfänger klicken Sie auf *Bericht planen* und Sie gelangen zum Zeitplanungsdialog. Dieser entspricht der Oberfläche, die Sie auch bei der *Aufgabenplanung* (Kapitel 10.4) verwenden. Mit dem Button *Aufgabe planen* schließen Sie den neuen Berichtversand ab. Sie finden diesen auch in der Aufgabenwarteschlange (Kapitel 10.7) unter dem Namen *SendReports* wieder.

Um einen bereits eingerichteten Versand zu verändern, klicken Sie den gewünschten Eintrag in der Übersichtsliste an. Im unteren Bereich werden Ihnen nun alle Details dazu angezeigt und können angepasst werden. Der Button *Berichtplanung ändern* führt Sie wieder zum Zeitplanungsdialog. Dieser muss bestätigt werden, um die textuellen und inhaltlichen Änderungen Ihrer Mail-Angaben zu speichern.



## 5.4 Bericht „Berechtigungs-Reapproval“

Dieser Bericht steht neben Administratoren nur Besitzern und ihren Vertretern zur Verfügung – letzteren aber nur in dem Zeitraum, in dem sie Vertreter sind. Die Auswahlliste *Datum auswählen* zeigt die Startzeitpunkte aller Reapproval-Läufe (auch des aktuell laufenden). Für einen Lauf zeigt ein Bericht für alle Ressourcen mit Reapproval-Markierung ihren aktuellen Reapproval-Status sowie den Besitzer und die Verantwortlichen.

## 5.5 Bericht „Berechtigungs-Reapproval: Berechtigungen“

Dieser Bericht steht neben Administratoren sowohl Besitzern als auch Verantwortlichen (inklusive ihrer Vertreter während der Vertretungszeit) zur Verfügung. Die Auswahlliste *Datum auswählen* zeigt die Startzeitpunkte aller Reapproval-Läufe (auch des aktuell laufenden). Nach der Auswahl eines Laufs lässt sich der Bericht auf eine bestimmte Ressource einschränken, alternativ können alle Ressourcen (nur solche mit Reapproval-Markierung) ausgegeben werden. Der Bericht zeigt pro Ressource den aktuellen Status, den Genehmiger, die bisher berechtigten Objekte (Benutzerkonten / Profile) mit ihrer Berechtigung sowie die Entscheidung des Genehmigers dazu (Bestätigt / Entzogen).

## 5.6 Bericht „Verarbeitungstätigkeiten einer Ressource“

Dieser Bericht steht nur den Klassifizierungsadministratoren zur Verfügung und führt datenschutzrelevante Informationen der verwalteten Ressourcen auf. Außer der Auflistung aller Klassifizierungsadministratoren wird jede verwendete Klassifizierung mit ihren Detailangaben gezeigt sowie die Ressourcen, die der jeweiligen Klassifizierung zugeordnet wurden.

Neben den Filtermöglichkeiten auf bestimmte lizenzierte Module und die Eingrenzung auf eine oder alle Ressourcen lassen sich außerdem die Klassifizierungen auswählen, die eine Ressource haben soll.

## 5.7 Bericht „Abweichende Berechtigungen“

Dieser Bericht zeigt an, welche abweichenden Berechtigungen das System nach einer Überprüfung auf den verwalteten Ressourcen gefunden hat. Hierbei werden die im Access Manager festgelegten Berechtigungen als Referenz verwendet.

Der erstellte Bericht enthält pro Ressource folgende Spalten:

**Datum:**
Zeitstempel zu dem die Berechtigung entdeckt wurde.

**Art der Abweichung:**
*Nicht autorisierter Benutzer* – Benutzer- / Gruppen-Objekt, das laut DB nicht in der AD-Gruppe enthalten sein durfte.

*Nicht autorisierte Berechtigung* – Benutzer- / Gruppen-Objekt, das laut DB nicht auf dem Filesystem berechtigt sein durfte.

*Fehlender Benutzer* – Benutzer- / Gruppen-Objekt, das laut DB in der AD-Gruppe fehlte.

*Fehlende AD-Gruppe* – AM-eigenes Gruppen-Objekt, das laut DB im Filesystem fehlte.

**Prinzipal:**
Das AD Objekt, welches editiert bzw. vom Filesystem entfernt wurde.

**Berechtigungen:**
Die fehlerhaften Berechtigungen des betroffenen AD Objektes.

**Deny-Regel:**
Gibt an, ob es sich um eine Verbotsregel handelte.

**Geerbt:**
Gibt an, ob das Recht geerbt wurde.

**Weitere Informationen:**
Hier wird bei *Fehlender Benutzer* und *Nicht autorisierter Benutzer* in der Spalte „Art der Abweichung“ das Benutzer- / Gruppen- Objekt angezeigt, das nicht in den AM AD-Gruppen enthalten sein / fehlen durfte.

## 5.8 Passwortberichte

Als AMPR-Administrator können Sie sich einen Bericht erstellen lassen, der über die im gewünschten Zeitraum erfolgten Passwort-Resets der Benutzer Auskunft gibt. Dieser Bericht ist nicht ad hoc einsehbar, sondern wird Ihnen per E-Mail zugestellt.

# 6 Berechtigungsmanagement mit Profilen & Vorlagen

Mit Profilen und Vorlagen wird das Berechtigungsmanagement flexibler und spart viel manuelle Berechtigungsarbeit. Man unterscheidet zwischen Profil- und Vorlagenmanagement.

Durch *Profile* können Sie logische Gruppen von Anwendern und Ressourcen definieren und hierdurch Berechtigungen einer Menge von Anwendern zuweisen. Profile bieten eine flexible Möglichkeit, Berechtigungen dynamisch nach selbstdefinierten Hierarchien zu gruppieren und zuzuweisen bzw. zu entziehen.

Mit *Globalen Vorlagen* können Sie Schablonen erstellen, durch die Sie künftig auf einfache Weise eine große Anzahl an immer gleichen Berechtigungen und Berechtigungsordnern mit wenigen Mausklicks verschiedenen Benutzer zuweisen. Diese Vorlagen sind explizit öffentlich, d.h. von mehreren ausgewählten Personen sicht- und nutzbar und können Verzeichnisse verschiedener Verantwortlicher umfassen. Das Erstellen persönliche Vorlagen als Verantwortlicher wird in Kapitel 4.2.5 beschrieben.

Vorlagen können nur auf Berechtigungsverzeichnisse angewendet werden, Berechtigungssites und Dritt-Elemente werden nicht unterstützt.

## 6.1 Arbeitsprinzip: Benutzer- und Organisationsprofile

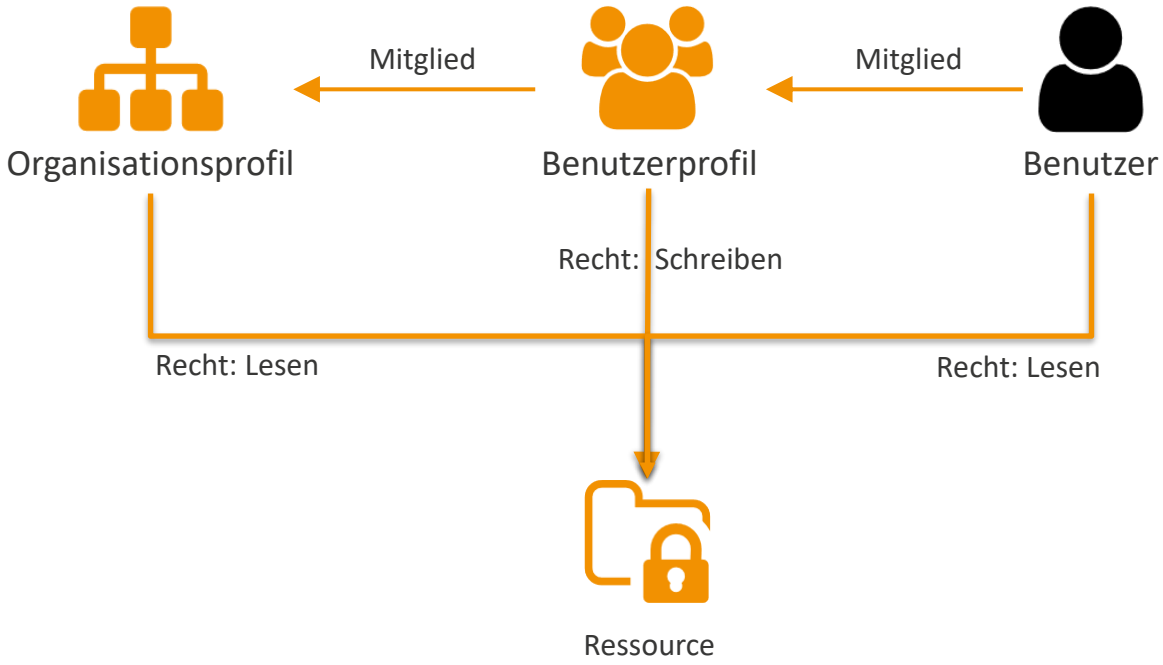
Das Berechtigungsmanagement mit Profilen ermöglicht die Abbildung von Unternehmensstrukturen durch eine dauerhafte Verknüpfung der Berechtigungen zu Benutzergruppen. Die logische Gruppierung von Anwendern und Ressourcen kann z.B. Berechtigungsprozesse aus dem Personalbereich erheblich vereinfachen, indem bei Mitarbeiterveränderungen (Neuzugänge, Abteilungswechsel, Mitarbeiterabgang) lediglich die der Abteilung oder dem Team zugeordneten Profile angepasst werden müssen.

Durch das Profilmanagement stehen Ihnen drei Varianten zum Berechtigen zur Verfügung:

- *Benutzerprofile:* In diesen können mehrere einzelne Benutzer in einem Benutzerprofil gruppiert werden, z.B. alle Mitarbeiter einer Projektarbeitsgruppe. Durch Zuweisung von Zugriffsrechten auf Ressourcen zu diesem Benutzerprofil erhalten alle Profilmitglieder automatisch diese Rechte. Wird eines der Zugriffsrechte auf eine Ressource im Benutzerprofil geändert oder entfernt, wirkt sich diese Änderung direkt auf die Berechtigung der Profilmitglieder aus.
- *Organisationsprofile:* Um die Abbildung von komplexen hierarchischen Strukturen im Berechtigungsmanagement zu ermöglichen, gibt es mit Organisationsprofilen eine weitere Gruppierungsstufe. Organisationsprofilen können ebenfalls Zugriffsrechte auf verschiedenen Ressourcen zugewiesen werden. Als Mitglieder können hier beliebig viele Benutzerprofile hinzugefügt werden, jedoch keine einzelnen Benutzer. Durch Mitgliedschaft eines

Benutzerprofils in einem Organisationsprofil erhalten alle Mitglieder des Benutzerprofils zusätzlich die Rechte, welche durch das Organisationsprofil gewährt werden. Wird eines der Zugriffsrechte auf eine Ressource im Organisationsprofil geändert oder entfernt, wirkt sich diese Änderung direkt auf die Berechtigungen der Profilmitglieder aus.

- *Persönliche Berechtigungen:* Außer Berechtigungen, die ein Benutzer aufgrund einer Team- oder Abteilungszugehörigkeit erhält, können zusätzliche „persönliche Rechte“ vergeben werden. Dies kann über *Persönliche Berechtigungen* erfolgen, indem Sie einem Benutzer explizite Zugriffsrechte auf eine Ressource geben. Werden die Profilberechtigungen verändert oder der Benutzer aus einem Profil entfernt, hat dies keine Auswirkungen auf seine persönlichen Berechtigungen.

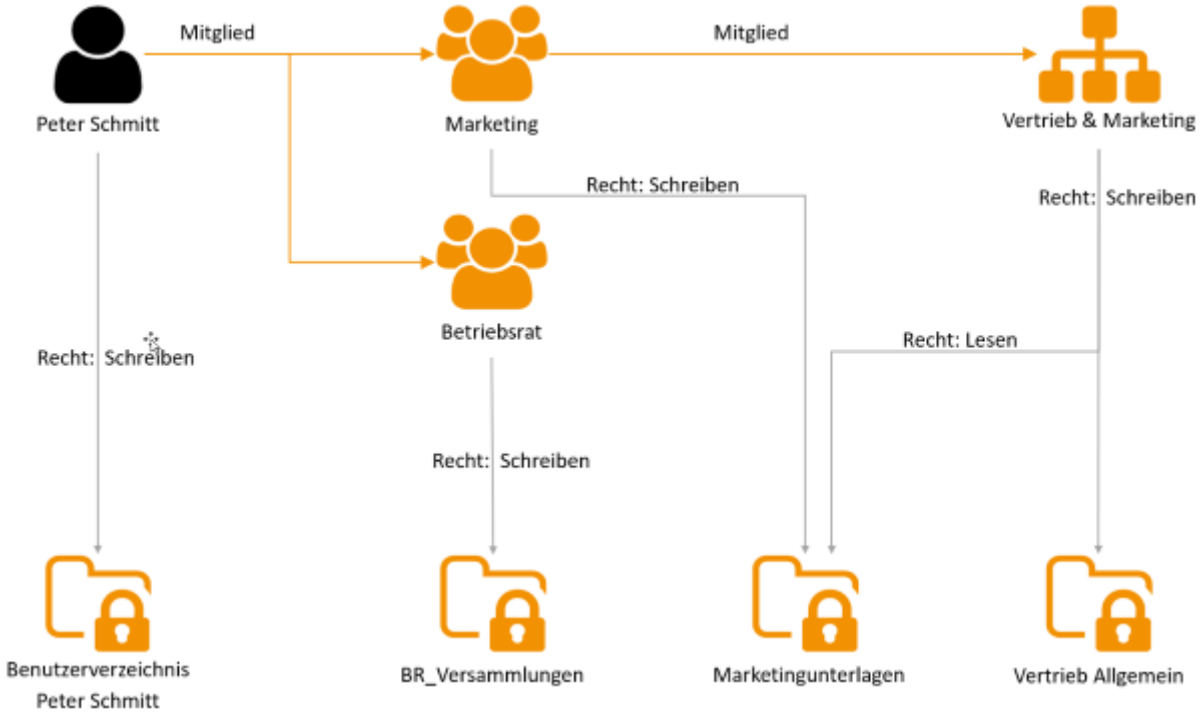



Durch das Arbeiten mit Profilen wird die Abbildung verschiedener Organisationsstrukturen ermöglicht. Hierdurch entsteht jedoch zusätzlich die Möglichkeit, dass einem Benutzer auf einer bestimmten Ressource mehrere Berechtigungen zugewiesen werden. Aus diesen verschiedenen Berechtigungen errechnet der Access Manager die sogenannte *effektive Berechtigung*. Sie entspricht grundsätzlich dem höchsten zugewiesenen Recht des Benutzers, wobei eine Schreiben-Berechtigung höher ist als eine Lesen-Berechtigung (bei SharePoint Berechtigungen ist die Gestalten-Berechtigung wiederum höher als die Schreiben-Berechtigung).

**Ein Beispiel:**

Der Mitarbeiter Peter Schmitt ist aufgrund seiner Abteilungszugehörigkeit Mitglied im Benutzerprofil *Marketing*. Dies ist ein Profil, welches logisch in den Bereich Sales & Marketing fällt, weshalb dieses Benutzerprofil Mitglied im Organisationsprofil *Sales & Marketing* ist. Zusätzlich ist Peter Schmitt jedoch im Betriebsrat und hierdurch Mitglied in dem dazugehörigen Benutzerprofil *Work Council*. Durch diese logische Zuordnung zu den verschiedenen Profilen erhält er Berechtigungen auf den Verzeichnissen *WC_Meetings* (durch Benutzerprofil Work Council), *Sales* (durch Organisationsprofil Sales & Marketing), sowie auf das Verzeichnis *Marketing*. Auf dem zuletzt genannten Verzeichnis erhält er sowohl aufgrund der Mitgliedschaft im Benutzerprofil *Marketing*, als auch aufgrund der Zugehörigkeit im Organisationsprofil *Sales & Marketing*, Berechtigungen. Er erhält hierfür Schreiben-Zugriff, da das höhere Recht durch das System errechnet wurde. Die Lesen-Berechtigung ist für ihn direkt zunächst nicht relevant, jedoch können weitere Benutzerprofile Mitglied im Organisationsprofil *Sales & Marketing* sein, welche kein zusätzliches Schreiben-Recht auf diesem Verzeichnis haben. In ihrem Fall wird das Lesen-Recht effektiv.

Zusätzlich hat der Benutzer Peter Schmitt eine persönliche Berechtigung auf seinem Benutzerverzeichnis *Peter Schmitt*.



# 6.2 Profil- und Clustermanagement

## 6.2.1 Cluster und Profile

Cluster, oder auch Profilcluster, stellen eine Gruppierungsmöglichkeit für Profile dar. Sie dienen lediglich der besseren Übersichtlichkeit und haben eine rein ordnende Funktion.

Alle Profile sind einem Cluster zugehörig – standardmäßig existiert als Wurzelelement immer der Cluster „/“, ohne weitere Cluster werden alle Profile hier angelegt.

Um Profile und Cluster verwalten zu können, benötigen Sie die Rolle *Profiladministrator*. Ein Profiladministrator darf Profile & Cluster erstellen, verschieben, verändern und löschen. Er kann alle existierenden Profile & Cluster sehen und bearbeiten, d.h. er kann ihre Namen und Cluster-Zugehörigkeit ändern, bei Profilen Ressourcen hinzufügen, entfernen, ihre Zugriffsrechte bestimmen sowie den oder die *Profilverantwortlichen* festlegen. Ein *Profilverantwortlicher* sieht nur die Profile, für die er als Verantwortlicher definiert wurde, um Mitglieder innerhalb der Profile zu verwalten. Er kann keine neuen Profile oder Cluster erstellen, verändern oder löschen.

In der Baumansicht links werden alle angelegten Cluster und Profile aufgelistet. Es werden zwei Profiltypen unterschieden:

- *Benutzerprofil* – Es können nur Benutzerkonten als Mitglieder zugewiesen werden.
- *Organisationsprofil* – Es können nur Benutzerprofile als Mitglieder zugewiesen werden, einzelne Benutzerkonten sind hier nicht vorgesehen. Ebenso können keine weiteren Organisationsprofile verschachtelt werden.

## 6.2.2 Cluster verwalten

Wählen Sie zunächst den Cluster aus, den Sie bearbeiten möchten. Im rechten Detailbereich erhalten Sie eine Reihe von Möglichkeiten zur weiteren Bearbeitung. Diese sind in Abschnitte unterteilt (*Neues Kindelement erstellen*, *Profilcluster bearbeiten*, *Cluster löschen*), in denen sich aufklappbare Unterabschnitte befinden können. Durch einen Klick auf einen solchen grau hinterlegten Unterabschnitt klappen Sie diesen auf und können die erforderlichen Informationen eingeben.

### 6.2.2.1 Cluster anlegen

Im Detailbereich klappen Sie unter *Neues Kindelement erstellen* den Unterabschnitt *Neues Cluster erstellen* auf und geben den neuen Clusternamen ein. Dieser Name darf innerhalb des Eltern-Clusters noch nicht existieren, in anderen Clustern jedoch schon. Nach Klick auf den Button *Cluster erstellen* erscheint der neue Cluster sofort links in der Baumansicht.

#### 6.2.2.2 Cluster umbenennen und verschieben

Im Abschnitt *Profilcluster bearbeiten* ändern Sie den Clusternamen oder geben einen anderen Clusterpfad an – hierbei erscheint eine Liste der möglichen Pfade, aus denen Sie auswählen können, andere Clusterpfade sind nicht möglich. Drücken Sie anschließend für jedes geänderte Feld den *Speichern* Button. Die Änderungen sind sofort in der Baumansicht sichtbar.

Sie erhalten eine Fehlermeldung, wenn ein Cluster in einen anderen verschoben werden soll, in dem bereits ein gleichnamiger Cluster existiert.

#### 6.2.2.3 Cluster löschen

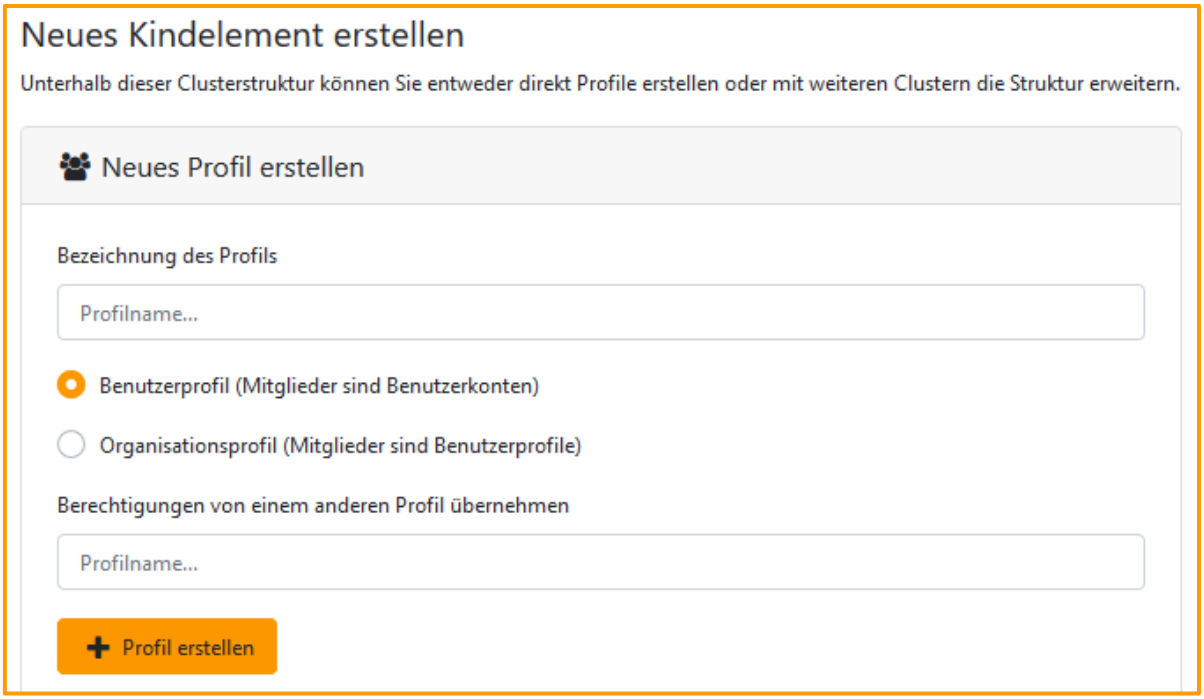
Da enthaltene Elemente (Profile und Cluster) des zu löschenden Clusters nicht mitgelöscht werden, geben Sie im Abschnitt *Cluster löschen* zunächst den Clusterpfad an, in den die Kindelemente verschoben werden sollen. Wenn es keine Kindelemente gibt, ist eine Angabe nicht nötig.

Sie erhalten eine Fehlermeldung, wenn ein Cluster in einen anderen verschoben werden soll, in dem bereits ein gleichnamiger Cluster existiert.

### 6.2.3 Profile verwalten

#### 6.2.3.1 Profil anlegen

Wählen Sie in der Baumansicht links zunächst den Cluster aus, in dem Sie das neue Profil erstellen möchten. Im Detailbereich rechts stehen Ihnen unter *Neues Profil erstellen* folgende Möglichkeiten zur Verfügung:



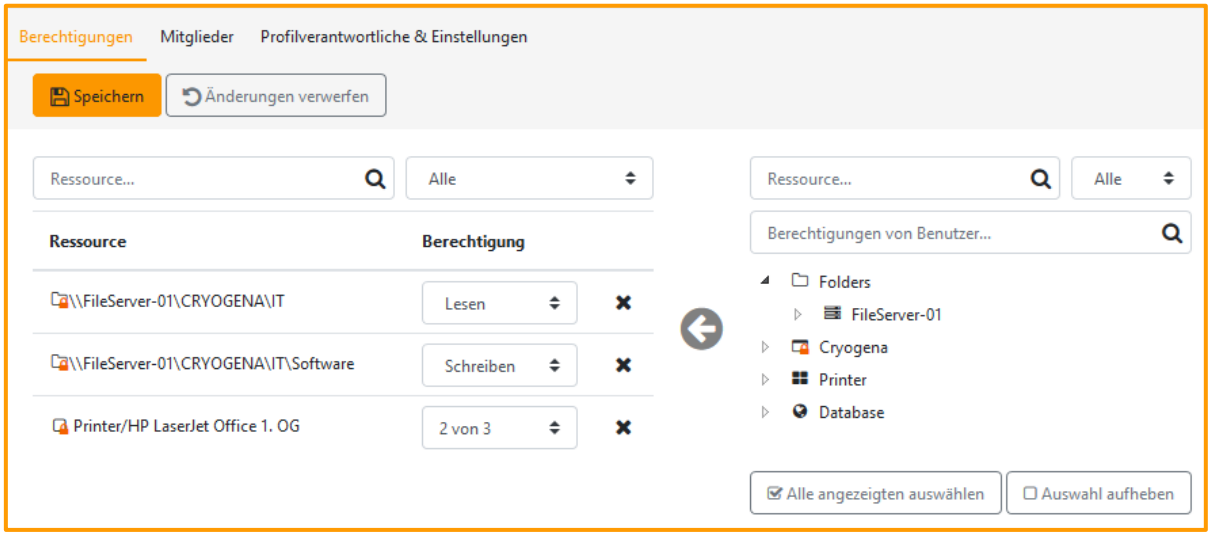

Geben Sie eine eindeutige *Bezeichnung des Profils* (Profilname) an. Diese darf noch nicht existieren, weder im aktuellen noch in anderen Clustern. Wählen Sie dann, ob Sie ein Benutzer- oder

Organisationsprofil erstellen möchten. Dieser Profiltyp ist im Nachgang nicht mehr änderbar. Sie können zusätzlich ein bestehendes Profil auswählen, dessen Ressourcen, auf die es berechtigt wurde, in das neue Profil übernommen werden (Feld *Berechtigungen von einem anderen Profil übernehmen*). Bitte beachten Sie, dass Mitglieder und Profilverantwortliche jedoch nicht übernommen werden.

Das neue Profil ist sofort in der Baumansicht sichtbar und im Detailbereich erscheinen die weiteren Bearbeitungsmöglichkeiten.

### 6.2.3.2 Berechtigungen verwalten

Wählen Sie in der Baumansicht links zunächst das zu bearbeitende Profil aus. Die Unterseite *Berechtigungen* im Detailbereich steht sowohl den *Profiladministratoren* als auch – mit reiner Anzeigemöglichkeit – den *Profilverantwortlichen* zur Verfügung.




In diesem Tab werden diejenigen Ressourcen zugewiesen und mit Rechten versehen, auf die die Mitglieder Zugriff erhalten. Um welches Zugriffsrecht es sich handelt, wird für jede Ressource einzeln festgelegt. In einem Profil können verschiedene Ressource-Arten kombiniert werden, d.h. ein Profil kann Berechtigungen gleichzeitig auf Verzeichnisse, SharePoint Sites und Dritt-Elemente enthalten.

---

*Ergänzende Berechtigungen bei Dritt-Elementen:*
*Wenn Sie nicht **sämtliche** Berechtigungen eines Elementes gewähren, werden die nicht gewährten Rechte bei einem Mitglied **nicht** entfernt, sofern das Mitglied diese bereits hat.*

---

Haben Sie die Rolle *Profiladministrator*, wird Ihnen neben der Liste der zugewiesenen Ressourcen eine weitere Liste angezeigt. Diese enthält die noch zuweisbaren Ressourcen. Per Drag-and-Drop oder über den Button werden neue Ressourcen in das Profil übernommen. Mit dem Button ✖ entfernen Sie einzelne Ressourcen. Es können nur verwaltete Ressourcen in das Profil übernommen werden.

Für beide Listen existieren oberhalb einige Eingabefelder zur Suche und Filterung innerhalb der enthaltenen Elemente. Das für die rechte Liste zusätzlich verfügbare Suchfeld *Berechtigungen von Benutzer* bietet eine Sonderfunktion:

Suchen Sie nach einem bestimmten Benutzer, zeigt die Liste alle Ressourcen, auf denen dieser Benutzer berechtigt wurde. Hierbei werden Ressourcen mit einem schwarzen Icon markiert, wenn der Anwender keine Berechtigungen hat, obwohl sie durch den Access Manager verwaltet werden. Durch diese Sonderregel können nun leicht mit dem Button *Alle angezeigten auswählen* alle berechtigten Ressourcen des Benutzers selektiert und in die linke Berechtigungsliste übernommen werden.

### 6.2.3.3 Mitglieder verwalten

Wählen Sie in der Baumansicht links zunächst das zu bearbeitende Profil aus. Die Unterseite *Mitglieder* im Detailbereich steht sowohl *Profiladministratoren* als auch *Profilverantwortlichen* zur Verfügung, allerdings haben Profiladministratoren hier lediglich lesenden Zugriff. Die Mitgliederzuweisung wird durch den Profilverantwortlichen vorgenommen. Hier werden Ihnen alle Mitglieder des gewählten Profils angezeigt, wobei Mitglieder bei Benutzerprofilen aus Benutzerkonten bestehen, während Mitglieder von Organisationsprofilen Benutzerprofile sind.


Profilverantwortliche können auf diesem Tab festlegen, welche Mitglieder die im Tab *Berechtigungen* definierten Zugriffsrechte erhalten sollen. Für jedes Mitglied können dabei die Mitgliedszeiträume individuell festgelegt werden. Existierende Konten / Profile können entfernt werden (Button *Entfernen* ✖ ), wodurch sie ihr Zugriffsrecht verlieren.

Neue Mitglieder werden einzeln über den Button *Benutzer hinzufügen* bzw. *Profil hinzufügen* berechtigt; dazu wird eine neue Eingabezeile in der Liste erzeugt, in der Sie das Mitglied eintragen. Über den Dreiecks-Button rechts daneben wird eine DropDown-Liste mit weiteren Möglichkeiten ausgeklappt:

*Mitglieder aus anderem Profil hinzufügen*: Geben Sie den Namen eines anderen Profils des gleichen Typs an (Benutzer- bzw. Organisationsprofil). Nun werden alle dort enthaltenen Mitglieder angezeigt

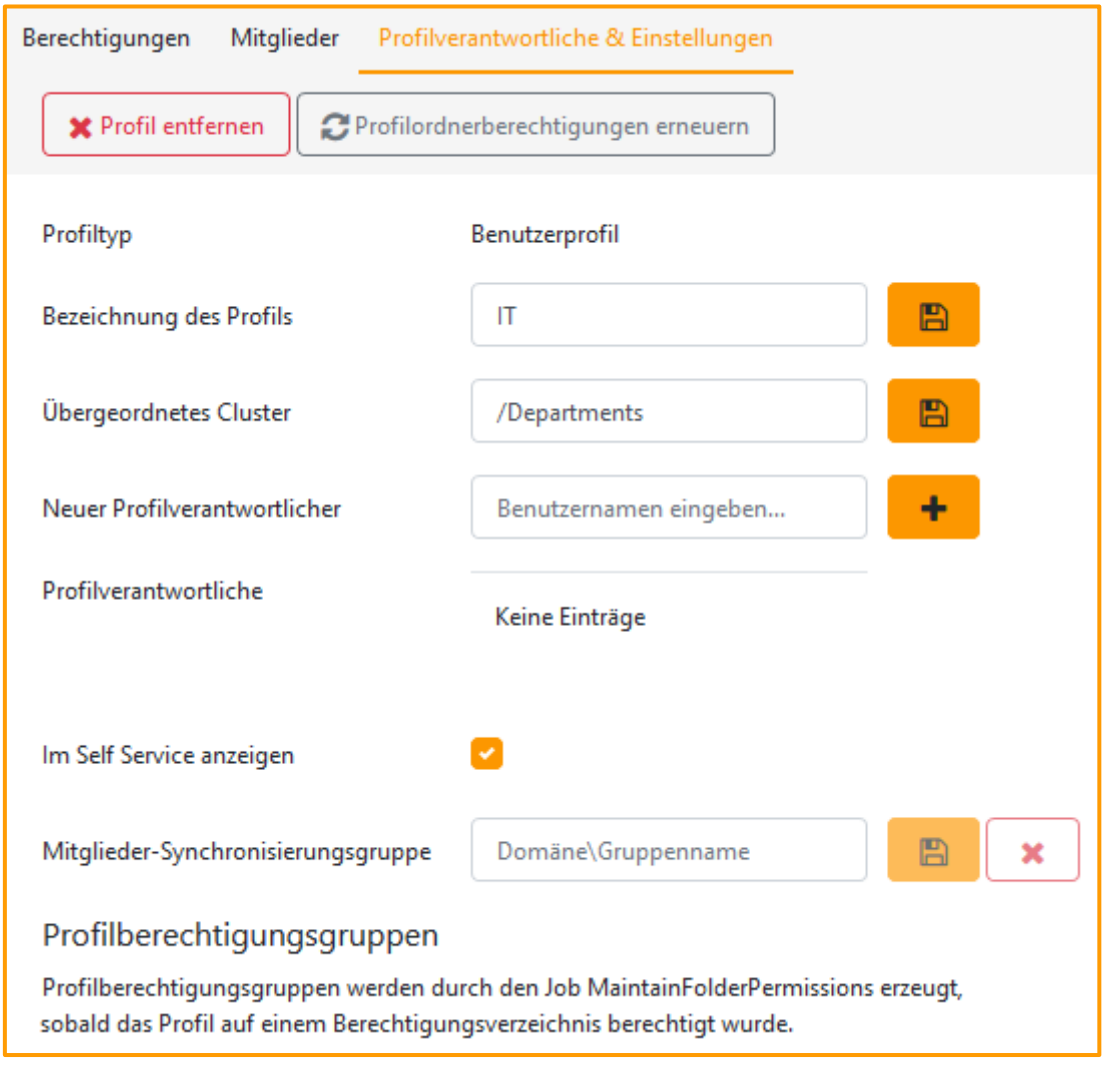
und Sie können die gewünschten selektieren. Diese werden nun als neue Mitglieder des aktuellen Profils eingefügt, sofern sie hier nicht bereits vorhanden sind.

*Benutzer aus AD-Gruppe hinzufügen*: In Benutzerprofilen steht zusätzlich die Option zur Verfügung, mehrere Benutzerkonten auf einmal hinzuzufügen. Geben Sie eine bekannte AD-Gruppe ein und wählen Sie die gewünschten Mitglieder aus der angezeigten Liste aus. Diese werden sofort der Mitgliederliste hinzugefügt, können aber noch nachträglich bearbeitet werden.

Darüber hinaus können Sie für jedes Mitglied über den Button jederzeit einen Kommentar eintragen bzw. alle bisherigen Kommentare anzeigen. Zur Übernahme klicken Sie *Speichern*.

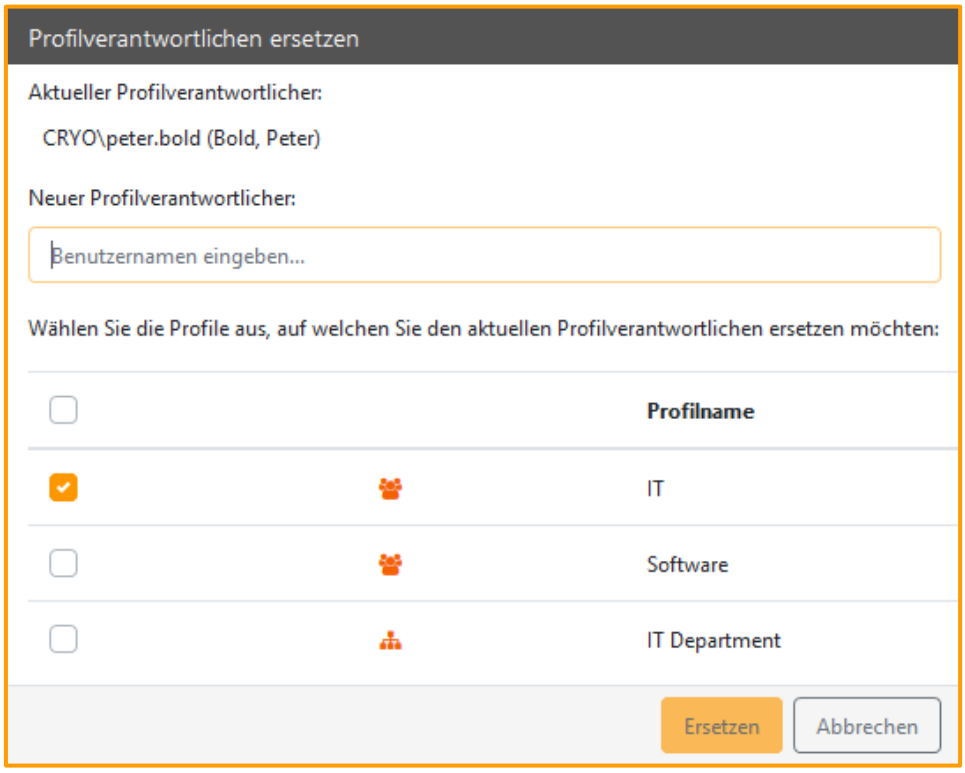
#### 6.2.3.4 Profilverantwortliche & Einstellungen

Wählen Sie in der Baumansicht links zunächst das zu bearbeitende Profil aus. Die Unterseite *Profilverantwortliche & Einstellungen* im Detailbereich ist nur für *Profiladministratoren* sichtbar.



Sie können hier die Bezeichnung des Profils (Namen) ändern sowie die Liste der *Profilverantwortlichen* bearbeiten und beliebig viele Personen eintragen, diese werden sofort in der unteren Liste angezeigt.

Neben dem *Entfernen* ( ✖ ) eines Profilverantwortlichen steht Ihnen mit dem Button *Ersetzen* ( ⇄ ) auch die Möglichkeit zur Verfügung, eine Person durch eine andere auszutauschen. Dabei wird eine Liste aller Profile angezeigt, für die die zu ersetzende Person derzeit verantwortlich ist. Über die Checkboxen lässt sich bestimmen, für welche Profile die Person ersetzt werden soll – initial ist nur das aktuelle Profil ausgewählt:



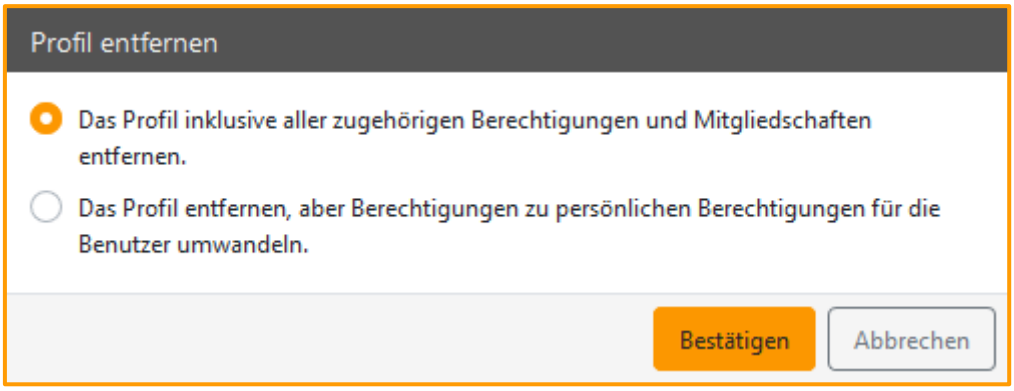

Neben der Verwaltung der Profilverantwortlichen können Sie weiterhin bestimmen, ob Sie dieses Profil *Im Self Service anzeigen* möchten, damit Anwender darauf eine Mitgliedschaft beantragen können. Dies ist nur möglich, wenn das Profil manuell über Profilverantwortliche verwaltet wird – bei einer automatischen Verwaltung (siehe nächste Option) ist das Profil nicht beantragbar.

*Mitglieder-Synchronisierungsgruppe*: Statt Profilverantwortliche zu bestimmen, die künftig die Mitglieder des Profils manuell verwalten, können Sie **alternativ** eine existierende AD-Gruppe angeben. Dadurch wird die manuelle Verwaltung de- und die automatische Verwaltung durch AD-Gruppen aktiviert. Damit werden in zyklischen Abständen die in der AD-Gruppe enthaltenen Benutzer ermittelt und als Mitglieder in das Benutzerprofil eingetragen. Somit erhalten diese Benutzer automatisch die Zugriffsrechte auf allen im Profil gesetzten Ressourcen. Ist ein bisheriges Mitglied des Benutzerprofils bei nun nicht mehr in der AD-Gruppe enthalten, wird seine Mitgliedschaft – und damit seine Zugriffsberechtigung – automatisch entfernt. Aus diesem Grund wird das Profil den Endanwendern auch nicht zur Beantragung angezeigt.

In der Profilliste links werden über Mitglieder-Synchronisierungsgruppen verwaltete Benutzerprofile mit einem Zahnrad-Symbol markiert (⚙).

Button *Profil entfernen*:

Möchten Sie ein Profil löschen, müssen Sie entscheiden, wie mit den bisher an die Mitglieder vergebenen Zugriffsrechten verfahren werden soll:




- *Das Profil inklusive aller zugehörigen Berechtigungen und Mitgliedschaften entfernen*
  Allen eingetragenen Benutzerkonten werden die Berechtigungen auf die zugeordneten Ressourcen entzogen. Hatte ein Benutzer weitere Berechtigungen auf einem der zugeordneten Ressourcen, bleiben diese weiterhin bestehen und treten ggf. in Kraft.
- *Das Profil entfernen, aber Berechtigungen zu persönlichen Berechtigungen für die Benutzer umwandeln*
  Diese Option wird nur bei Benutzerprofilen angezeigt. Mit ihr wird zwar das Profil gelöscht, die Berechtigungen bleiben jedoch in Form von persönlichen Berechtigungen der Benutzer, die Mitglied im Profil waren, erhalten.
- *Das Profil entfernen, aber Berechtigungen zu Benutzerprofilberechtigungen umwandeln*
  Diese Option wird nur bei Organisationsprofilen angezeigt. Hiermit werden die Ressource-Berechtigungen auf alle zum Organisationsprofil gehörenden Benutzerprofile kopiert bzw. – sofern dort schon vorhanden – ggf. aktualisiert. Eine Aktualisierung geschieht dann, wenn das Organisationsprofil ein höheres Recht (z.B. Schreiben) für eine Ressource definiert hatte als bisher im Benutzerprofil vorgesehen.

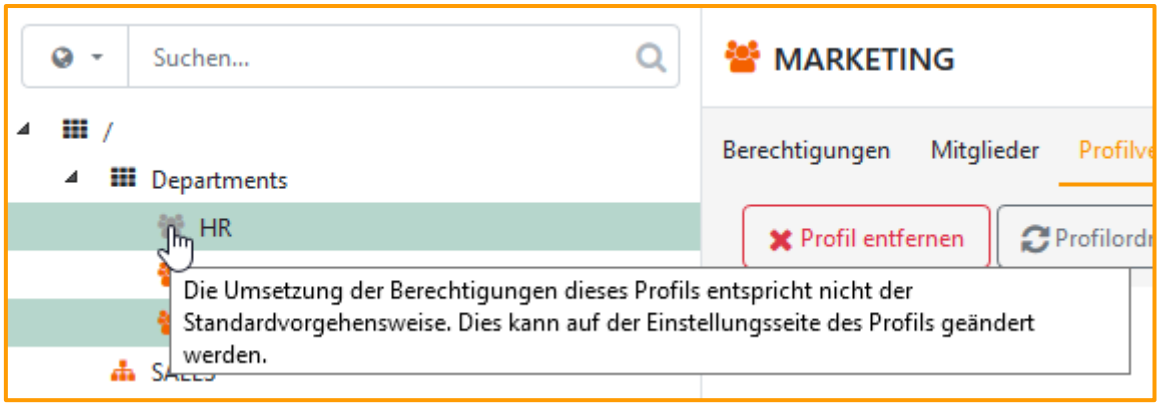
Handelt es sich bei dem Profil um ein Benutzerprofil, welches mit der Technik der *Profilgruppen* arbeitet (siehe Kapitel 12.3), werden die zugehörigen Profilgruppen in der AD automatisch ohne Nachfrage ebenfalls gelöscht, wenn sie auf den betroffenen Verzeichnissen nicht mehr berechtigt sind.

---

*Verwenden Sie Profilgruppen daher nicht außerhalb des Access Manager für eigene Zwecke.*

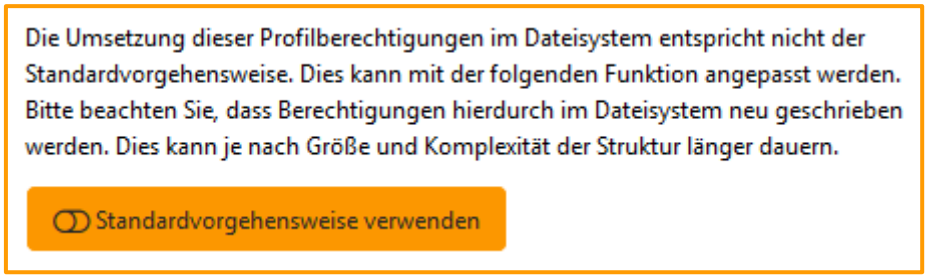
---

### 6.2.4 Nicht-Standard Benutzerprofile




Der *Administrator* des Access Manager kann zwischen zwei verschiedenen technischen Umsetzungen der Verzeichnisberechtigungen in Profilen wählen. Alle Benutzerprofile, die nicht dem aktuell gesetzten Standardverfahren entsprechen, erscheinen in der Profilliste grau und werden durch ein Tooltip erklärt. Es handelt sich nicht um eine Fehlermeldung, die Verwendung funktioniert weiterhin und kann ignoriert werden. Diese Profile können aber, falls von Ihnen gewünscht, selektiv auf das gesetzte Standard-Verfahren umgestellt werden:

Wählen Sie das entsprechende Benutzerprofil aus und wechseln Sie zum Tab *Profilverantwortliche & Einstellungen*. Hier gibt es nun einen weiteren Button:



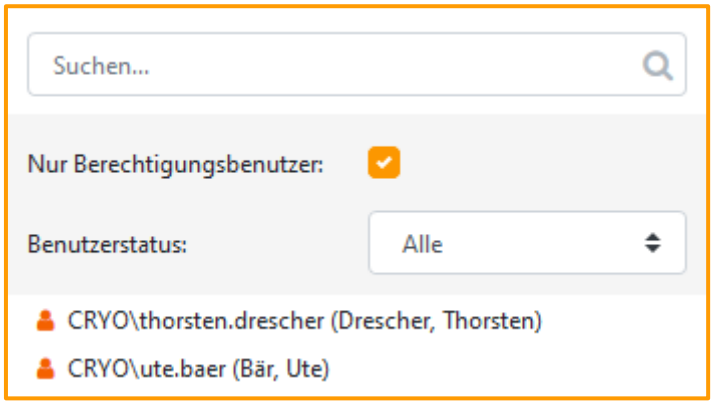

Hiermit werden im Hintergrund die technischen Änderungen für die neue Berechtigungslogik vorgenommen und stehen danach zur Verfügung. Informationen über die Vor- und Nachteile der verwendeten Technik finden Sie im Kapitel 12.3 für Administratoren. Für die eigentliche Profilverwaltung sind sie jedoch nicht von Belang und werden hier nicht weiter beschrieben.

---

*Dies ist eine rein interne technische Änderung; an den bestehenden Berechtigungen, an der Bedienlogik und der Optik ändert sich nichts.*

---

## 6.3 AD-Benutzer




Als *Profilverantwortlicher* können Sie hier – ähnlich wie ein Ressource-Verantwortlicher – zu allen Benutzern, die Mitglieder Ihrer Profile sind, Informationen abrufen.

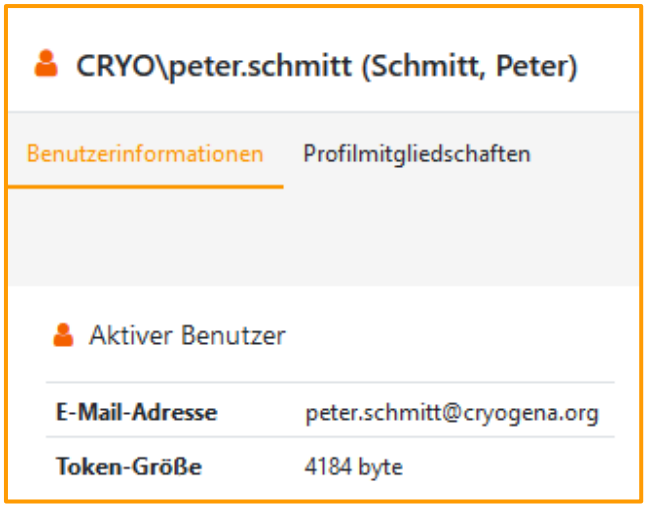
Die Personenliste links listet alle Benutzerkonten auf und bietet verschiedene Möglichkeiten der Filterung an. Neben der Möglichkeit, über die Sucheingabe einen bestimmten User zu finden, können Sie mit der Checkbox *Nur Berechtigungsbenutzer* nur die Konten anzeigen lassen, die bereits auf einem Ihrer Profile berechtigt wurden. Zusätzlich kann über die Dropdown-Liste *Benutzerstatus* bestimmt werden, ob (de-)aktivierte Nutzerkonten angezeigt werden sollen. In jeder Filterung werden zunächst nur die ersten 100 Treffer angezeigt – daher gibt es am Ende der Liste die Möglichkeit auch die restlichen Konten anzuzeigen. Je nach Anzahl kann dies mehrere Sekunden dauern.

Benutzerkonten ist ein Symbol vorangestellt, das Auskunft über ihren aktuellen Status im Access Manager gibt:

- Aktiver Benutzer mit Berechtigungen / Rollen
- Aktiver Benutzer ohne Berechtigungen / Rollen
- Inaktiver Benutzer mit Berechtigungen / Rollen
- Inaktiver Benutzer ohne Berechtigungen / Rollen
- Blacklisted Benutzer mit Berechtigungen / Rollen
- Im AD gelöschter Benutzer mit Berechtigungen / Rollen (kann auch mit „***“ markiert sein)

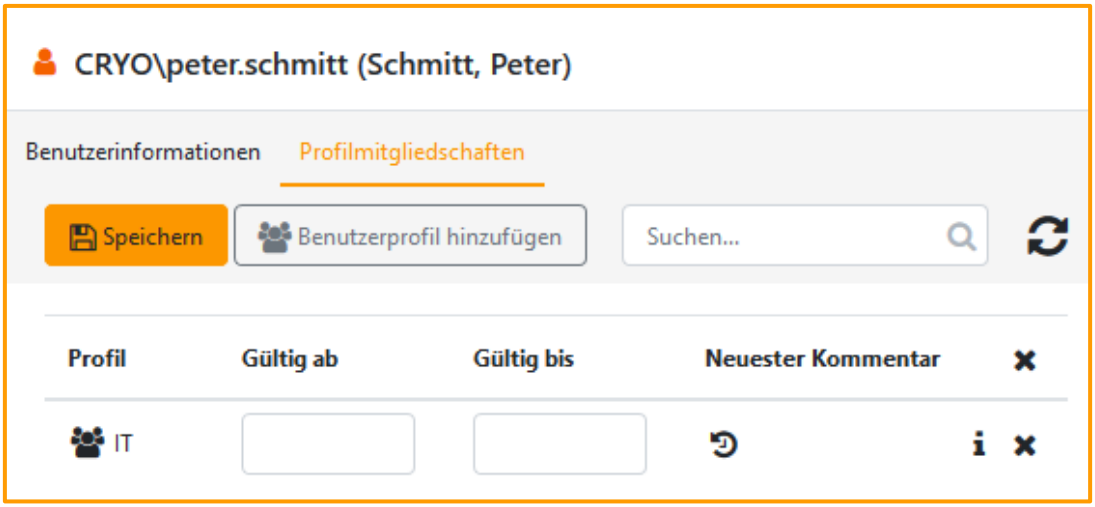
Bei sogenannten *Blacklisted Benutzern* handelt es sich um normale Benutzerkonten, die vom Administrator auf eine „Schwarze Liste“ gesetzt wurden. Damit werden sie in den üblichen Suchmasken und Eingabevervollständigungen nicht mehr berücksichtigt und nur angezeigt, falls sie bereits über Berechtigungen oder Rollen verfügen. Ohne Antrag lassen sich keine neuen Berechtigungen vergeben, es können lediglich bestehende Berechtigungen entfernt werden. Vorhandene Rechte werden vom Access Manager weiterhin überprüft und gepflegt. Außerdem sind die betreffenden Anwender weiterhin in der Lage Anträge im Management Portal zu stellen.

### 6.3.1 Detail-Tab „Benutzerinformationen“




Im Tab *Benutzerinformationen* werden zunächst allgemeine Informationen über das Benutzerkonto gezeigt. Diese umfassen z.B. die E-Mail-Adresse und das Benutzerverzeichnis (sofern verfügbar) und weitere technische Angaben.

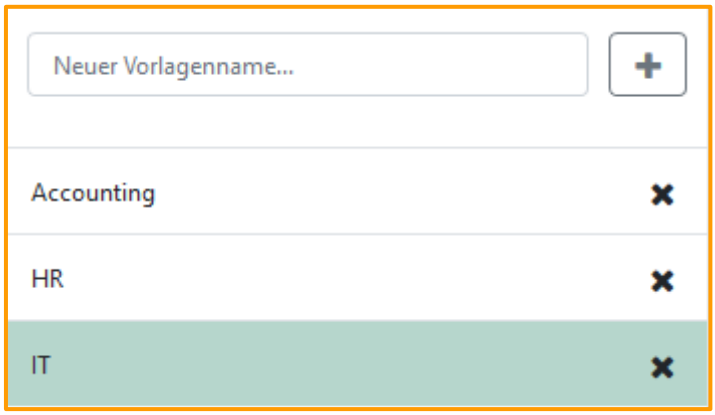
### 6.3.2 Detail-Tab „Profilmitgliedschaften“




Im Unterschied zum Ressource-Verantwortlichen sieht der Profilverantwortliche hier ein Tab mit den Benutzerprofilmitgliedschaften des gewählten Benutzers – dies umfasst auch Profile, für die die Mitgliedschaft erst später beginnt und derzeit noch nicht besteht. Änderungen am Zeitraum sind hier ebenfalls möglich. Zu jedem aufgeführten Benutzerprofil können Sie sich über das Info-Symbol anzeigen lassen, auf welche Verzeichnisse das Profil berechtigt wurde. Darüber hinaus lässt sich ein Profil hier entfernen (Kreuz-Symbol), was bedeutet, dass der Benutzer aus dem Profil entfernt wird und damit die Zugriffsrechte auf die Verzeichnisse des Profils verliert. Umgekehrt kann der Benutzer durch Hinzufügen eines Profils zu dessen Mitglied gemacht werden. Es ist ebenfalls möglich, über das Kreuz-Symbol im Tabellenkopf den Benutzer aus allen Profilen auf einmal zu entfernen.

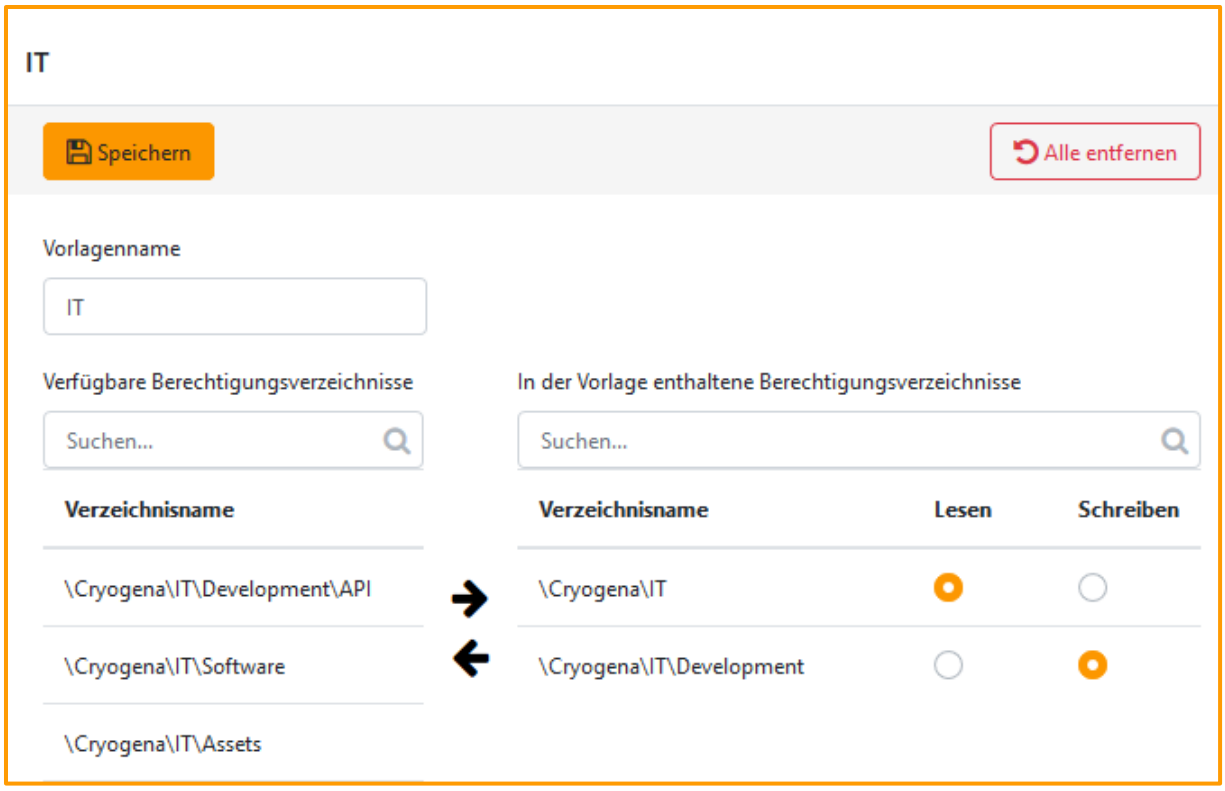
## 6.4 Globales Vorlagenmanagement

Haben Sie die Rolle *Vorlagenadministrator*, dürfen Sie globale Vorlagen erstellen, verändern und löschen. Im oberen Teil der Seite gibt es ein Eingabefeld, um eine neue Vorlage zu erstellen sowie eine Tabelle, die die bereits angelegten Vorlagen anzeigt:

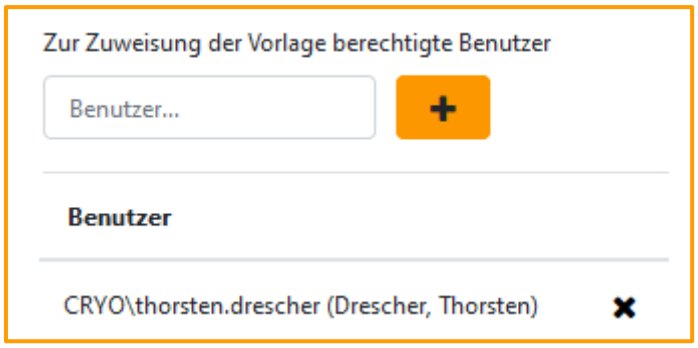



Nach Auswahl einer Vorlage zur Bearbeitung erscheinen weitere Elemente, mit denen Sie die Vorlage anpassen können, z.B. den Namen ändern. Zur Verzeichnisübernahme zeigt die darunter liegende Tabelle *Verfügbare Berechtigungsverzeichnisse* alle Berechtigungsordner an, die im Access Manager bekannt sind. Hier lassen sich beliebige Ordner entweder per Drag and Drop oder über den Rechts-Pfeil in die Berechtigungsliste rechts einfügen (bzw. umgekehrt auch wieder daraus entfernen).

Rechts zeigt die Berechtigungsliste alle in der Vorlage enthaltenen Berechtigungsordner mit den jeweils gesetzten Zugriffsrechten, die sich hier noch anpassen lassen. Über den Button *Alle entfernen* lassen sich alle Verzeichnisse auf einmal aus der Liste löschen.



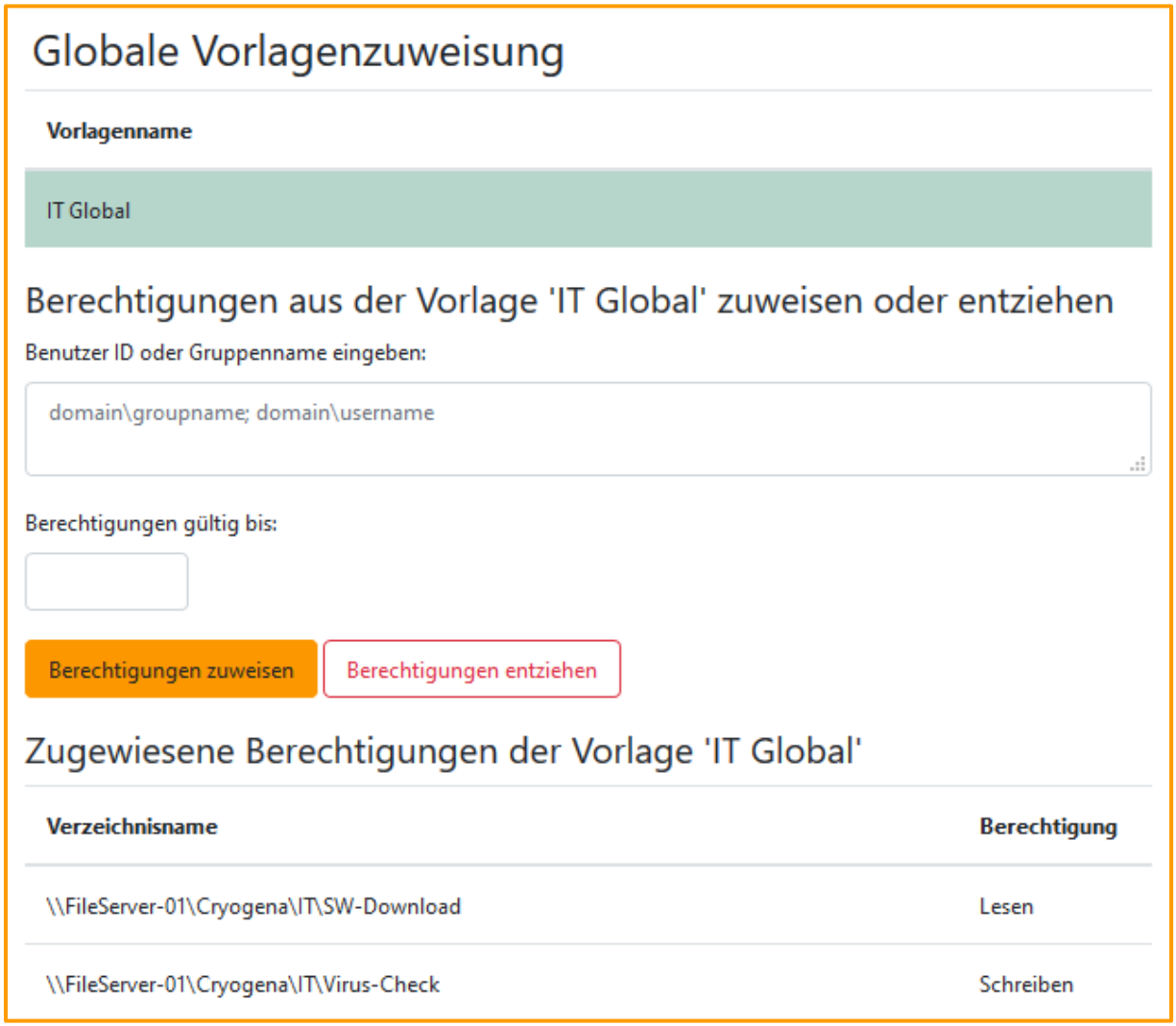

Für jede Vorlage legen Sie im letzten Abschnitt eine Benutzerliste fest mit den Personen, die diese Vorlage zur Berechtigungsvergabe nutzen dürfen.




Diese Benutzer erhalten automatisch die Rolle *Globaler Vorlagenbenutzer*. Sie erhalten dadurch jedoch keine weitergehenden Verwaltungsrechte wie *Verantwortlicher* oder *Besitzer* und können auch keine abweichenden Rechte setzen. Dennoch sollten Sie als Vorlagenadministrator die späteren Vorlagenbenutzer mit Bedacht auswählen, um unbeabsichtigte Ausweitungen der Zugriffsrechte zu vermeiden.

## 6.5 Globale Vorlagen zuweisen

Wurden Sie dazu berechtigt bestimmte Vorlagen zu verwenden (siehe voriges Kapitel) – d.h. Sie haben die Rolle *Globaler Vorlagenbenutzer* erhalten – werden Ihnen diese Vorlagen in einer Tabelle aufgeführt. Analog zu den privaten Vorlagen eines *Verantwortlichen* haben Sie damit die Möglichkeit, andere Benutzer auf einen definierten Satz von Berechtigungsordnern zu berechtigen. Als Globaler Vorlagenbenutzer können Sie Vorlagen allerdings nicht verändern, auch erhalten Sie keine Möglichkeiten zur Berechtigungsverwaltung auf den enthaltenen Verzeichnissen.




Wählen Sie oben eine Vorlage aus, erweitert sich die Anzeige um zwei Bereiche. Direkt darunter dient der Abschnitt dazu, die Benutzer und Gruppen zu definieren, denen die entsprechenden Rechte zugewiesen oder entzogen werden sollen. Dabei werden mehrere Einträge durch Semikola voneinander getrennt. Die Angabe eines Ablaufdatums der Rechte ist zusätzlich möglich. Darunter sehen Sie zur Kontrolle, welche Verzeichnisse mit welchen Berechtigungen die Vorlage enthält.

### 6.5.1 Berechtigung zuweisen / entziehen

Da es vorkommen kann, dass ein von der Rechte-Zuweisung per Vorlage betroffener Benutzer bereits Zugriffsrechte auf einem der enthaltenen Verzeichnisse hat, ist es wichtig zu wissen, dass grundsätzlich keine Reduzierung vorhandener Rechte erfolgt – bestehende höherwertige Rechte haben immer Vorrang[4].

Wurde kein Enddatum angegeben, erfolgt die Berechtigungsänderung unter Berücksichtigung obiger Regel sofort und dauerhaft; andernfalls gilt:

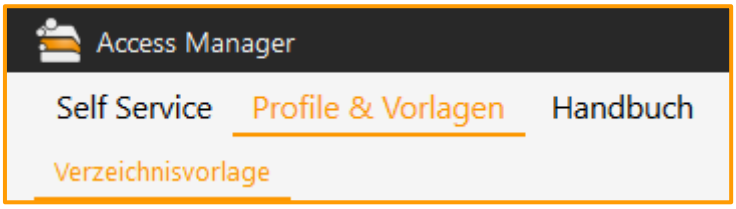
- *Berechtigungen zuweisen*: Allen angegebenen Benutzern und Gruppen werden die jeweiligen Zugriffsrechte auf die Verzeichnisse sofort zugewiesen und das Ablaufdatum wird gesetzt (unter Berücksichtigung obiger Regel). Dadurch kann sich das zuvor ggf. vorhandene Ablaufdatum verlängern.

- *Berechtigungen entziehen*: Es werden keine neuen Rechte gesetzt, jedoch werden bereits bestehende Rechte der Benutzer und Gruppen mit dem Ablaufdatum versehen, sofern es sich um das gleiche Recht wie in der Vorlage handelt (d.h. nur bei Lesen/Lesen bzw. Schreiben/Schreiben) und ein ggf. schon bestehendes Ablaufdatum erst später greifen würde. Das bedeutet, dass sich ein Berechtigungszeitraum höchstens verkürzen, jedoch nie verlängern kann.

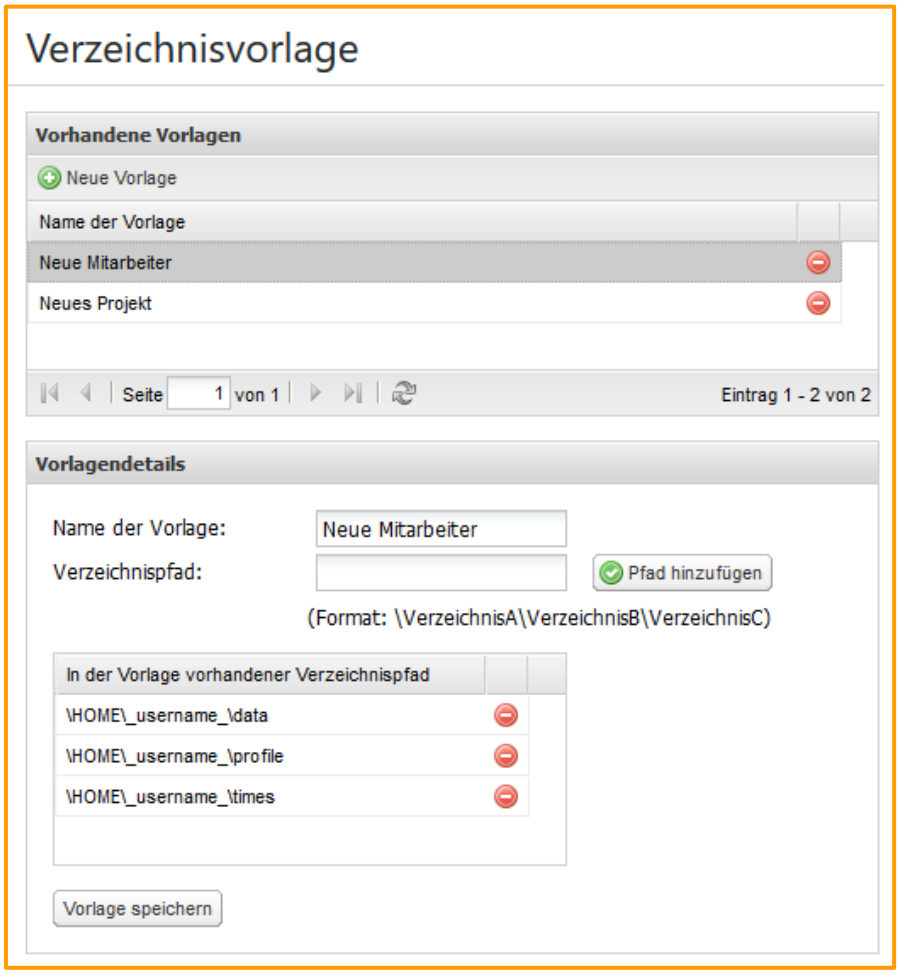
Klicken Sie abschließend auf *Berechtigungen zuweisen* bzw. *Berechtigungen entziehen*, werden die Berechtigungen für alle angegebenen Benutzer durchgesetzt und sie – sowie Sie als Verantwortlicher – werden darüber per Email informiert.

[4] D.h. hat ein Benutzer bereits Schreibrecht auf ein Verzeichnis, behält er dieses, auch wenn die Vorlage ein Leserecht vergibt.

## 6.6 Verzeichnisvorlagen administrieren




Die Seite *Verzeichnisvorlagen* ermöglicht die Verwaltung von Vorlagen, die der einfachen Erstellung von mehrfach benötigten Verzeichnisstrukturen dienen. Einmal definierte Vorlagen können auf der Seite *Struktur* beliebig oft zum Anlegen vieler, ggf. verschachtelter Verzeichnisse verwendet werden.




Ein Klick auf *Neue Vorlage* erstellt eine neue, leere Vorlage. Vergeben Sie hier einen eindeutigen, noch nicht verwendeten Namen.

Unter *Vorhandene Vorlagen* werden die bisher erstellten Vorlagen aufgelistet. Nach Auswahl einer Vorlage werden im Bereich *Vorlagendetails* der Name der Vorlage und die zu erstellenden Verzeichnisse angezeigt. Mit *Pfad hinzufügen* übernehmen Sie einen neuen Verzeichnispfad in die Vorlage. Die Änderungen werden mit *Vorlage speichern* gesichert.

# 7 Datenschutzklassifizierungen

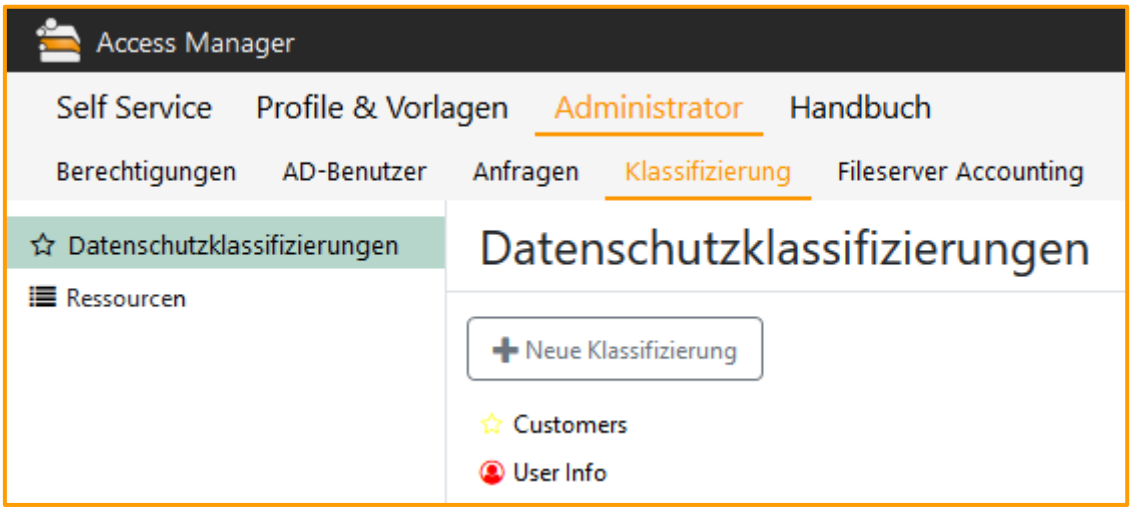
## 7.1 Arbeitsprinzip: Kennzeichnung personenbezogener Daten gemäß EU-DSGVO

Sogenannte *Klassifizierungen* bestehen im Access Manager aus einer Kombination von Klassen personenbezogener Daten gemäß der Europäischen Datenschutz-Grundverordnung. Eine Klassifizierung hat einen Namen, ein Symbol und eine Beschreibung und wird verwendet, um einzelne verwaltete Ressourcen zu markieren, die besondere Beachtung im Hinblick auf den Datenschutz benötigen.

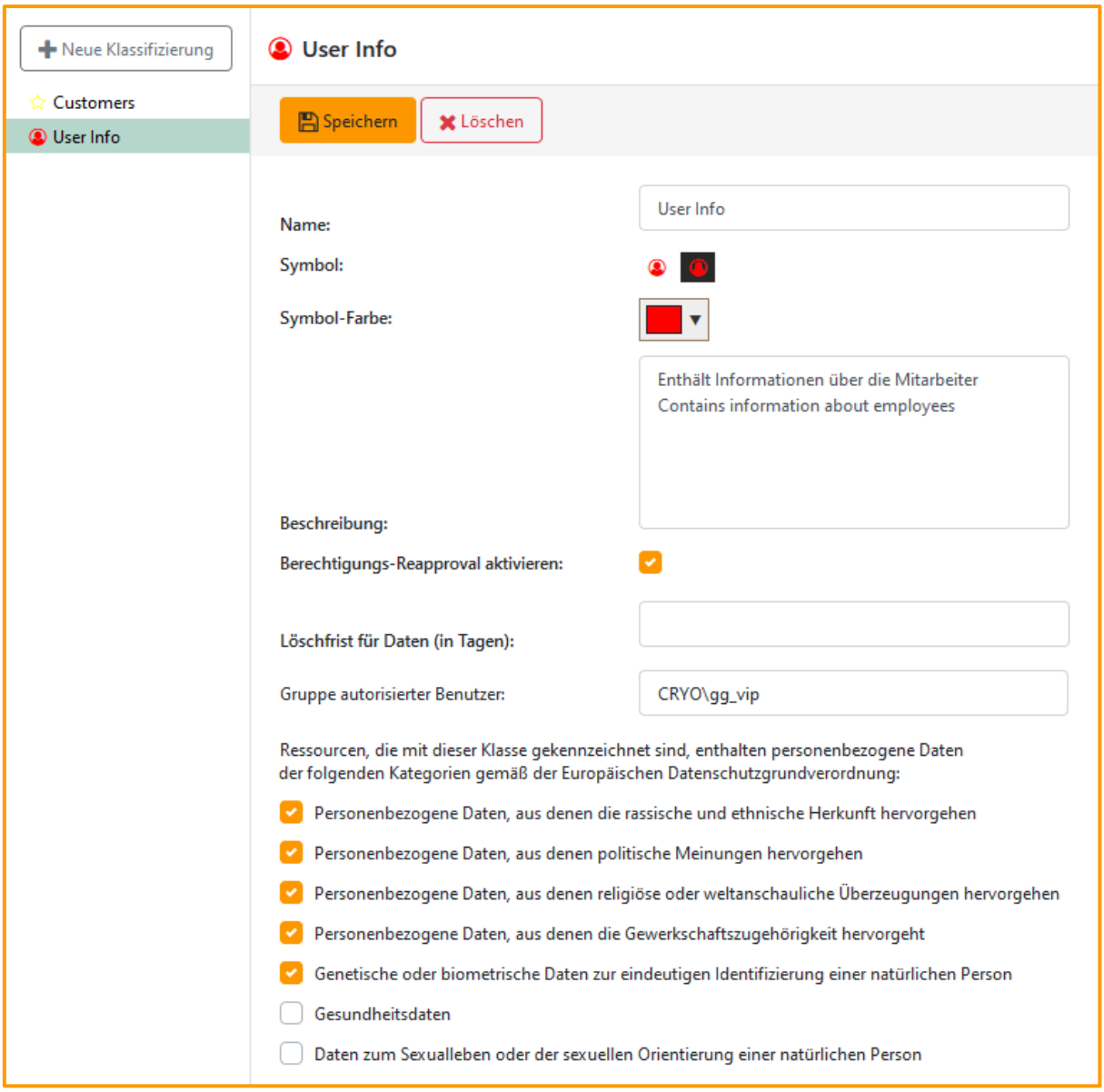
Darüber hinaus können Klassifizierungen auch ohne Datenschutz-Überlegungen verwendet werden, etwa um Ressourcen inhaltlich zu kennzeichnen oder um sie in einem *Reapproval*-Zyklus auf gültige Berechtigungen zu überprüfen.

Ein Klassifizierungsadministrator erstellt und verwaltet die Klassifizierungen (siehe folgendes Kapitel) und stellt sie den Besitzern von verwalteten Ressourcen zur Verwendung bereit (siehe Kapitel 4.3.2.2).

## 7.2 Datenschutzklassen definieren




Als *Klassifizierungsadministrator* verwalten Sie Klassifizierungen, die von *Ressource-Besitzern* verwendet werden können.




Neben der notwendigen Angabe eines Namens ist die Auswahl eines Symbols und seiner Farbe eine hilfreiche Einstellung, um klassifizierte Verzeichnisse leichter identifizieren zu können. Die auswählbaren Kategorien sind von der EU-DSGVO vorgegeben und nicht änderbar. Aus ihrer Kombination leitet sich die Schutzbedürftigkeit der damit markierten Verzeichnisse ab. Einmal erstellt, kann eine Klassifizierung von jedem Ressource-Besitzer verwendet, jedoch nicht verändert werden.

Die Aktivierung der Option *Berechtigungs-Reapproval aktivieren* führt dazu, dass alle Ressourcen, die ein Besitzer mit dieser Klassifizierung versieht, künftig am Reapproval-Prozess teilnehmen und von den jeweiligen Verantwortlichen überprüft werden müssen. Der Klassifizierungsadministrator legt also die zu prüfenden Ressourcen nicht selbst fest, sondern gibt dem Besitzer die Möglichkeit dies zu tun.

Die Angabe *Löschfrist für Daten (in Tagen)* ist eine rein informative Angabe, deren Einhaltung durch die Software nicht geprüft wird. Es handelt sich um eine Erinnerung gemäß EU-DSGVO, Ressourcen mit dieser Klassifizierung regelmäßig inhaltlich zu *bereinigen*, nicht zu *prüfen*.

*Gruppe autorisierter Benutzer:* Tragen Sie hier eine AD-Gruppe ein, werden nur Mitglieder dieser Gruppe (d.h. Benutzerkonten) als zu berechtigende Personen auf einer mit dieser Klassifizierung versehenen Ressource zugelassen. Es ist zwar weiterhin möglich, andere Personen auf der Ressource hinzuzufügen, diese werden jedoch effektiv keine Berechtigung erhalten, solange sie nicht in die o.g. AD-Gruppe aufgenommen wurden.

---

***Sonderfall bei der Verwendung von Profilgruppen (siehe Kapitel 12.7.3.19):***
*Wenn Sie eine oder mehrere so geschützte Ressourcen innerhalb eines Profils verwenden, werden nur Benutzer berechtigt, die auf **alle** geschützten Ressourcen zugreifen dürfen. Das bedeutet umgekehrt, sobald ein Benutzer auf mindestens eine geschützte Ressource **nicht** berechtigt ist, wird er auf **keiner** Ressource dieses Profils berechtigt.*

*Werden keine Profilgruppen verwendet, ist eine Mischberechtigung jedoch möglich, da hier die Berechtigungen pro Verzeichnis (und nicht pro Profil) vergeben werden.*

---

**Löschen einer Klassifizierung:**

Mit dem Button *Löschen* wird die Klassifizierung sofort entfernt, wenn sie nicht bereits verwendet wird. Ist dies der Fall, erhalten Sie einen Hinweis und die Klassifizierung bleibt bestehen. Eine Änderung ist aber weiterhin möglich.

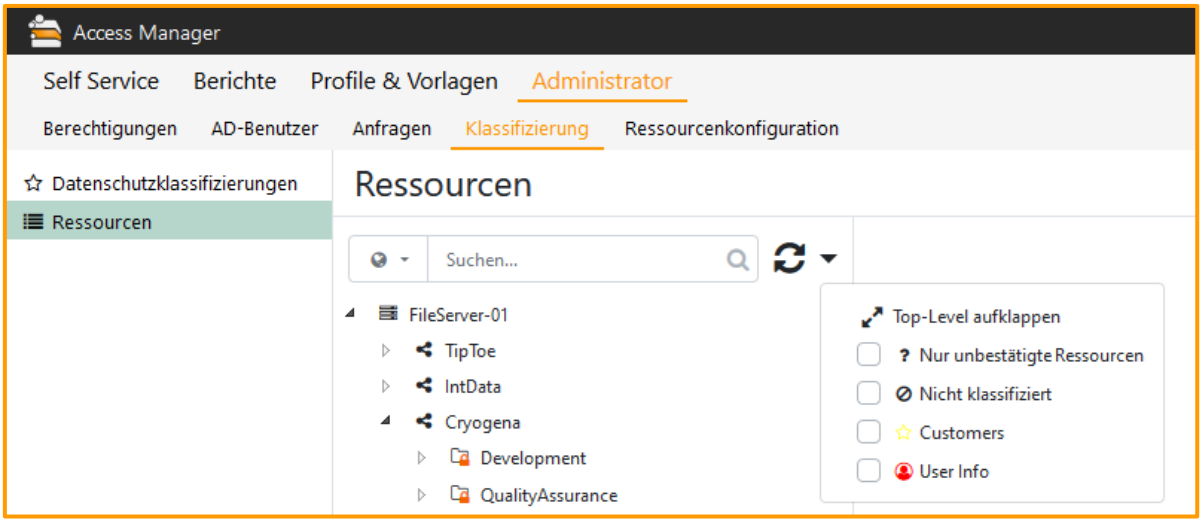
## 7.3 Ressourcen überprüfen


Als *Klassifizierungsadministrator* können Sie hier alle verwalteten Ressourcen einsehen. Für jede Ressource werden Ihnen dabei die Besitzer und Verantwortlichen angezeigt (nicht veränderbar) sowie die Beschreibung und die Klassifizierung – beides können Sie ändern. Außerdem können Sie – wie ein Ressource-Besitzer – die Klassifizierung einer Ressource wechseln und weitere Informationen editieren (siehe auch Kapitel 4.3.2.2).

Diese Unterseite stellt eine auf die Klassifizierung beschränkte Untermenge der Seite *Berechtigungen* für *Administratoren* dar, die nur dem Klassifizierungsadministrator zur Verfügung steht, da dieser weniger Rechte zur Ressourcenverwaltung hat als ein Administrator.

**Ressource-Filter:**

Zum schnellen Finden stehen Ihnen im Ressourcen-Baum neben der textuellen Suche über den DropDown-Button erweiterte Filtermöglichkeiten auf Klassifizierungsinformationen zur Verfügung:




Hier lässt sich nach einer oder mehrerer Klassifizierungen filtern; auch eine Einschränkung auf derzeit nicht klassifizierte Ressourcen ist möglich. Diese Option ist unverträglich mit der Möglichkeit, nur unbestätigte Ressourcen aufzuführen, da diese per Definition klassifiziert sind. Was unbestätigte Ressourcen sind, erklärt Kapitel 4.3.2.2.

# 8 Ressourcen Administration

Der *BAYOOSOFT Access Manager* dient zur Unterstützung und Entlastung der Unternehmens-IT bei Fragen und der Umsetzung von Berechtigungen in Dateisystemen, SharePoint sowie verschiedensten Diensten von Drittanbietern für die Anwender. Über eine webbasierte Oberfläche lassen sich auf einfache Weise beliebig viele Ressourcen hinzufügen und die Benutzerrechte unabhängig und flexibel verwalten.

Dazu definiert der Access Manager den Begriff *Verwaltete Ressource*, womit verdeutlicht wird, dass eine solche Ressource vom Access Manager dauerhaft auf die korrekte Vergabe der gewünschten Zugriffsrechte kontrolliert und aktualisiert wird. Darüber hinaus lassen sich gezielt Ressourcen von der Verwaltung durch den Access Manager ausnehmen – in diesem Fall spricht man von sogenannten *freien Ressourcen*.

Die Realisierung der Zugriffsverwaltung erfordert keine zusätzlichen Software-Werkzeuge: Alle Funktionen werden mit den vorhandenen serverseitigen Mitteln einer Standard-Windows-Infrastruktur realisiert (Active Directory Gruppen & User, NTFS-Freigaben und -Rechtevergaben). Der Access Manager dient letztlich als Verwaltungsaufsatz, die eigentliche Benutzerauthentifizierung und -autorisierung wird weiterhin durch die Windows Server Funktionalität gewährleistet. Ein Ausfall des Access Manager-Systems hat daher keinerlei Auswirkung auf die tatsächlichen Zugriffsmöglichkeiten der Anwender, lediglich Management und Reporting vorhandener Berechtigungen sind dann nicht möglich.

## 8.1 Arbeitsprinzip: Auto-Berechtigungskorrektur

Der Access Manager verwendet eigene AD-Berechtigungsgruppen auf den verwalteten Ressourcen, etwa einem Verzeichnis im Dateisystem. Berechtigungen, die vor der Verwaltungsübernahme dort gesetzt waren, werden ausnahmslos entfernt und durch die eigenen Gruppen ersetzt, welche mit Standardberechtigungen für Lesen, Ändern und Browsen (Nur Verzeichnis öffnen, aber keine Dateien / Unterverzeichnisse lesen) versehen werden. Über die Benutzungsoberfläche festgelegte Berechtigungen werden in den AD-Gruppen und dem Dateisystem umgesetzt und zusätzlich in der AM-Datenbankgespeichert. Dadurch bleibt die volle Kontrolle über die Berechtigungsvergabe erhalten.

In zyklischen Abständen führt der Access Manager einen SOLL-IST Abgleich durch und prüft die in der Datenbank gespeicherte Berechtigungssituation (SOLL) gegen den Zustand der AD-Gruppen und den Berechtigungen im Dateisystem (IST). Fallen hierbei Abweichungen auf, werden AD und Dateisystem auf den Stand der Datenbank zurückgesetzt, d.h. die definierten Rechte werden wiederhergestellt.

Analog gilt dies ebenso für die Ressourcentypen SharePoint Sites und Dritt-Elemente.

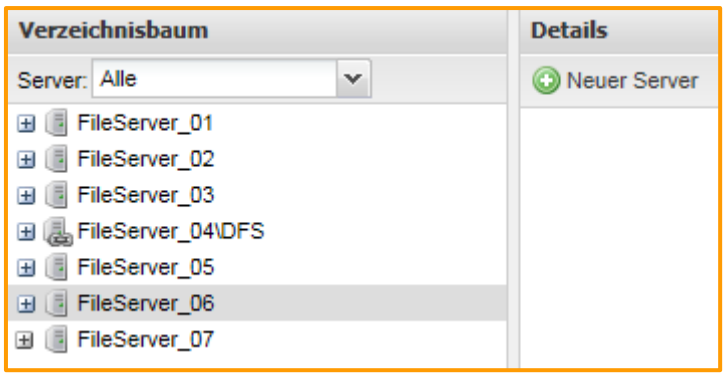
## 8.2 Einstiegspunkte konfigurieren


Diese Seite erlaubt Ihnen das Einbinden Ihrer Ressourcen, den sog. Einstiegspunkten, in den Access Manager. Nur Ressourcen, die hier hinterlegt und korrekt konfiguriert werden, unterliegen der Rechteverwaltung durch den Access Manager.

Je nach Lizenz finden Sie in der Ressourcenliste links verschiedene Ressourcentypen, über die Sie angepasste Verwaltungsmöglichkeiten im rechten Bereich administrieren:

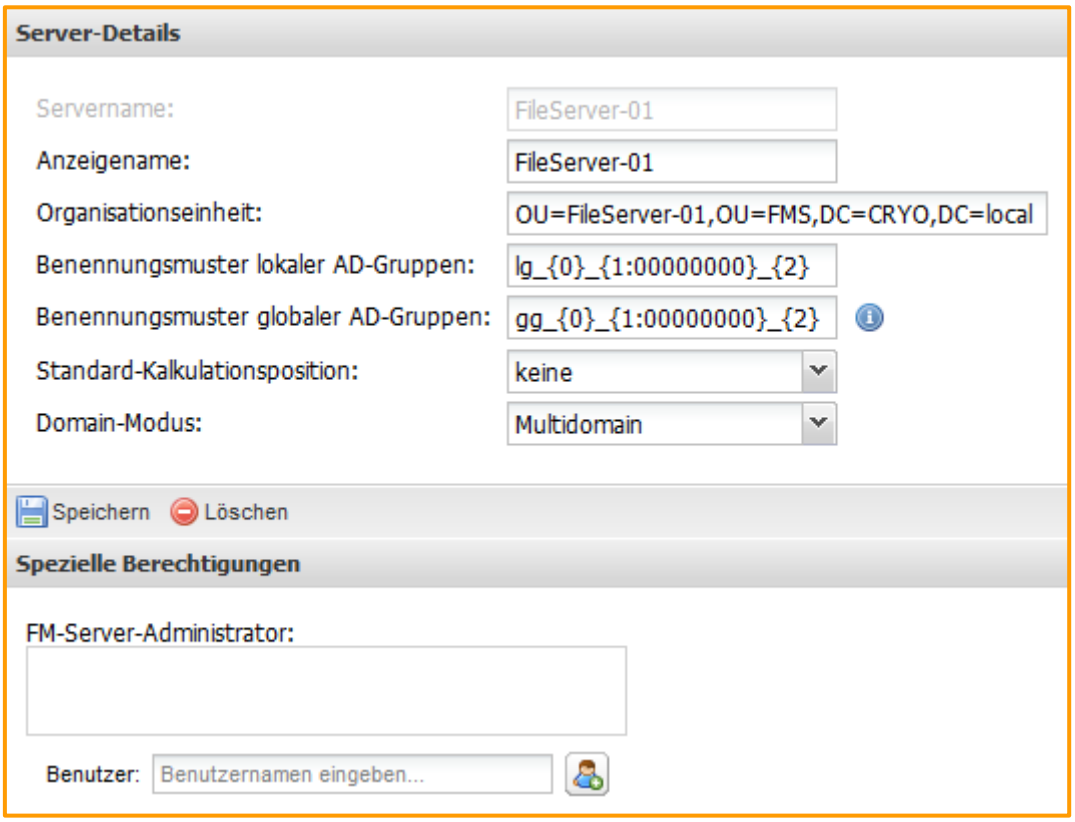
- Fileserver
- SharePoint
- 3rd Party (Dritt-Elemente)

### 8.2.1 Fileserver




Im Verzeichnisbaum sehen Sie alle eingerichteten Fileserver und ihre Shares. Klicken Sie den gewünschten Eintrag an, um seine Details im rechten Bereich zu sehen und zu editieren. Mit dem Button *Neuer Server* bzw. *Neues Share* fügen Sie einen entsprechenden Einstiegspunkt hinzu.

#### 8.2.1.1 Server-Details




Ist ein Server bereits im Access Manager vorhanden, können Sie alle Parameter bis auf seinen Namen nachträglich ändern – nur über den Namen wird der Server im Netz identifiziert.

Wenn Sie einen neuen Server hinzufügen, füllen Sie die folgenden Werte:

*Servername:* Geben Sie hier nur den eindeutigen Namen des Fileservers im Netzwerk an. Zusammen mit dem später anzugebenden Share-Namen wird der Access Manager daraus den UNC-Pfad \\SERVER\SHARE generieren, den Sie auch sonst in Windows verwenden.

*Beschreibung:* Ein beschreibender Name Ihres Servers (Pflichtangabe).

*Organisationseinheit:* Tragen Sie hier die OU im Active Directory ein, in der die vom Access Manager erstellten Berechtigungsgruppen gespeichert werden. Am einfachsten ist es, wenn Sie im AD die Eigenschaften der OU öffnen, auf das Tab *Attribut-Editor* wechseln und dort den Wert von *distinguishedName* kopieren.

*Benennungsmuster lokaler / globaler AD-Gruppen:* Benennungsregeln für den Access Manager, mit denen Sie das Namensformat der Berechtigungsgruppen gemäß Ihren Vorgaben steuern. Es stehen drei Platzhalter (in geschweiften Klammern) zur Verfügung, die dynamisch ersetzt werden:

- {0} Der Hostname des Servers, wie Sie ihn unter *Servername* eingetragen haben
- {1} Die Verzeichnis-ID (fortlaufende interne Nummer)
- {2} Die Abkürzung der Berechtigung (r, w oder b für Lese-, Schreib- oder Browse-Gruppe)

Die Verwendung von {0} ist optional, die Platzhalter {1} und {2} müssen jedoch verwendet werden, um eindeutige Gruppennamen zu generieren.

*Domain-Modus:* Welche der beiden o.g. Benennungsmuster verwendet werden, hängt vom Domain-Modus des Servers ab. Es muss einer von drei möglichen Modi ausgewählt werden:

- *Einzeldomain*
  Es werden AD-Gruppen vom Typ „Sicherheitsgruppe – Global“ erstellt und verwaltet. Verwenden Sie diesen Modus, wenn Sie nur eine Domain haben. Der Speicherverbrauch des Kerberos-Tokens der Benutzerkonten wird damit am wenigsten belastet.
- *Multidomain*
  Es werden AD-Gruppen vom Typ „Sicherheitsgruppe – Lokal (in Domäne)“ erstellt und verwaltet. Verwenden Sie diesen Modus, wenn Sie mehrere Domains haben / haben werden oder wenn Sie unsicher sind. Dies ist die Standardeinstellung. Der Speicherverbrauch des Kerberos-Tokens der Benutzerkonten wird dadurch allerdings am meisten belastet.
- *Multidomain optimiert*
  Es werden sowohl globale als auch lokale AD-Gruppen erstellt und verwaltet. Abhängig von der Domain des Benutzers und des Servers wird dynamisch entschieden, zu welchem Gruppentyp der Benutzer hinzugefügt wird. Dieser Modus kann dabei helfen, die Größe des Kerberos-Tokens des Benutzerkontos zu minimieren.

---

*Falls diese Einstellung nachträglich geändert wird, müssen auf diesem Server alle Berechtigungen von Benutzern aus fremden Domains entfernt werden (nur bei Umschaltung von Multi- auf Einzeldomain). Außerdem muss die Aufgabe „MaintainAccessPermission“ erneut ausgeführt werden.*

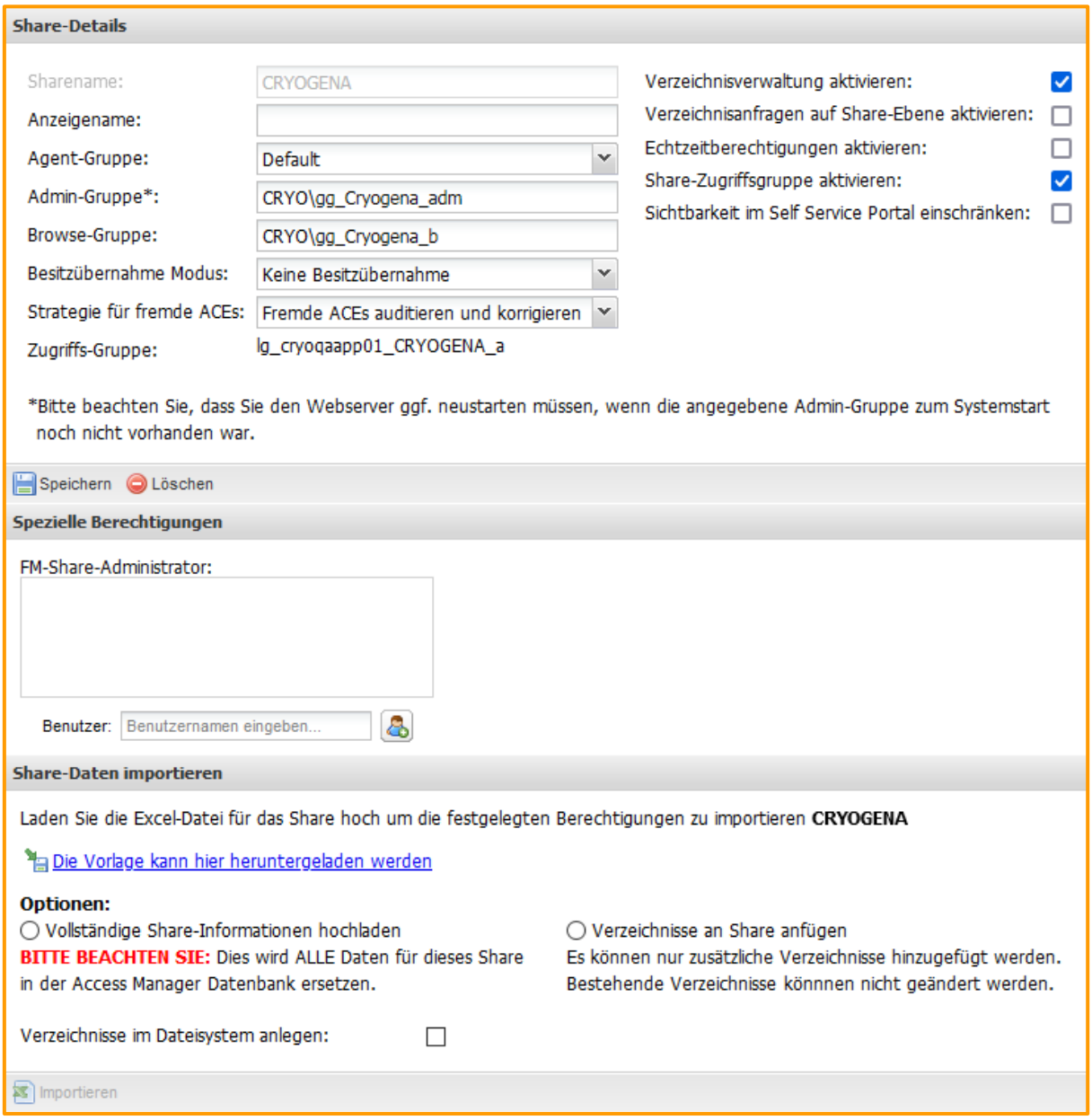
---

Klicken Sie auf *Speichern* damit die Änderungen wirksam werden. Falls Sie einen neuen Server hinzugefügt haben, erscheint er nun im Verzeichnisbaum.

Mit Klick auf *Löschen* wird der Server inklusive seiner Shares aus dem Access Manager entfernt werden, sodass er nicht mehr verwaltet wird. Bitte beachten Sie, dass dabei ebenfalls die Benutzerrechte vom Dateisystem entfernt wird. Dies kann je nach Größe der Shares einige Zeit dauern.

*Spezielle Berechtigungen:* Tragen Sie hier Benutzer ein, die berechtigt sein sollen, die Rechte dieses Servers bzw. aller seiner Shares zu verwalten (*FM-Server-Administratoren*).

### 8.2.1.2 Share-Details




Um ein neues Share hinzuzufügen, klicken Sie zunächst den entsprechenden Server an, dann *Neues Share*.

*Sharename:* Geben Sie hier ausschließlich den Namen des Shares an. Zusammen mit dem Server-Namen wird der Access Manager daraus den UNC-Pfad \\SERVER\SHARE generieren, den Sie auch sonst in Windows verwenden.

*Anzeigename:* Mit dieser Angabe wird dieser Name auf der Seite *Anfragen* anstelle des eigentlichen Share-Namens angezeigt.

*Agent-Gruppe:* Hier legen Sie die Gruppe der AM-Agenten fest, die die Aufgaben für das Share bearbeiten soll. Standard ist die Gruppe *Default*. Mehr Informationen zu Agent-Gruppen finden Sie im Kapitel 10.2.

*Admin-Gruppe* & *Browse-Gruppe:* Diese AD-Gruppen werden vom Access Manager auf die Verzeichnisse geschrieben und erlauben der Software sowie den Anwendern grundsätzlichen Zugriff. Diese Gruppen müssen schon im AD vorhanden sein, sie werden nicht automatisch erstellt.

*Besitzübernahme Modus:* Access Manager kann auf verwalteten Verzeichnissen den Besitzer aller enthaltenen Verzeichnisse und Dateien auf sich selbst ändern. Sie haben folgende Auswahlmöglichkeiten:

- *Keine Besitzübernahme:* Diese Einstellung wird empfohlen. Hierbei belässt der AM den aktuellen Besitzer im Dateisystem, auch wenn ein Verzeichnis neu verwaltet wird. Zum Schutz gegen ungewollte Veränderungen durch die Endanwender im Dateisystem ist es wichtig, dass die Freigabe so vorbereitet wurde, dass die **Freigabe-Berechtigungen** den Anwendern **nur Lese- und Änderungsrechte, keinesfalls jedoch Vollzugriff gewähren**.
- *Besitzübernahme ohne Protokollierung:* Sobald ein Verzeichnis durch Access Manager verwaltet wird, übernimmt das System den Besitz aller darunterliegenden Verzeichnisse und Dateien, protokolliert dies aber nicht.
- *Besitzübernahme mit Protokollierung:* Wie oben, jedoch erstellt der Access Manager für jedes übernommene Objekt einen Protokoll-Eintrag in der Datenbank, so dass Sie später über den Bericht *Besitzübernahme einer Ressource nach Verzeichnis* nachvollziehen können, wer vor der Übernahme der ursprüngliche Besitzer war. Diese Option wird nur für Ausnahmefälle empfohlen, da dadurch sehr viele Einträge die Datenbank immens vergrößern und sich die Protokollierung negativ auf die Performance auswirkt.

Für diese Einstellung existieren Optionen in den Systemeinstellungen, die den Standardwert vorgeben (siehe Kapitel 12.7.3ff).

---

*Bitte beachten Sie, dass es hier um den Besitzer im Sinne des Dateisystems geht, nicht um die Rolle* Besitzer *innerhalb des Access Manager!*

---

*Strategie für fremde ACEs:* Diese Einstellung muss nur in den seltensten Fällen geändert werden, sie beeinflusst direkt die Prüfung korrekt gesetzter Berechtigungen im Filesystem durch die planbare Aufgabe *MaintainAccessPermissions*. Sie haben folgende Auswahlmöglichkeiten:

- *Fremde ACEs auditieren und korrigieren:* Dies ist die empfohlene Standard-Einstellung. Bei der Prüfung auf unzulässige Rechte-Veränderungen im Dateisystem werden alle Abweichungen zur Access Manager-Definition protokolliert und dann behoben. Hiermit erhalten Sie die maximale Sicherheit vor ungewollten Rechte-Ausdehnungen.

- *Fremde ACEs auditieren:* Die Aufgabe überprüft zwar die verwalteten Verzeichnisse und protokolliert Abweichungen, lässt aber zusätzlich auf dem Dateisystem eingetragene Konten- und Gruppenberechtigungen bestehen. Fehlende Objekte oder veränderte Berechtigungen (z.B. Schreiben statt Lesen) werden weiterhin korrigiert. Hierdurch ist eine ungewollte Rechte-Erweiterung möglich.
- *Fremde ACEs ignorieren:* Hiermit werden zusätzlich im Dateisystem gesetzte Berechtigungen ebenfalls nicht korrigiert, aber außerdem auch nicht protokolliert. Hierdurch ist eine ungewollte und unerkannte Rechte-Ausweitung möglich. **Diese Einstellung wird nicht empfohlen!**

*Verzeichnisverwaltung aktivieren:* Hiermit wird bestimmt, ob Verzeichnisse auf dem Share aktiv verwaltet werden. Falls die Verzeichnisverwaltung nicht aktiviert ist, gibt es folgende Einschränkungen:

- Das Share wird nicht im Management Portal angezeigt.
- Die Zugriffsberechtigungen werden nicht verwaltet (erstellt, geprüft, korrigiert).
- Es wird keine Informationsdatei mit den Verantwortlichen erstellt.
- Eine zyklische Bereinigung von Verzeichnissen wird nicht durchgeführt.

*Verzeichnisanfragen auf Share-Ebene aktivieren:* Damit ermöglichen Sie es den Anwendern, ein Share auszuwählen und dort direkt ein neues Verzeichnis zu beantragen. Andernfalls können neue Verzeichnisse ausschließlich innerhalb eines schon existierenden Verzeichnisses beantragt werden. Voraussetzung dafür ist, dass bereits ein *Besitzer* für ein Share eingetragen wurde.

*Echtzeitberechtigungen aktivieren:* Hiermit schreibt der Access Manager neue Benutzer nicht nur in die entsprechenden AD-Gruppen, sondern berechtigt sie auch direkt im Dateisystem. Dies ermöglicht dem Benutzer sofortigen Zugriff auf das Verzeichnis, ohne sich bei Windows ab- und wieder anmelden zu müssen. Diese ACE wird nach 24 Stunden automatisch aus dem Dateisystem entfernt. Bitte beachten Sie, dass diese Einstellung ggf. negative Auswirkungen auf die Fileserver-Performance haben kann, falls sie bei Verzeichnissen mit vielen Dateien aktiviert ist. Außerdem können nachträgliche Berechtigungsveränderungen innerhalb des Zeitraums von 24 Stunden, die die gleichen Benutzer betreffen, ggf. nicht korrekt abgebildet werden.

*Share-Zugriffsgruppe aktivieren:* Der Access Manager legt eine spezielle AD-Gruppe an, die alle Benutzer enthält, die Lese- oder Schreibzugriff auf mindestens einem Verzeichnis in diesem Share haben. Diese Gruppe kann beispielsweise verwendet werden, um in einem Logon-Skript zu überprüfen, ob dieses Share dem Benutzer als Netzlaufwerk verbunden werden soll. Für diese Funktionalität muss die Aufgabe *UpdateShareAccessGroups* geplant werden. Falls der Domain-Modus des Servers auf *Multidomain optimiert* gesetzt ist, werden eine globale und eine lokale Zugriffsgruppe angelegt.

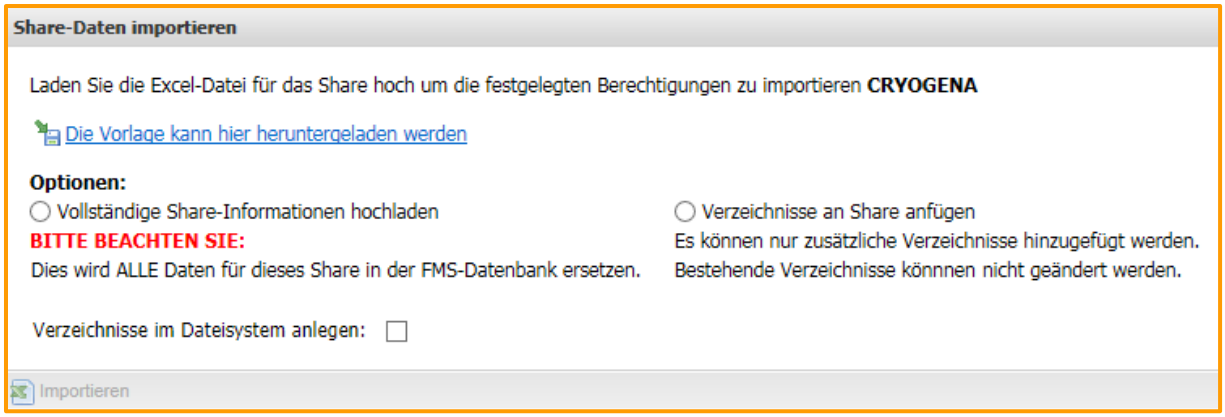
*Sichtbarkeit im Self Service Portal einschränken:* Aktivieren Sie diese Checkbox, wenn das Share nur bestimmten Benutzern / Benutzergruppen auf der Beantragungsseite angezeigt werden soll. Diese fügen Sie im darunterliegenden Abschnitt *Spezielle Berechtigungen* in der Liste *Sichtbarkeit auf folgende AD-Gruppen und Benutzer einschränken* hinzu.

Klicken Sie auf *Speichern* damit die Änderungen wirksam werden. Falls Sie ein neues Share hinzugefügt haben, erscheint es nun im Verzeichnisbaum.

Mit Klick auf *Löschen* wird das Share aus dem Access Manager entfernt werden, sodass es nicht mehr verwaltet wird. Bitte beachten Sie, dass dabei ebenfalls die Benutzerrechte vom Dateisystem entfernt wird. Dies kann je nach Größe des Shares einige Zeit dauern.

*Spezielle Berechtigungen:* Tragen Sie hier Benutzer ein, die berechtigt sein sollen, die Rechte nur dieses Shares zu verwalten (*FM-Share-Administratoren*).

#### *8.2.1.2.1 Berechtigungsinformationen importieren*




Der Bereich Share-Details enthält einen weiteren Abschnitt, *Share-Daten importieren*. Hier können Sie die in einer Excel-Datei gespeicherten Berechtigungsdaten eines kompletten Shares importieren. Der Import bezieht sich zunächst nur auf die Access Manager-Datenbank. In der Datei angegebene Verzeichnisse werden im Dateisystem nur dann erstellt, wenn diese im Dateisystem noch nicht existieren und die Option *Verzeichnisse im Dateisystem anlegen* aktiviert ist. Die Excel-Datei kann manuell angelegt, durch den NTFS Permission Analyzer (separates Programm) oder durch den Export vorhandener Verzeichnisdaten generiert werden. In jedem Fall muss sie dem im folgenden Kapitel beschriebenen Format entsprechen.

Alle zu importierenden Verzeichnisdaten müssen sich auf das aktuell ausgewählte Share beziehen. Dementsprechend müssen alle Verzeichnisnamen mit dem korrekten Server-Share-Pfad beginnen (UNC-Notation).

Zunächst entscheiden Sie durch die Auswahl der entsprechenden Option, was bei dem Import mit ggf. schon vorhandenen Berechtigungsinformationen auf den Verzeichnissen des Shares geschehen soll:

- *Vollständige Share-Informationen hochladen*
  Der Import **ersetzt** alle bisher in der Datenbank vorhandenen Berechtigungsdaten der Verzeichnisse im Share durch die neuen Informationen.
- *Verzeichnisse an Share anfügen*
  Der Import fügt neue Berechtigungsdaten hinzu für bisher freie Verzeichnisse – vorhandene Daten können nicht überschrieben werden. Falls ein zu importierendes Verzeichnis schon als Berechtigungsverzeichnis existiert, wird der Import abgebrochen. Damit wird ein versehentliches Überschreiben verhindert.

Haben Sie eine Option angeklickt, wählen Sie im Dateidialog die Import-Datei. Mit Bestätigung der Auswahl wird die Datei sofort zum AM-Server hochgeladen und eine intensive Validierung der Inhalte durchgeführt.

Sollte die Datei Fehler enthalten wird eine Liste der ermittelten Probleme angezeigt und die Aktion beendet. Es werden keine Daten importiert oder verändert.

Wurden keine Fehler gefunden, kann der Import mit einem Klick auf den nun aktivierten Button *Importieren* gestartet werden.

Nach dem erfolgreichen Import sind die neuen Berechtigungen in der Datenbank angelegt. Um die Berechtigungen in das Dateisystem zu schreiben, muss die Aufgabe *MaintainAccessPermission* ausgeführt werden; erst dann werden die Rechte effektiv umgesetzt.

#### *8.2.1.2.2 Format der Import-Datei*

Bei der zu importierenden Datei muss es sich um eine Excel-Datei (Dateiendung „.xlsx“, Office 2007 und neuer) handeln. Die erste Zeile der Datei enthält die Spaltenüberschriften, danach folgen die zu importierenden Werte. Die im Folgenden aufgeführten Spalten stellen die vom Access Manager verwendeten Informationen bereit. Sie sind teilweise – abhängig von administrativen Einstellungen – optional und können in beliebiger Reihenfolge erscheinen. Zur Vereinfachung der Dateierstellung kann eine Vorlagen-Datei heruntergeladen werden, die im Abschnitt *Share-Daten importieren* verlinkt ist.

Eine Datei darf Leerzeilen enthalten, diese werden beim Import ignoriert. Sollte ein Benutzerkonto in mehreren Zeilen auf demselben Verzeichnis mit unterschiedlichen Rechten aufgeführt werden (einmal Lesen, einmal Schreiben), wird es im Access Manager mit dem höheren Recht (Schreiben) berechtigt. Doppelte Benutzereinträge in der Import-Datei stellen somit kein Problem dar.

---

*Import-Dateien aus älteren Versionen können wegen unterschiedlicher Spaltennamen erst nach einer Anpassung verwendet werden.*

---

**Diese Spalten werden vom Access Manager beim Import verwendet:**

| Spaltenname: **FOLDER** | Pflichtfeld: **Ja** |
|---|---|
| **Format** | **Beschreibung** |
| \\Server\Share\Verzeichnispfad | UNC-Pfad des zu importierenden Verzeichnisses inklusive Server und Share. |

| Spaltenname: **READ** | Pflichtfeld: **Ja** |
|---|---|
| **Format** | **Beschreibung** |
| "X" oder leer | Der im Feld SAM-ACCOUNTNAME eingetragene Benutzer hat Leseberechtigung.<br>Falls SAM-ACCOUNTNAME gefüllt ist, muss READ oder WRITE gesetzt sein.<br>Falls WRITE gesetzt ist, erhält der Benutzer Schreibberechtigung. |

| Spaltenname: **WRITE** | Pflichtfeld: **Ja** |
|---|---|
| **Format** | **Beschreibung** |
| "X" oder leer | Der im Feld SAM-ACCOUNTNAME eingetragene Benutzer hat Schreibberechtigung.<br>Falls SAM-ACCOUNTNAME gefüllt ist, muss READ oder WRITE gesetzt sein. |

| Spaltenname: **SAM-ACCOUNTNAME** | Pflichtfeld: **Ja** |
|---|---|
| **Format** | **Beschreibung** |
| Domain\Username | Login-Name (Attributname „SamAccountName“ im Active Directory) eines Benutzers, der Lese- oder Schreibberechtigung haben soll.<br>Das Feld muss gefüllt sein, falls READ oder WRITE gesetzt ist.<br>Es ist möglich, keinen Benutzer zu berechtigen. In diesem Fall muss aber eine Zeile existieren, in der OWNER und RESPONSIBLE angegeben sind. Dadurch wird der Access Manager das angegebene Verzeichnis zu einem Berechtigungsverzeichnis machen, aber noch keinen Benutzer berechtigen. |

| Spaltenname: **OWNER** | Pflichtfeld: **Ja** |
|---|---|
| **Format** | **Beschreibung** |
| Domain\Username | Login-Name (Attributname „SamAccountName“ im Active Directory) des Besitzers. |

| Spaltenname: **RESPONSIBLE 1-X** | Pflichtfeld: **Ja** |
|---|---|
| **Format** | **Beschreibung** |
| Domain\Username | Login-Name (Attributname „SamAccountName“ im Active Directory) der Verantwortlichen 1 bis beliebig.<br>Mindestens der erste Verzeichnisverantwortliche muss angegeben werden, weitere sind optional. |

| Spaltenname: **INHERITRIGHTS** | Pflichtfeld: **Ja** |
|---|---|
| **Format** | **Beschreibung** |
| "X" oder leer | Zeigt an, ob das Verzeichnis die Benutzerberechtigungen seines übergeordneten Berechtigungsverzeichnisses erben soll. |

| Spaltenname: **VISIBLEINSELFSERVICE** | Pflichtfeld: **Ja** |
|---|---|
| **Format** | **Beschreibung** |
| "X" oder leer | Zeigt an, ob das Verzeichnis im Management Portal angezeigt werden soll. |

| Spaltenname: **COMMENT** | Pflichtfeld: **Siehe Beschreibung** |
|---|---|
| **Format** | **Beschreibung** |
| Freitext oder leer | Pro berechtigtem Benutzer wird ein Text eingetragen, der später als Kommentar an der Benutzerberechtigung angezeigt wird.<br>Sofern die administrative Einstellung „CommentsAreMandatoryDuringImport“ aktiviert ist, muss diese Spalte existieren und jede Benutzerberechtigung muss über einen Kommentar verfügen. Ist die Einstellung inaktiv, werden Kommentare übernommen sofern vorhanden, die Spalte darf aber auch komplett fehlen. |

#### *8.2.1.2.3 Mögliche Validierungsfehler*

Vor dem tatsächlichen Import der Datei werden die Daten auf Fehler überprüft. Schlägt die Validierung fehl, werden die problematischen Zeilen mit Nummer, Fehlerart und ggf. zusätzlichen Informationen aufgelistet. Hierbei werden verschiedene Fehlerarten unterschieden:

| Fehlerart | **InvalidServerOrShare** |
|---|---|
| Beschreibung | Der ausgewählte Server und Share für den Datenimport entsprechen nicht dem eingetragenen Server und Share in der Import-Datei. |
| Behebung | Stellen Sie sicher, dass der vollständige UNC-Pfad in der Import-Datei den richtigen Server und Verzeichnisfreigabe entspricht. |

| Fehlerart | **RightsFolderExists** |
|---|---|
| Beschreibung | Beim Import wurde *Verzeichnisse an Share anfügen* ausgewählt, das Berechtigungsverzeichnis existiert jedoch bereits im AM. Existierende Berechtigungsverzeichnisse werden bei dieser Option weder überschrieben noch verändert. |
| Behebung | Löschen Sie das existierende Berechtigungsverzeichnis aus dem Access Manager oder entfernen Sie die entsprechenden Zeilen aus der Excel-Datei. |

| Fehlerart | **MissingColumn** |
|---|---|
| Beschreibung | Mindestens eine Pflichtspalte wurde nicht gefunden. |
| Behebung | Überprüfen Sie, dass alle notwendigen Spalten vorhanden und korrekt benannt sind. |

| Fehlerart | **MissingOwner** |
|---|---|
| Beschreibung | Es wurde kein Besitzer angegeben. |
| Behebung | Geben Sie den Besitzer an. |

| Fehlerart | **DifferentOwners** |
|---|---|
| Beschreibung | Es wurden verschiedene Besitzer für dasselbe Verzeichnis angegeben. |
| Behebung | Stellen Sie sicher, dass für jedes Verzeichnis immer derselbe Besitzer angegeben wird. |

| Fehlerart | **MissingResponsible** |
|---|---|
| Beschreibung | Es wurde kein Verantwortlicher angegeben. |
| Behebung | Geben Sie für jedes Verzeichnis mindestens einen Verantwortlichen an. |

| Fehlerart | **DifferentResponsibles** |
|---|---|
| Beschreibung | In einer Spalte wurden verschiedene Verantwortliche für dasselbe Verzeichnis angegeben. |
| Behebung | Stellen Sie sicher, dass alle Verantwortlichen eines Verzeichnisses in einer Spalte gleich sind. |

| Fehlerart | **InvalidPermission** |
|---|---|
| Beschreibung | Es wurde ein Benutzer angegeben, aber nicht definiert, ob dieser Lese- oder Schreibberechtigung hat. |
| Behebung | Setzen Sie READ oder WRITE, um die Berechtigungen für den Benutzer festzulegen. |

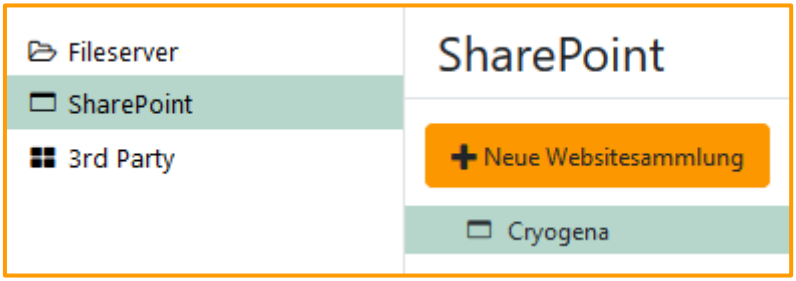
| Fehlerart | **InvalidUser** |
|---|---|
| Beschreibung | READ oder WRITE ist gesetzt, aber es wurde kein Benutzer angegeben. |
| Behebung | Geben Sie einen Benutzer bei SAM-ACCOUNTNAME an oder entfernen Sie READ und WRITE. |

| | |
|---|---|
| Fehlerart | **InvalidUser** |
| Beschreibung | Der angegebene Benutzer ist im Access Manager nicht bekannt. |
| Behebung | Stellen Sie sicher, dass der angegebene Benutzer bekannt ist. Führen Sie die Aufgabe *ADUserImport* aus, um die aktiven AD-Benutzer in die Datenbank zu importieren und überprüfen Sie die Schreibweise in der Excel-Datei.<br>Diese Meldung erscheint auch, wenn ein deaktivierter Benutzer importiert werden soll, die Option *AllowRetiredUserImport* in den Einstellungen jedoch aktiviert wurde. |

| | |
|---|---|
| Fehlerart | **InvalidInheritance** |
| Beschreibung | Die gewünschte Verzeichnis-Vererbung ist nicht möglich. |
| Behebung | Stellen Sie sicher, dass das erbende Verzeichnis unterhalb eines bestehenden / bereits definierten Berechtigungsverzeichnisses steht. Ein Verzeichnis kann nicht erben, wenn es das erste Berechtigungsverzeichnis unterhalb eines Shares sein soll. |

| | |
|---|---|
| Fehlerart | **MissingComment** |
| Beschreibung | Mindestens ein erforderlicher Kommentar wurde nicht angegeben. |
| Behebung | Ist die administrative Einstellung „CommentsAreMandatoryDuringImport“ aktiv, erhalten Sie diesen Fehler, wenn entweder die Spalte COMMENT komplett fehlt oder wenigstens für einen berechtigten Benutzer kein Kommentar existiert. |

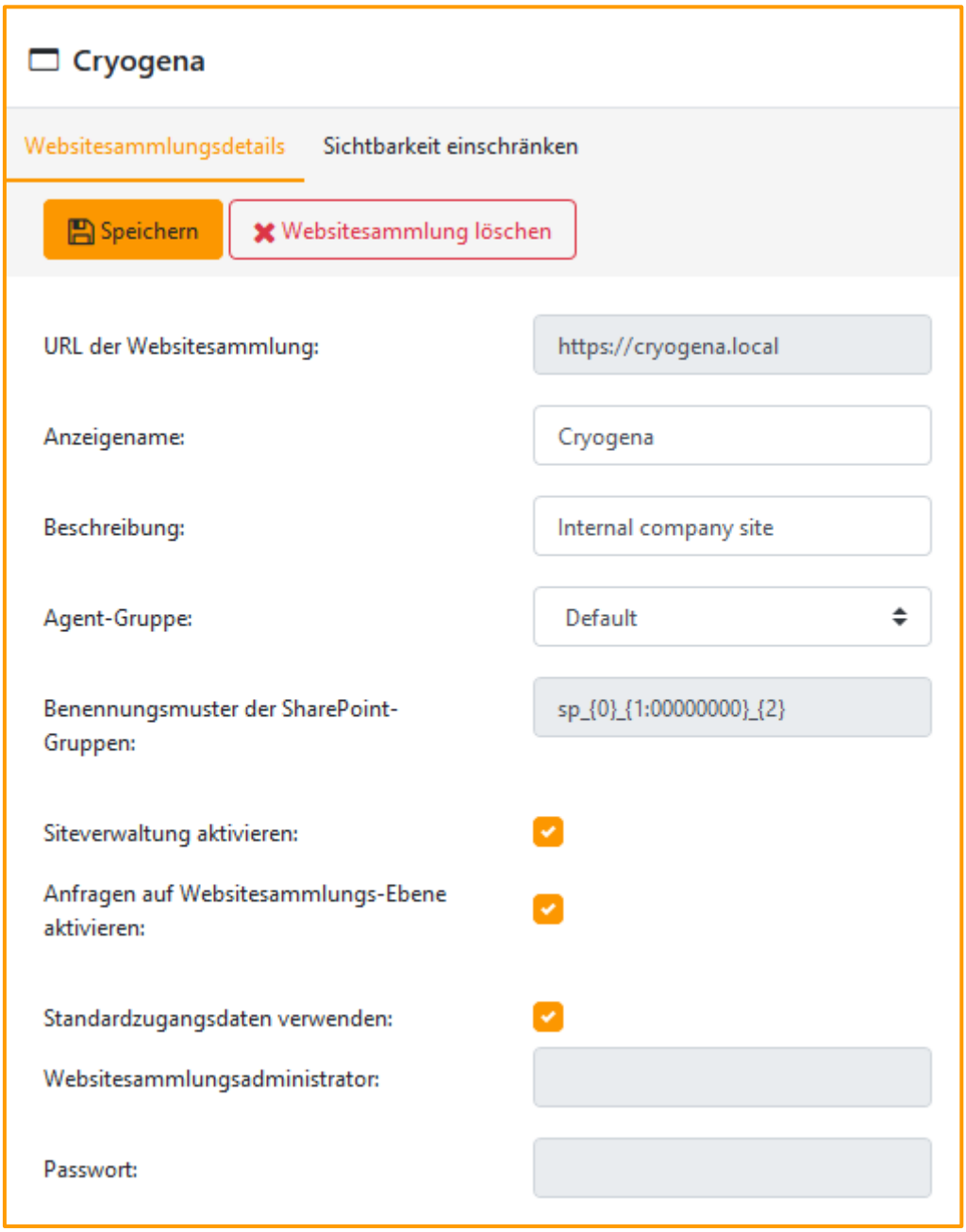
### 8.2.2 SharePoint




Dieser Bereich legt fest, welche Websitesammlungen der Access Manager verwalten soll.

Im Site-Baum sehen Sie alle eingerichteten Websitesammlungen. Klicken Sie den gewünschten Eintrag an, um seine Details im rechten Bereich zu sehen und zu editieren. Mit dem Button *Neue Websitesammlung* fügen Sie einen entsprechenden Einstiegspunkt hinzu.

#### 8.2.2.1 Websitesammlung-Details




Ist eine Websitesammlung bereits im Access Manager vorhanden, können Sie viele Parameter nachträglich ändern, nicht jedoch die URL – nur über diese wird die SharePoint Site im Netz identifiziert.

Wenn Sie eine neue Websitesammlung hinzufügen, füllen Sie die folgenden Werte:

*URL der Websitesammlung:* Die vollständige URL der SharePoint Site inkl. des Protokolls (http, https).

*Anzeigename:* Mit diesem Namen erscheint Ihre Websitesammlung im Access Manager.

*Beschreibung:* Hier geben Sie zwingend eine Beschreibung der Websitesammlung an.

*Agent-Gruppe:* Hier legen Sie die Gruppe der AM-Agenten fest, die die Aufgaben für den Server bearbeiten soll. Standard ist die Gruppe *Default*. Mehr Informationen zu Agent-Gruppen finden Sie im Kapitel 10.2.

*Benennungsmuster der SharePoint-Gruppen:* Es handelt sich um Benennungsregeln für den Access Manager, mit denen Sie das Namensformat der Berechtigungsgruppen gemäß Ihren Vorgaben steuern. Es stehen drei Platzhalter (in geschweiften Klammern) zur Verfügung, die dynamisch ersetzt werden:

- {0} Der Name der Site, wie Sie ihn unter *Anzeigename* eingetragen haben
- {1} Die Site-ID (fortlaufende interne Nummer)
- {2} Die Abkürzung der Berechtigung (r, w oder d für Lese-, Schreib- oder Design-Gruppe)

Die Verwendung von {0} ist optional, die Platzhalter {1} und {2} müssen jedoch verwendet werden, um eindeutige Gruppennamen zu generieren.

*Siteverwaltung aktivieren:* Hiermit wird bestimmt, ob Sites dieser Sammlung aktiv verwaltet werden. Falls die Verwaltung nicht aktiviert ist, gibt es folgende Einschränkungen:

- Die Websitesammlung wird nicht im Management Portal angezeigt.
- Die Zugriffsberechtigungen werden nicht verwaltet (erstellt, geprüft, korrigiert).

*Anfragen auf Websitesammlungs-Ebene aktivieren:* Damit ermöglichen Sie es den Anwendern, eine Websitesammlung auszuwählen und dort direkt eine neue Site zu beantragen. Andernfalls können neue Sites ausschließlich innerhalb einer schon existierenden Websitesammlung beantragt werden. Voraussetzung dafür ist, dass bereits ein *Besitzer* für die Sammlung eingetragen wurde.

*Standardzugangsdaten verwenden:* Wenn der Server der Websitesammlung eine Verbindung mit Ihrem Active Directory hat, können Sie diese Option aktivieren. Es wird dann das Access Manager Benutzerkonto verwendet.

*Websitesammlungsadministrator* & *Passwort:* Wenn der Server nicht mit dem Active Directory verbunden ist (z.B. bei Verwendung von Office365), geben Sie hier die entsprechenden Zugangsdaten ein.

Klicken Sie auf *Speichern* damit die Änderungen wirksam werden. Falls Sie eine neue Websitesammlung hinzugefügt haben, erscheint sie nun im Verzeichnisbaum.

Mit Klick auf *Löschen* wird die Websitesammlung inklusive ihrer Sites aus dem Access Manager entfernt werden, sodass sie nicht mehr verwaltet wird.

**Erweiterung für SharePoint Online:**

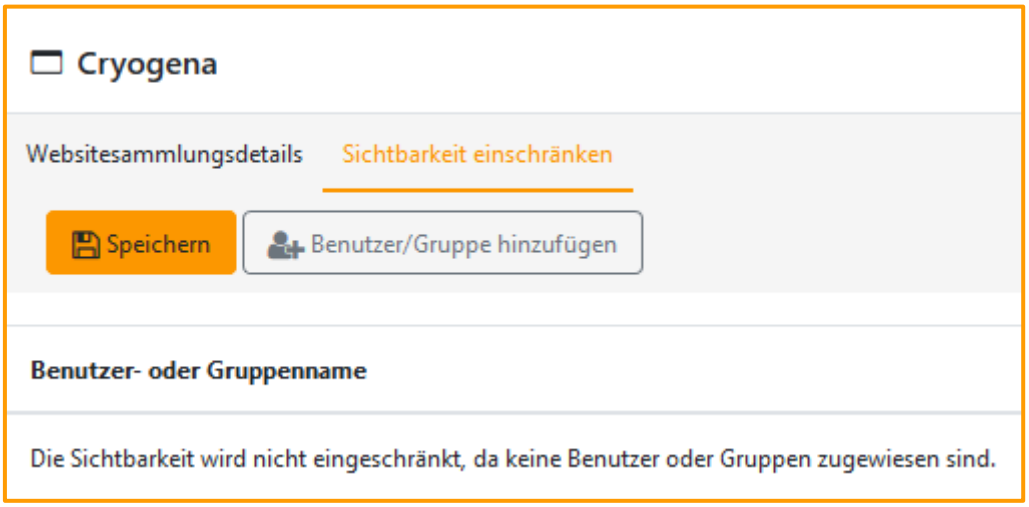
Sofern Sie SharePoint 365 in der Cloud (SharePoint Online) verwenden, sind zusätzliche Einstellungen vorzunehmen.

Der Access Manager muss als Anwendung in Azure registriert werden. Bitte notieren Sie sich in diesem Zuge die folgenden Werte **(Wichtig, da diese Werte nachher teilweise nicht mehr verfügbar sind):**

- Anwendungs-ID (Client)
- Clientschlüssel
- Authentifizierungsendpunkt

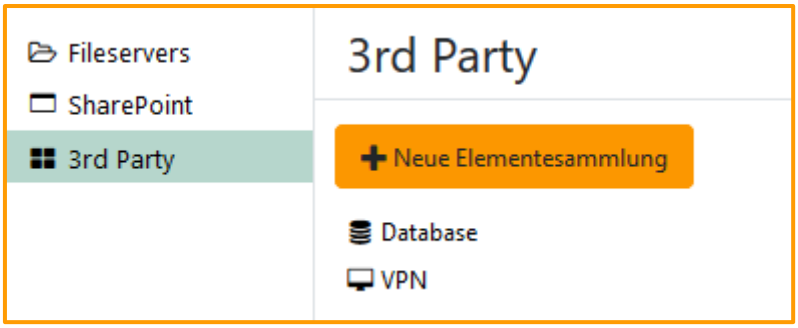
Diese werden beim Hinzufügen einer Site Collection in den Access Managers benötigt:


### 8.2.2.2 Sichtbarkeit einschränken




Wenn die Websitesammlung nur bestimmten Benutzern / Benutzergruppen auf der Beantragungsseite angezeigt werden soll, tragen Sie sie in diese Liste ein und speichern Sie sie.

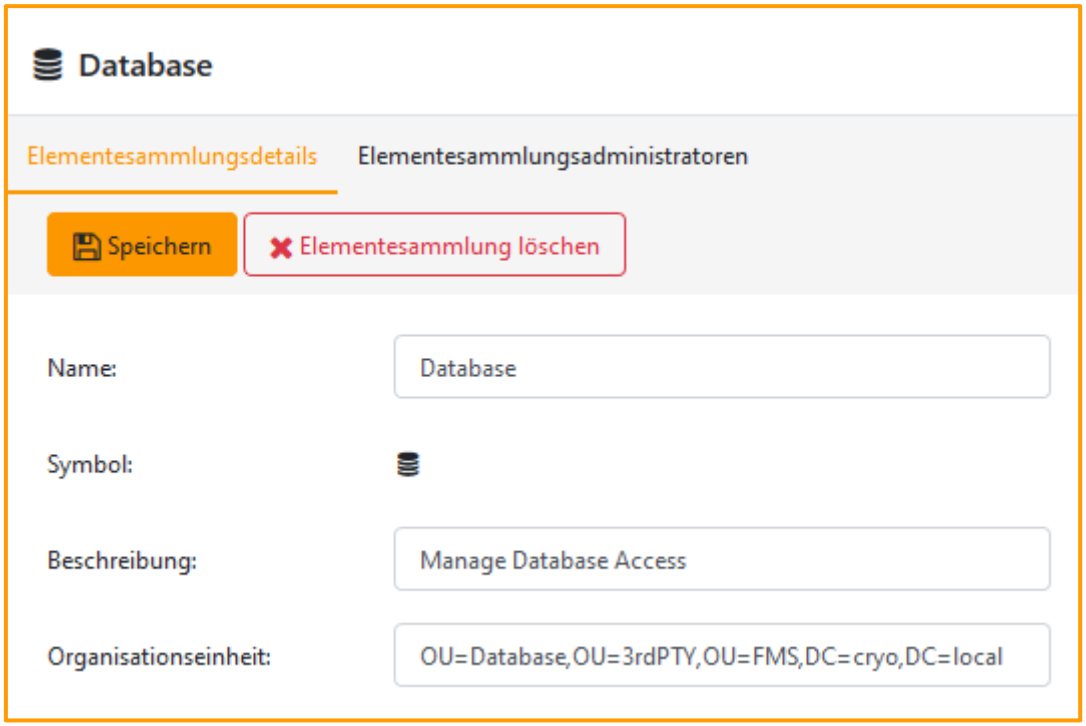
### 8.2.3 3rd Party




Dieser Bereich legt fest, in welche thematischen Elementesammlungen die AD-Gruppen geordnet werden sollen, deren Mitgliedschaften in Form von Elementen verwaltet werden.

Im Elemente-Baum sehen Sie alle eingerichteten Elementesammlungen. Klicken Sie den gewünschten Eintrag an, um seine Details im rechten Bereich zu sehen und zu editieren. Mit dem Button *Neue Elementesammlung* fügen Sie einen entsprechenden Einstiegspunkt hinzu.

#### 8.2.3.1 Elementesammlung-Details




Ist eine Elementesammlung bereits im Access Manager vorhanden, können Sie die Parameter auch nachträglich ändern.

Wenn Sie eine neue Elementesammlung hinzufügen, füllen Sie die folgenden Werte:

*Name:* Mit diesem Namen erscheint Ihre Elemente-Sammlung im Access Manager.

*Symbol:* Wählen Sie ein Symbol aus, welches am besten zu Ihrer thematischen Sammlung passt.

*Beschreibung:* Ein Freitext, der der Information des Elementesammlungsadministrators dient.

*Organisationseinheit:* Tragen Sie hier die OU im Active Directory ein, in der die vom Access Manager erstellten Berechtigungsgruppen der späteren Elemente gespeichert werden. Am einfachsten ist es, wenn Sie im AD die Eigenschaften der OU öffnen, auf das Tab *Attribut-Editor* wechseln und dort den Wert von *distinguishedName* kopieren. Der Access Manager muss schreibenden Zugriff auf die OU und ihre Unterobjekte besitzen. Es ist möglich, für zwei verschiedene Elementesammlungen dieselbe OU anzugeben.

Klicken Sie auf *Speichern* damit die Änderungen wirksam werden. Falls Sie eine neue Elementesammlung hinzugefügt haben, erscheint sie nun im Sammlungsbaum.

Mit Klick auf *Elementesammlung löschen* wird die Sammlung komplett aus dem Access Manager entfernt. Die enthaltenen Elemente werden dabei ebenfalls gelöscht, deren angebundene AD-Gruppe werden jedoch nicht verändert. Wenn Sie dies wünschen, entfernen Sie zunächst die Berechtigungsverwaltung der enthaltenen Elemente einzeln (siehe Kapitel 8.4.4.3.6).

#### 8.2.3.2 Berechtigungsset – Logik für die Rechtevergabe

Eine Elementesammlung definiert einen Satz verschiedener Berechtigungen für ein Element, die frei wählbar sind, wobei jede Berechtigung auf eine eigene AD-Gruppe gemappt wird, wenn später ein Element in dieser Sammlung erstellt wird. Bitte beachten Sie, dass hier nicht wirklich Berechtigungen vergeben werden: Sie geben hier lediglich eine Beschreibung (Namen) der Berechtigung an, die Ihre Dritt-Applikation später mit der entsprechenden AD-Gruppe verknüpft. Ein Berechtigungssatz kann auch aus nur einer Berechtigung bestehen.

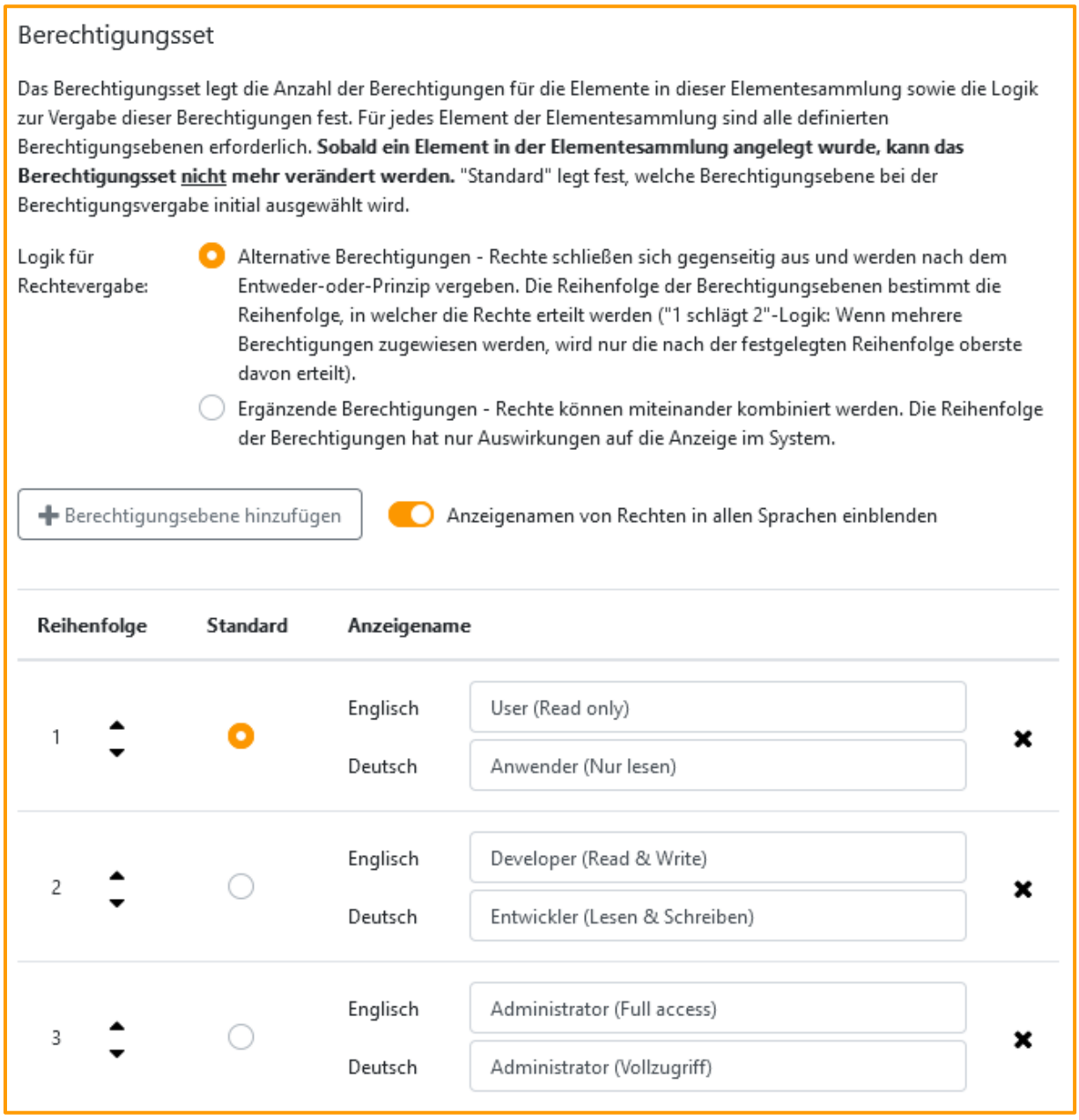
In jedem Berechtigungsset wird ein Standardrecht ausgewählt. Bei der späteren Rechtevergabe auf ein Element durch einen Verantwortlichen, Administrator oder Profiladministrator wird zunächst dieses Recht vorgeschlagen, analog zum Standardrecht (meistens *Lesen*) bei einem Verzeichnis.

Es gibt zwei Arten der Berechtigungslogik: Alternative und ergänzende Berechtigungen.

#### *8.2.3.2.1 Alternative Berechtigungen*

Bei alternativen Berechtigungen kann immer nur eine Berechtigung des Satzes vergeben werden, sie lassen sich nicht kombinieren.

Beispiel Datenbankzugriff:

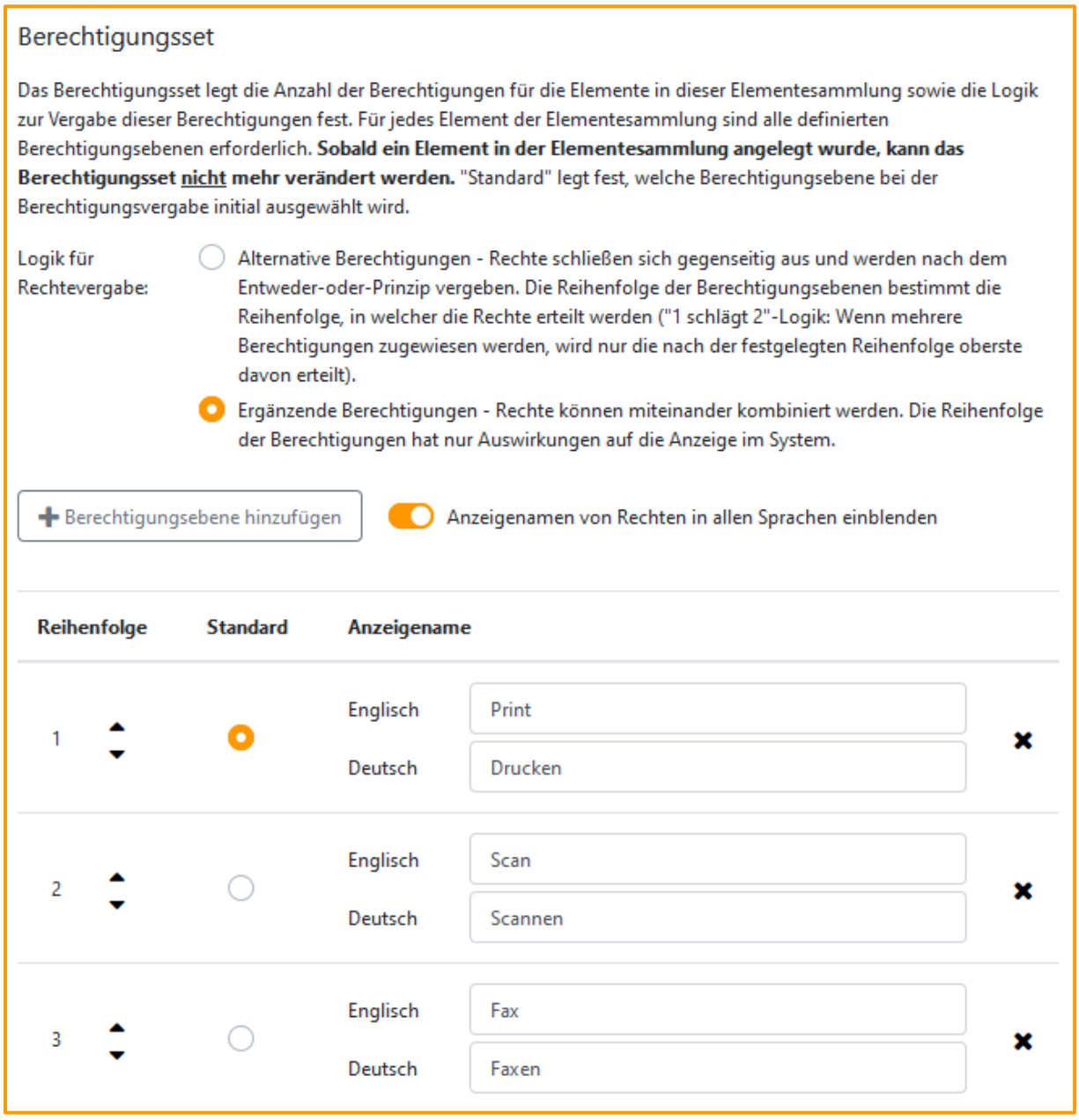



Hierbei muss sich der Anwender bei der Beantragung eines Zugriffs auf eine DB für eine Zugriffsart entscheiden; er kann nur eine der aufgeführten Zugriffe erhalten. Diese Logik ist vergleichbar mit den Zugriffsarten Lesen / Schreiben bei Verzeichnissen – auch dort entscheidet man sich entsprechend.

#### *8.2.3.2.2 Ergänzende Berechtigungen*

Bei ergänzenden Berechtigungen können mehrere Berechtigungen des Satzes gleichzeitig vergeben werden. Dies wird am ehesten genutzt, wenn die Einzelrechte sich nicht gegenseitig widersprechen.

Beispiel Multifunktionsdrucker:



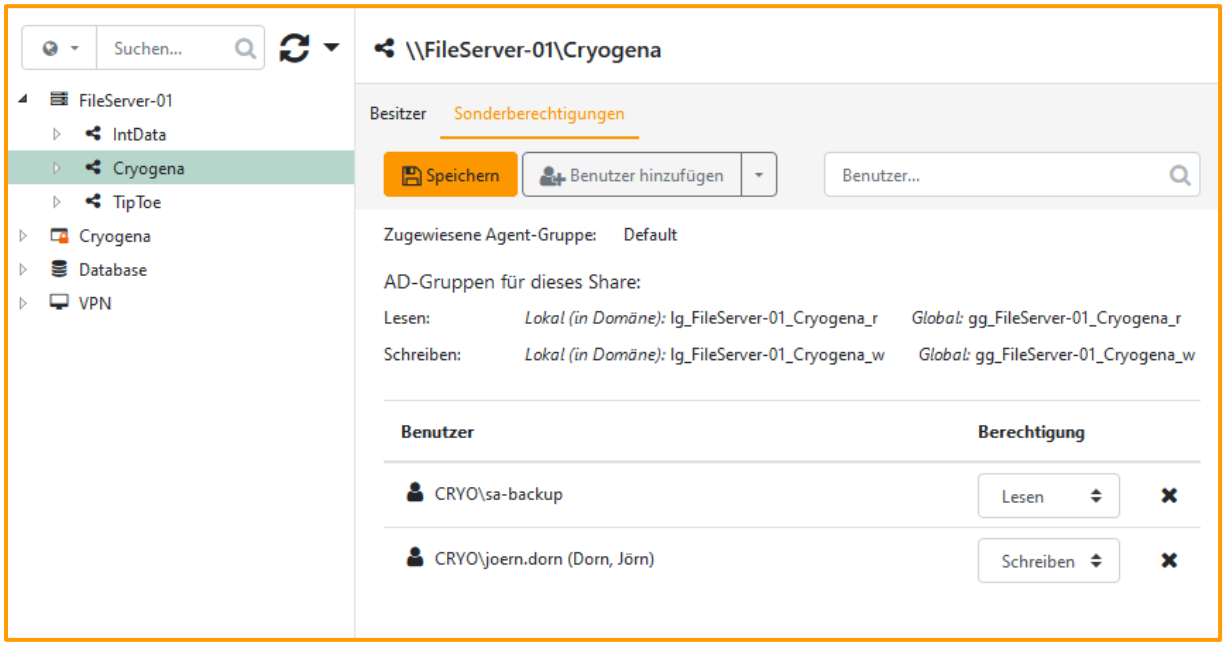

Hierbei kann der Anwender gleichzeitig mehrere verschiedene Funktionen desselben Druckers erhalten, da diese unabhängig voneinander sind.

#### 8.2.3.3 Elementesammlungsadministratoren

In diesem Tab können Sie Benutzer eintragen, die nur diese Elementesammlung verwalten dürfen, also nicht die weiter reichende Rolle *3rd-Party-Administrator* erhalten haben.

## 8.3 Sonderberechtigungen auf Einstiegspunkten verwalten

Als *(FM-)Administrator* haben Sie dieselben Möglichkeiten der Berechtigungsverwaltung wie ein *Verantwortlicher* auch, d.h. Sie können auf jeder Ressource Benutzerrechte verändern. Zusätzlich können Sie für den Ressourcentyp „Dateisystem“ sog. *Sonderberechtigungen* auf Share-Ebene setzen:




Der Access Manager erstellt per se für jedes Fileshare mindestens zwei zusätzliche AD-Gruppen (vier, wenn der Domain-Modus *Multidomain optimiert* für den Fileserver verwendet wird), die mit Lesen bzw. Schreiben berechtigt werden. Diese Gruppen werden nicht auf dem Share-Verzeichnis (Einstiegspunkt) selbst berechtigt, sondern auf allen verwalteten Verzeichnissen sowie deren (nicht verwalteten) Unterverzeichnissen. Da diese Gruppen initial keine Mitglieder enthalten, findet hierdurch keine ungewollte Rechteausweitung statt. Sie können über diese Sonderberechtigungen selbst Benutzerkonten in die Gruppen aufnehmen. Der Zweck der Sonderberechtigungen ist, dass Sie auf einfache und schnelle Weise z.B. Maschinenkonten für automatisiertes Backup / Restore auf allen Verzeichnissen erlauben können oder auch Abteilungsleiter, die grundsätzlich auf alle Verzeichnisse zugreifen können sollen – dies erspart Ihnen die Arbeit, sie separat auf jedem verwalteten Verzeichnis berechtigen zu müssen. Sonderberechtigungen lassen sich nur von *Administratoren*, nicht jedoch von *Verantwortlichen* bestimmen und erscheinen auch nicht in einem *Reapproval*.

## 8.4 Ressourcenverwaltung

Abhängig von Ihrer speziellen Administratorrolle (*Administrator, FM-Administrator, FM-Server-Administrator, FM-Share-Administrator, SP-Administrator* oder *3rd-Party Administrator*) können Sie besondere Informationen und Rechte / Rollen auf den verschiedenen Ressourcen-Typen einsehen und bearbeiten.

### 8.4.1 Server Ebene

Wenn Sie einen Server auswählen, werden Ihnen im Detailbereich die relevanten Daten angezeigt. Dazu gehören etwa der Servername und der Domänen-Modus, der diesem Server zugewiesen wurde. Diese Informationen sind nicht veränderbar.

### 8.4.2 Share Ebene

Wenn Sie ein Share auswählen, wird Ihnen im Detailbereich zunächst der aktuelle Besitzer angezeigt, der auch gewechselt werden kann, wodurch auch alle Besitzer auf den untergeordneten Verzeichnisebenen überschrieben werden.

Zusätzlich können Sie unter *Sonderberechtigungen* Lese- und Schreibberechtigungen für Benutzer auf allen Berechtigungsverzeichnissen dieses Share gleichzeitig verwalten, siehe das vorige Kapitel 8.3.

### 8.4.3 Elementesammlung Ebene

Wenn Sie eine Elementesammlung auswählen, werden Ihnen im Detailbereich die relevanten Daten angezeigt. Dazu gehören etwa der Sammlungsname und die OU in der AD, die dieser Sammlung zugewiesen wurde. Diese Informationen sind nicht veränderbar.

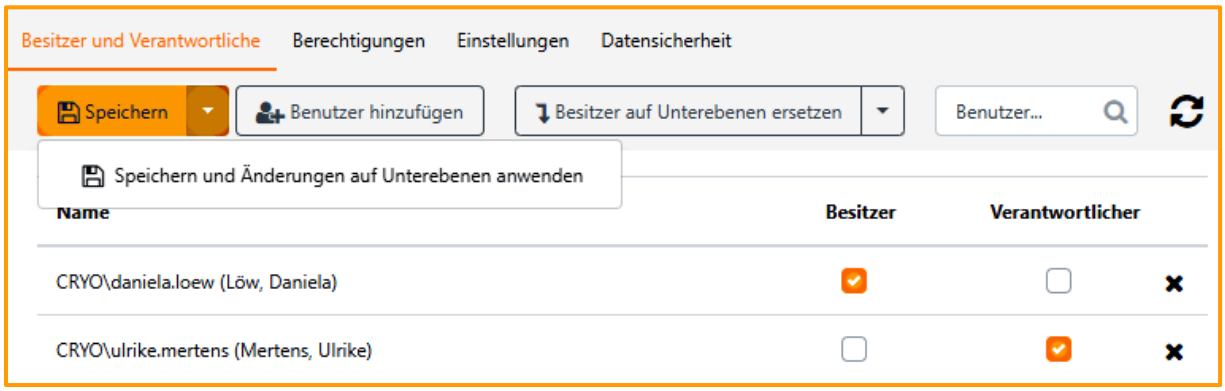
Im Tab *Skripteinstellungen* können Sie eigene PowerShell Skripte angeben, die bei bestimmten Aktionen automatisch ausgeführt werden, siehe Kapitel 8.4.4.3.7.

### 8.4.4 Ressource-Ebene

Unter *Ressource-Ebene* versteht man die Ressourcen, die unterhalb eines Shares, einer SharePoint Site Collection oder auch einer Elementesammlung liegen, d.h. es handelt sich um freie oder auch verwaltete Verzeichnisse, Sites und Dritt-Elemente.

Die im Folgenden beschriebenen Funktionen im jeweiligen Detailbereich sind zwar prinzipiell bei allen Ressourcen-Typen gleich, doch gibt es Detailunterschiede, die durch die Natur des jeweiligen Typs begründet sind.

#### 8.4.4.1 Tab „Besitzer und Verantwortliche"




In diesem Tab können Sie die Besitzer und Verantwortlichen eintragen, ändern oder entfernen. Neue Benutzer, die entweder die Rolle *Besitzer* oder *Verantwortlicher* übernehmen sollen, können durch Eingabe des Benutzernamens in das entsprechende Feld und den Button *Benutzer hinzufügen* in der Tabelle ergänzt werden. Durch An-/Abwählen der Checkbox einer entsprechenden Rolle in der Zeile eines Benutzers können Sie die Rollen entsprechend anpassen. Änderungen werden erst durch den Button *Speichern* wirksam.

Um Rollenänderungen nicht nur auf einzelnen berechtigten Ressourcen vorzunehmen, sondern diese ohne weiteren Aufwand auch auf untergeordneten Ressource-Strukturen übernehmen zu können, stehen für Fileserver Management und Share Point Management zusätzlich zum einfachen *Speichern* weitere Optionen zur Verfügung:

##### *8.4.4.1.1 Speichern und Änderungen auf Unterebenen anwenden*

Diese Option dient dazu, exakt die vorgenommene(n) Änderung(en) auf untergeordneten Elementen zu übernehmen. Vorher bestehende Rollenzuordnungen werden hierbei nicht übernommen.

##### *8.4.4.1.2 Besitzer / Verantwortliche auf Unterebenen ersetzen*

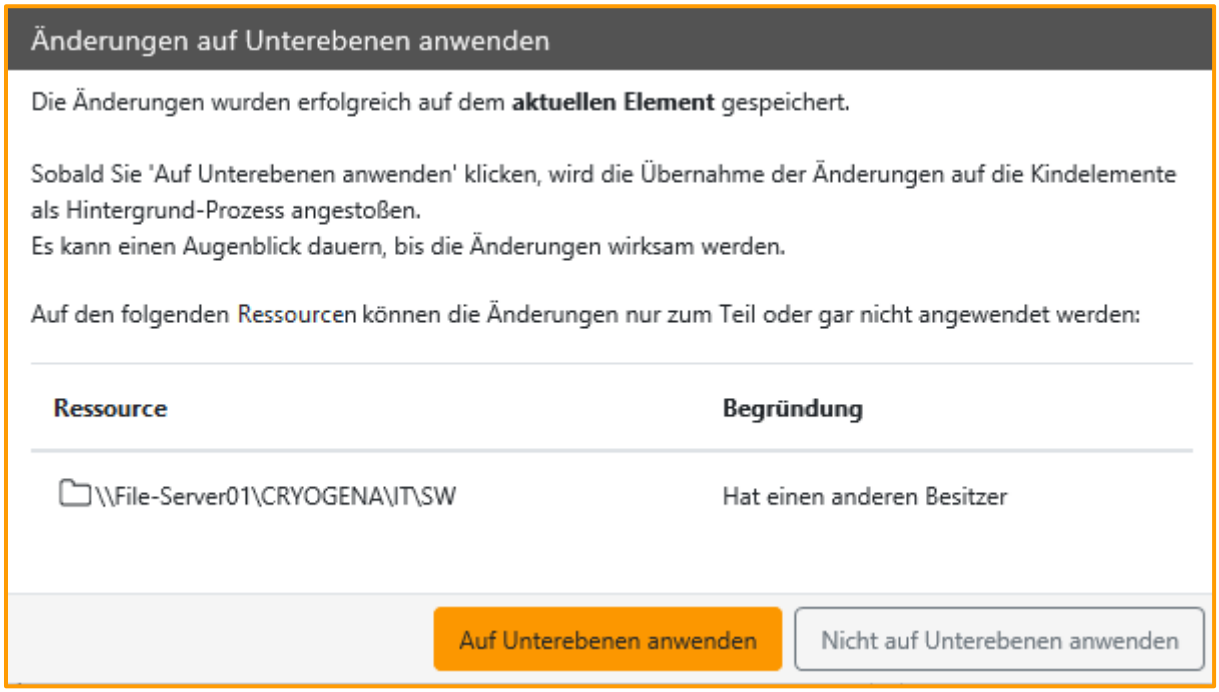
Im Gegensatz zur ersten Option wird hier die auf der berechtigten Ressource gesetzte Rollenverteilung je nach Auswahl (*Besitzer / Verantwortlicher auf Unterebenen ersetzen*) vollständig auf untergeordnete Ressourcen repliziert, und zwar unabhängig von deren IST-Zustand.

Ähnlich wie beim einfachen Speichern gibt es einige Einschränkungen, die sich aus der Unterscheidung zwischen freien / verwalteten Ressourcen im Access Manager ergeben. Es werden grundsätzlich nur solche Änderungen für das jeweilige Unterelement übernommen, die dessen Status nicht verändern, also z.B. aus einem freien Ordner einen Berechtigungsordner machen würden oder umgekehrt. Allgemeine Informationen zum Arbeitsprinzip *Verantwortliche & Besitzer* entnehmen Sie Kapitel 4.1 ff.

Die wichtigsten Punkte zusammengefasst:

- Ein freier Ordner kann einen Besitzer, aber keinen Verantwortlichen haben.
  → Hinzugefügte / geänderte Besitzer werden übernommen, aber keine Verantwortlichen.
- Ein Berechtigungsordner hat genau einen Besitzer und mindestens einen Verantwortlichen.
  → Besitzer werden nicht ersatzlos entfernt oder hinzugefügt. Verantwortliche werden nur dann ersatzlos entfernt, wenn noch mindestens ein Verantwortlicher auf dem Berechtigungsfolder verbleibt.
- Eine Sharepoint-Site kann mehrere Besitzer und Verantwortliche haben.
  → Verantwortliche und Besitzer werden nur dann ersatzlos entfernt, wenn noch mindestens ein Verantwortlicher und ein Besitzer auf der Site verbleibt.

Der Access Manager prüft auf die o.g. Bedingungen und wird die verwalteten Ressourcen, für die die gespeicherten Änderungen nicht übernommen werden können, mit einer Begründung auflisten. Erst nach Drücken des Buttons *Fortfahren* wird die Aktion ausgelöst und durch einen Job umgesetzt.




Beachten Sie in diesem Zusammenhang ebenfalls den Unterschied zwischen Entfernen eines Benutzers und dem Entziehen der Rolle eines Benutzers. Entziehen Sie z.B. einem Benutzer für eine verwaltete Ressource die Rolle *Besitzer*, so verliert er diese auch auf untergeordneten Ebenen. Löschen Sie hingegen einen Besitzer von einer verwalteten Ressource, so wird dieser Benutzer unabhängig von seiner Rolle auch auf Unterelementen gelöscht, also auch dann, wenn er auf Unterelementen die Rolle *Verantwortlicher* innehat.

Ein paar Fallbeispiele:

Sie **entfernen** von Berechtigungsordner A den *Besitzer* Peter Schmitt und ersetzen ihn, indem Sie den Besitzer Ralf Müller hinzufügen.
Was passiert, wenn:

- Sie wählen *Speichern und Änderungen auf Unterebene übernehmen.*
  - Unterordner A1 hat den Besitzer Peter Schmitt. Dieser wird durch den Besitzer Ralf Müller ersetzt.
  - Unterordner A2 hat den Besitzer Lisa Meier. Diese wird nicht entfernt. Da ein Berechtigungsfolder nur einen Besitzer haben kann, wird Ralf Müller auch nicht hinzugefügt (abweichend von einer SharePoint Site, die auch mehrere Besitzer haben kann).
- Sie speichern und wählen *Besitzer auf Unterebenen ersetzen*
  - Ralf Müller wird auf allen Unterordnern als Besitzer gesetzt. Andere Besitzer werden dabei entfernt.

Sie **löschen** von Berechtigungsordner A den *Besitzer* Peter Schmitt und ersetzen ihn, indem Sie den Besitzer Ralf Müller hinzufügen
Was passiert, wenn:

- Sie wählen *Speichern und Änderungen auf Unterebene übernehmen.*
  - Unterordner A1 hat zwei Verantwortliche: Lisa Meier und Peter Schmitt. Peter Schmitt wird als Verantwortlicher gelöscht.

Sie **entfernen** von Berechtigungsordner A den einzigen *Verantwortlichen* Peter Schmitt und ersetzen ihn, indem Sie den Verantwortlichen Ralf Müller hinzufügen
Was passiert, wenn:

- Sie wählen *Speichern und Änderungen auf Unterebene übernehmen.*
  - Unterordner A1 hat den Verantwortlichen Peter Schmitt. Dieser wird durch den Verantwortlichen Ralf Müller ersetzt.
  - Unterordner A2 hat den Verantwortlichen Lisa Meier. Diese wird nicht entfernt. Da ein Berechtigungsordner aber mehr als nur einen Verantwortlichen haben kann, wird Ralf Müller als Verantwortlicher hinzugefügt.
- Sie speichern und wählen *Verantwortliche auf Unterebenen ersetzen*
  - Ralf Müller wird auf allen Unterordnern als Verantwortlicher gesetzt. Andere Verantwortliche werden dabei entfernt.

Sie haben auf Berechtigungsordner A zwei Verantwortliche, Peter Schmitt und Ralf Müller. Sie entfernen Peter Schmitt aus der Verantwortlichenrolle.

Was passiert, wenn:

- Sie wählen *Speichern und Änderungen auf Unterebene übernehmen.*
  - Unterordner A1 hat nur einen Verantwortlichen: Peter Schmitt. Da mit Peter Schmitt der letzte Verantwortliche gelöscht würde, wird keine Aktion ausgelöst.
  - Unterordner A2 hat zwei Verantwortliche: Peter Schmitt und Lisa Meier. Peter Schmitt wird als Verantwortlicher entfernt.
- Sie speichern und wählen *Verantwortliche auf Unterebenen ersetzen*
  - Ralf Müller wird auf allen Unterordnern als Verantwortlicher gesetzt. Andere Verantwortliche werden dabei entfernt.

#### 8.4.4.2 Tab „Berechtigungen"

Als Administrator haben Sie hier dieselben Möglichkeiten wie ein Verantwortlicher. Die Funktionen sind im Kapitel 4.2.2.1 ausführlich beschrieben.

Zusätzlich haben Sie erweiterte Möglichkeiten, um Benutzer zu berechtigen. Die DropDown-Liste *Benutzer hinzufügen* enthält einen weiteren Punkt, *Sondergruppe hinzufügen*:

Hiermit geben Sie eine AD-Gruppe angeben, welche als Sonderberechtigungsgruppe auf dem Verzeichnis berechtigt werden soll. Ihr kann kein Ablaufdatum oder Kommentar hinzugefügt werden. Bitte beachten Sie, dass Sondergruppen nicht in die Lizenzzählung des Access Manager einfließen, diese Gruppen aber auch nicht auditiert werden und nicht in Berichten erscheinen. Sonderberechtigungsgruppen sollten im Hinblick auf Zugriffssicherheit und Nachvollziehbarkeit mit Bedacht eingesetzt werden. Diese Funktion steht nur für den Ressourcen-Typ *Verzeichnis* zur Verfügung.

Darüber hinaus können Sie über den Button *Exportieren* die aktuell berechtigten Benutzer in eine Excel-Datei schreiben. Umgekehrt können Sie mit *Importieren* die Benutzerberechtigungen anhand einer Excel-Datei im entsprechenden Format (siehe unten) einlesen und dem Ordner / der Site zuweisen. Haben Sie die gewünschte Datei ausgewählt, entscheiden Sie im nächsten Schritt, ob die zu importierenden Benutzerberechtigungen nur für die aktuell ausgewählte Ressource oder zusätzlich auch für alle untergeordneten verwalteten Ressourcen gesetzt werden sollen. Bei der Validierung der Importdatei erkannte Fehler werden in einer Liste angezeigt – in diesem Fall wird nichts importiert. Folgende Fehlertypen werden erkannt:

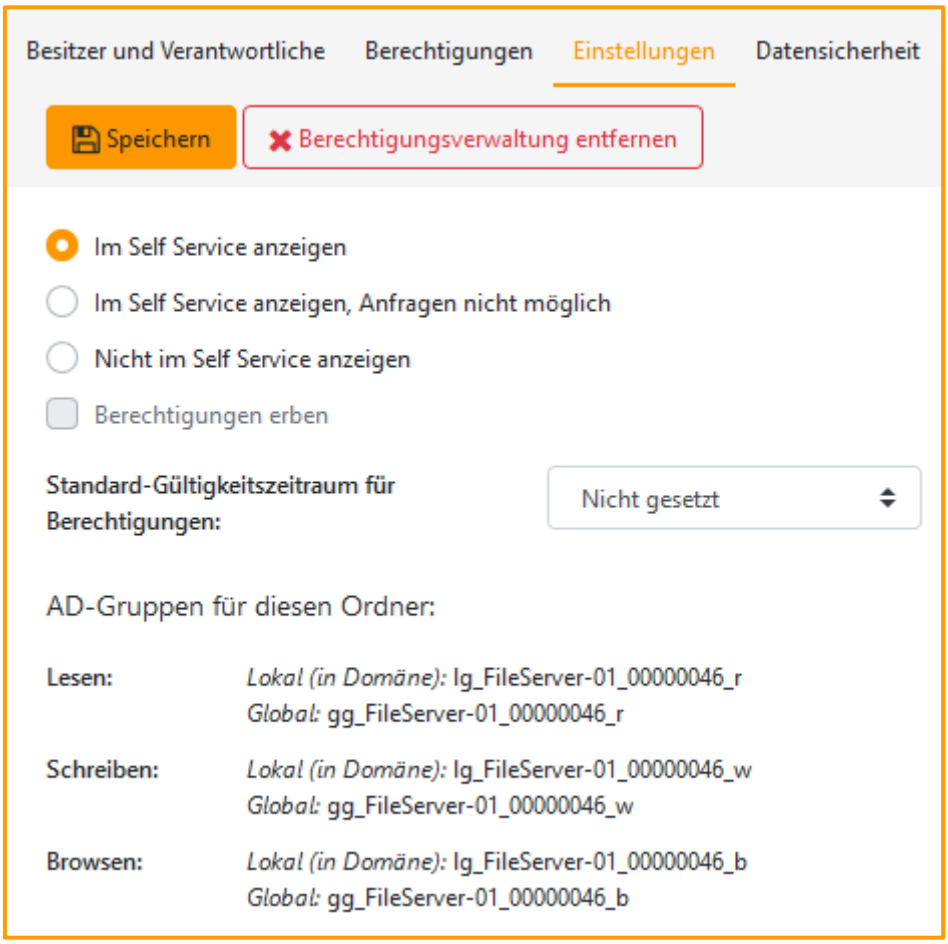
- InvalidUser
- InvalidPermission
- InvalidValidThroughDate
- MissingColumns
- NothingToImport

Die Excel-Datei muss in einem definierten Format vorliegen, das im Folgenden beschrieben wird. Im Dialog *Berechtigungen importieren* können Sie eine Vorlagendatei herunterladen (Link *Vorlage für Excel-Datei herunterladen*).

Die erste Zeile der Excel-Datei enthält ausschließlich die Spaltenüberschriften *USERID, READ, WRITE, DESIGN* und *EXPIRATIONDATE* (Reihenfolge beachten). Jede weitere Zeile in der Datei enthält die Berechtigungsdefinition für jeweils einen Benutzer:

- Die Spalte *USERID* enthält den Benutzernamen im Format *Domain\Benutzer* (SamAccountName).
- Die Spalte *READ* enthält ein „X“, falls der Benutzer eine Leseberechtigung erhalten soll. Andernfalls ist die Spalte leer.
- Die Spalte *WRITE* enthält ein „X“, falls der Benutzer eine Schreibberechtigung erhalten soll. Andernfalls ist die Spalte leer.
- Die Spalte *DESIGN* enthält ein „X“, falls der Benutzer eine Gestaltenberechtigung erhalten soll (gilt nur bei SharePoint Sites). Andernfalls ist die Spalte leer.
- Die Spalte *EXPIRATIONDATE* enthält optional ein Ablaufdatum. Falls die Berechtigung nicht ablaufen soll, ist die Spalte leer.

#### 8.4.4.3 Tab „Einstellungen“




Dieses Tab gibt Ihnen die Möglichkeit verschiedene Einstellungen an der ausgewählten Ressource vorzunehmen. Abhängig vom Ressourcen-Typ sind ggf. nicht alle Optionen verfügbar.

#### 8.4.4.3.1 Sichtbarkeit im Management Portal für Antragsteller:

Über die folgenden Optionen legen Sie fest, ob und wie die Ressource den Anwendern (Antragstellern) im Ressourcen-Baum angezeigt werden soll:

*Im Self Service anzeigen* blendet die Ressource ein. Der Anwender kann die üblichen Anträge stellen.

*Im Self Service anzeigen, Anfragen nicht möglich* blendet die Ressource ebenfalls ein, erlaubt aber keine Anträge durch die Anwender – die Ressource wird dargestellt, als sei sie nicht verwaltet. Diese Option steht nur Verzeichnisse und SharePoint Sites zur Verfügung, für Dritt-Elemente jedoch nicht.

*Nicht im Self Service anzeigen* blendet diese Ressource sowie alle darunter liegenden aus – dies gilt auch, wenn es sich bei den Kind-Ressourcen um verwaltete handeln sollte.

---

*Durch diese Einstellung wird keinerlei Einfluss auf die Sichtbarkeit und die Zugriffsmöglichkeiten der Ressource auf dem realen Verzeichnis bzw. SharePoint Site genommen.*

---

#### 8.4.4.3.2 Vererbung von Berechtigungen

Mit der Checkbox *Berechtigungen erben* (nur bei Verzeichnissen verfügbar) können Sie für diesen Berechtigungsordner einstellen, dass die Benutzerberechtigungen des übergeordneten Berechtigungsordners auf diesen Ordner vererbt werden. Es handelt sich hierbei – auch in den NTFS-Berechtigungen – tatsächlich um eine Vererbung: Die Rechte werden nicht von oben *kopiert*. Diese Checkbox ist deaktiviert, wenn der aktuelle Ordner der erste in der Berechtigungshierarchie ist, da er von niemandem erben kann. Im Falle eines freien Ordners (kein Berechtigungsordner) kann die Vererbung nicht ausgeschaltet werden, da solche Ordner ihre Berechtigungen in jedem Fall vom Eltern-Verzeichnis erben.

#### 8.4.4.3.3 Standard-Dauer von Berechtigungen

Die DropDown-Liste *Standard-Gültigkeitszeitraum für Berechtigungen* (nur bei Verzeichnissen und SharePoint Sites verfügbar) legt einen Zeitraum fest: Wenn ein Antragsteller ein Ablaufdatum angibt, das den eingestellten Gültigkeitszeitraum überschreitet, wird es entsprechend vorverlegt[5]. Der Verantwortliche kann das Ablaufdatum beim Bearbeiten der Anfrage jedoch frei festlegen.

#### 8.4.4.3.4 Verwendete Berechtigungsgruppen

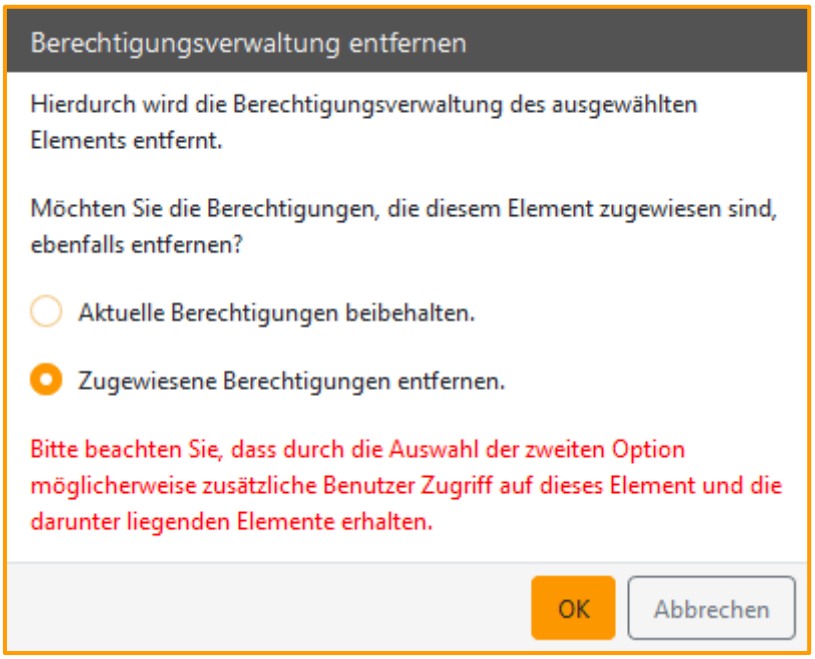
Der Abschnitt *AD-Gruppen* bzw. *SharePoint-Gruppen* zeigt die der ausgewählten Ressource zugewiesenen Berechtigungsgruppen an. Dies dient lediglich der Information; diese Gruppenzuweisungen werden vom System verwaltet und können nicht manuell geändert werden.

[5] Ablaufdatum ist dann z.B. heute + 3 Monate

#### *8.4.4.3.5 Berechtigungsverwaltung entfernen (Verzeichnisse & Sites)*

Der Button *Berechtigungsverwaltung entfernen* können Sie eine Berechtigungsressource (Verzeichnis oder Site) in eine nicht verwaltete Ressource umwandeln. Hier müssen Sie eine Entscheidung bzgl. des Rechtemanagements zu treffen:
Die aktuell auf einer Ressource gesetzten Benutzerrechte können entweder komplett entfernt oder alternativ beibehalten werden. Behalten Sie die aktuellen Rechte bei, haben weiterhin dieselben Personen Zugriff wie zuvor. Sollen die Rechte entfernt werden, unterscheidet sich das Verhalten abhängig vom Ressourcen-Typ (Verzeichnis bzw. Site):

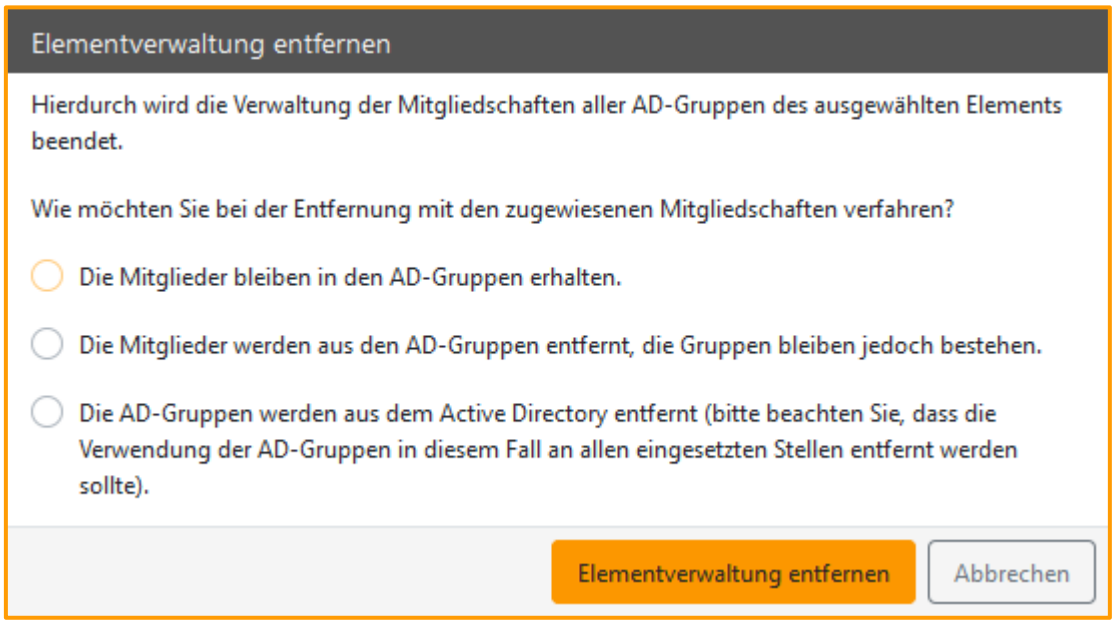
Bei Verzeichnissen wird die Vererbung wieder aktiviert und die im darüber liegenden Verzeichnis berechtigten Benutzer erhalten Zugriff. Bei SharePoint Sites bleibt die Site noch für diejenigen Benutzer zugreifbar, die zusätzlich direkt in SharePoint berechtigt wurden – alle durch den Access Manager berechtigten Benutzer verlieren dagegen ihren Zugriff.



#### *8.4.4.3.6 Berechtigungsverwaltung entfernen (Dritt-Elemente)*

Der Button *Elementverwaltung entfernen* löscht nicht nur die aktuellen Benutzerberechtigungen, sondern auch das Element selbst. Hier müssen Sie eine Entscheidung bzgl. der verwendeten AD-Gruppen zu treffen:

Die AD-Gruppe bleibt unverändert, d.h. alle noch berechtigten Benutzer bleiben Mitglieder dieser Gruppe. Alternativ kann die Gruppe komplett geleert werden, bleibt aber bestehen. Dies ist der einfachste Weg, um beim Entfernen des Elements effektiv alle Berechtigungen zu entfernen und die Konsistenz Ihrer Infrastruktur zu gewährleisten. Wenn Sie sicher sind, dass diese AD-Gruppe an keiner weiteren Stelle innerhalb Ihres Unternehmens mehr genutzt wird, können Sie mit der dritten Option auch die AD-Gruppe selbst löschen und damit Ihr System sauber halten.




#### *8.4.4.3.7 Ausführung von PowerShell Skripten (Dritt-Elemente)*

Als *AM-Administrator* haben Sie die Möglichkeit, für Elementesammlungen und Elemente eigene PowerShell-Skripte zu hinterlegen, die bei bestimmten Aktionen automatisch ausgeführt werden. Dazu gehört z.B. das Hinzufügen neuer Elemente zu einer Sammlung oder auch das Hinzufügen neuer Mitglieder zu einem Element. Bitte beachten Sie die Hinweise für die technische Unterstützung von PowerShell-Skripten im Kapitel 12.2.

**Skripte für Elementesammlungen:**

Wählen Sie eine Elementesammlung aus und klicken Sie auf das Tab *Einstellungen*. Skripte können für verschiedene Ereignisse hinterlegt werden:

1. Wenn der Sammlung ein neues Element hinzugefügt wird
2. Wenn ein Element aus der Sammlung entfernt wird
3. Wenn einem Element der Sammlung ein neues Mitglied hinzugefügt wird

4. Wenn ein Mitglied von einem Element der Sammlung entfernt wird

Sofern Skripte für die Ereignisse 3 und 4 hinterlegt werden, gelten sie für alle Elemente dieser Sammlung und ersetzen damit die Skripte, die ggf. auf den Elementen selbst gesetzt wurden. Den Skripten stellt der Access Manager unterschiedliche Variablen zur Abfrage zur Verfügung, bspw. den Namen des betreffenden Elements und die zugrunde liegende AD-Gruppe.

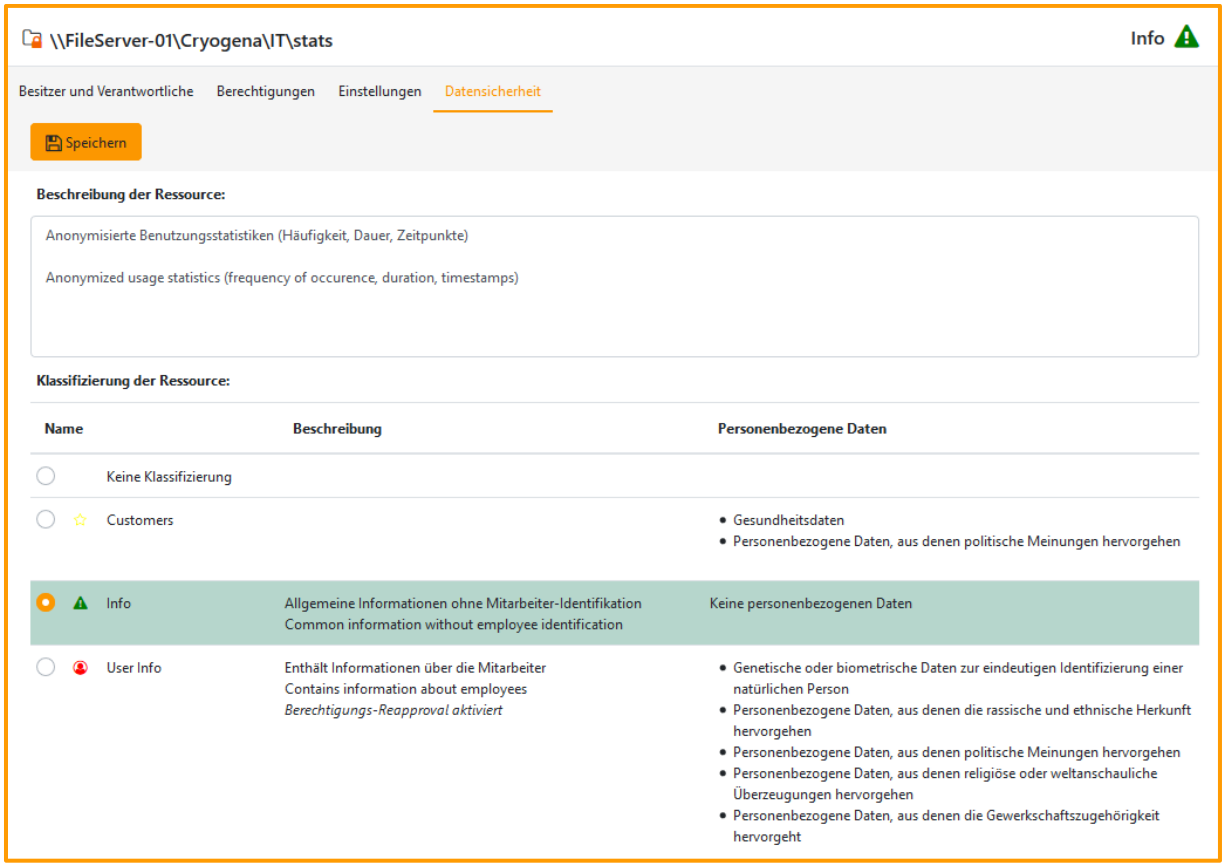
**Skripte für Elemente-Berechtigungen:**

Wählen Sie ein Element aus und klicken Sie auf das Tab *Einstellungen*. Skripte können *pro Berechtigung* eines Elementes für diese Ereignisse hinterlegt werden:

1. Wenn einem Mitglied die gewählte Berechtigung erteilt wird
2. Wenn einem Mitglied die gewählte Berechtigung entzogen wird

Sofern für diese Ereignisse bereits auf Elementsammlungsebene ein Skript hinterlegt wurde, ist hier keine Eintragung mehr möglich. Den Skripten stellt der Access Manager verschiedene Variablen zur Abfrage zur Verfügung.

### 8.4.4.4 Tab „Datensicherheit“



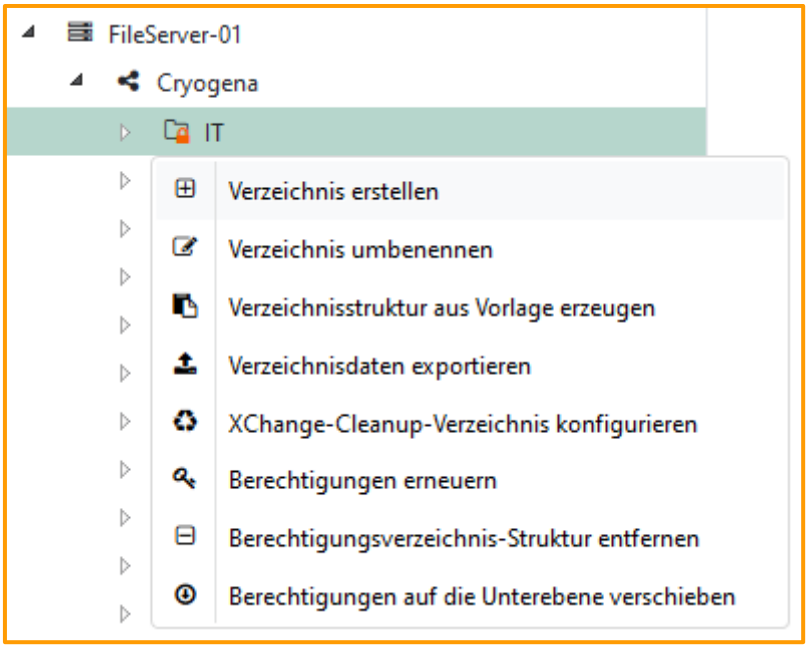

Diese Seite ist nur bei verwalteten Ressourcen verfügbar. Abhängig von der administrativen Einstellung kann oder muss ein beschreibender Text für diese Ressource eingegeben werden. Darüber hinaus

können Sie die Ressource durch eine der vorgegebenen Klassifizierungen markieren und auch nachträglich ändern. Das Entfernen einer Klassifizierung von einer Ressource erfolgt durch die Auswahl des Eintrags *Keine Klassifizierung*.

Die zugewiesenen EU-DSGVO Kategorien einer Klassifizierung können Sie nur als *Klassifizierungsadministrator* setzen.

Die eingestellte Klassifizierung ist für normale Anwender (Antragsteller) nicht sichtbar. Der Verantwortliche einer klassifizierten Ressource erkennt diese am Symbol bei neuen Anträgen. Sie wird außerdem im Detailbereich einer ausgewählten Ressource im Tab *Berechtigungen* angezeigt.

### 8.4.5 Kontextmenü im Ressourcen-Baum




Ein Rechtsklick auf eine Ressource im Baum öffnet das Kontextmenü. Hier stehen Ihnen diverse Aktionen zur Verfügung, die im Folgenden erläutert werden. Die tatsächlich verfügbaren Aktionen sind abhängig von der Art der angewählten Ressource.

#### 8.4.5.1 Site erstellen

*Site erstellen* öffnet ein Dialogfenster, in dem der gewünschte Name der neuen Site eingeben und eine gewünschte SharePoint Vorlage ausgewählt wird. Welche SharePoint Vorlagen verfügbar sind ist abhängig von den „Layout und Seitenvorlage Einstellungen“ in SharePoint. Bei der Site-Benennung werden die administrativ definierten Validierungsregeln verwendet. Die neue Site wird unter der im Ressourcen-Baum angeklickten Site angelegt und automatisch ausgewählt. Zunächst handelt es sich bei der neuen Site nicht um eine Berechtigungssite, da ihr noch kein Verantwortlicher zugewiesen wurde. Die Besitzer werden von der übergeordneten Site übernommen.

#### 8.4.5.2 Site umbenennen

Mit dieser Aktion kann die ausgewählte Site umbenannt werden. Alle Einstellungen bleiben erhalten, lediglich der Name sowie die URL der Site werden geändert. Hierbei werden die administrativ definierten Validierungsregeln verwendet.

#### 8.4.5.3 Element umbenennen

Hiermit geben Sie einem Element einen neuen Namen sofern er in dieser Elementesammlung noch nicht existiert. Alle weiteren Einstellungen bleiben erhalten.

#### 8.4.5.4 Verzeichnis erstellen

*Verzeichnis erstellen* öffnet ein Dialogfenster, in dem Sie den gewünschten Namen des neuen Verzeichnisses eingeben. Hierbei werden die administrativ definierten Validierungsregeln verwendet. Das neue Verzeichnis wird unter dem aktuellen Verzeichnis angelegt und automatisch ausgewählt. Zunächst handelt es sich bei dem neuen Verzeichnis nicht um ein Berechtigungsverzeichnis, da ihm noch kein Verzeichnisadministrator zugewiesen wurde. Der Verzeichnisbesitzer wird vom übergeordneten Verzeichnis übernommen.

#### 8.4.5.5 Verzeichnisstruktur aus Vorlage erzeugen

Diese Aktion öffnet einen Dialog, in dem eine Vorlage zur Verzeichniserstellung ausgewählt wird. Der Button *Verzeichnisse erstellen* legt die neuen Verzeichnisse unter dem gewählten Verzeichnis entsprechend der gewählten Vorlage an. Die verfügbaren Vorlagen werden im Funktionsbereich *Verzeichnisvorlagen* verwaltet.

#### 8.4.5.6 Verzeichnis umbenennen

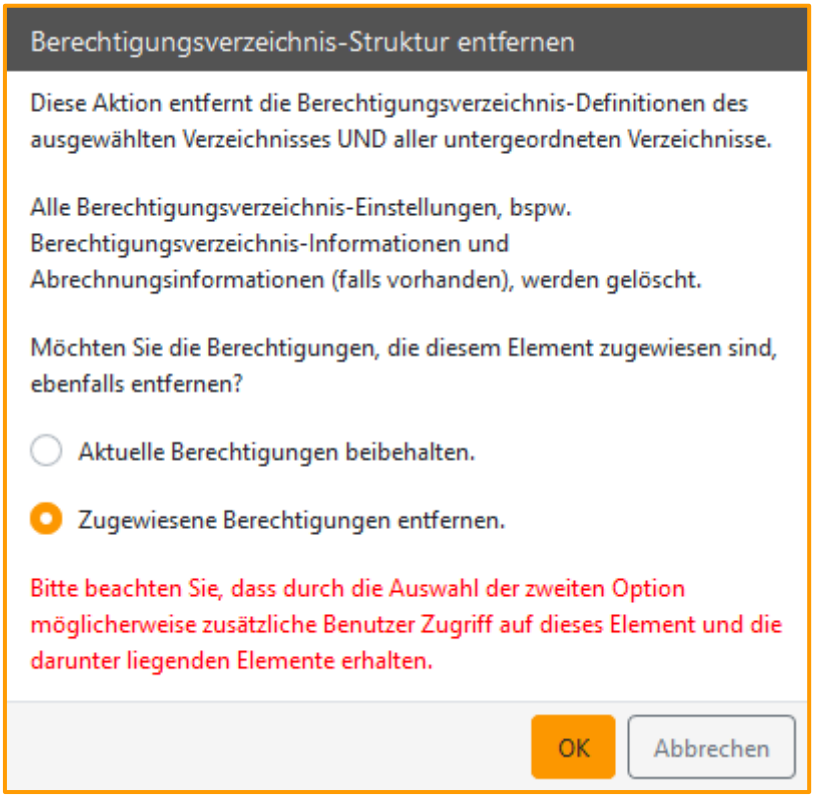
Hiermit geben Sie einem Element einen neuen Namen sofern er in diesem Verzeichnis noch nicht existiert. Alle weiteren Einstellungen bleiben erhalten. Hierbei werden die administrativ definierten Validierungsregeln verwendet.

#### 8.4.5.7 Verzeichnisdaten exportieren

Diese Aktion exportiert die aktuellen Benutzerberechtigungen des angewählten Berechtigungsverzeichnisses und aller untergeordneten Berechtigungsverzeichnisse als Excel-Datei. Diese können Sie als Administrator jederzeit wieder in ein Share importieren (siehe Kapitel 8.2.1.2.1).

#### 8.4.5.8 Berechtigungsverzeichnis-Struktur entfernen

Diese Aktion entfernt alle Berechtigungsverzeichnis-Definitionen des angewählten und aller untergeordneter Verzeichnisse. Danach handelt es sich um normale Verzeichnisse, die nicht vom Access Manager verwaltet werden. Wählen Sie dazu aus, was mit den den Verzeichnissen aktuell zugewiesenen Berechtigungen passieren soll:




- Die aktuell zugewiesenen Berechtigungen bleiben erhalten, werden aber nicht mehr durch Access Manager verwaltet.
- Die aktuell zugewiesenen Berechtigungen werden entfernt und die Vererbung von übergeordneten Berechtigungen aktiviert (empfohlen).

#### 8.4.5.9 Berechtigungen erneuern

Mit dieser Aktion werden die zuvor veränderten Besitzer, Verantwortlichen und berechtigten Benutzer in die AM-Datenbank und in die SharePoint Sites bzw. in die AD/Fileserver eingetragen. Dazu plant das System eigenständig eine neue einmalige Aufgabe mit sofortigem Ausführungszeitpunkt.

#### 8.4.5.10 XChange-Cleanup-Verzeichnis konfigurieren


Die Funktion *XChange Cleanup* ermöglicht die Verwaltung von Verzeichnissen, deren Inhalte automatisch gelöscht werden sollen, sobald sie über einen bestimmten Zeitraum nicht verwendet wurden. Diese Verzeichnisse werden als *Cleanup-Verzeichnisse* bezeichnet.

Es erscheint ein Eingabefeld, in dem Sie das gewünschte Alter der Dateien bezogen auf ihre letzte Verwendung angeben. Die Einrichtung wird mit dem Button *Cleanup aktivieren* abgeschlossen und hinter dem Verzeichnis erscheint ein neues Symbol. Ab sofort werden Dateien, die das angegebene Alter überschreiten, automatisch gelöscht. Gleiches gilt für leere Verzeichnisse und solche, die nur überalterte Dateien enthalten. Wird kein Alter angegeben, wird der Cleanup-Status entfernt, das Verzeichnis wird nicht mehr überwacht; das Verzeichnis und alle darin enthaltenen Dateien werden dabei nicht vom Dateisystem gelöscht.

Beachten Sie, dass für diese Funktion die Planung der Aufgaben *XChangeFileScan* und *XChangeCleanUp* erforderlich ist.

## 8.5 3rd Party Elemente anlegen

Innerhalb einer von Ihnen administrierten Elementesammlung können Sie neue Elemente erstellen, die Berechtigungsset und -logik der Sammlung verwenden (siehe Kapitel 8.2.3.2).

Wählen Sie zunächst die gewünschte Elementesammlung aus und dort das Tab *Element erstellen.* Geben Sie den gewünschten Namen des neuen Elements ein und optional eine Beschreibung. Der Name darf innerhalb der aktuellen Elementesammlung noch nicht verwendet werden. Darunter werden Ihnen die durch die Elementesammlung definierten Rechte aufgelistet, die Sie nun mit einer AD-Gruppe verbinden müssen, wofür zwei Möglichkeiten bereitstehen:

### 8.5.1 Vorhandene AD-Gruppen verwenden

Tragen Sie den Namen der gewünschten AD-Gruppe ein (die Auto-Vervollständigung hilft Ihnen bei der Suche). Diese Gruppe darf noch nicht von einem anderen Recht oder Element verwendet werden (auch nicht in einer anderen Elementesammlung), da es zu Überschneidungen und Inkonsistenzen bei der Mitgliedschaftsverwaltung käme. Wählen Sie danach die Benutzer der Gruppe aus, die weiterhin enthalten sein sollen; diese bleiben in der Gruppe erhalten, alle anderen werden vom Access Manager entfernt.

---

*Für eine korrekte Funktion stellen Sie sicher,*
*dass der Access Manager schreibenden Zugriff auf diese AD-Gruppe hat.*

*Verwenden Sie **niemals** dieselbe AD-Gruppe mehrfach,*
*da dies zu konkurrierenden und sich widersprechenden Rechte-Prüfungen führen wird.*

---

### 8.5.2 Neue AD-Gruppe erstellen

Tragen Sie den Namen der zu erstellenden AD-Gruppe ohne Domäne ein. Sofern diese Gruppe bereits existiert, wird das System darauf hinweisen. Legen Sie außerdem den Gruppenbereich und -typ fest. Die Gruppe wird in derjenigen OU angelegt, die der AM-Administrator für diese Elementesammlung festgelegt hat und kann von Ihnen nicht beeinflusst werden.

### 8.5.3 Skripte zuweisen

Eigene PowerShell Skripte, die bei Berechtigungsvergabe oder -entzug ausgeführt werden, können in dieser Phase nicht angegeben werden, sondern erst, wenn das neue Element erstellt wurde. Siehe dazu Kapitel 8.4.4.3.7.

# 9 Fileserver Accounting

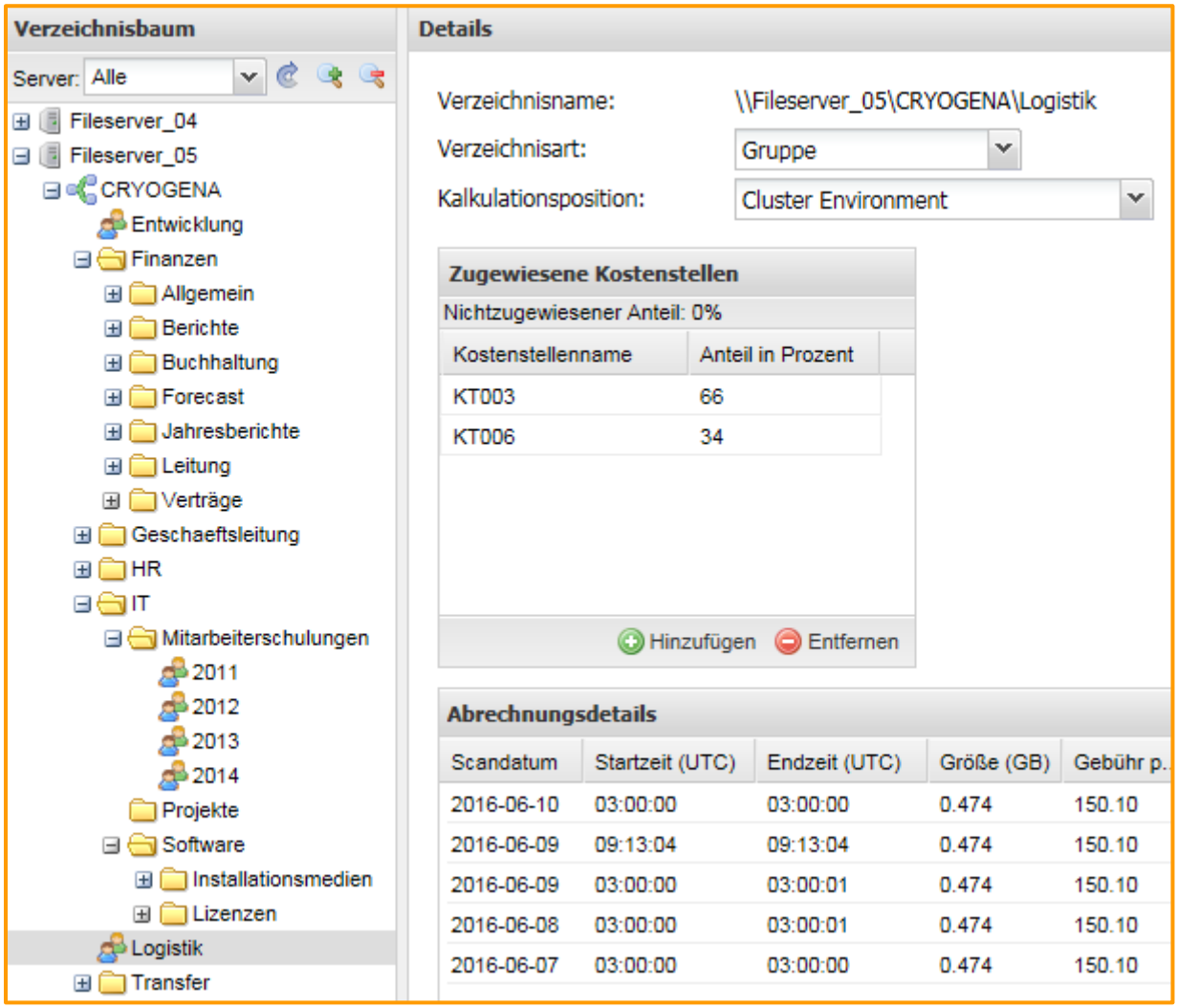

## 9.1 Arbeitsprinzip: Kostenstellenbasierte Erfassung der Speicherplatznutzung

Das optionale Modul *Fileserver Accounting* stellt Funktionalitäten zum Ermitteln und Darstellen von Kosteninformationen auf Verzeichnisebene zur Verfügung. Der Access Manager kennt zwei Abrechnungstypen durch die sich Ordner als Abrechnungsverzeichnis definieren lassen – *Gruppe* und *Home*. Eine *Kosteneinheit* bestimmt die veranschlagten Kosten pro Gigabyte benutztem Speicherplatz (Stückpreis).

Ein Abrechnungsverzeichnis das als *Gruppe* definiert wurde, wird in seiner Größe berechnet und die resultierenden Kosten werden anteilig auf eine oder mehrere Kostenstellen verteilt.

Bei einem Abrechnungsverzeichnis mit der Definition *Home* wird jeder Unterordner als sog. Home-Verzeichnis eines bestimmten Benutzers behandelt – in diesem Fall werden die ermittelten Kosten dem jeweils definierten Benutzer berechnet.

## 9.2 Abrechnungsverzeichnisse definieren




Die Seite *Struktur* bietet Funktionen zum Festlegen von Abrechnungsverzeichnissen. Ein Abrechnungsverzeichnis wird durch eine Verzeichnisart und eine Kalkulationsposition, welche die Gebühr pro Gigabyte belegtem Verzeichnisspeicher angibt, definiert.

### 9.2.1 Verzeichnisarten

Es gibt fünf Verzeichnisarten, die für ein Abrechnungsverzeichnis definiert werden können:

| Verzeichnisart | Beschreibung |
|---|---|
| Home | Dieser Ordner wird als Home-Verzeichnis definiert. Der Abrechnungsdurchlauf behandelt jeden Unterordner dieses Verzeichnisses als eigenes Home-Verzeichnis eines expliziten Benutzers. Diese Ordner werden durch ihren Verzeichnisnamen identifiziert, der dem Benutzerkonto entsprechen muss. |
| Gruppe | Dieser Ordner wird als Gruppenverzeichnis definiert. Der belegte Verzeichnisspeicher wird den jeweils festgelegten Kostenstellen anteilig berechnet. |
| Unberücksichtigt | Dieser Ordnertyp kann verwendet werden, um das entsprechende Verzeichnis beim nächsten Abrechnungsdurchlauf zu ignorieren. Die ermittelten Daten der letzten Abrechnungsdurchläufe, z. B. für die Kostenstellenzuordnung, bleiben erhalten. Dieser Ordnertyp sollte nur vorübergehend verwendet werden. |
| Keine | Dies ist der Standardtyp für einen Verzeichnis. Es wurde noch kein Abrechnungsverzeichnis definiert.<br>**Hinweis:** Wenn der Ordnertyp eines Verzeichnisses von *Home* oder *Gruppe* auf *Keine* gewechselt wird, werden die Daten für die Kostenstellenzuordnung, aus der AM-Datenbank entfernt. Es können zwar immer noch ermittelte Daten der letzten Abrechnungsdurchläufe exportiert werden, aber das zurückgesetzte Verzeichnis wird nicht mehr als Abrechnungsverzeichnis behandelt. |
| Zu definieren | Dieser Ordnertyp sollte nur bei der Erst-Erstellung eines Abrechnungsverzeichnisses vorübergehend verwendet werden, z. B. wegen noch unbekannter Verzeichnisart. Verzeichnisse dieses Ordnertyps werden in der Abrechnung nicht berücksichtigt. |

Das Icon ⚠ signalisiert, dass das betreffende Verzeichnis wegen eines aufgetretenen Fehlers nicht kalkulierbar ist, z. B. weil der Zugriff auf das Verzeichnis fehlschlug.

### 9.2.2 Interaktives Festlegen von Abrechnungsverzeichnisdaten

Im Detailbereich rechts werden Ihnen zum gewählten Abrechnungsverzeichnis detaillierte Informationen angezeigt. Hier können Sie auch die Abrechnungswerte anpassen oder ein neues Abrechnungsverzeichnis festlegen.

Für ein Gruppenverzeichnis etwa ist es notwendig Kostenstellen einzurichten, auf denen der belegte Verzeichnisspeicher verrechnet werden kann. Die Verzeichnisart kann erst dann gespeichert werden, wenn der gesamte prozentuale Kostenverteilungsschlüssel (Quota) auf die verantwortlichen Kostenstellen verteilt wurde. Kostenstellen und deren Kostenverteilungsschlüssel können in der Liste *Zugewiesene Kostenstellen* hinzugefügt werden. Die zur Verfügung stehenden Kostenstellen werden auf der Seite *Kostenstellen* verwaltet (siehe Kapitel 9.4).

Nachdem Sie die Änderungen der Abrechnungsverzeichniseinstellungen gespeichert haben, sollten Sie die Aufgabe *AccountingScan* (siehe Kapitel 10.6.5.2) zeitnah ausführen um die Ermittlung korrekter Daten für die Abrechnungsberichte zu gewährleisten.

Um ein Verzeichnis abrechenbar zu machen, wählen Sie es im Verzeichnisbaum aus. Im Detailbereich rechts stehen Ihnen Felder zur Einrichtung zur Verfügung:

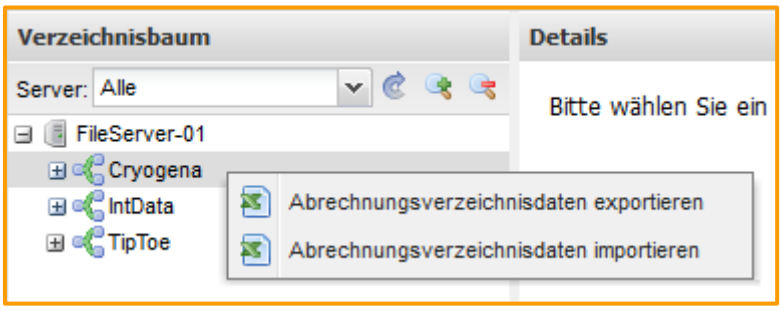
*Verzeichnisart:* Mit dieser Dropdown-Liste bestimmen Sie den Typ des Abrechnungsverzeichnisses.

*Kalkulationsposition:* Wählen Sie aus den verfügbaren Kalkulationspositionen die passende aus.

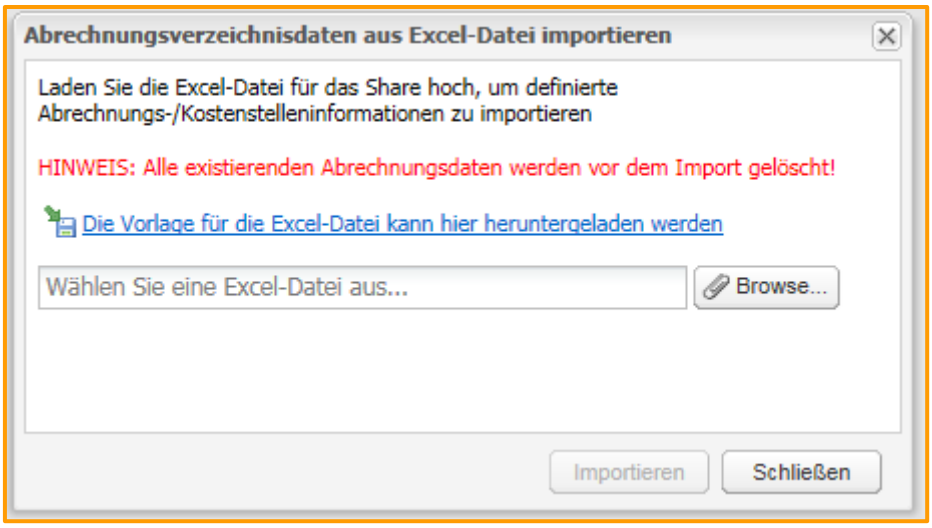
*Zugewiesene Kalkulationspositionen:* Bei der Verzeichnisart *Gruppe* bestimmen Sie in dieser Liste die betroffenen Kostenstellen sowie deren anteilige Kostenübernahme.

Denken Sie daran, die Einstellungen mit dem Button *Speichern* am unteren Ende der Seite zu sichern.

### 9.2.3 Import von Abrechnungsverzeichnisdaten




Über das Kontextmenü eines Shares können Sie eine Excel-Datei importieren, die die Abrechnungsverzeichnisse en bloc für das gesamte Share definiert. Bitte beachten Sie, dass die enthaltenen Informationen über Kostenstellen, Kalkulationspositionen etc. bereits im Access Manager angelegt sein müssen.



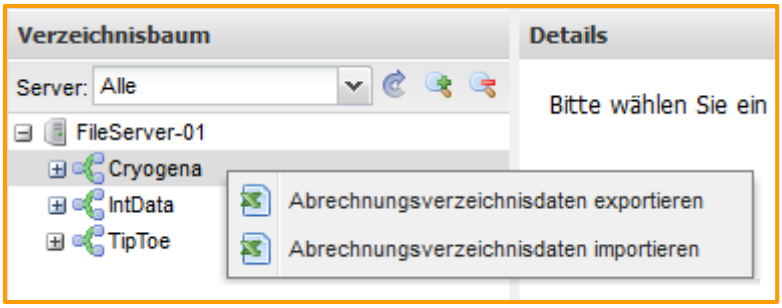

In dem Import-Dialogfenster können Sie eine vorformatierte Excel-Vorlage herunterladen, die bereits alle erforderlichen Datenspalten für eine Eigenerstellung der Inhalte mitbringt. Eine Beschreibung der Datenspalten finden Sie im Kapitel 9.2.5. Mit dem *Browse* Button wählen Sie eine vorhandene Datei aus, welche zunächst inhaltlich validiert wird. Es wird eine Erfolgsmeldung angezeigt und der Button *Importieren* aktiviert, sofern keine Fehler gefunden wurden.

---

*Ein Import ersetzt alle bisherigen Abrechnungsverzeichnisdaten für das gewählte Share. Bestehende Daten werden während des Imports komplett gelöscht und wieder neu erstellt, falls diese in der Import-Datei vorhanden sind.*

---

### 9.2.4 Export von Verzeichnisdaten




Über das Kontextmenü eines Shares können Sie eine Excel-Datei exportieren, die die Abrechnungsverzeichnisse en bloc für das gesamte Share enthält. Die Excel-Datei kann manuell bearbeitet und auf Wunsch wieder importiert werden.

### 9.2.5 Aufbau der Excel-Datei

Die Import-Datei muss eine Excel-Datei (.xlsx, Office 2007 oder neuer) sein, die alle Spalten in der exakten Reihenfolge beinhaltet und den inhaltlichen Anforderungen genügt, um erfolgreich importiert werden zu können. Bei einem Export vorhandener Abrechnungsverzeichnisdaten ist dies bereits sichergestellt.

*Der Name des Tabellenblattes muss „AccountingData“ lauten, damit es beim Import erkannt wird.*

| Spalte A: **FOLDER** | Pflichtfeld: **Ja** |
|---|---|
| **Format** | **Beschreibung** |
| \\Server\Share\Verzeichnis | Die UNC-Pfadangabe des zu importierenden Abrechnungsverzeichnisses, bestehend aus dem Namen des Servers, des Shares sowie des Verzeichnisses. |

| Spalte B: **COSTCENTER1** | Pflichtfeld: **Siehe Beschreibung** |
|---|---|
| **Format** | **Beschreibung** |
| Text | Der Name der ersten Kostenstelle.<br>Erforderlich, wenn die Verzeichnisart *Gruppe* lautet (siehe Spalte V – TYPE_NAME). |

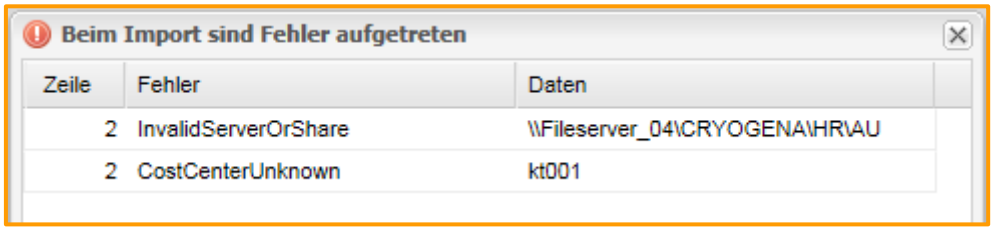
| Spalte C: **PERCENTAGE1** | Pflichtfeld: **Siehe Beschreibung** |
|---|---|
| **Format** | **Beschreibung** |
| Eine ganze Zahl zwischen 1 und 100 | Der Kostenverteilungsschlüssel der Spalte COSTCENTER 1. Die Summe der Verteilungsschlüssel aller gesetzten Kostenstellen muss exakt 100 ergeben.<br>Erforderlich, wenn COSTCENTER1 angegeben wurde. |

| Spalte D-U: **COSTCENTER2-10 & PERCENTAGE2-10** | Pflichtfeld: **Nein** |
|---|---|
| **Format** | **Beschreibung** |
| Wie COSTCENTER1 / PERCENTAGE1 | Wie COSTCENTER1 / PERCENTAGE1<br>Optional, aber PERCENTAGEx muss immer zusammen mit COSTCENTERx angegeben werden. |

| Spalte V: **TYPE_NAME** | Pflichtfeld: **Ja** |
|---|---|
| **Format** | **Beschreibung** |
| Eines der Wörter HOME, GROUP, IGNORE, TOBEDEFINED | Der Ordnertyp des Abrechnungsverzeichnisses. |

| Spalte W: **PRICING ITEM ID** | Pflichtfeld: **Nein** |
|---|---|
| **Format** | **Beschreibung** |
| Text | Die ID der Kalkulationsposition des Abrechnungsverzeichnisses. Sie ist nur gültig in Kombination mit den Ordnertypen HOME, GROUP, IGNORE. Ist die ID nicht gesetzt, wird automatisch der Standardwert für die Kalkulationsposition genommen (Einstellung in den administrativen Grundeinstellungen). |

### 9.2.6 Mögliche Validierungsfehler beim Import




Im Falle einer negativen Überprüfung der Importdatei zeigt ein Fehlerprotokoll die aufgetretenen Probleme mit Zeilennummer, Fehlertyp und den inkorrekten Daten. Die Datei kann in diesem Fall nicht importiert werden, bis die Fehler manuell behoben wurden. Es werden folgende Fehler unterschieden:

| Fehlerart | **InvalidServerOrShare** |
|---|---|
| Beschreibung | Der ausgewählte Server und Share für den Datenimport ist nicht identisch mit dem eingetragenen Server und Share in der Import-Datei. |
| Behebung | Stellen Sie sicher, dass der vollständige UNC-Pfad in der Import-Datei den richtigen Server und Verzeichnisfreigabe entspricht. |

| Fehlerart | **InvalidFolder** |
|---|---|
| Beschreibung | Das angegebene Verzeichnis in der Import-Datei existiert nicht im Dateisystem. |
| Behebung | Erstellen Sie das Verzeichnis und führen Sie den Import erneut durch. |

| Fehlerart | **NestedAccountingFolders** |
|---|---|
| Beschreibung | Eine Verschachtelung von Abrechnungsverzeichnissen wurde erkannt. Beispiel: \\Server\Share\c\d - Verzeichnis c und d sind Abrechnungsverzeichnisse. |
| Behebung | Eine Verschachtelung von Abrechnungsverzeichnissen ist, um Mehrfachberechnungen zu vermeiden, im Access Manager nicht möglich. |

| Fehlerart | **InvalidCostCenterPercentageFormat** |
|---|---|
| Beschreibung | Ein falsches Dezimalzahlformat wurde in einer Prozentsatzspalte erkannt. |
| Behebung | Korrigieren Sie Ihre Eingabe zu einer korrekten Dezimalzahl. |

| Fehlerart | **InvalidCostCenterPercentageSum** |
|---|---|
| Beschreibung | Die Summe aller angegebenen Prozentsätze entspricht nicht 100. |
| Behebung | Korrigieren Sie die einzelnen Prozentsätze, so dass die Summe 100 ergibt. |

| Fehlerart | **SameCostCenterSingleFolder** |
|---|---|
| Beschreibung | Für ein Abrechnungsverzeichnis wurde die gleiche Kostenstelle in derselben Zeile mehrmals angegeben. |
| Behebung | Geben Sie für ein Abrechnungsverzeichnis nur verschiedene Kostenstellen an. |

| Fehlerart | **CostCenterMissing** |
|---|---|
| Beschreibung | Ein Prozentsatz wurde angegeben, aber keine zugehörige Kostenstelle. |
| Behebung | Definierten Sie für jeden angegebenen Prozentsatzwert auch eine entsprechende Kostenstelle. |

| Fehlerart | **CostCenterUnknown** |
|---|---|
| Beschreibung | Die angegebene Kostenstelle ist unbekannt. |
| Behebung | Erstellen Sie zunächst die Kostenstelle im Access Manager und führen Sie den Import erneut durch. |

| Fehlerart | **InvalidCostCenterPercentageValue** |
|---|---|
| Beschreibung | Der Prozentsatzwert einer Kostenstelle liegt außerhalb des gültigen Bereichs. |
| Behebung | Korrigieren Sie den Prozentsatzwert der betreffenden Kostenstelle. |

| Fehlerart | **InvalidPricingItemId** |
|---|---|
| Beschreibung | Eine unbekannte Kalkulationsposition ID wurde angegeben. |
| Behebung | Verwenden Sie eine im Access Manager vorhandene Kalkulationsposition ID. |

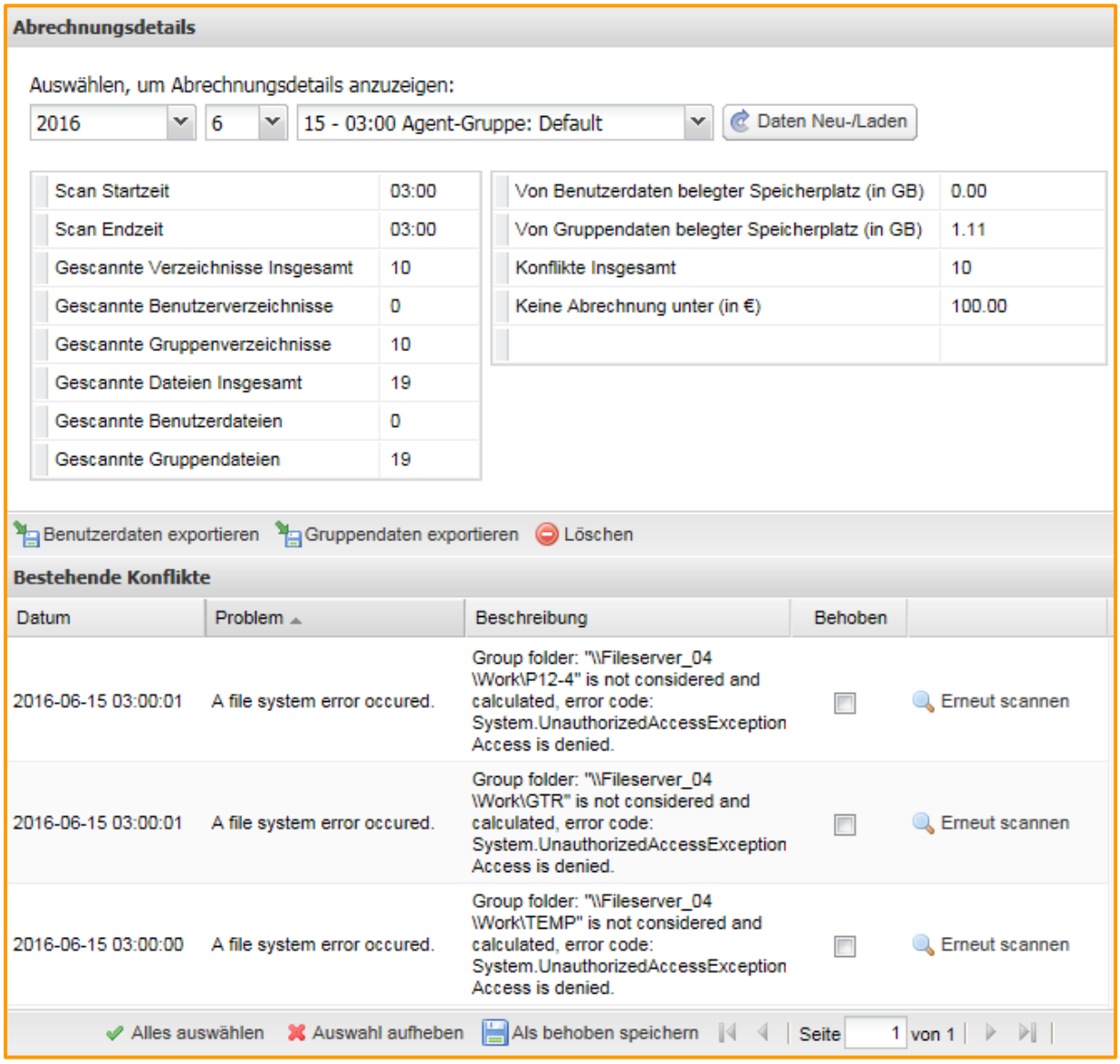
| Fehlerart | **InvalidPricingItemTypeNameCombination** |
|---|---|
| Beschreibung | Die Kombination aus definierter Kalkulationsposition und Abrechnungsverzeichnistyp ist ungültig. |
| Behebung | Kalkulationspositionen können nur dem Abrechnungsverzeichnistypen HOME, GROUP und IGNORE. |

| Fehlerart | **InvalidOrMissingTypeName** |
|---|---|
| Beschreibung | Entweder ist der Typ des Abrechnungsverzeichnisses unbekannt oder es wurde kein Typ angegeben. |
| Behebung | Geben Sie einen der folgenden Abrechnungsverzeichnistypen an: HOME, GROUP, IGNORE, TOBEDEFINED. |

| Fehlerart | **InvalidCostCenterTypeNameCombination** |
|---|---|
| Beschreibung | Die Kombination aus definierter Kostenstelle und Abrechnungsverzeichnisart ist ungültig. |
| Behebung | Kostenstellen können nur für die Abrechnungsverzeichnistypen GROUP und IGNORE zugewiesen werden. |

| Fehlerart | **DuplicateFolder** |
|---|---|
| Beschreibung | Der gleiche Abrechnungsverzeichnisname wurde mehrmals angegeben. |
| Behebung | Die angegebenen Abrechnungsverzeichnisnamen müssen eindeutig sein. |

## 9.3 Abrechnungsdetails einsehen




Die Seite *Daten* gibt eine Übersicht der während eines Abrechnungsdurchlaufs gesammelten Informationen bzw. Fehler und erlaubt den Export dieser Daten in einfache Textdateien.

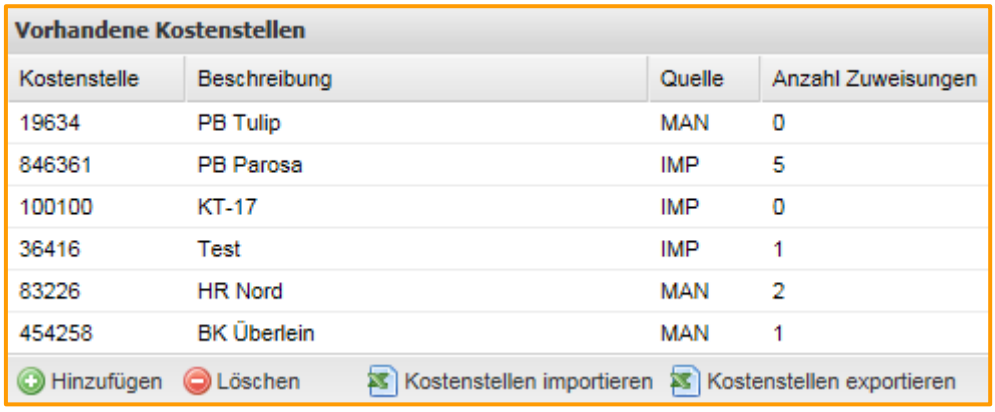
Im Abschnitt *Abrechnungsdetails* im oberen Teil kann ein bestimmter Abrechnungsdurchlauf ausgewählt werden. Da pro Tag mehrere Durchläufe, ggf. auch in verschiedenen Agent-Gruppen, stattgefunden haben können, wählen Sie Jahr, Monat und Tag / Uhrzeit / Agent-Gruppe getrennt aus. Nach dieser Auswahl wird darunter eine Zusammenfassung des gewählten Durchlaufs angezeigt.

Die Buttons *Benutzerdaten exportieren* und *Gruppendaten exportieren* erstellen CSV-formatierte Textdateien, die Abrechnungsdaten für Abrechnungsverzeichnisse vom Typ *Home* (Benutzerdaten) oder *Gruppe* (Gruppendaten) enthalten. Die Inhaltsstruktur der Dateien wird in den administrativen Einstellungen festgelegt. Beim Export werden nur Einträge geschrieben, die tatsächlich abgerechnet werden[6] – dadurch kann es vorkommen, dass eine Exportdatei gar keine oder dem Anschein nach zu wenig Einträge enthält.

Der Abschnitt *Bestehende Konflikte* im unteren Teil listet beim Abrechnungsdurchlauf ermittelte Probleme auf. Wenn Fehler wie z. B. “Keine Kostenstellenzuordnung verfügbar” aufgetreten sind oder ein Share nicht zur Verfügung stand, können Sie die Überprüfung mit dem Button *Erneut scannen* wiederholen. Solange Konflikte bestehen, spiegeln die exportierten Daten nicht die tatsächliche Abrechnungssituation wider.

[6] Dies hängt vom Parameter „NoChargeBelow“ in den administrativen Einstellungen ab.

## 9.4 Kostenstellen konfigurieren




Auf dieser Seite werden die Kostenstellen angezeigt und verwaltet. Die Tabelle zeigt neben der Kostenstellen-ID (Spalte *Kostenstelle*) und ihrer Beschreibung auch den Weg, über den sie in das System gelangt ist (Spalte *Quelle*), sowie einen Zähler, wie oft sie bereits von Abrechnungsverzeichnissen verwendet wird.

Kostenstellen können nicht editiert, sondern nur neu angelegt (Button *Hinzufügen*) oder gelöscht werden (Button *Löschen*), sofern sie manuell ins System gelangt sind (Quelle: *MAN*) und zurzeit nicht zugewiesen sind (*Anzahl Zuweisungen* = 0).

### 9.4.1 Kostenstellen importieren

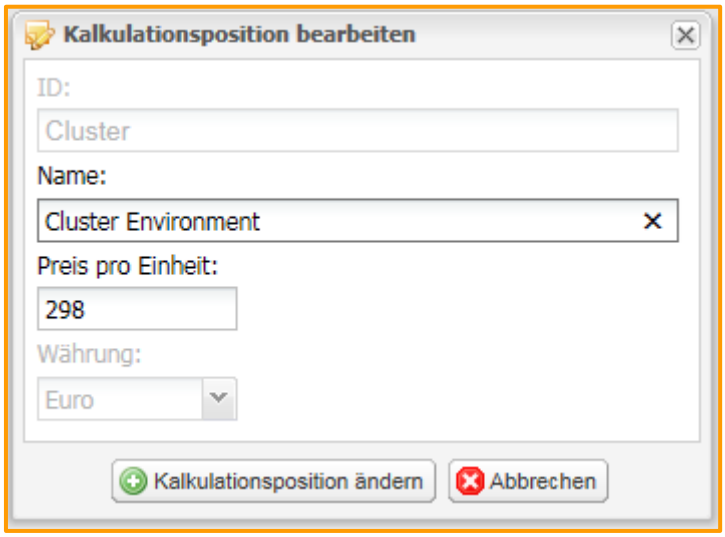
Kostenstellen können – neben dem manuellen Hinzufügen – auf zwei Arten ins System gelangen:

1. Mit dem Button *Kostenstellen importieren* lesen Sie eine Excel-Datei ein, welche aus den beiden Spalten „COSTCENTER“ und „DESCRIPTION“ besteht. Nach Auswahl der gewünschten Datei wird diese zunächst validiert und im Erfolgsfall importiert. Solche Kostenstellen erhalten den Quelleneintrag *MAN*. Bereits im System bestehende Kostenstellen werden anhand ihrer ID identifiziert und ihre Beschreibung wird aktualisiert, falls es sich um eine manuell importierte Kostenstelle (Quelle: *MAN*) handelt. Existierende Kostenstellen aus einem AD-Import (Quelle: *IMP*) bleiben von dem manuellen Import unberührt.
2. Über eine geplante Aufgabe *CostCenterImport* können zyklisch die unternehmensweit bekannten Kostenstellen aus dem Active Directory eingelesen und aktualisiert werden. AD-Verbindungsdaten werden in den administrativen Einstellungen vorgenommen. Solche Kostenstellen tragen als Quelle das Kürzel *IMP* und können nicht manuell gelöscht werden.

## 9.5 Kalkulationspositionen konfigurieren

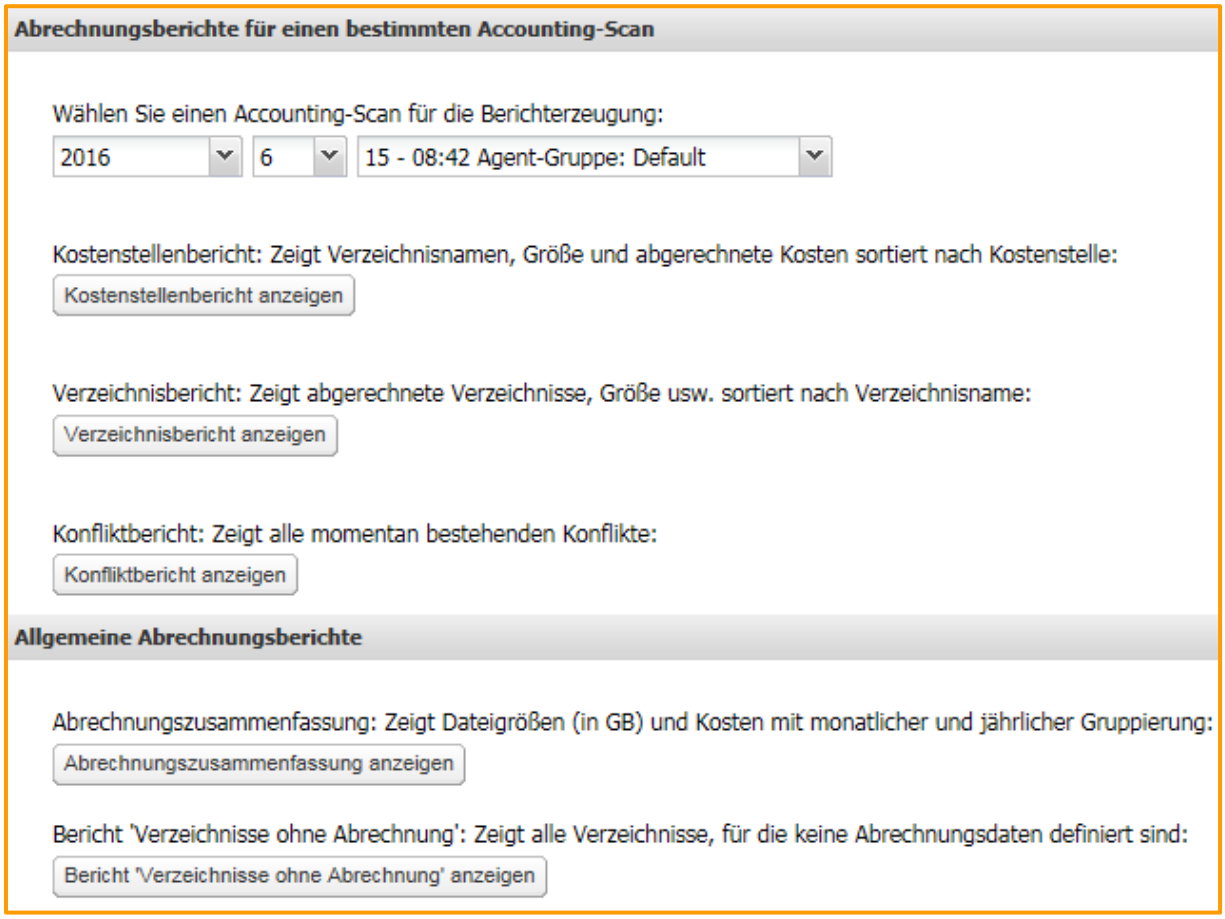

Hier werden die Kalkulationspositionen angezeigt und verwaltet. Die Tabelle zeigt neben der ID einer Position ihrem Namen, den Preis pro Einheit (1 Einheit = 1 GigaByte Speicherplatz) sowie einen Zähler, wie oft sie bereits in Abrechnungsverzeichnissen verwendet wird.

Kalkulationspositionen können nur gelöscht werden, wenn sie zurzeit nicht zugewiesen sind (*Anzahl Zuweisungen* = 0). Das Editieren ist jedoch jederzeit möglich.




Der Bearbeitungsdialog erlaubt die Änderung des Namens sowie des Preises. Die ID darf nicht verändert werden, da über sie die eindeutige Zuordnung realisiert wird.

## 9.6 Abrechnungsberichte




Die Seite *Berichte* ermöglicht es Ihnen, verschiedene Berichte mit unterschiedlichen thematischen Aussagen zu erstellen. Es wird zwischen allgemeinen Berichten und solchen, die auf einem konkreten Abrechnungsdurchlauf basieren, unterschieden. Da pro Tag mehrere Durchläufe, ggf. auch in verschiedenen Agent-Gruppen, stattgefunden haben können, wählen Sie Jahr, Monat und Tag / Uhrzeit / Agent-Gruppe getrennt aus. Nach dieser Auswahl aktivieren sich die Buttons zur Erstellung der durchlaufabhängigen Berichte.

Die jeweiligen Buttons öffnen den Bericht in einem neuen Tab im Browser. Über den Button *Exportieren* laden Sie den Bericht in verschiedenen Formaten herunter. Im Folgenden werden die verfügbaren Berichte erläutert.

### 9.6.1 Kostenstellenbericht

Dieser Bericht listet alle verwendeten Kostenstellen auf und zeigt an, in welchen Abrechnungsverzeichnissen sie mit welchem Kostenanteil involviert sind.

### 9.6.2 Verzeichnisbericht

Dieser Bericht listet alle Abrechnungsverzeichnisse auf und zeigt die involvierten Kostenstellen mit ihren anteiligen Kosten.

### 9.6.3 Konfliktbericht

Dieser Bericht zeigt die während eines Abrechnungsdurchlaufs aufgetretenen Probleme. Es handelt sich um die gleichen Daten, die auf der Seite *Daten* im Abschnitt *Bestehende Konflikte* angezeigt werden.

### 9.6.4 Abrechnungszusammenfassung

Dieser Bericht zeigt eine historisierte Liste der Zahlungsdaten (verbrauchter & abgerechneter Speicher, nominelle & berechnete Gebühr), gruppiert nach Jahr und Monat.

### 9.6.5 Verzeichnisse ohne Abrechnung

Dieser Bericht führt alle Berechtigungsverzeichnisse auf, die nicht zusätzlich als Abrechnungsverzeichnisse definiert sind, also nicht über die Verzeichnisart *Home* oder *Gruppe* verfügen.

## 9.7 Home-Verzeichnis Ausnahmen definieren (Benutzer-Whitelist)

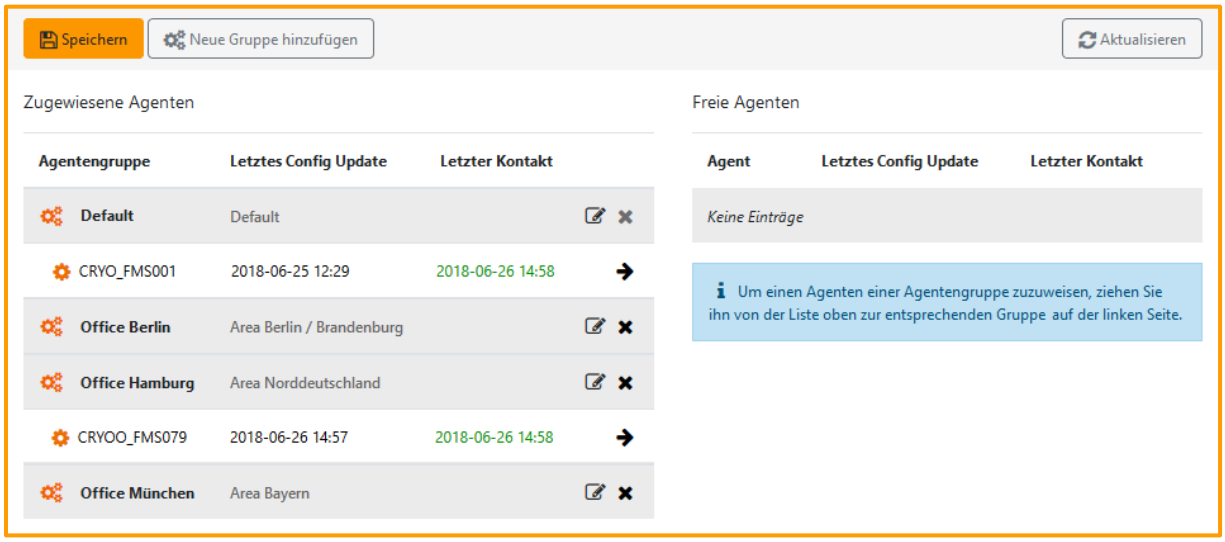

Auf dieser Seite verwalten Sie die Benutzer, die von der Abrechnung der Home-Verzeichnisse ausgenommen werden sollen. Speicherplatz, der von den hier eingetragenen Benutzerkonten im Home-Verzeichnis belegt wird, fließt nicht in die Abrechnung ein. Benutzer können zu dieser Liste jederzeit hinzugefügt und entfernt werden.

# 10 Aufgabenplanung

## 10.1 Arbeitsprinzip: Aufgabenabarbeitung mit Agenten

Im Access Manager werden alle Aufgaben, die außerhalb der eigentlichen Anwendung ausgeführt werden müssen (also z.B. Zugriffe auf das AD, Fileserver, SharePoint Sites und Dritt-Elemente), durch separat auf anderen Maschinen installierte sogenannte *Agenten* erledigt. Mehrere Agenten werden in *Agent-Gruppen* zusammengefasst und übernehmen selbsttätig die Aufteilung vieler Aufgaben untereinander. *Aufgaben* unterscheiden sich nach Typen, etwa für die AD-Synchronisation mit der Access Manager-Datenbank oder die Überprüfung und Korrektur von Berechtigungen auf eine Ressource. Üblicherweise werden Aufgaben einmalig vom Access Manager-Administrator so geplant, dass sie dauerhaft wiederholend ausgeführt werden und damit den reibungslosen Betrieb sicherstellen.

## 10.2 Agent-Gruppen




Auf dieser Seite werden bereits installierte Agenten in Agent-Gruppen zusammengefasst. Eine Gruppe kann beliebig viele Agenten umfassen, aber ein Agent kann nur einer Gruppe angehören. Die hier vorbereiteten Gruppen werden den verwalteten Shares zugewiesen (siehe Kapitel 8.2.1.2), wodurch Sie bestimmen, welche installierten Agenten welchen Server bearbeiten.

Die Agent-Gruppe *Default* existiert immer und muss mindestens einen Agenten enthalten. Nur Agenten dieser Gruppe führen AD-nahe Aufgaben aus (z.B. *AdUserImport*), daher sollte der Agent auf einem Rechner installiert sein, der eine schnelle interne Verbindung zum Active Directory besitzt. Weitere Agent-Gruppen respektive ihre zugehörigen Agenten werden üblicherweise für entfernte Standorte angelegt, um von der dortigen schnellen lokalen Anbindung an die Fileserver zu profitieren.

Die Seite ist in zwei Bereiche unterteilt. Links werden die existierenden Agent-Gruppen mit ihren Agenten aufgelistet. Die rechte Tabelle zeigt die bereits installierten, aber noch keiner Gruppe

zugewiesenen Agenten („Freie Agenten“). Der angezeigte Agent-Name entspricht dem, der bei der Installation des Agenten vergeben wurde und wird standardmäßig automatisch nach dem Schema <DOMAIN>_<RECHNERNAME> zusammengesetzt. Daher kann am Namen abgelesen werden, auf welchem Rechner der Agent installiert wurde.

Jede Agent-Gruppe benötigt einen eindeutigen Namen und eine optionale Beschreibung. Der Name kann nachträglich nicht mehr geändert werden, über das Symbol *Bearbeiten* lässt sich die Beschreibung anpassen.

Unterhalb einer Gruppe werden die zugehörigen Agenten aufgelistet. Die Einträge zeigen den Namen des Agenten, den Zeitpunkt der letzten Aktualisierung der Konfiguration und den Zeitpunkt des letzten Kontakts an. Das Entfernen einer Agent-Gruppe (Symbol *Gruppe löschen* ✖ ) ist nur möglich, wenn die Gruppe weder einen Agenten enthält noch einem Server zugewiesen ist. Die Gruppe *Default* kann nicht gelöscht werden.

Mit dem Button *Neue Gruppe hinzufügen* wird eine neue Agent-Gruppe erstellt. Geben Sie hier Name und Beschreibung der Gruppe ein.

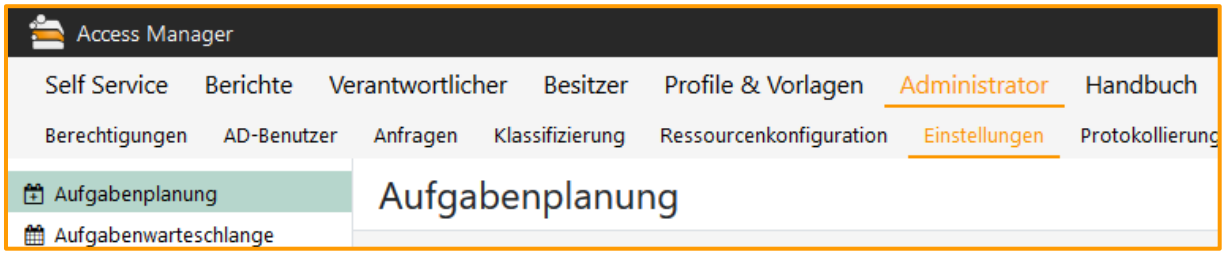
Agenten einer Gruppe werden über den Button *Agenten entfernen* ➔ herausgenommen und erscheinen dadurch wieder in der rechten Tabelle der freien Agenten.

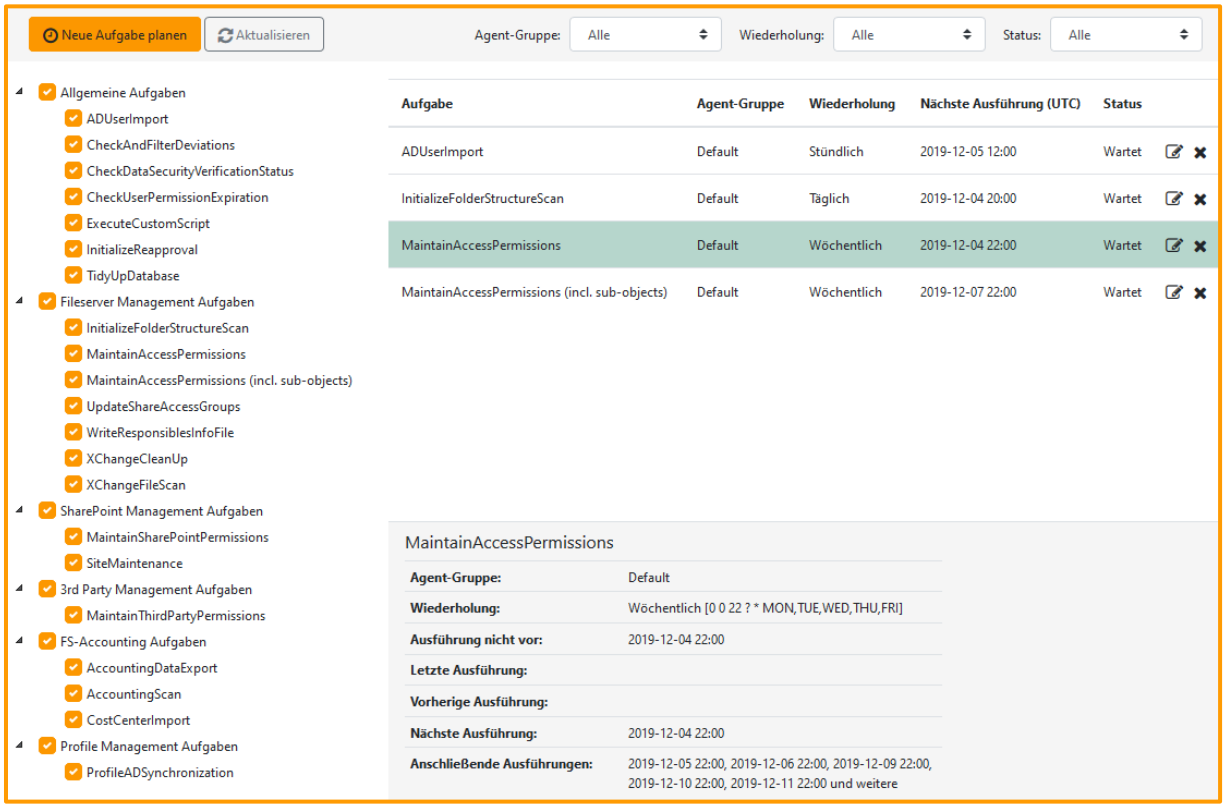
Freie Agenten können einer Gruppe zugewiesen werden, indem sie per Drag & Drop auf den entsprechenden Gruppeneintrag gezogen werden.

Freie Agenten können über das Symbol ✖ gelöscht werden. Diese Funktion dient ausschließlich dazu, nicht mehr auf dem Rechner installierte Agenten aus der AM-Datenbank zu löschen. Noch installierte Agenten, die über diese Funktion gelöscht werden, verbinden sich erneut mit dem Access Manager und werden danach auch automatisch wieder in der Liste freier Agenten aufgeführt.

Alle Änderungen werden erst mit Klick auf *Speichern* wirksam.

# 10.3 Übersicht geplanter Aufgaben



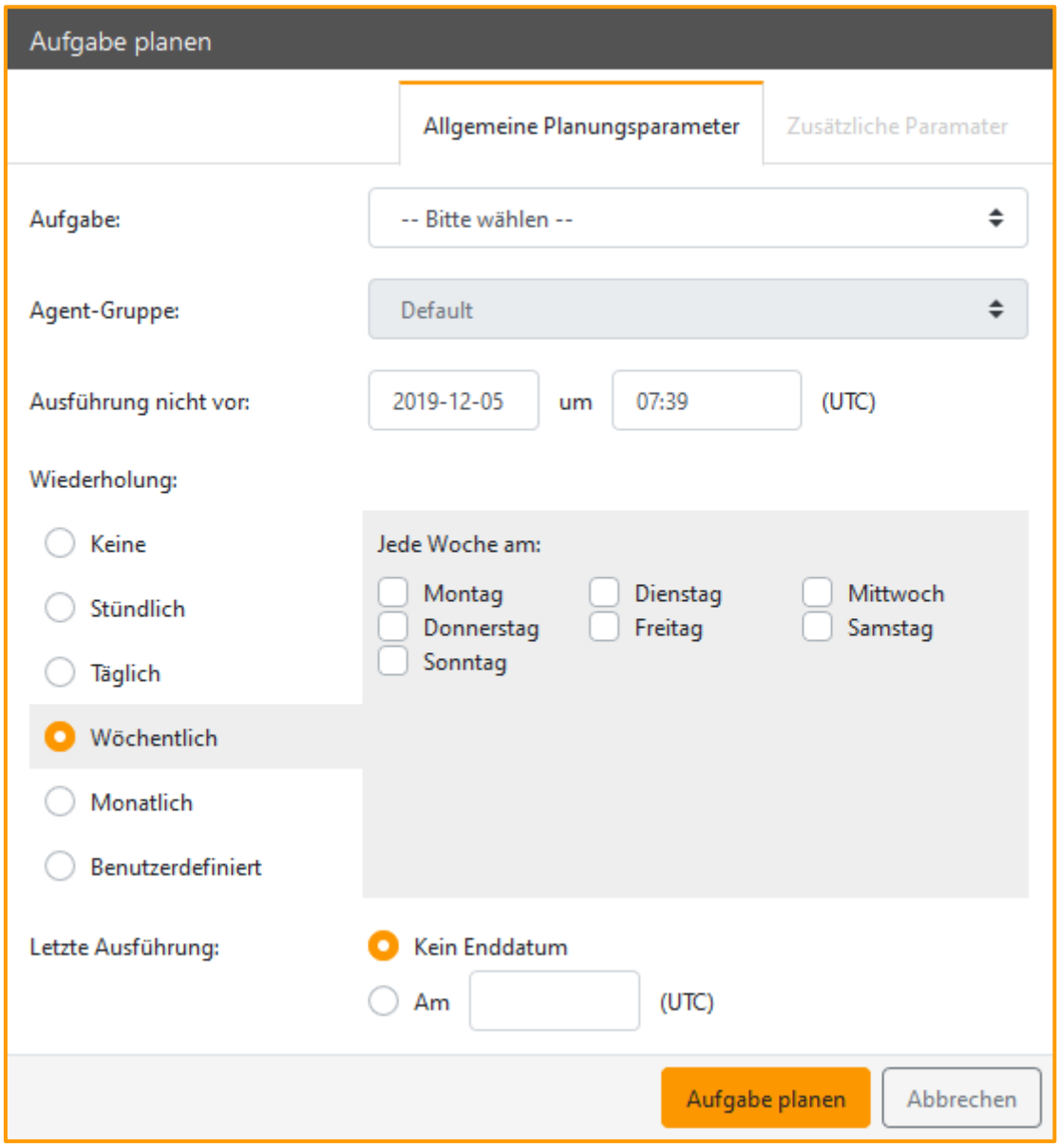




In der *Aufgabenplanung* definieren Sie regelmäßig wiederkehrende Aufgaben für eine Agent-Gruppe. Je nach lizenzierten Modulen werden im linken Bereich die entsprechenden Aufgaben (nach Modul gruppiert) angezeigt und können zur übersichtlicheren Anzeige in der Aufgabenliste an- oder abgewählt werden. Standardmäßig sind alle für den Benutzer verfügbaren Aufgaben ausgewählt.

Die Aufgabenliste rechts zeigt Ihnen die Aufgaben, welche bereits geplant wurden, mit einigen wichtigen Eckdaten an. Diese können anhand der Agentengruppe, des Wiederholungstyps oder ihres Status´ gefiltert werden. Durch die Auswahl einer Aufgabe aus der Liste werden weitere Informationen zu Wiederholungsintervallen, nächster Ausführung etc. im unteren Bereich angezeigt.

## 10.4 Aufgaben planen

Verwenden Sie den Button *Neue Aufgabe planen* oder das Kontextmenü eines Aufgabentyps, öffnet sich im linken Bereich ein Overlay, in welchem Sie die Konfiguration einer neuen Aufgabe vornehmen.




*Aufgabe:* Wählen Sie hier den gewünschten Aufgabentyp aus.

*Agent-Gruppe:* Falls Sie mehrere Agent-Gruppen erstellt haben und der Aufgabentyp es erlaubt, setzen Sie hier die gewünschte Gruppe – dadurch definiert sich auch, welche (File-)Server bearbeitet werden. Falls erforderlich, erstellen Sie die gleiche Aufgabe mehrfach mit der jeweiligen Agent-Gruppe.

*Ausführung nicht vor:* Hier wird automatisch der aktuelle Zeitpunkt eingetragen (Koordinierte Weltzeit, UTC, also nicht Ihre lokale Zeit). Ändern Sie Datum und Uhrzeit ggf. ab, insbesondere, wenn Sie die Aufgabe zyklisch wiederholen lassen wollen.

*Wiederholung:* Wählen Sie hier den gewünschten Wiederholungsrhythmus aus und setzen Sie die jeweils notwendigen Angaben ein.

*Letzte Ausführung:* Optional können Sie die Wiederholungen beschränken, indem Sie ein Datum für die letzte Ausführung der Aufgabe angeben (selten erforderlich).

Sind alle Angaben gemacht, starten Sie die Aufgabe mit dem Button *Aufgabe planen*. Damit wird sie in die Aufgabenliste übernommen und entsprechend ihrer Konfigurationen ausgeführt.

### 10.4.1 Benutzerdefinierte Wiederholung

Wiederholungen werden immer durch cron-Ausdrücke definiert. Sollten die entsprechenden Möglichkeiten für den Wiederholungsrhythmus für Sie nicht passen, können Sie alternativ unter *Benutzerdefiniert* einen eigenen cron-Ausdruck angeben.

Der Aufbau eines cron-Ausdrucks besteht aus sechs Teilen, die jeweils durch ein Leerzeichen getrennt sind und in dieser Reihenfolge folgende Bedeutung haben:

**A B C D E F**

A: Sekunden (wird nicht benutzt und kann immer auf 0 stehen)
B: Minute (0-59)
C: Stunde (0-23)
D: Tag des Monats (1-31)
E: Monat (1-12)
F: Ausführungskommando (wenn nicht benötigt, muss hier ein Fragezeichen als Platzhalter stehen)

Beispiele:

- Jährliche Wiederholung am 1. Februar um 9:05 Uhr:
  **0 5 9 1 2 ?**
- Halbjährliche Wiederholung am 15. März & 15. September um 9:05 Uhr:
  **0 5 9 15 3/6 ?**
  → Die Angabe 3/6 (keine Leerzeichen enthalten!) bedeutet Startmonat (3) mit Wiederholung nach 6 Monaten
- Stündliche Ausführung von Mo-Fr zwischen 7 und 21 Uhr:
  **0 0 7-21 ? * MON-FRI**
- Tägliche Ausführung, alle zwei Stunden zwischen 7:30 und 21:30 Uhr:
  **0 30 7,9,11,13,15,17,19,21 * * ?**

## 10.5 Best Practice: Empfohlene Planungsintervalle für Pflege- und Wartungsaufgaben

Für eine dauerhaft zuverlässige Funktion des gesamten Access Manager-Systems ist eine korrekte und an Ihre individuellen Anforderungen angepasste Planung einiger Aufgaben unerlässlich. Dieses Kapitel gibt einige allgemeingültige Hinweise und beispielhafte Aufgabenplanungen, die Sie bzgl. Ausführungszeitpunkt und Wiederholfrequenz anpassen sollten, um bspw. Aktualisierungslatenzen und Wartungsfenster der IT-Systeme zu berücksichtigen.

### 10.5.1 Obligatorische Aufgaben

Diese Aufgaben sollten Sie in jedem Fall planen – sie sind für die Grundfunktionen zwingend erforderlich, abhängig von Ihren lizenzierten Modulen. Eine Funktionsbeschreibung der Aufgaben finden Sie im folgenden Kapitel 10.6.

#### 10.5.1.1ADUserImport

Um Änderungen an Benutzerkonten und Gruppen im AD möglichst schnell im Access Manager zu reflektieren, sollte die Wiederholung möglichst häufig geschehen, wir empfehlen alle 30-60 Minuten.

Dies ist unproblematisch, da diese Aufgabe auch bei mehreren Tausend Einträgen nur wenige Minuten benötigt.

#### 10.5.1.2TidyUpDatabase

Planen Sie diese Aufgabe am besten einmal täglich. Wir empfehlen zur Lastverteilung ggü. den anderen Aufgaben die frühen Morgenstunden.

#### 10.5.1.3(Fileserver Management) InitializeFolderStructureScan

Planen Sie diese Aufgabe einmal täglich, am besten in den Abendstunden, außerhalb der Bürozeiten. Diese Aufgabe greift lesend auf den Fileserver zu, daher sollte sie nach Möglichkeit außerhalb eines Wartungsfensters des Servers laufen. Bei vielen Berechtigungsverzeichnissen auf einem Server (viele Hundert) kann diese Aufgabe Zeit im Stundenbereich benötigen und den Fileserver belasten, sie sollte daher nicht mit zu hoher Frequenz geplant werden.

*Führen Sie sie auf jeden Fall **vor** einer MaintainAccessPermissions Aufgabe aus.*

#### 10.5.1.4(Fileserver Management) MaintainAccessPermissions

Diese Aufgabe sollte einmal täglich an Werktagen (Mo-Fr) laufen, am besten in den Abendstunden, außerhalb der Bürozeiten. Diese Aufgabe greift lesend & schreibend auf den Fileserver zu, daher sollte sie außerhalb eines Wartungsfensters des Servers laufen. Bei vielen Berechtigungsverzeichnissen auf einem Server (viele Hundert) kann diese Aufgabe Zeit im Stundenbereich benötigen und den Fileserver belasten, sie sollte daher nicht mit zu hoher Frequenz geplant werden.

*Führen Sie sie auf jeden Fall **nach** einer InitializeFolderStructureScan Aufgabe aus.*

#### 10.5.1.5 (Fileserver Management) MaintainAccessPermissions (incl. sub-objects)

Da diese Aufgabe identisch zur zuvor genannten ist, jedoch deutlich mehr Filesystem-Objekte (Unterverzeichnisse und Dateien) bearbeitet, sollte sie komplementär geplant werden, am besten einmal wöchentlich. Da die Bearbeitungszeit je nach Datenmenge und Performanz des Fileservers über 24 Stunden betragen kann, empfehlen wir einen Start am Freitagabend / Samstagmorgen.

*Führen Sie sie auf jeden Fall **nach** einer InitializeFolderStructureScan Aufgabe aus.*

#### 10.5.1.6 (SharePoint Management) SiteMaintenance

Planen Sie diese Aufgabe einmal täglich, am besten in den Abendstunden, außerhalb der Bürozeiten. Diese Aufgabe greift lesend auf den SharePoint Server zu, daher sollte sie nach Möglichkeit außerhalb eines Wartungsfensters des Servers laufen.

*Führen Sie sie auf jeden Fall **vor** einer MaintainSharePointPermissions Aufgabe aus.*

#### 10.5.1.7 (SharePoint Management) MaintainSharePointPermissions

Diese Aufgabe sollte einmal täglich laufen, am besten in den Abendstunden, außerhalb der Bürozeiten. Diese Aufgabe greift lesend & schreibend auf den SharePoint Server zu, daher sollte sie außerhalb eines Wartungsfensters des Servers laufen.

*Führen Sie sie auf jeden Fall **nach** einer SiteMaintenance Aufgabe aus.*

#### 10.5.1.8 (3rd Party Management) MaintainThirdPartyPermissions

Es ist ausreichend, diese Aufgabe einmal täglich auszuführen. Da hierbei lediglich lesend und schreibend auf das AD zugegriffen wird, ist die Ausführungsdauer üblicherweise recht kurz (Sekunden bis wenige Minuten) und die Aufgabe kann bei Bedarf auch häufiger ausgeführt werden.

#### 10.5.1.9 (Fileserver Accounting) AccountingScan

Planen Sie diese Aufgabe einmal täglich, am besten in den Abendstunden, außerhalb der Bürozeiten. Diese Aufgabe greift lesend auf den Fileserver zu, daher sollte sie nach Möglichkeit außerhalb eines Wartungsfensters des Servers laufen.

### 10.5.2 Empfohlene Aufgaben

Die folgenden Aufgaben sind nicht in jedem Fall notwendig, sollten aber zumindest prophylaktisch angelegt werden, da sie für bestimmte optionale Funktionen benötigt werden. Werden die Funktionen nicht verwendet, werden die Aufgaben zwar trotzdem ausgeführt jedoch gleich wieder beendet und belasten daher das System nicht.

#### 10.5.2.1 CheckUserPermissionExpiration

Planen Sie diese Aufgabe am besten einmal täglich. Wir empfehlen die frühen Morgenstunden vor den Bürozeiten, damit die Anwender die Nachricht mit der korrekten Tagesdauer direkt zum Arbeitsbeginn vorliegen haben.

#### 10.5.2.2ProfileADSynchronization

Um Änderungen an Benutzerkonten und Gruppen im AD möglichst schnell im Access Manager zu reflektieren, sollte die Wiederholung möglichst häufig geschehen, wir empfehlen alle 30-60 Minuten.

Dies ist unproblematisch, da diese Aufgabe auch bei mehreren Tausend Einträgen nur wenige Minuten benötigt.

#### 10.5.2.3(Fileserver Management) UpdateShareAccessGroups

Um Änderungen an den Berechtigungen im Access Manager möglichst schnell in der Share-Zugriffsgruppe im AD zu reflektieren, sollte die Wiederholung möglichst häufig geschehen, wir empfehlen alle 30-60 Minuten.

#### 10.5.2.4(Fileserver Management) XChangeFileScan

Planen Sie diese Aufgabe einmal täglich, am besten in den Abendstunden, außerhalb der Bürozeiten. Diese Aufgabe greift lesend auf den Fileserver zu, daher sollte sie nach Möglichkeit außerhalb eines Wartungsfensters des Servers laufen. Je nach Datenmenge in den CleanUp-Verzeichnissen kann die Ausführung einige Zeit dauern; planen Sie daher für die Bearbeitung genügend Zeit ein, d.h. die Folge-Aufgabe sollte mindestens zwei Stunden später beginnen.

*Führen Sie sie auf jeden Fall **vor** einer XChangeCleanUp Aufgabe aus.*

#### 10.5.2.5(Fileserver Management) XChangeCleanUp

Planen Sie diese Aufgabe einmal täglich, am besten in den Abendstunden, außerhalb der Bürozeiten. Diese Aufgabe greift lesend und schreibend auf den Fileserver zu, daher sollte sie außerhalb eines Wartungsfensters des Servers laufen.

*Führen Sie sie auf jeden Fall **nach** einer XChangeFileScan Aufgabe aus.*

## 10.6 Verfügbare Aufgabentypen

Die verschiedenen Aufgabentypen sind gruppiert nach Modulen bzw. Zuständigkeiten. Je nach Lizenz sind daher nicht alle Aufgaben für Sie sichtbar.

### 10.6.1 Allgemeine Aufgaben

#### 10.6.1.1 ADGroupImport

Importiert die AD-Gruppen in die AM-Datenbank und aktualisiert ggf. bereits vorhandene und geänderte Einträge.

#### 10.6.1.2 ADUserImport

Importiert die AD-Benutzer in die AM-Datenbank und aktualisiert ggf. bereits vorhandene und geänderte Einträge. Führt danach automatisch die Aufgabe ADGroupImport (siehe oben) aus sowie CheckPermittedButUnauthorizedUsers (siehe unten).

#### 10.6.1.3 CheckAndFilterDeviations

Sendet E-Mails mit Listen von Abweichungen von Berechtigungen zwischen dem Dateisystem und der AM-Konfiguration an AM-Administratoren, Besitzer, Verantwortliche sowie deren Vertretungen. Es werden nur Abweichungen berücksichtigt, die seit der letzten Ausführung der Aufgabe aufgetreten sind.

#### 10.6.1.4 CheckDataSecurityVerificationStatus

Mit dieser Aufgabe werden den Klassifizierungsadministratoren Info-Mails geschickt mit allen klassifizierten Ressourcen, welche keinen überprüften und bestätigten Status haben. Eine Mail enthält die 100 ersten gefundenen Ressourcen, deren Status sich seit dem letzten Prüfungslauf geändert hat.

#### 10.6.1.5 CheckPermittedButUnauthorizedUsers

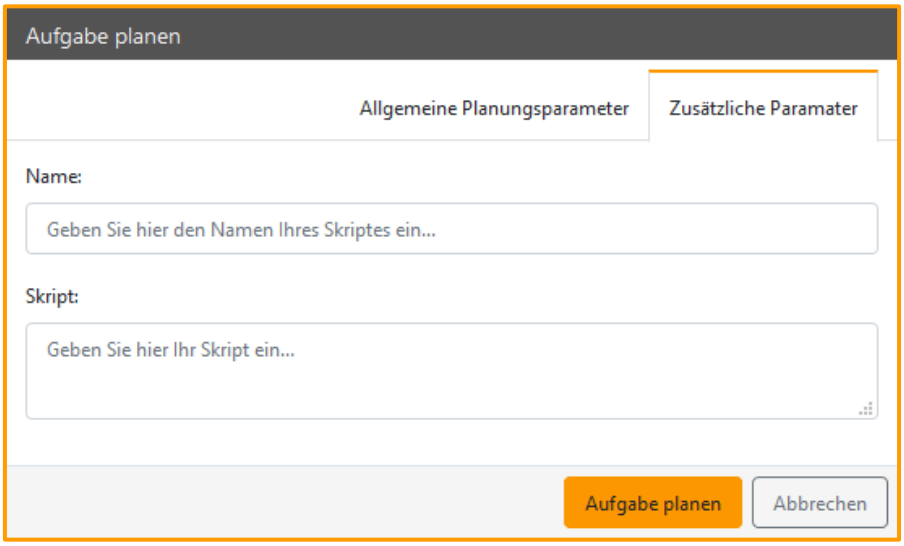
Erstellt eine Auswertung, ob ein Benutzer auf einer Ressource berechtigt wurde, für die er per Klassifizierung nicht autorisiert ist. Über zwei administrative Optionen kann eingestellt werden, ob Administratoren und / oder Verantwortliche per E-Mail benachrichtigt werden sollen (siehe Kapitel 12.7.1.12 und 12.7.1.14).

#### 10.6.1.6 CheckUserPermissionExpiration

Benachrichtigt Benutzer per E-Mail, deren Zugriffsberechtigung auf eine bestimmte Ressource (Verzeichnis, Element, …) innerhalb eines konfigurierbaren Zeitraums abläuft.

#### 10.6.1.7ExecuteCustomScript

Diese Aufgabe führt ein benutzereigenes PowerShell-Skript aus. Dieses wird auf dem Tab *Zusätzliche Parameter* eingegeben:




*Name*: Vergeben Sie einen optionalen Namen für die auszuführende Aufgabe. Diese wird später in der Warteschlange angezeigt. Hierbei handelt es sich *nicht* um den Namen der Skript-Datei.

*Skript*: In diesem Textfeld tragen Sie das auszuführende PowerShell-Skript ein. Dabei kann es sich um den kompletten Quelltext handeln oder um den Aufruf einer Skriptdatei. Bitte beachten Sie die technischen Hinweise in Kapitel 12.2.

#### 10.6.1.8InitializeReapproval

Stößt einen neuen Reapproval-Lauf an. Durch die zeitliche Planung dieser Aufgabe werden die Reapproval-Intervalle festgelegt, während die Dauer eines Laufs sowie die Intervalle für die Erinnerungsmails in den Administrationseinstellungen konfiguriert werden. Dadurch werden automatisch weitere Aufgaben vom Access Manager geplant (ReapprovalReminder, FinishReapproval).

#### 10.6.1.9TidyUpDatabase

Zum Ablaufdatum werden zeitlich begrenzte Berechtigungen aus dem Dateisystem entfernt, die Informationen bleiben jedoch weiterhin in der Datenbank als Einträge bestehen. Diese Aufgabe bereinigt besagte Einträge und ebenso für Vertreterrollen. Diese werden nach Ablauf so lange in der AM-Datenbank – und in der Oberfläche mit Ablaufdatum sichtbar – vorgehalten, bis sie durch den jeweils nächsten Job-Lauf entfernt werden. Zusätzlich löst der Job nach Ablauf einer Vertreterrolle eine entsprechende Info-Mail an den jeweiligen Vertreter aus.

Weiterhin entfernt die Aufgabe Berechtigungen von Benutzerkonten, die nicht mehr im AD gefunden werden, sofern die entsprechende Option aktiviert wurde (siehe Kapitel 12.7.1.6). Es empfiehlt sich deshalb, den Job täglich zu planen.

## 10.6.2 Fileserver Management Aufgaben

### 10.6.2.1 InitializeFolderStructureScan

Synchronisiert die Verzeichnisstruktur in der AM-Datenbank mit der im Dateisystem. Dazu werden mehrere Kind-Aufgaben erstellt, die parallele Verzeichnisstrukturen gleichzeitig prüfen. Darüber hinaus werden diese Aufgaben ggf. in der jeweiligen Agent-Gruppe erstellt, die einem Fileserver zugeordnet ist. Zusätzlich entfernt die Aufgabe abgelaufene Besitzer- und Verantwortlichen-Vertretungen.

### 10.6.2.2 MaintainAccessPermissions

Setzt die Zugriffsberechtigungen der Berechtigungsverzeichnisse im Dateisystem entsprechend der im Access Manager vorgenommenen Einstellungen. Hierbei werden auch ggf. zusätzlich im Dateisystem existierende Rechte entfernt bzw. fehlende hinzugefügt. Solche Abweichungen werden in der AM-Datenbank protokolliert.

### 10.6.2.3 MaintainAccessPermissions (incl. sub-objects)

Setzt die Zugriffsberechtigungen der Berechtigungsverzeichnisse im Dateisystem entsprechend der im Access Manager vorgenommenen Einstellungen und überschreibt zusätzlich die Zugriffsberechtigungen aller in Berechtigungsverzeichnissen enthaltenen Verzeichnisse und Dateien. Hierbei werden auch ggf. zusätzlich im Dateisystem existierende Rechte entfernt bzw. fehlende hinzugefügt. Solche Abweichungen werden in der AM-Datenbank protokolliert.

### 10.6.2.4 UpdateShareAccessGroups

Stellt sicher, dass die AD-Gruppen für den Share-Zugriff vorhanden sind und die richtigen Mitglieder haben. Alle Benutzerkonten, die mindestens eine Zugriffsberechtigung auf dem betreffenden Share haben, werden die zugehörige Share-Zugriffsgruppe geschrieben.

### 10.6.2.5 WriteResponsiblesInfoFile

Legt die Admin-Info-Datei eines Berechtigungsverzeichnisses an bzw. aktualisiert sie. Diese Datei beinhaltet Informationen über die Verantwortlichen der entsprechenden Verzeichnisse.

### 10.6.2.6 XChangeCleanUp

Löscht veraltete Dateien und Verzeichnisse in Cleanup-Verzeichnissen basierend auf den in der *XChangeFileScan* Aufgabe gesammelten Informationen.

### 10.6.2.7 XChangeFileScan

Liest das Datum der letzten Verwendung aller Dateien in Cleanup-Verzeichnissen aus und bestimmt, welche Dateien und Verzeichnisse zu löschen sind. Diese Informationen werden in der *XChangeCleanUp* Aufgabe verwendet. Die Altersbestimmung der zu löschenden Objekte beginnt mit dem ersten Scan, d.h. an diesem Datum startet der Tageszähler mit Null. Eine Bereinigung findet also frühestens nach dem zweiten Scan durch diesen Job statt, wenn das definierte Alter überschritten sein sollte.

### 10.6.3 SharePoint Management Aufgaben

#### 10.6.3.1 MaintainSharePointPermissions

Setzt die Zugriffsberechtigungen der Berechtigungssite in SharePoint entsprechend der im Access Manager vorgenommenen Einstellungen. Hierbei werden auch ggf. zusätzlich in SharePoint existierende Rechte entfernt bzw. fehlende hinzugefügt. Solche Abweichungen werden in der AM-Datenbank protokolliert.

#### 10.6.3.2 SiteMaintenance

Synchronisiert die Sitestruktur in der AM-Datenbank mit der in SharePoint und informiert ggf. Besitzer über das Fehlen von Verantwortlichen.

### 10.6.4 3rd Party Management Aufgaben

#### 10.6.4.1 MaintainThirdPartyPermissions

Analog zur Aufgabe *MaintainAccessPermissions* (siehe Kapitel 10.6.2.2) überprüft und korrigiert diese Aufgabe die Mitgliedschaften der angegebenen Benutzer für Dritt-Elemente.

### 10.6.5 FS-Accounting Aufgaben

#### 10.6.5.1 AccountingDataExport

Exportiert die ermittelten Daten des letzten Abrechnungsdurchlaufs der ausgewählten Agent-Gruppe in das Verzeichnis, das in den administrativen Einstellungen des Accounting-Moduls festgelegt wurde.

#### 10.6.5.2 AccountingScan

Startet den Abrechnungsdurchlauf aller definierten Abrechnungsverzeichnisse für die ausgewählte Agent-Gruppe. Jede Verzeichnisgröße wird aus dem zugewiesenen Benutzer oder Kostenstelle(n) berechnet.

#### 10.6.5.3 CostCenterImport

Importiert Kostenstellen, die im AD hinterlegt sind. Der genaue Ablageort wird in den administrativen Einstellungen des Accounting-Moduls eingestellt. Kostenstellen, die über diese Aufgabe importiert wurden, erhalten den Vermerk *IMP*, im Gegensatz zu manuell erstellten oder über einen manuell angestoßenen Excel-Import (Vermerk *MAN*) erzeugte Kostenstellen.

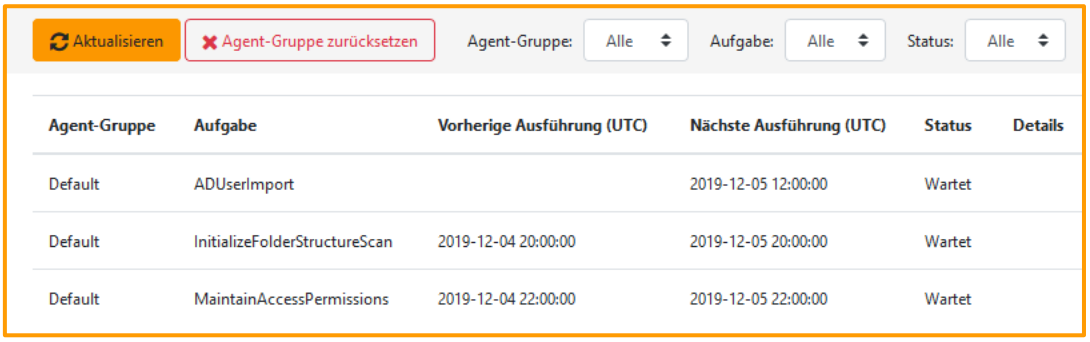
## 10.6.6 Profil Management Aufgaben

### 10.6.6.1 ProfileADSynchronization

Wurde im Profilmanagement einem Benutzerprofil statt der Mitgliederverwaltung durch Profilverantwortliche eine AD-Benutzergruppe zugewiesen, liest diese Aufgabe die enthaltenen Benutzerkonten aus (verschachtelte Mitgliedsgruppen werden – bis auf vordefinierte Windows-Gruppen – bis hinunter zur Benutzerkontenebene ebenfalls aufgelöst) und trägt diese als Mitglieder des Profils ein. Benutzerkonten, die im letzten Durchlauf noch in der AD-Gruppe enthalten waren, inzwischen aber entfernt wurden, verlieren ihre Zugriffsrechte.

Hat der Access Manager auf ein Konto / eine Gruppe innerhalb der zu synchronisierenden Gruppe keinen Zugriff (bspw. wegen falsch gesetzter Rechte im AD oder einer externen Gruppe in einer anderen Domäne, für die kein Trust besteht), werden diese Konten nicht übernommen.

## 10.7 Aktuelle Aufgabenwarteschlange einsehen




| Agent-Gruppe | Aufgabe | Vorherige Ausführung (UTC) | Nächste Ausführung (UTC) | Status | Details |
|---|---|---|---|---|---|
| Default | ADUserImport | | 2019-12-05 12:00:00 | Wartet | |
| Default | InitializeFolderStructureScan | 2019-12-04 20:00:00 | 2019-12-05 20:00:00 | Wartet | |
| Default | MaintainAccessPermissions | 2019-12-04 22:00:00 | 2019-12-05 22:00:00 | Wartet | |

Die Seite *Aufgaben-Warteschlange* bietet Ihnen einen Überblick über alle laufenden und geplanten Aufgaben. Hier werden auch Aufgaben angezeigt, die nicht manuell von Ihnen, sondern automatisch vom Access Manager erstellt wurden.

*Agent-Gruppe*: Hier steht die Gruppe, innerhalb welcher die Aufgabe ausgeführt wird. Damit werden nur die Server bearbeitet, denen diese Agent-Gruppe zugeordnet wurde (siehe auch Kapitel 10.2).

*Aufgabe*: Zeigt den Aufgabentyp an. Hier können neben den manuell planbaren Aufgaben (siehe Kapitel 10.5 und 10.4) auch weitere erscheinen (z.B. *RemoveDirectAcl*, *MaintainADPermission*), die vom System automatisch angelegt wurden sowie Aufgaben für den Berichtversand (*SendReports*, siehe Kapitel 5.3).

*Vorherige Ausführungszeit (UTC), Nächste Ausführungszeit (UTC)*: Geben Auskunft über den zuletzt durchgeführten und den nächsten geplanten Durchlauf. Bitte beachten Sie, dass alle Uhrzeiten immer in Koordinierter Weltzeit (UTC) angezeigt werden und damit nicht Ihrer lokalen Zeitzone entsprechen.

*Status*: Der aktuelle Zustand, in dem sich die Aufgabe befindet, kann einen von drei Werten enthalten: „Wartet“, „Läuft“ oder „Blockiert“. Der Status „blockiert“ wird erreicht, wenn mehrere Aufgaben desselben Typs innerhalb derselben Agent-Gruppe ausgeführt werden sollen und zusätzlich eine gleichzeitige Ausführung nicht möglich ist (z.B. weil zwei Rechte-Überprüfungen dasselbe Verzeichnis bearbeiten sollen). Die blockierte Aufgabe wird nach der Beendigung der aktuell laufenden ausgeführt.

Die Anzeige der Aufgabeninformationen wird nicht automatisch aktualisiert. Um Veränderungen im Status der Aufgaben zu sehen, verwenden Sie den Button *Aktualisieren*. Mit den DropDown-Filterlisten schränken Sie die angezeigten Aufgaben nach verschiedenen Kriterien ein (Agent-Gruppe, Aufgabentyp, Status).

Mit dem Button *Agent-Gruppe zurücksetzen* entfernen Sie alle Aufgaben für eine auszuwählende Agent-Gruppe, die nicht wiederholend geplant sind oder sich im Fehler-Zustand befinden.

---

*Der Reset einer Agent-Gruppe stoppt alle aktuell laufenden Aufgaben, was Einfluss auf den laufenden Betrieb des Systems haben kann und sollte daher nur in Ausnahmefällen durchgeführt werden.*

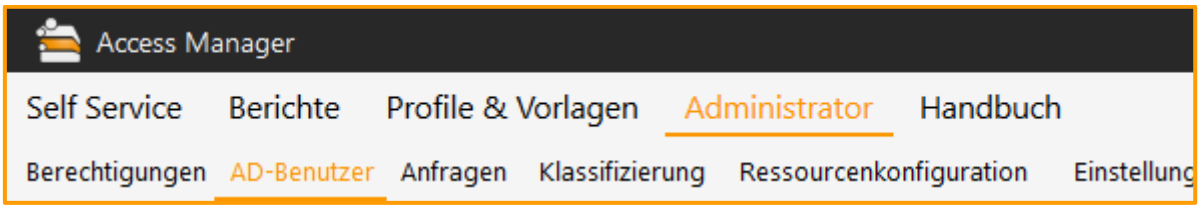
---

# 11 Benutzerverwaltung

## 11.1 Arbeitsprinzip: AD-User Provisioning

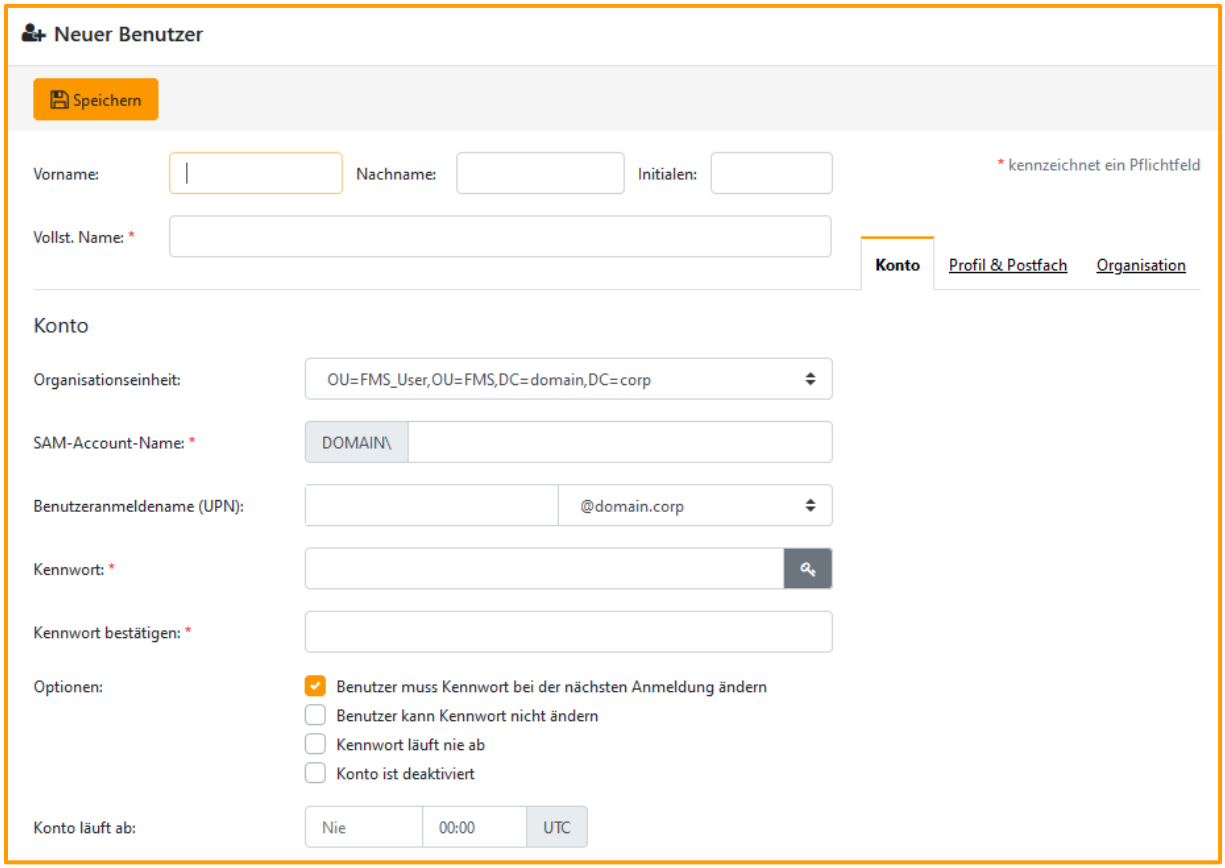
Der Access Manager stellt Ihnen als AM-Administrator Funktionen zur Verfügung, um ohne eigenen Zugriff auf das Active Directory neue Benutzerkonten anzulegen, bestehende zu verwalten und zu deaktivieren. Neben dem Vorteil des zentralen Zugangs zu vielen Belangen der Benutzerkontenverwaltung lässt sich so ein erhöhter Zugriffsschutz auf Ihr AD etablieren, da ggf. weniger Personen die entsprechenden Rechte direkt im AD erhalten müssen: das Access Manager User Provisioning erfolgt nur im Auftrag eines AM-Administrators, jedoch unter Nutzung das AM-eigenen Kontos. Darüber hinaus werden solche Aktionen ebenfalls protokolliert und lassen sich im Audit (Kapitel 12.8) nachvollziehen.

Zur Benutzerverwaltung wechseln Sie als *Administrator* auf die Seite *AD-Benutzer*:



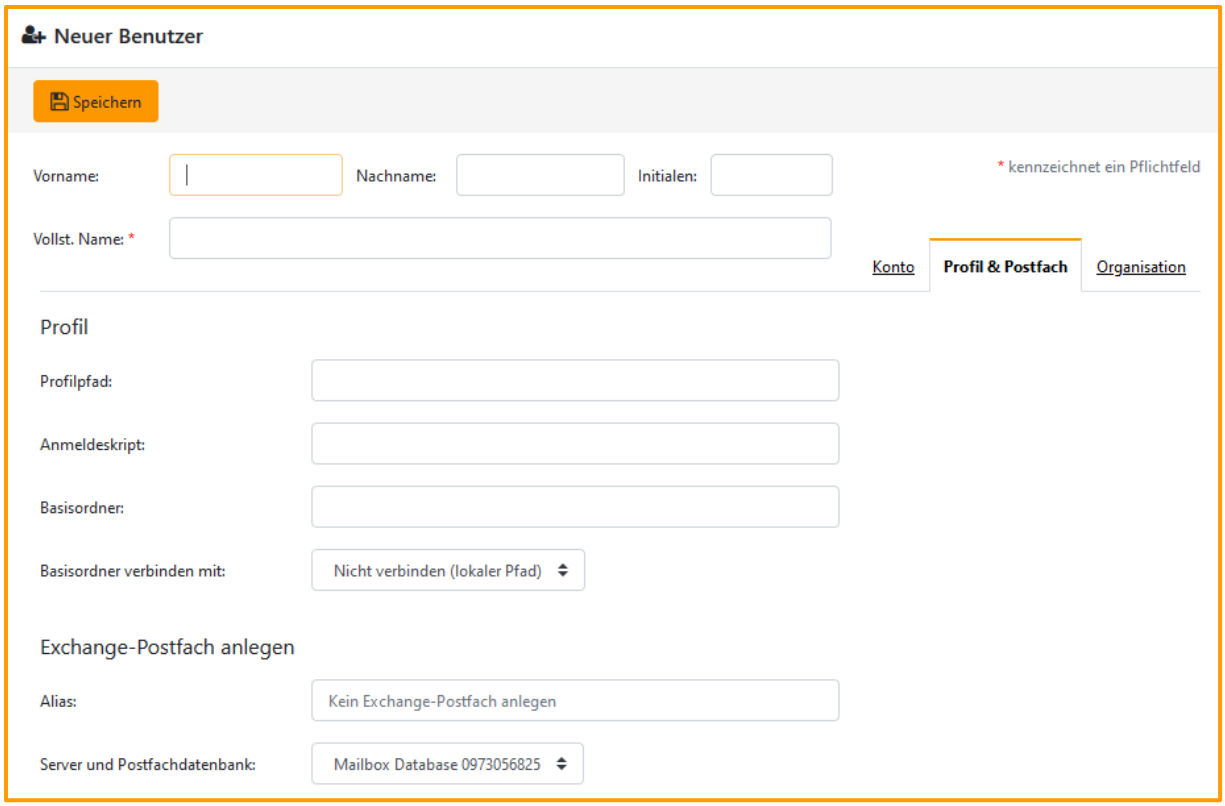
## 11.2 AD-Benutzer anlegen

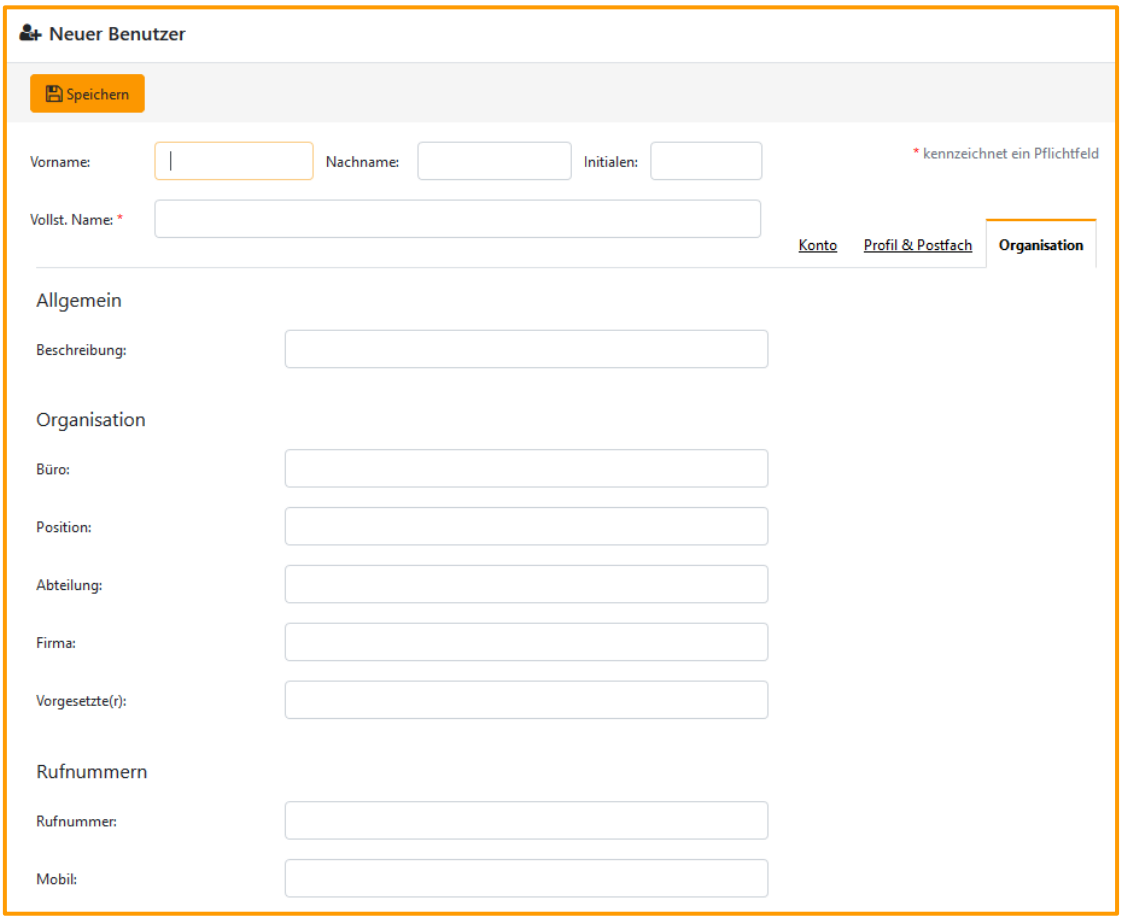
Über den Button *Neuer Benutzer* können Sie direkt im Access Manager ein neues Benutzerkonto im AD erstellen, inklusive der Erstellung eines Exchange-Postfachs. Der Button mit dem Uhr-Symbol startet sofort eine AD-User Import Aufgabe, um den Access Manager mit dem AD abzugleichen. Diese Möglichkeiten stehen nur zur Verfügung, wenn in den administrativen Einstellungen die entsprechenden Optionen korrekt konfiguriert wurden.




Abhängig von den administrativen Vorgaben stehen Ihnen eine oder mehrere Organisationseinheiten zur Auswahl, in denen das neue Benutzerkonto erstellt werden kann. Die zur Verfügung stehenden UPN-Suffixe folgen ebenfalls den administrativen Einstellungen. Über die Kennwort-Optionen können Sie ein Passwort vergeben. Dies kann entweder durch manuelle Eingabe geschehen oder automatisch über das Schlüsselsymbol, wobei die Access Manager- und AD-Kennwortrichtlinien zu berücksichtigen sind. Wird das Passwort vom AM erzeugt, erscheint es nur einmalig im Klartext innerhalb eines Popup-Fensters und muss jetzt notiert werden. Ein späteres Nachschauen ist aus Sicherheitsgründen nicht möglich. Die Aktion der Passwortänderung erscheint außerdem im Audit.

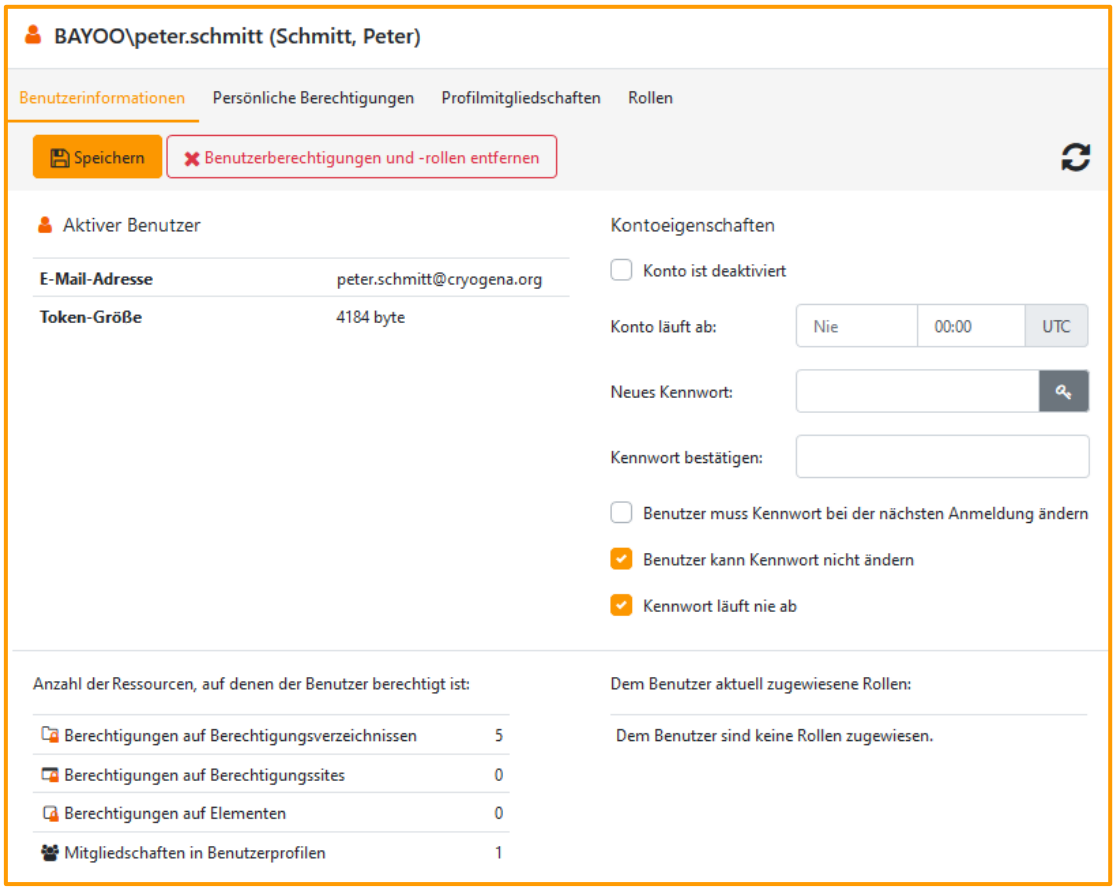
Die Kennwortoptionen, Angaben zum Benutzerprofil, sowie die im Tab „Organisation“ mitzugebenden Attribute entsprechen den aus dem AD bekannten Eigenschaften eines Benutzerkontos und befüllen diese. Weiterhin gibt es die Möglichkeit, für den Benutzer ein Exchange Postfach anzulegen. Der Reiter „Profil“ ändert dann seinen Namen in „Profil & Postfach“.


Neuer Benutzer
Speichern
Vorname:
Nachname:
Initialen:
* kennzeichnet ein Pflichtfeld
Vollst. Name: *
Konto
Profil & Postfach
Organisation
Profil
Profilpfad:
Anmeldeskript:
Basisordner:
Basisordner verbinden mit:
Nicht verbinden (lokaler Pfad)
Exchange-Postfach anlegen
Alias:
Kein Exchange-Postfach anlegen
Server und Postfachdatenbank:
Mailbox Database 0973056825


Neuer Benutzer
Speichern
Vorname:
Nachname:
Initialen:
* kennzeichnet ein Pflichtfeld
Vollst. Name: *
Konto
Profil & Postfach
Organisation
Allgemein
Beschreibung:
Organisation
Büro:
Position:
Abteilung:
Firma:
Vorgesetzte(r):
Rufnummern
Rufnummer:
Mobil:

## 11.3 Benutzerinformationen

Sie können jedes im Access Manager bekannte Benutzerkonto in der Benutzerliste links auswählen. Rechts erhalten Sie viele Informationen zu diesem Konto, fachlich unterteilt in mehreren Tabs. Standardmäßig wird das Tab *Benutzerinformationen* geöffnet:



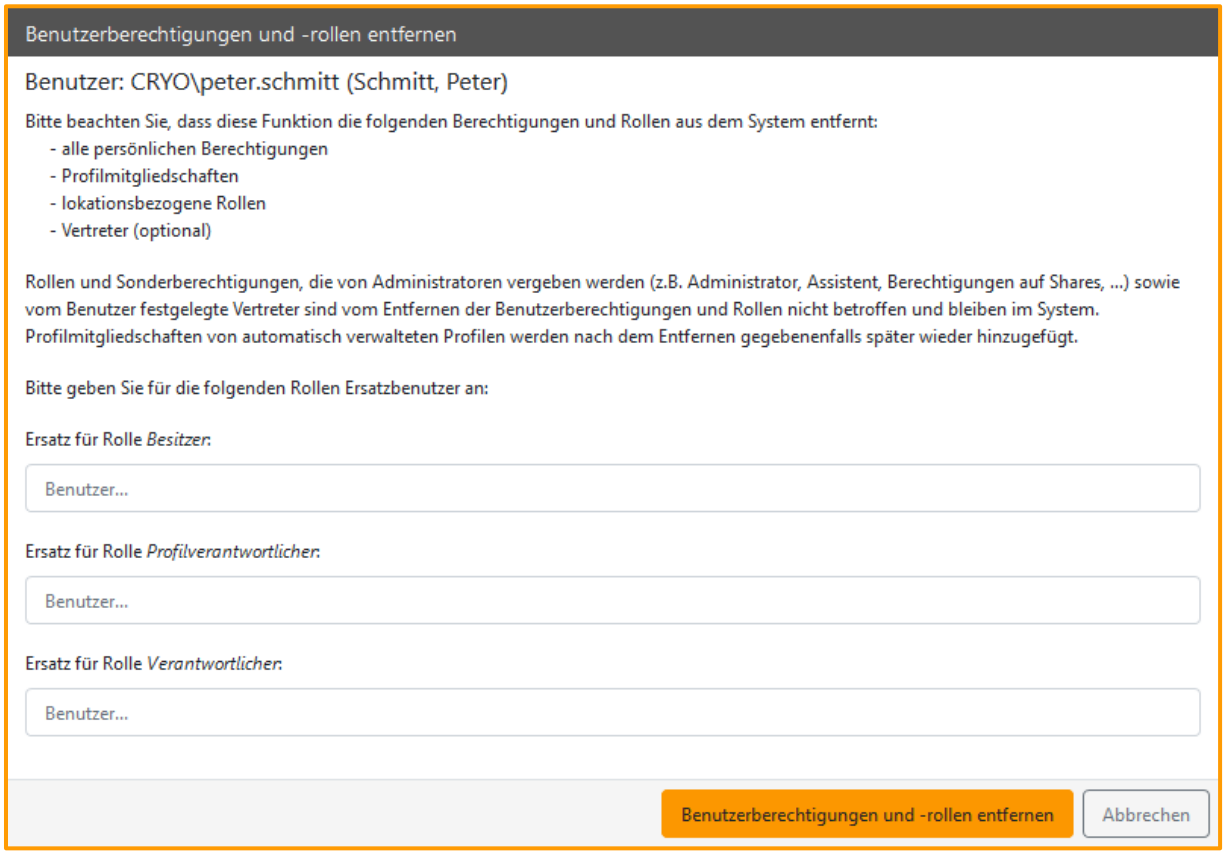

Neben den Basisdaten wird Ihnen eine Zusammenfassung der berechtigten Ressourcen sowie der zugewiesenen Rollen angezeigt.

Der Bereich *Kontoeigenschaften* stellt Ihnen sicherheitstechnische Basisfunktionen für die AD-Konten der Benutzer zur Verfügung. Sie können ein Benutzerkonto de- oder reaktivieren, mit einem Ablaufdatum versehen und ein neues Passwort vergeben. Hierbei handelt es sich nicht um Access Manager-interne Daten: Mit dem Button *Speichern* werden diese Attribute direkt im AD-Konto des Benutzers geschrieben.

Über die Kennwort-Optionen können Sie das Passwort des Benutzers zurücksetzen. Dies kann entweder durch manuelle Eingabe geschehen oder automatisch über das Schlüsselsymbol, wobei die Access Manager- und AD-Kennwortrichtlinien zu berücksichtigen sind. Wird das Passwort vom AM erzeugt, erscheint es nur einmalig im Klartext innerhalb eines Popup-Fensters und muss jetzt notiert werden. Ein späteres Nachschauen ist aus Sicherheitsgründen nicht möglich. Die Aktion der Passwortänderung erscheint außerdem im Audit.

### 11.3.1 Alle Benutzerrechte löschen

Außerdem haben Sie auf dieser Seite mit dem Button *Benutzerberechtigungen und -rollen entfernen* die Möglichkeit, die Berechtigungen und Rollen eines Benutzers vollständig zu löschen. Es erscheint der folgende Dialog:

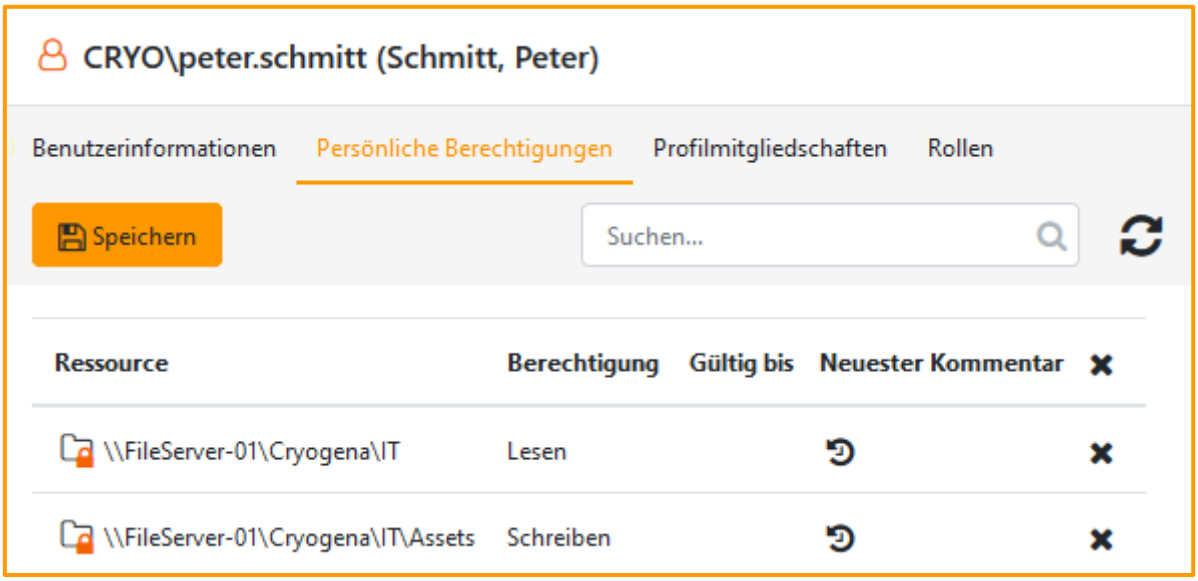



Hier werden die Zugriffsberechtigungen komplett entfernt. Da den Rollen eines Benutzers eine besondere Bedeutung zukommt, können diese meist nicht einfach entfernt werden. Stattdessen müssen Sie ein Ersatzbenutzer angeben, der künftig die Aufgaben übernimmt – dies kann für jede Rolle eine andere Person sein.

Mit dieser Funktion lassen sich alle Daten auf einmal entfernen. Sollen dagegen bspw. nur Berechtigungen, jedoch keine Rollen gelöscht werden, lässt sich dies separat auf den folgenden Tabs erledigen.

## 11.4 Persönliche Berechtigungen

Im Tab *Persönliche Berechtigungen* werden die Ressourcen mit dem jeweils vergebenen Recht und dem ggf. gesetzten Ablaufdatum aufgeführt. Im Gegensatz zu einem *Verantwortlichen* sehen Sie als *Administrator* hier jedoch tatsächlich alle Ressourcen, nicht nur jene in Ihrem Verantwortungsbereich.




Für jede Ressource können Sie die Zugriffsberechtigung ändern (Dropdown-Liste), ein Ablaufdatum setzen, Kommentare einsehen / hinzufügen sowie die Berechtigung ganz entfernen (Kreuz-Symbol). Über das Kreuz-Symbol im Tabellenkopf können auch alle Berechtigungen auf einmal entfernt werden. Darüber hinaus können auch Berechtigungen auf weitere Verzeichnisse vergeben werden (Button *Ordner hinzufügen*). Alle Änderungen werden nicht sofort durchgeführt, sondern es wird die geänderte Zeile zunächst farblich markiert und erst beim Klick auf *Speichern* übernommen. Da für alle diese Aktionen keine Beantragung erforderlich ist, werden auch keine automatischen Benachrichtigungsemails an die Betroffenen versendet.

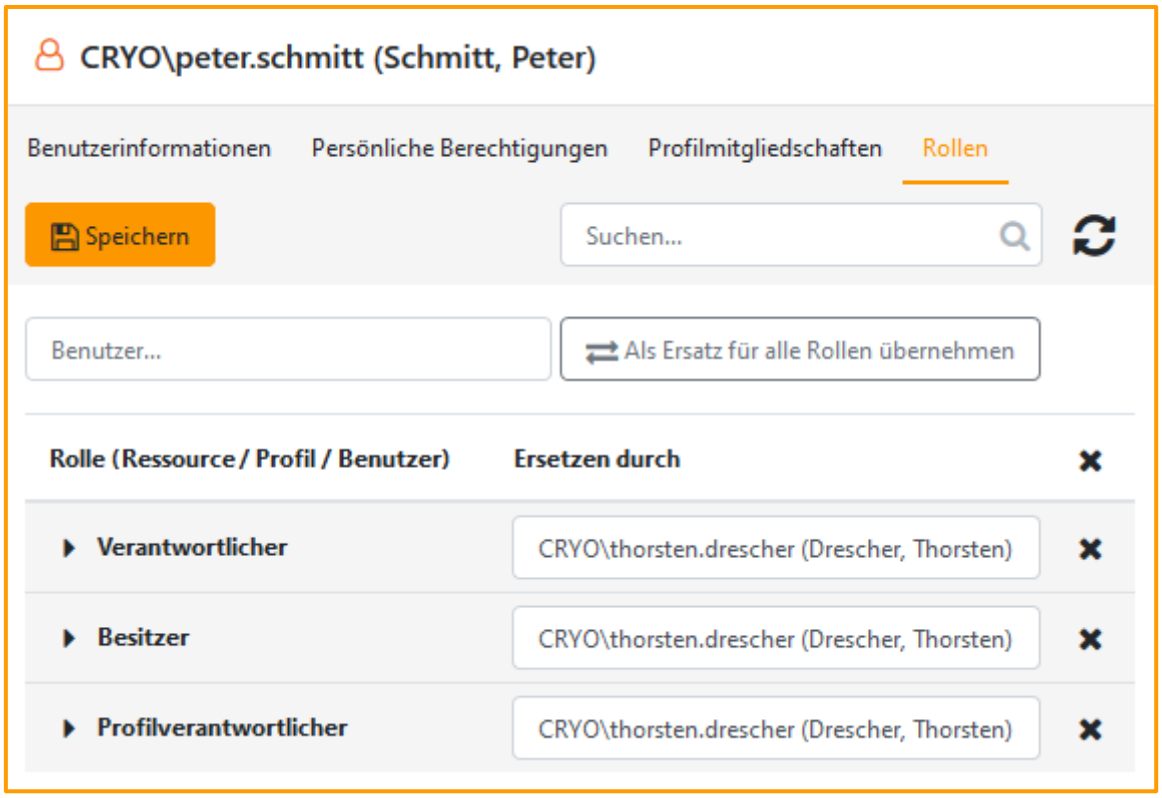
## 11.5 Profilmitgliedschaften des Benutzers

Im Tab *Profilmitgliedschaften* werden die Profile mit dem ggf. gesetzten Start- und Ablaufdatum aufgeführt. Im Gegensatz zu einem *Profilverantwortlichen* sehen Sie als *Profiladministrator* hier jedoch tatsächlich alle Profile, nicht nur jene in Ihrem Verantwortungsbereich – dies umfasst auch Profile, für die die Mitgliedschaft erst später beginnt und derzeit noch nicht besteht


Zu jedem aufgeführten Benutzerprofil bietet das Info-Symbol eine Anzeige, auf welche Verzeichnisse das Profil berechtigt wurde, außerdem wird Ihnen die AD-Gruppe angezeigt, über die der Benutzer Mitglied wurde, sofern das entsprechende Profil automatisch statt manuell verwaltet wird. Änderungen am Zeitraum sind hier möglich, darüber hinaus können Sie ein Profil hier entfernen (Kreuz-Symbol), was bedeutet, dass der Benutzer aus dem Profil entfernt wird und damit die Zugriffsrechte auf die Verzeichnisse des Profils verliert. Umgekehrt kann der Benutzer durch Hinzufügen eines Profils (via Button *Benutzerprofil hinzufügen*) zum Mitglied des Profils gemacht werden.

## 11.6 Systemrollen des Benutzers

Im Tab *Rollen* werden Ihnen als *Administrator* alle weiteren AM-eigenen Rollen des gewählten Benutzers angezeigt (z.B. Vertreterrollen, Profilverantwortlicher und Site-, Server- und Share-Administratoren, …). Klappen Sie einen Rolleneintrag auf, können Sie über das Kreuz-Symbol dem Benutzer die Rolle für die jeweilige Ressource entziehen. Im Falle der Verantwortlichen-Rolle ist dies nur möglich, wenn der Anwender nicht der einzige Verantwortliche ist (Symbol ist grau / deaktiviert). Analog gilt für Besitzerrollen, dass diese nicht entfernt werden können, wenn lediglich ein Besitzer für eine Ressource existiert. Pro Rolle können Sie unterschiedliche Ersatzpersonen bestimmen oder über den Button *Als Ersatz für alle Rollen übernehmen* einen anderen Benutzer direkt in alle aufgeführten Rollen übernehmen und den bisherigen gleichzeitig entfernen:



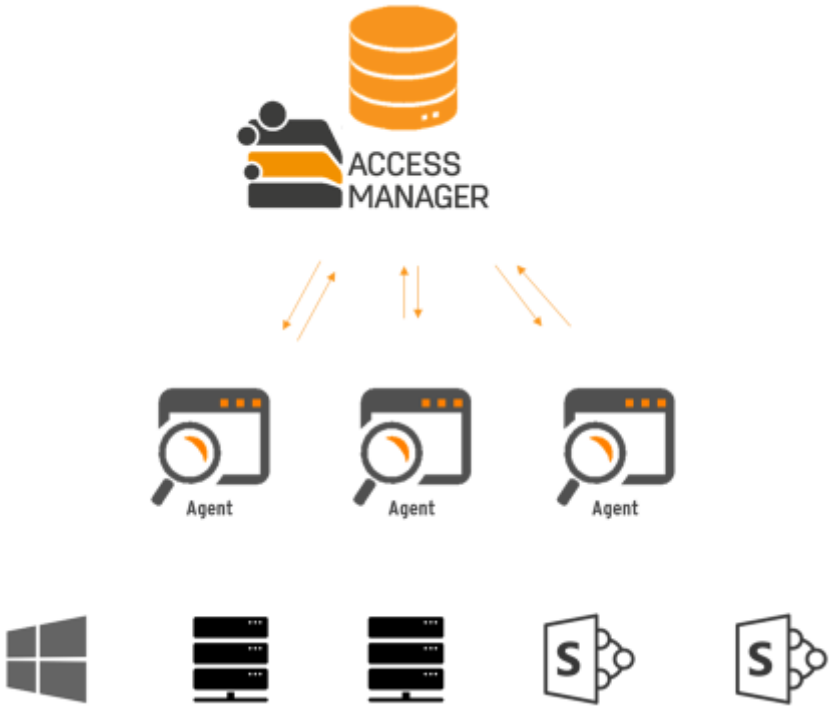
# 12 Systemadministration

## 12.1 Architektur und Arbeitsprinzip

Der Access Manager setzt die klassische verteilte Client-Server-Architektur um und verwendet dabei das Agentenkonzept zur parallelen Ausführung mehrerer Tasks in großen und verteilten Umgebungen.


Auf einem dedizierten AM-Server läuft die eigentliche Applikation als Web-Anwendung unter IIS und bietet den Benutzern das Management Portal als Schnittstelle an. Auf derselben oder einer anderen Maschine läuft die AM-Datenbank (MS SQL Server), in der sämtliche Verwaltungs- und Protokolldaten gespeichert werden. Ebenfalls hier oder auf weiteren Servern ist der AM-Agent installiert, welcher sich um die Durchführung der Aufgaben kümmert. Die AM-Komponenten greifen lesend und schreibend sowohl auf das AD zu (zur Erstellung und Befüllung der Berechtigungsgruppen) als auch auf die angeschlossenen Fileserver (zum Eintragen der NTFS-Berechtigungen).

Es können ein oder mehrere Agenten installiert werden:




Ein Agent ist als Windows-Dienstprogramm realisiert und muss auf mindestens einem Server laufen (häufig auf demselben Server, auf dem auch der Access Manager installiert ist, wahlweise auch auf einem Fileserver). Eine Aufgabe ist im Normalfall eine wiederholend geplante Arbeitsanweisung für einen Agent, z.B. das Prüfen und Korrigieren von Zugriffsrechten im Dateisystem. Dadurch werden ohne weiteres manuelles Zutun die einmal festgelegten Benutzerrechte permanent aufrechterhalten. Zur Durchführung der Aufgaben greift der Agent auf die Datenbank zu und liest die benötigten Daten aus. Umgekehrt schreibt er auch die Ergebniswerte (z.B. Fehlermeldungen der AD und der Fileserver, Zeitstempel der Durchführung usw.) in die Datenbank zurück. Obwohl ein Agent mehrere Fileserver bearbeiten kann, ist es gerade in großen Infrastrukturen mit vielen oder örtlich weit verteilten File- und AD-Servern sinnvoll, mehrere Agenten IT-technisch nah zu installieren und die Aufgaben strategisch zu verteilen. Dies minimiert Netzwerklast und Latenzen in der Kommunikation mit dem zentralen AM-Server.

## 12.2 Technisches Konzept: Eigene PowerShell Skripte

Der Access Manager bietet an verschiedenen Stellen die Möglichkeit, eigene PowerShell-Skripte auszuführen.

---

*Die Verwendung benutzerdefinierter Skripte erfolgt auf eigene Verantwortung.*
*Die BAYOONET AG übernimmt keine Verantwortung für Fehler, Defekte und Datenverluste,*
*die durch den Einsatz kundeneigener Skripte entstehen.*

---

Das System unterstützt die Ausführung von Skripten unter PowerShell Version 4 und 5. Skripte werden immer als eine Aufgabe, d.h. durch einen AM-Agenten ausgeführt. Somit laufen sie auf der Maschine, auf der der ausführende Agent installiert ist und unter dem dafür eingerichteten Benutzerkonto. Zwar ist es möglich, den Quelltext eines PowerShell-Skripts direkt in dem jeweiligen Eingabefeld anzugeben, sinnvoller ist es jedoch, hier lediglich den Namen einer fertigen Skript-Datei einzutragen. Diese Datei muss vom Agenten erreichbar sein: Skript-Aufgaben werden immer von einer zugewiesenen Agent-Gruppe bearbeitet, die beliebig viele Agenten enthalten kann. Daher ist zu beachten, dass ein Skript potentiell von jedem dieser Agenten ausgeführt werden kann. Die Skript-Datei muss daher entweder auf jedem Agent-Rechner unter demselben Pfad installiert sein oder zentral auf einem von allen Agent-Rechnern zugreifbaren Share liegen, wobei wir letzteres wegen der einfacheren Pflege empfehlen.

Bitte verwenden Sie in Ihren Skripten **nicht** die Ausgabe-Befehle `Write-Host` und `Write-Information` – diese sind generell für eine Automatisierung ungeeignet und produzieren Fehlermeldungen. Benutzen Sie stattdessen `Write-Output`.

Sofern ein Skript bei der Ausführung Fehler produziert, finden Sie diese auf der Seite *Administrator → Protokollierung → System-Log*.

Beispiele für eigene Scripts, auch unter Verwendung der vom Access Manager übergebenen Variablen, finden Sie im Kapitel 14.

### 12.2.1 Aufrufmöglichkeiten

In dem jeweiligen Texteingabefeld „Skript“ kann entweder der Quelltext des PowerShell-Skripts eingegeben werden oder aber eine PowerShell-Datei (*.ps1), die dann abgearbeitet wird.

Bitte beachten Sie, dass bei der Verwendung mehrerer AM-Agenten nicht festgelegt werden kann, welcher Agent das Skript ausführen wird. Alle Rechner, auf denen Agenten installiert sind, müssen daher über identische PowerShell-Versionen, Ausführungsberechtigungen, eventuelle zusätzlich erforderliche PowerShell-Module sowie ggf. Zugriffsberechtigungen auf Drittsysteme (sofern von den Skripten benötigt) verfügen. **Skripte werden immer mit dem AM-Agent-Benutzerkonto ausgeführt.**

Da eine visuelle Ausgabe nicht möglich ist, sollten Sie für die Ausgabe immer eine Log-Datei via `Write-Output` o.ä. vorsehen (benutzen Sie jedoch niemals `Write-Host` oder `Write-Information`).

#### 12.2.1.1 Eingabe: Source Code

Wenn Sie Quelltext eingeben, wird dieser auf der Zielmaschine direkt ausgeführt, als würden Sie jede einzelne Zeile auf der Kommandozeile ausführen. Relative Verzeichnisangaben sind dadurch nicht möglich, da das aktuelle Ausführungsverzeichnis nicht bekannt ist. Eine Log-Datei müssen Sie dementsprechend mit absolutem Pfad angeben:

```
$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
```

Wenn dieses Skript vom Access Manager ausgeführt wird, finden Sie die Ausgabe-Datei im Verzeichnis C:\tmp\ auf der Maschine, auf der der Agent installiert ist, welcher die Aufgabe ausgeführt hat.

#### 12.2.1.2 Eingabe: Name einer Skript-Datei

In den meisten Fällen ist es sinnvoller, eine vorhandene Skript-Datei (*.ps1) anzugeben, welche von AM-Agent ausgeführt wird. Der Agent führt die Datei lokal aus. Insbesondere wenn mehr als ein Agent in der zugewiesenen Agent-Gruppe installiert ist, ist unklar, welcher Agent das Skript ausführen wird. Daher muss die identische Skript-Datei auf allen entsprechenden Agent-Rechnern an derselben Stelle gespeichert sein. Der Aufruf sieht dann so aus (Inhalt des Texteingabefeldes *Skript*):

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

Die bessere Alternative ist, das Skript zentral auf einem Share abzulegen, auf das jeder Agent-Rechner und das AM-Agent-Benutzerkonto zugreifen darf. Das erleichtert die Pflege des Skripts und die Verteilung desselben kann nicht vergessen werden. Der Aufruf lautet dann zum Beispiel:

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

Verwenden Sie in beiden Fällen möglichst immer eine absolute Pfadangabe zur Vermeidung von Zweideutigkeiten und setzen Sie eventuell erforderliche Anführungszeichen nie um den kompletten Pfad (d.h. nicht als erstes Zeichen), da diese Syntax nicht erkannt wird. Es ist ausreichend, die Anführungszeichen nur um die Pfadteile zu setzen, die Leerzeichen enthalten. Diese Syntax ist valide:

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

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

## 12.3 Technisches Konzept: Profilberechtigungen über eigene AD-Gruppen

Neben dem bisherigen Verfahren zur Benutzerberechtigungen auf Verzeichnisse im Dateisystem über *Profile* existiert ein alternatives zweites Verfahren.

Nach dem bisherigen Verfahren werden Mitglieder eines Benutzerprofils immer in die entsprechende AD-Gruppe des Berechtigungsverzeichnisses (=Verzeichnis-AD-Gruppe) eingetragen, genau wie bei der persönlichen Berechtigung eines Benutzers. Im Dateisystem ist effektiv kein Unterschied vorhanden; es ist dort nicht mehr erkennbar, ob ein Benutzerkonto durch ein (Benutzer-)Profil oder eine persönliche Berechtigung Zugriff erhält.

Das neue Verfahren erzeugt für jedes AM-Benutzerprofil eine eigene AD-Gruppe (=Profil-AD-Gruppe) und trägt hier die Mitglieder ein. Diese Profil-AD-Gruppe wird im Dateisystem auf jedem zugehörigen Berechtigungsverzeichnis entweder mit Lesen oder Schreiben berechtigt (je nach Auswahl im Profil), das heißt dieselbe AD-Gruppe wird mehrfach für verschiedene Verzeichnisse verwendet. Die weiterhin für persönliche Berechtigungen verwendeten Verzeichnis-AD-Gruppen werden bei diesem Verfahren nicht mit den Benutzer-Mitgliedern des Profils befüllt.

Beide Verfahren können im Access Manager parallel verwendet und im laufenden Betrieb von einem in das andere Verfahren ohne Datenverluste umgewandelt werden.

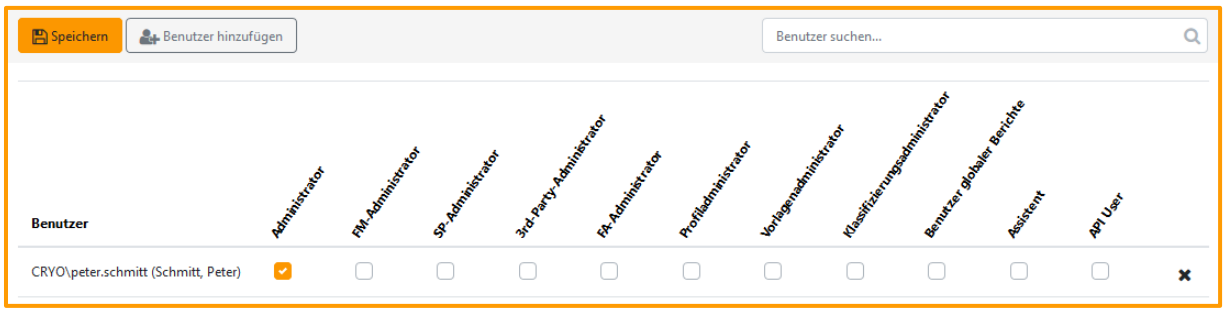
### 12.3.1 Vergleich der technischen Ansätze

Die klassische Technik sorgt bei einem Benutzer für ein schnell wachsendes Kerberos-Token wenn er auf vielen Verzeichnissen berechtigt wird, da er in allen Verzeichnis-AD-Gruppen Mitglied wird. Mit der neuen Technik dagegen ist er nur in wenigen Profil-AD-Gruppen Mitglied, kann aber dennoch auf vielen Verzeichnissen berechtigt sein. Die Umsetzung von hinzugefügten oder gelöschten Profilmitgliedern im Dateisystem beschleunigt sich enorm (insbesondere bei vielen Verzeichnissen in einem Profil), da nicht mehr die jeweiligen Verzeichnis-AD-Gruppen bearbeitet werden müssen, sondern nur die einzelne betroffene Profil-AD-Gruppe.

Die Verwendung von Profil-AD-Gruppen sorgt nicht für insgesamt weniger AD-Gruppen und steigert damit nicht die Übersichtlichkeit der Berechtigungen im Dateisystem. Es ist außerdem nicht möglich bereits vorhandene kundeneigene AD-Gruppen als Profil-AD-Gruppen zu verwenden, da dies zu schwer nachvollziehbaren Fehlfunktionen durch fehlende Zugriffsrechte und unpassende Gültigkeitsbereiche (globale / lokale AD-Gruppen) führen könnte.

## 12.4 Systemrollen zuweisen


Die Seite Systemrollen ermöglicht Ihnen als AM-*Administrator* die Verwaltung von Benutzern, die bestimmte Module und Funktionen innerhalb des Access Managers ausführen dürfen. Jedem Benutzer werden dazu Rollen zugewiesen, auf deren Basis die Zugriffsberechtigungen auf die lizenzierten Module festgelegt werden; diese lassen sich beliebig kombinieren.




Mit dem Button *Benutzer hinzufügen* erzeugen Sie einen neuen Eintrag, in dem Sie das gewünschte Benutzerkonto angeben. Aktivieren Sie dann mindestens eine Rolle, da Konten ohne Rolle automatisch entfernt werden. Auch über den Button *Entfernen* (Kreuz-Symbol) können Sie einen bereits bestehenden Benutzereintrag löschen.

Die Aufgaben und Rechte der einzelnen Rollen sind im Kapitel 2.3.2 beschrieben.

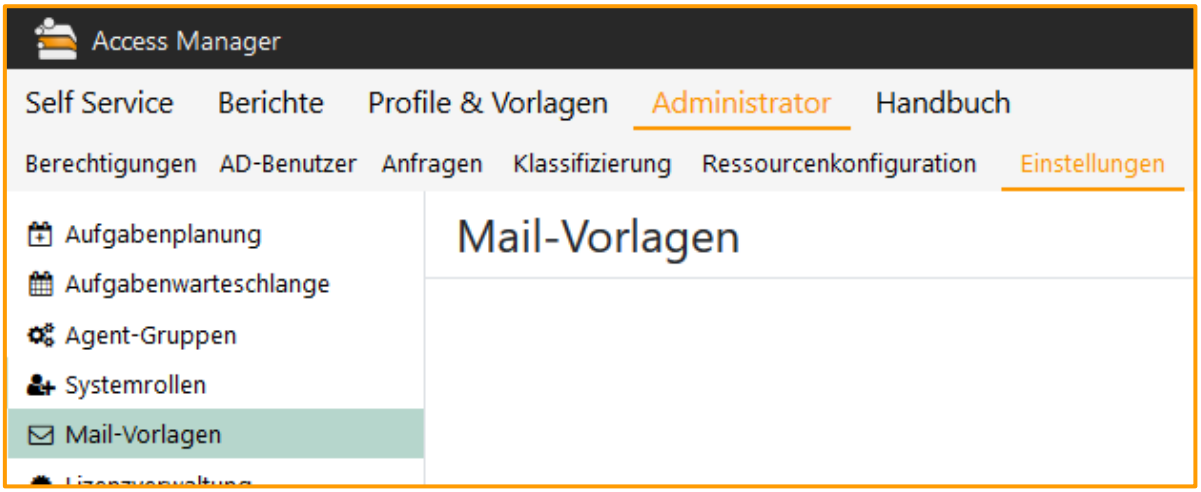
Bitte beachten Sie, dass die Rolle Administrator nicht automatisch alle anderen Rollen umfasst, diese sollten Sie daher zusätzlich aktivieren, wenn ein Administrator umfassende Rechte im Access Manager System erhalten soll.

### 12.4.1 Passwort Reset Systemrollen (AMPR Rollenverwaltung)

Setzen Sie das zusätzliche Produkt AMPR ein und haben Sie die *AMPR-Rolle Administrator*, gibt es in den Administrator-Einstellungen einen weiteren Bereich, in dem Sie die Rollen der User innerhalb des AMPR verwalten können:

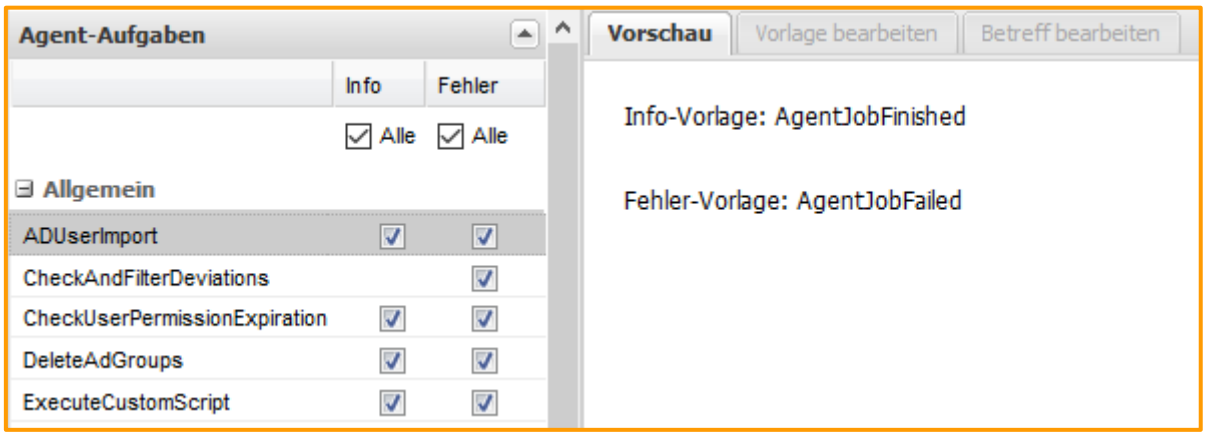

*Dieser Menüpunkt stellt die Funktionen des Programms AMPR zur Verfügung.*
*Eine Beschreibung aller Funktionen finden Sie im zugehörigen AMPR-Handbuch.*

## 12.5 System-Mailing konfigurieren




Auf der Seite *Mail-Vorlagen* können Sie den Aufbau und die Versandoptionen der Access Manager-Mails einsehen und bearbeiten. Der linke Bereich ist in drei aufklappbare Abschnitte unterteilt: Agent-Aufgaben, Agent-Vorlagen und Workflow-Vorlagen. Unter den Agent- und Workflow-Vorlagen können Sie Aussehen und Inhalt der zu versendenden Mails überprüfen und verändern; unter Agent-Aufgaben wird festgelegt, in welchen Fällen eine Mail versandt werden soll und Sie sehen, welche Mail-Vorlage verwendet wird.

### 12.5.1 Agent-Aufgaben




Im Abschnitt *Agent-Aufgaben* können Sie festlegen, ob und in welchen Fällen die AM-Administratoren bzw. Benutzer mit AM-Rollen nach der Ausführung einer Aufgabe über deren Ergebnis per E-Mail informiert werden sollen. Hierbei wird zwischen Informations- und Fehler-Mails unterschieden.

*Informations-Mails* werden nach jeder Ausführung einer Aufgabe versendet. Diese E-Mails basieren auf der fest zugeordneten Agent-Vorlage *AgentJobFinished* (siehe nächstes Kapitel). Die enthaltenen Informationen sind vom Typ der Aufgabe abhängig. Sie umfassen beispielsweise Beginn und Ende der Ausführung oder Informationen über Zugriffsberechtigungen.

*Fehler-Mails* werden nur dann – und zusätzlich zu einer Info-Mail – versendet, wenn bei der Ausführung einer Aufgabe Fehler auftreten. Der Aufbau aller Fehler-Mails wird durch die Vorlage *AgentJobFailed* festgelegt.

Um den Versand von Informations- oder Fehler-Mails an AM-Administratoren zu unterdrücken, entfernen Sie das entsprechende Häkchen (*Info* oder *Fehler*) in der Zeile der jeweiligen Mail-Vorlage. Die Änderungen werden nach einem Klick auf *Speichern* wirksam.

Sofern für eine Aufgabe nur eine *Fehler*-Checkbox vorhanden ist, existiert für die Info-Mail eine separate Vorlage, da die anzuzeigenden Informationen die sonst übliche Menge übersteigen und eine solche Mail zwingend fallabhängig verschickt werden muss. Dies betrifft z.B. die Aufgaben *CheckAndFilterDeviations*, *InitializeReapproval* und *FinishReapproval*.

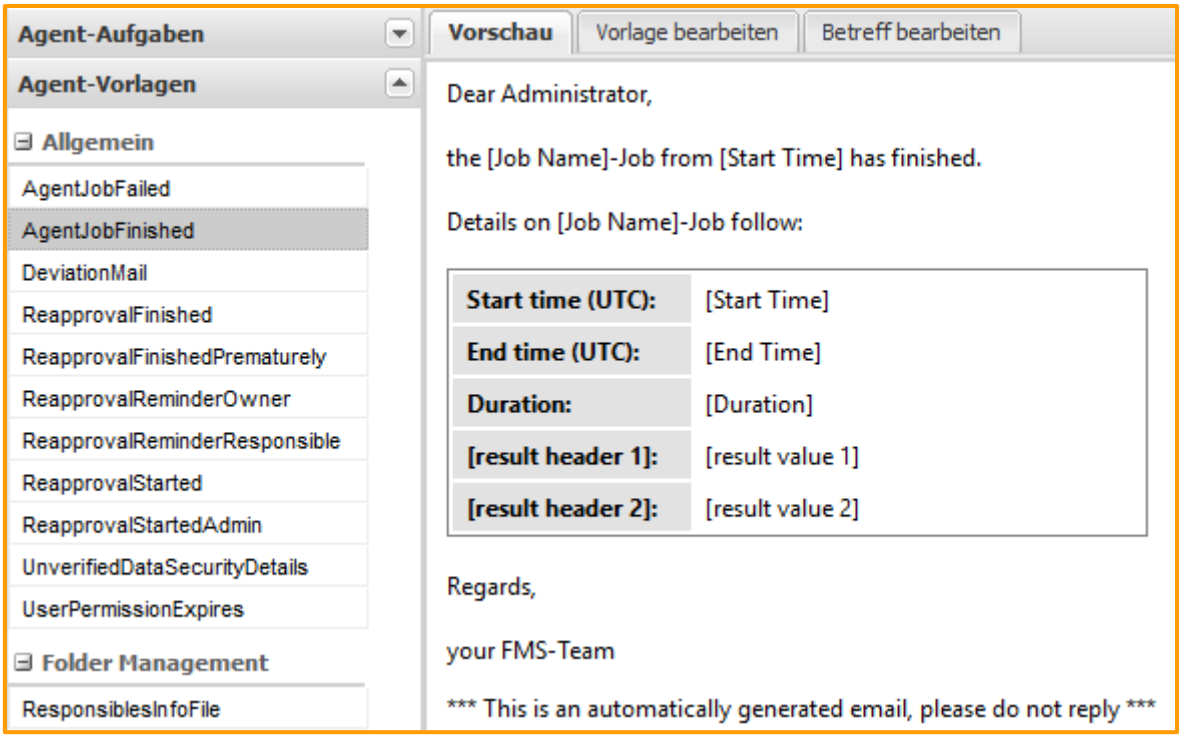
Eine Ausnahme bildet die Aufgabe *ExecuteCustomScriptInternal*: Hierbei handelt es sich um eine intern häufig verwendete Aufgabe, bei der es nicht sinnvoll ist, ständig ihre korrekte Ausführung mitzuteilen.

### 12.5.2 Agent- / Workflow-Vorlagen

Im Abschnitt *Workflow-Vorlagen* werden diejenigen Mail-Vorlagen verwaltet, die über den Status eines Access Manager-*Workflows* informieren. Im Gegensatz zu *Agent-Vorlagen* wird der Versand dieser E-Mails nicht durch die Ausführung geplanter Aufgaben ausgelöst, sondern durch konkrete Aktionen von Benutzern (Antragsteller und Bearbeiter). Dies umfasst beispielsweise das Anfordern oder Gewähren von Zugriffsberechtigungen. Daher werden diese E-Mails ausschließlich an Benutzer verschickt – Administratoren werden nicht über Workflows informiert.

Im Gegensatz zu Agent-Vorlagen sind Workflow-Vorlagen werkseitig immer zweisprachig ausgeführt. Dies können Sie jederzeit selbst ändern – siehe das folgende Kapitel.

### 12.5.3 Mail-Vorlagen anzeigen und bearbeiten




Die Liste der Mail-Vorlagen ist thematisch in *Agent-Vorlagen* und *Workflow-Vorlagen* unterteilt, die Bearbeitungsmöglichkeiten sind jedoch identisch.

Wählen Sie eine Vorlage aus, wird diese rechts mit Beispieldaten im Tab *Vorschau* angezeigt, sodass Sie die finale Darstellung der entsprechenden E-Mails überprüfen können.

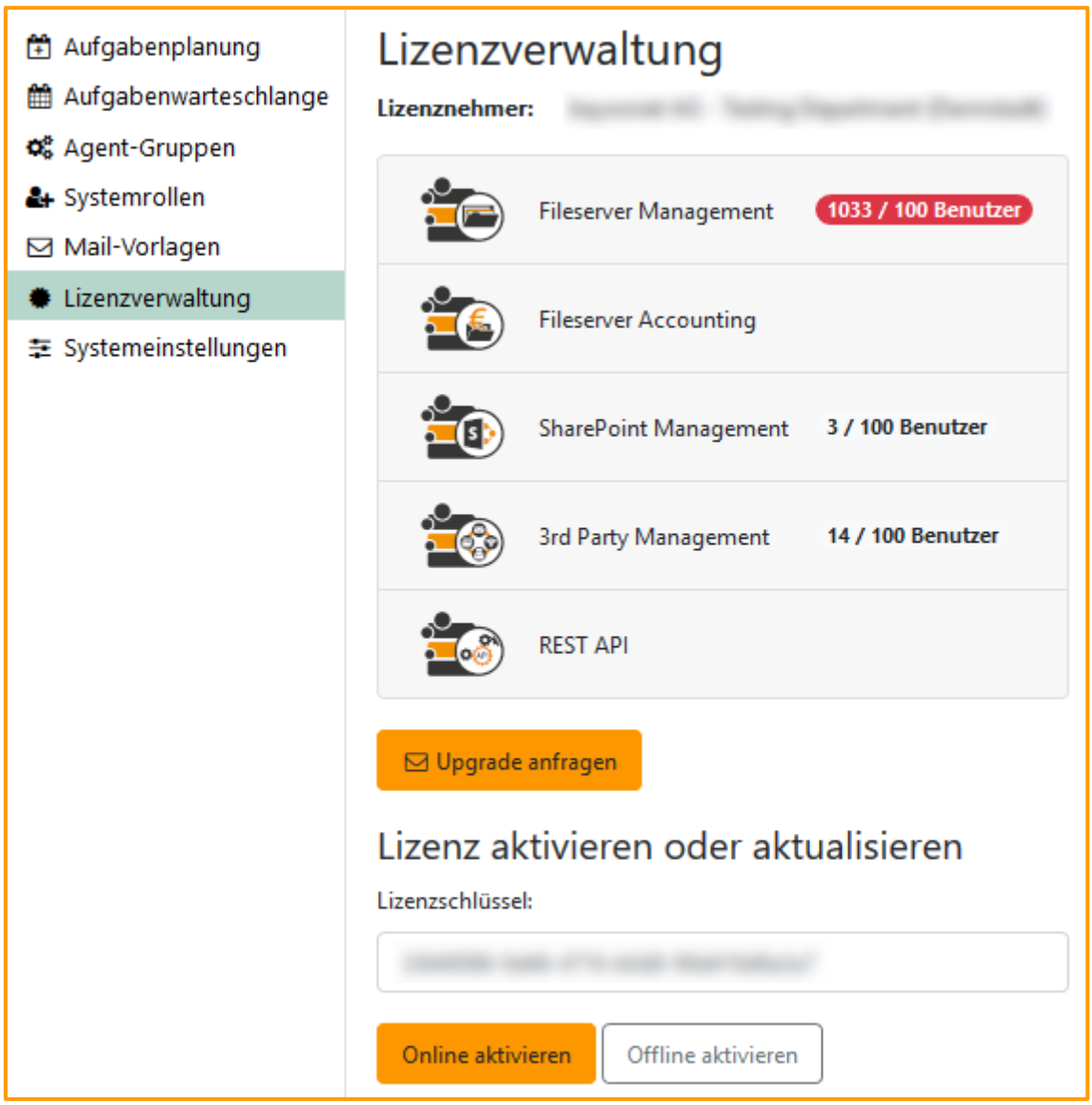
Im Tab *Bearbeiten* wird der Quelltext der E-Mail angezeigt und kann dort bearbeitet werden – Kenntnisse von HTML, CSS und XSLT sind von Vorteil. Der Button *Speichern* überprüft die Änderungen auf Basis einer XSLT-Spezifikation und speichert sie ab, falls keine Fehler aufgetreten sind. Mit *Zurücksetzen* werden alle Änderungen an der Vorlage (auch zuvor gespeicherte) verworfen und die Werkseinstellungen wiederhergestellt.

Im Tab *Betreff bearbeiten* können Sie den Betreff der Mail ändern, wobei je nach Vorlage verschiedene Platzhalter verwendet werden können, die das System automatisch beim Versand der Mail befüllt. Bitte beachten Sie, dass eine variable Auswahl für englischen oder deutschen Betreff **nicht** möglich ist.

### 12.5.4 Überschreiben / Behalten von Vorlagen bei Programm-Updates

Bei einem Update des Access Managers werden die werkseitig integrierten Vorlagen ebenfalls aktualisiert. Sofern Sie jedoch einzelne Vorlagen bereits angepasst haben, bleiben diese erhalten und werden in keiner Weise verändert. Erst die Funktion *Zurücksetzen* (im Tab *Bearbeiten*) stellt wieder die Standard-Vorlagen bereit, wodurch eigene Veränderungen verworfen werden.

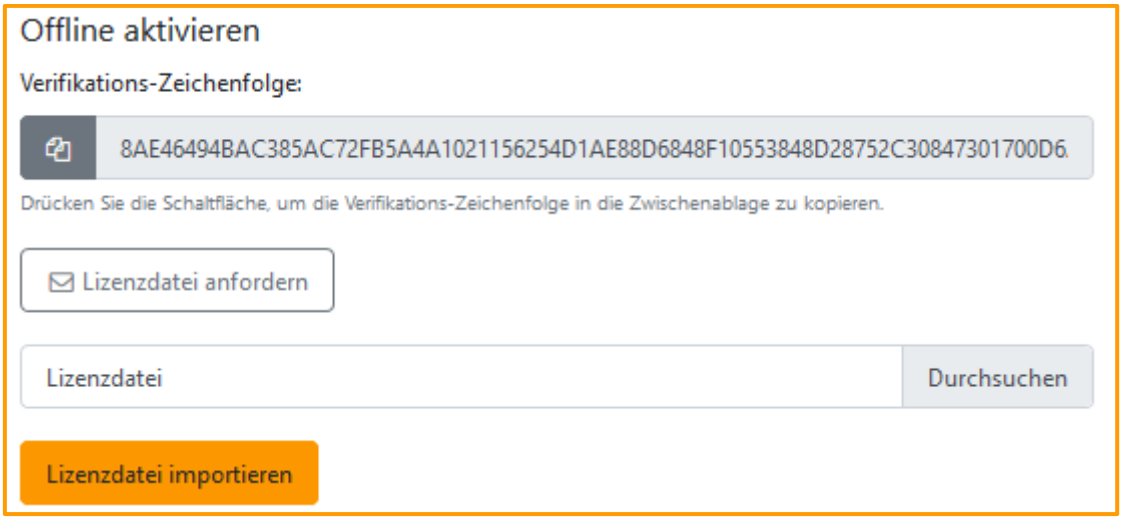
## 12.6 Lizenzverwaltung




Um ein oder mehrere Module verwenden zu können, müssen diese über eine Lizenz aktiviert werden. Dies geschieht auf der Seite *Lizenzverwaltung*.

### 12.6.1 Lizenz eintragen / aktualisieren

Um ein neues Modul freizuschalten oder eine Erhöhung Ihrer Nutzerzahl einzutragen, tragen Sie einmalig den Lizenzschlüssel ein, den Sie beim Erwerb einer Lizenz erhalten haben und klicken Sie den Button *Online aktivieren*. Nun werden die benötigten Lizenzen via Internet vom Lizenz-Server der BAYOONET AG abgerufen und die lizenzierten Module freigeschaltet. Sollte Ihr AM-Server keinen Zugriff auf das Internet haben, können Sie alternativ die Funktion *Offline aktivieren* verwenden. Dazu erhalten Sie weitere Eingabe-Elemente:



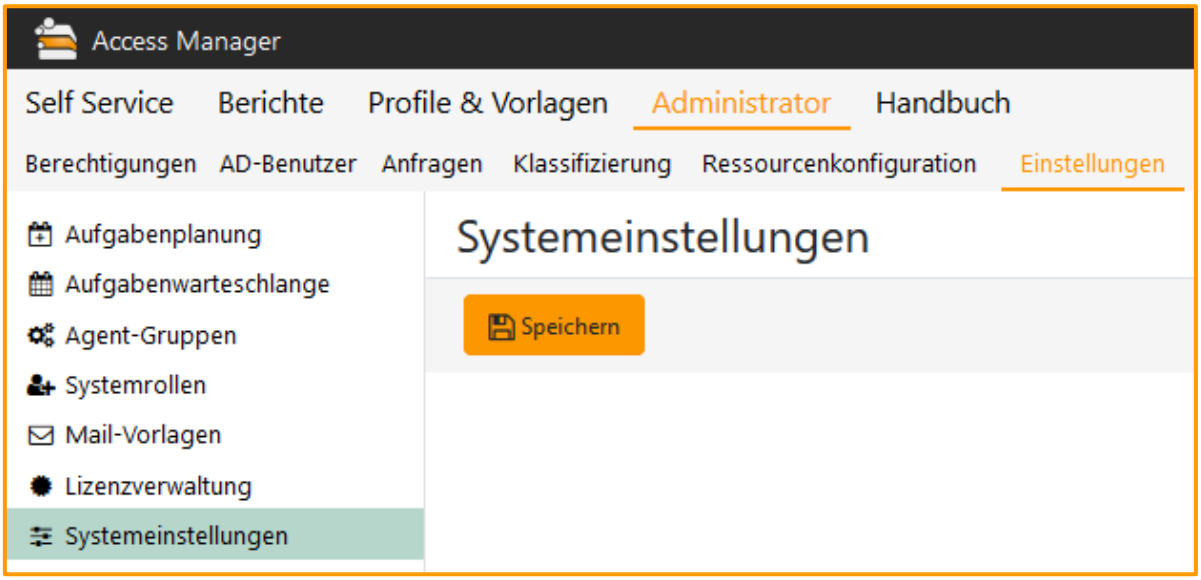

Klicken Sie den Button *Lizenzdatei anfordern*. Damit wird eine Mail in Ihrem Standard-Mailclient erstellt, die bereits alle notwendigen Daten enthält. Alternativ kopieren Sie die angegebene Verifikations-Zeichenfolge in eine eigene E-Mail. Senden Sie die Mail an die Supportabteilung der BAYOONET AG (*support@accessmanager.net*). Durch das Support-Team wird Ihnen eine Lizenz-Datei per Email zurückgesendet, die Sie lokal speichern und anschließend mit dem Button *Lizenzdatei importieren* in das System einspielen. Nun werden Ihnen wie weiter oben gezeigt die lizenzierten Module mit der jeweiligen Lizenzmenge angezeigt.

**Hinweis:** Neu eingespielte Lizenz-Updates können bis zu 10 Minuten benötigen, bis sie aktiv sind.

### 12.6.2 Lizenz erhöhen

Benötigen Sie eine Erhöhung Ihres aktuellen User-Limits, können Sie mit dem Button *Upgrade anfragen* eine Anfrage per Mail an die Vertriebsabteilung der BAYOONET AG (*sales@accessmanager.net*) senden. Geben Sie darin die gewünschte Lizenzmenge an und tragen Sie ggf. weitere Empfänger für das zu erstellende Angebot ein. Sie erhalten dann umgehend die gewünschten Informationen.

## 12.7 Generelle Einstellungen




Diese Seite verwaltet die grundlegenden globalen Access Manager Einstellungen. Jede Einstellung hat einen Namen und einen Wert / Wertelisten. Alle Einstellung sind nach ihren zugehörigen Modulen gruppiert und alphabetisch sortiert.

Die Einstellungen werden in den entsprechenden Wertefeldern geändert. Über den Button *Rückgängig* lassen sich vor dem Speichern die jeweiligen originalen Werte wiederherstellen. Die neuen Werte werden erst mit Klick auf *Speichern* übernommen und sind sofort ohne Neustart des Access Manager wirksam.

In der Suchmaske im oberen Bereich können Sie nach den Namen einer bestimmten Einstellung suchen; nur diese wird Ihnen dann – im entsprechenden Modul – angezeigt.

Im Folgenden werden alle globalen Einstellungen der zurzeit erhältlichen Module erläutert.

### 12.7.1 Modul „Administration“

#### 12.7.1.1 AdditionalAdData

Diese Einstellung erlaubt das Erstellen einer Liste von Feldern des AD-Benutzerobjekts. Die hier spezifizierten Felder werden beim User-Import zusätzlich von jedem Benutzerkonto ausgelesen und im Management Portal als Zusatzinformation bei jeder Benutzerangabe angezeigt. Je nach gewählter Oberflächensprache wird dabei die englische oder deutsche Beschreibung vorangestellt. Bitte beachten Sie:

- Die zusätzlichen Daten können von *jedem* Anwender des Management Portals eingesehen werden, also auch von normalen Benutzern ohne Verwaltungsfunktion. Es sollten daher keine vertraulichen oder sensiblen Felder verwendet werden (bspw. `accountExpires`, `lastLogonTimestamp`, …).
- Einige vordefinierte Felder im Benutzerobjekt sind nicht im AD Global Catalog gespeichert und werden daher nicht über mehrere Domain Controller repliziert. Die Anzeige eines solchen Feldes ist damit abhängig vom verbundenen DC und nicht konsistent. Verwenden Sie daher nur replizierte Felder – bei selbst erstellten Feldern sollte die Replikation normalerweise aktiviert sein.
- Bestimmte Felder (u.a. `displayName`) werden bereits intern vom Access Manager verwendet und können nicht zusätzlich angezeigt werden.

#### 12.7.1.2 AllowRenewAccessSettingsByOwners

Wird diese Option aktiviert, können *Besitzer* die Benutzerberechtigungen auf einer verwalteten Ressource aktualisieren. Dazu erscheint im Kontextmenü der Ressource der Eintrag *Berechtigungen erneuern*.

#### 12.7.1.3 AllowRetiredUserImport

Import von deaktivierten oder abgelaufenen AD-Benutzerkonten zulassen oder verbieten. Dies bezieht sich auf den Import von Share-Berechtigungen; die Validierung wird fehlschlagen, wenn die Excel-Datei deaktivierte Konten enthält und diese Option deaktiviert wurde.

#### 12.7.1.4 ApproverCommentsAreMandatory

Falls diese Option aktiviert ist, sind Bearbeiter von Benutzeranfragen (Besitzer, Verantwortliche oder Administratoren) dazu gezwungen, bei der Bearbeitung einen Kommentar anzugeben.

#### 12.7.1.5 CalculateTokenSizeOnADUserImport

Berechnung der ungefähren Kerberos-Token-Größe während der Aufgabe *ADUserImport* aktivieren oder deaktivieren.

#### 12.7.1.6 CleanUpPermissionsOfDeletedAdUsers

Ist diese Option aktiviert, werden die Berechtigungen von Benutzerkonten, die im AD nicht mehr gefunden werden, aus dem Access Manager automatisch entfernt. „Nicht im AD gefunden“ kann bedeuten, dass das Konto tatsächlich gelöscht wurde oder aber an eine Stelle (OU) verschoben wurde,

auf die der Access Manager keinen Zugriff hat. Hierfür muss die Aufgabe *TidyUpDatabase* (Kapitel 10.6.1.9) eingeplant sein.

Folgende Daten werden entfernt:

- Persönliche Berechtigungen
- Mitgliedschaften in Profilen, dadurch Berechtigungen auf damit verbundenen Ressourcen
- Vertreter-Rollen für Verantwortliche und Besitzer

---

***Explizit bestehen bleiben*** *Rollen als Verantwortlicher und Besitzer. Diese Rollen können nicht ohne Festlegung einer Ersatzperson entfernt werden und müssen daher manuell erfolgen.*

---

#### 12.7.1.7 CommentsAreMandatoryDuringImport

Wenn diese Option aktiviert ist, müssen Sie bei einem Share-Datenimport (Kapitel 8.2.1.2.1) in der Excel-Datei für jede Zeile die Spalte COMMENT mit einer Begründung für diese Berechtigung füllen, andernfalls ist ein Import nicht möglich.

#### 12.7.1.8 Database

Dieser nicht veränderbare Wert gibt Auskunft, wo die AM Datenbank gespeichert ist.

#### 12.7.1.9 DeviationFilterLimit

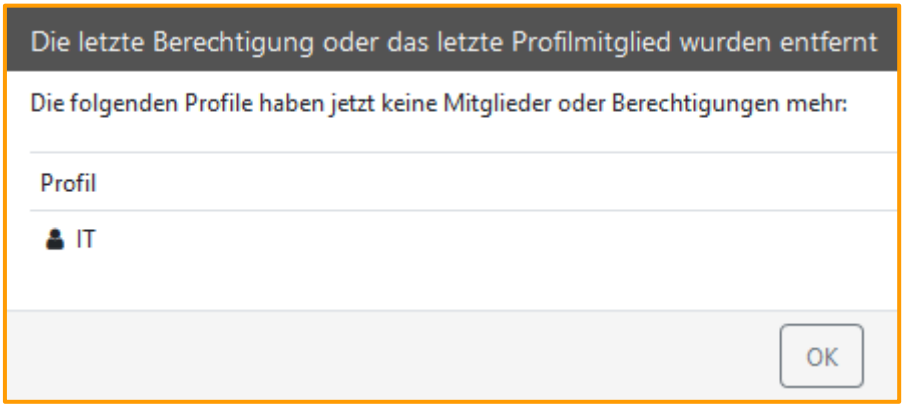
Hiermit wird eingestellt, wie viele erkannte, aber nicht relevante Berechtigungsabweichungen auf einmal aus der Anzeige herausgefiltert werden. Ist die Anzahl zu hoch, kann das Filtern länger dauern und damit die Abarbeitung anderer Aufgaben blockieren.

---

*Diese Einstellung sollte nur bei speziellen Problemen mit der Laufzeit von Berechtigungsbereinigungen verändert werden.*

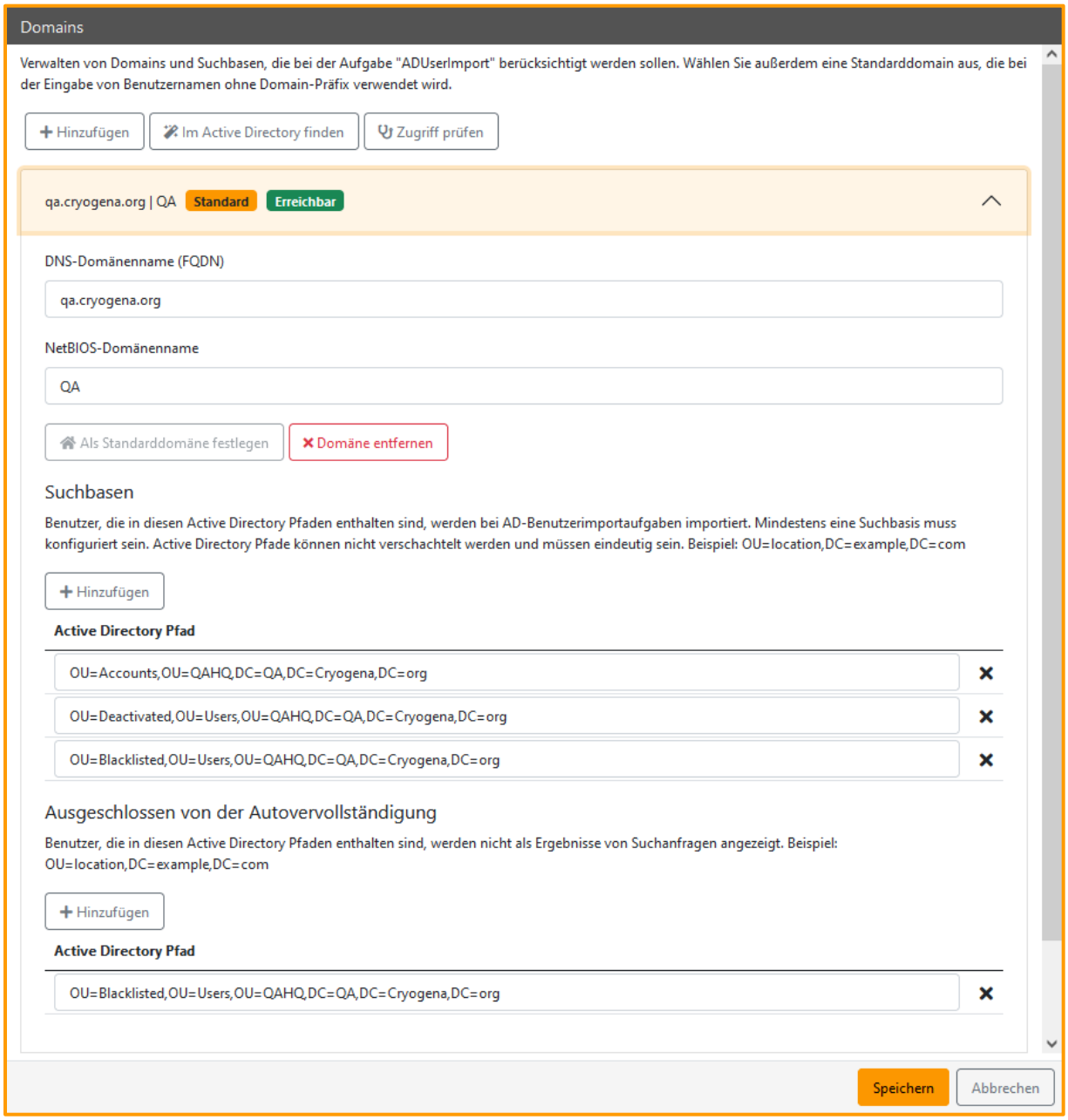
---

#### 12.7.1.10 DisplayLastPermissionOrMemberRemovedWarning



Legt fest, ob dem Rechte-Bearbeiter ein Informationsfenster angezeigt werden soll, wenn er die letzte Berechtigung von einer Ressource entfernt. Die Information erscheint, wenn bspw. einem Profil die Berechtigung auf ein Verzeichnis entzogen wird und diese Berechtigung die letzte war, die auf dem Verzeichnis existierte. In diesem Fall kann nun niemand mehr auf das Verzeichnis zugreifen. Aber auch umgekehrt wird der Bearbeiter gewarnt, wenn er etwa Verzeichnisberechtigungen bearbeitet und dabei ein Profil entfernt: hier kann das System feststellen, dass dies die letzte Berechtigung war, die das Profil hatte und es nun also auf keine Ressource mehr zugreifen darf.

#### 12.7.1.11 Domains



In diesem Dialog werden die Domains, Sub-Domains und (externe) Trusts eingetragen, die bei Ausführung der Aufgabe *ADUserImport* (Kapitel 10.6.1.1) ausgelesen werden sollen. Alle hier nicht aufgeführten Lokationen werden dementsprechend auch nicht berücksichtigt.

Mit dem Button *Im Active Directory finden* werden alle öffentlich bekannten Lokationen eingetragen, mit *Hinzufügen* können Sie die Liste auch manuell um weitere Domänen erweitern. Verwenden Sie den Button *Zugriff prüfen* um festzustellen, ob die gefundenen Domänen tatsächlich erreichbar sind. Sind sie es nicht, sollten Sie die entsprechenden Einträge über den Entfernen-Button (Kreuz-Symbol) löschen, wenn Sie sicher sind, dass es sich nicht um eine temporäre Kommunikationsstörung handelt, die zu beheben ist.

*Sofern bei der Ausführung der Aufgabe ADUserImport eine der hier eingetragenen Domänen nicht abgerufen werden kann, findet auch für die anderen Domänen keine Aktualisierung statt und eine Fehler-Mail wird verschickt. Überprüfen und korrigieren Sie in diesem Fall daher umgehend diese Domänenliste bzw. beheben Sie das Konnektivitätsproblem.*

Mit dem Button *Als Standarddomäne festlegen* aktivieren Sie diejenige Domäne, die als erster Vorschlag verwendet werden soll, wenn Sie später ein Benutzerkonto eingeben, welches in mehreren Domänen existiert.

**Suchbasen**

Innerhalb jeder eingetragenen Domäne existiert mindestens eine Suchbasis (OU), ab der nach zu importierenden Benutzerkonten gesucht wird. Dabei werden alle darunter liegenden Pfade ebenfalls durchsucht. Standardmäßig wird hier die oberste Ebene vorgeschlagen; Sie können den Startpfad jedoch auf tieferliegende Pfade ändern und außerdem mehrere Suchbasen angeben.

---

*Die vom Access Manager verwendeten Benutzerkonten **müssen** in einer Suchbasis enthalten sein.*
*Suchbasen **dürfen nicht** ineinander verschachtelt werden.*
*Benutzer, die nicht in den Suchbasen gefunden werden, können sich auch nicht an der Access Manager Webseite anmelden – der AM ist für sie nicht nutzbar.*

---

**Ausgeschlossen von der Autovervollständigung**

Geben Sie hier einen oder mehrere Suchpfade an, in denen Benutzerkonten liegen, die nicht angezeigt werden sollen, wenn Sie – z.B. beim Hinzufügen einer persönlichen Berechtigung – ein Benutzerkonto eingeben. Die dabei erscheinende Auflistung passender Konten wird solche Konten nicht enthalten und Sie reduzieren damit das Risiko unerwünschter Benutzerberechtigungen.

---

*Hier angegebene Pfade **müssen** in den o.a. Suchpfaden enthalten sein.*

---

#### 12.7.1.12 EmailAdministratorIfPermittedUserIsNotInAuthorizedGroup

Wenn aktiviert, erhalten alle Administratoren eine E-Mail, in der die Benutzer aufgeführt sind, die im Access Manager auf einer Ressource Berechtigungen erhalten haben, für die sie per Klassifizierung nicht autorisiert wurden. Dies weist auf eine falsche Rechtevergabe durch einen Entscheider hin und sollte überprüft werden.

#### 12.7.1.13 EmailIfPermissionExpiresInXDays

Anzahl an Tagen, die ein Benutzer im Voraus informiert wird, bevor seine Dateisystemberechtigungen entfernt werden.

#### 12.7.1.14 EmailResponsibleIfPermittedUserIsNotInAuthorizedGroup

Wenn aktiviert, erhalten alle zuständigen Verantwortlichen eine E-Mail, in der die Benutzer aufgeführt sind, die im Access Manager auf einer Ressource Berechtigungen erhalten haben, für die sie per Klassifizierung nicht autorisiert wurden. Dies weist auf eine falsche Rechtevergabe durch einen Entscheider hin und sollte überprüft werden.

#### 12.7.1.15 EnableProfileMembershipRequests

Ist diese Einstellung aktiviert, können Anwender die Mitgliedschaft in einem Benutzerprofil beantragen. Die Beantragung funktioniert analog zu allen anderen Ressourcen-Typen (Verzeichnisse, Sites, Drittelemente…). Ein Profil steht nur dann zur Beantragung zur Verfügung, wenn es manuell (d.h. durch benannte *Profilverantwortliche*) verwaltet wird, nicht jedoch bei automatischer Verwaltung durch eine Synchronisierungsgruppe.

#### 12.7.1.16 ExchangeMailServers

Konfiguriert die Exchange-Server, Zugangsdaten und Datenbanken zum Anlegen von Exchange-Postfächern für AD-Benutzer. Mithilfe des Buttons können Sie die konfigurierte Verbindung vor dem Speichern testen.

#### 12.7.1.17 GlobalAssistantAdGroup

Hier können Sie eine AD-Gruppe angeben, deren Mitglieder im Access Manager die Rolle *Assistent* erhalten – effektiv dürfen dann diese Anwender auch für andere Personen Anträge stellen. Diese Option wird deaktiviert, wenn Option *GlobalAssistantAllUsers* (Kapitel 12.7.1.19) aktiviert ist. Es ist dem *Administrator* weiterhin möglich, einzelnen Anwendern explizit die Rolle *Assistent* zuzuweisen (siehe Kapitel 12.4).

#### 12.7.1.18 GlobalAssistantAdGroupCacheSeconds

Wenn Sie in der o.g. Option eine AD-Gruppe angegeben haben, wartet der Access Manager diese Anzahl an Sekunden, bevor er die Gruppe erneut einliest und die Mitgliederliste aktualisiert.

#### 12.7.1.19 GlobalAssistantAllUsers

Diese Option bestimmt, ob per se alle Anwender die Rolle *Assistent* erhalten – effektiv darf dann jeder Anwender auch für andere Personen Anträge stellen.

#### 12.7.1.20 MailServer

SMTP-Einstellungen für den Mail-Versand. Es öffnet sich ein Popup-Fenster mit weiteren Einstellungen. Aktivieren Sie die Checkbox *Eine Test-E-Mail verschicken*, um eine Mail zu schicken an das Konto, mit dem Sie im Moment angemeldet sind. Dieses Konto muss Emails empfangen können.

#### 12.7.1.21 ManagedLocationDescriptionIsMandatory

Zu jeder verwalteten Ressource kann eine Beschreibung eingegeben werden. Diese Einstellung erzwingt die Eingabe.

#### 12.7.1.22 ManagementConsoleUrl

Die URL der Management Konsole. Diese muss mit einem Slash („/“) enden. Es empfiehlt sich, http Secure zu verwenden.

#### 12.7.1.23 ManualsPath

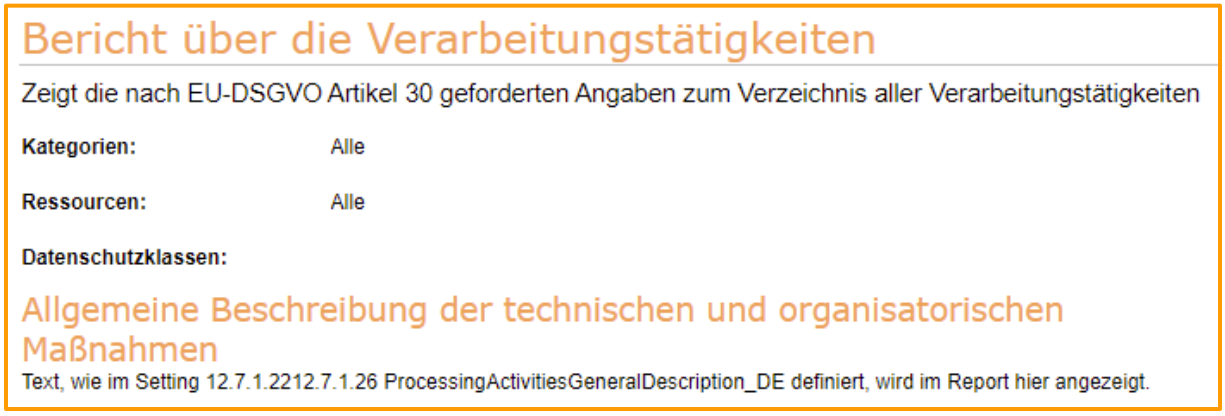
Der Pfad zu den Benutzerhandbüchern, die im Management Portal verlinkt sind. Es kann sich dabei um einen lokalen oder SMB-Pfad handeln – URLs sind nicht möglich. Bitte beachten Sie, dass der Menüpunkt *Handbuch* im Hauptmenü eingeblendet wird, sobald mindestens eine Datei im PDF-Format im angegebenen Pfad gefunden wird. Alle PDF-Dateien werden dann automatisch mit ihrem Dateinamen aufgeführt und zum Download verlinkt.

#### 12.7.1.24 PermissionCommentsAreMandatory

Ist diese Option aktiviert, muss ein Bearbeiter (Verantwortlicher, Administrator) bei der Änderung von Benutzer-Zugriffsrechten einen Kommentar eingeben. Dies umfasst alle Arten von Änderungen: Recht hinzufügen, entfernen, umstellen (z.B. von Lesen nach Schreiben), Ablaufdatum anpassen sowie Benutzer einem Profil hinzufügen / entfernen. Diese Einstellung greift nicht bei Änderungen an Profil-Zugriffsrechten.

#### 12.7.1.25 ProcessingActivitiesGeneralDescription, ProcessingActivitiesGeneralDescription_DE

Der englische und deutsche Text, der in der allgemeinen Beschreibung technischer und organisatorischer Maßnahmen des Berichts *Verarbeitungstätigkeiten einer Ressource* erscheint:


Bericht über die Verarbeitungstätigkeiten

Zeigt die nach EU-DSGVO Artikel 30 geforderten Angaben zum Verzeichnis aller Verarbeitungstätigkeiten

**Kategorien:** Alle

**Ressourcen:** Alle

**Datenschutzklassen:**

Allgemeine Beschreibung der technischen und organisatorischen Maßnahmen

Text, wie im Setting 12.7.1.2212.7.1.26 ProcessingActivitiesGeneralDescription_DE definiert, wird im Report hier angezeigt.

#### 12.7.1.26 ReapprovalMaxDurationInDays

Legt fest, wie lang ein Reapproval-Lauf dauern soll. Wird ein Lauf bspw. alle drei Monate geplant, könnte eine sinnvolle Dauer 30 Tage betragen. Zum Ende der Laufzeit wird automatisch eine Aufgabe geplant, die den Lauf beendet und eine Informationsmail an die betroffenen Besitzer, Verantwortlichen und die Administratoren verschickt.

#### 12.7.1.27 ReapprovalReminderInterval

Hiermit wird der Zeitraum in Tagen zwischen den Erinnerungsmails gesetzt, die an die vom Reapproval betroffenen Verantwortlichen gesendet werden. Es werden innerhalb der zuvor konfigurierten Reapproval-Dauer immer drei Erinnerungsmails versandt. Wird dieses Intervall z.B. auf 7 Tage gesetzt, werden in den ersten drei Wochen die Erinnerungen verschickt sowie – gemäß dem obigen Beispiel – eine weitere Woche später mit Ende des Reapproval-Laufs die Abschlussmail.

#### 12.7.1.28 RequestsCommentsAreMandatory

Falls diese Option aktiviert ist, werden Benutzer zur Eingabe eines Kommentars gezwungen, wenn sie über das Management Portal Anfragen stellen.

#### 12.7.1.29 RevokeOpenPermissionsOnFinishReapproval

Wenn im Rahmen eines Reapproval-Laufs nicht alle Ressourcen von den Verantwortlichen überprüft wurden, können beim Abschluss des Laufs alle nicht bestätigten Berechtigungen automatisch entfernt werden.

#### 12.7.1.30 SelfServicePortalUrl

Die URL des Management Portals. Diese muss mit einem Slash („/“) enden. Es empfiehlt sich, HTTP Secure zu verwenden.

#### 12.7.1.31 UploadPathForImportFiles

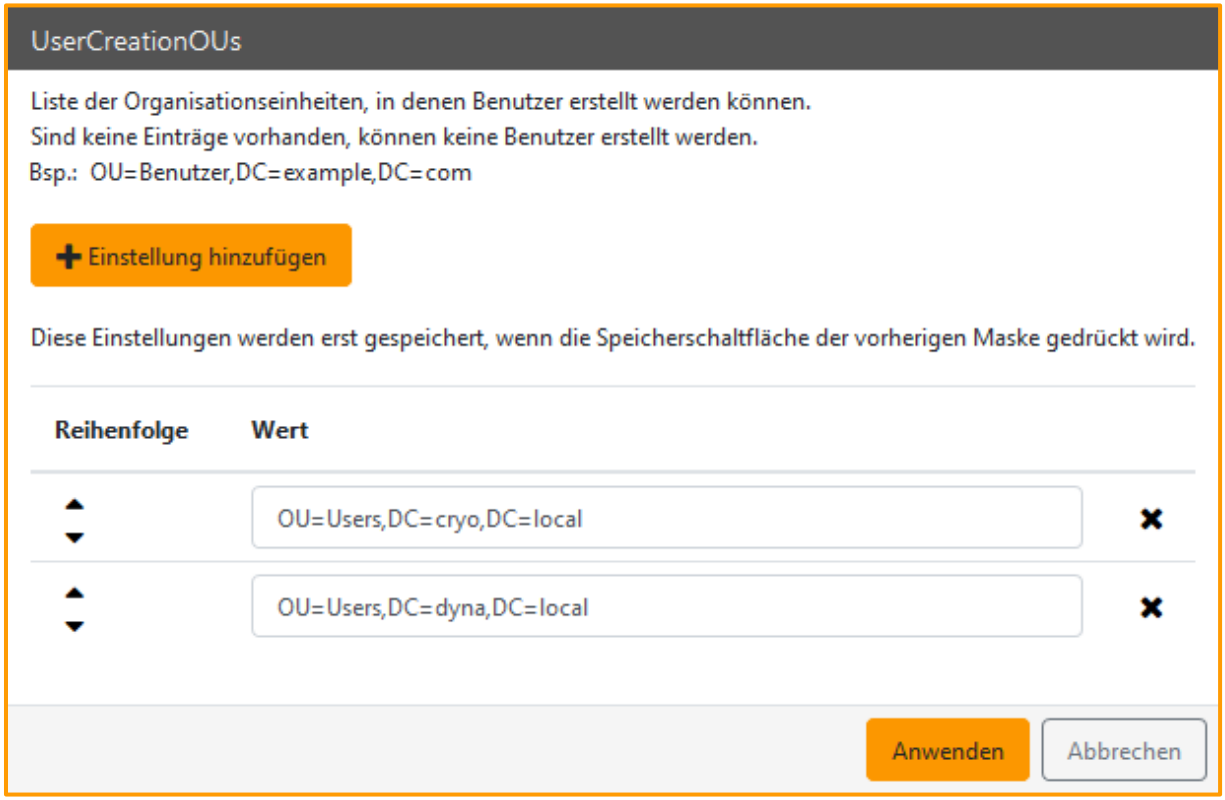
Der Pfad zum Ablegen importierter Share-Daten zur späteren Nachvollziehbarkeit. Diese muss mit einem Backslash ("\") enden.

#### 12.7.1.32 UserCreationJobScheduleTime

Neu erstellte Benutzer befinden sich zunächst im Status „Neu erstellter Benutzer“. Der Job *FinalizeUserCreation* prüft, ob für diesen Benutzer bereits Access Manager-Berechtigungen gesetzt sind, setzt diese um und setzt den Benutzer in den Status „Aktiv“. Dieses Setting bestimmt die Anzahl der Minuten zwischen Neuanlage eines Benutzers und dem Job-Start. Auch der Job *UserCreationScript* wird erst nach dieser Wartezeit gestartet. Mit dieser Wartezeit kann sichergestellt werden, dass die Synchronisation über mehrere DCs abgeschlossen ist, bevor weitere Aktionen vom Access Manager auf dem AD durchgeführt werden.

#### 12.7.1.33 UserCreationOUs

Access Manager bietet beim Anlegen neuer Benutzer über ein Drop-Down-Menu eine Liste der Organisationseinheiten an, in denen ein Benutzerkonto angelegt werden kann. Diese Liste wird hier gepflegt. Über das Symbol wird ein Dialog geöffnet, in dem der Liste OUs hinzugefügt oder aus ihr entfernt werden können.




Ist diese Liste leer, können keine Benutzer angelegt werden, und der Button *Neue Benutzer* wird nicht angezeigt.

*Hier angegebene OUs **müssen** innerhalb einer Domänen-spezifischen Suchbasis liegen (siehe Kap. 12.7.1.11).*

### 12.7.1.34 UserCreationPasswordLength

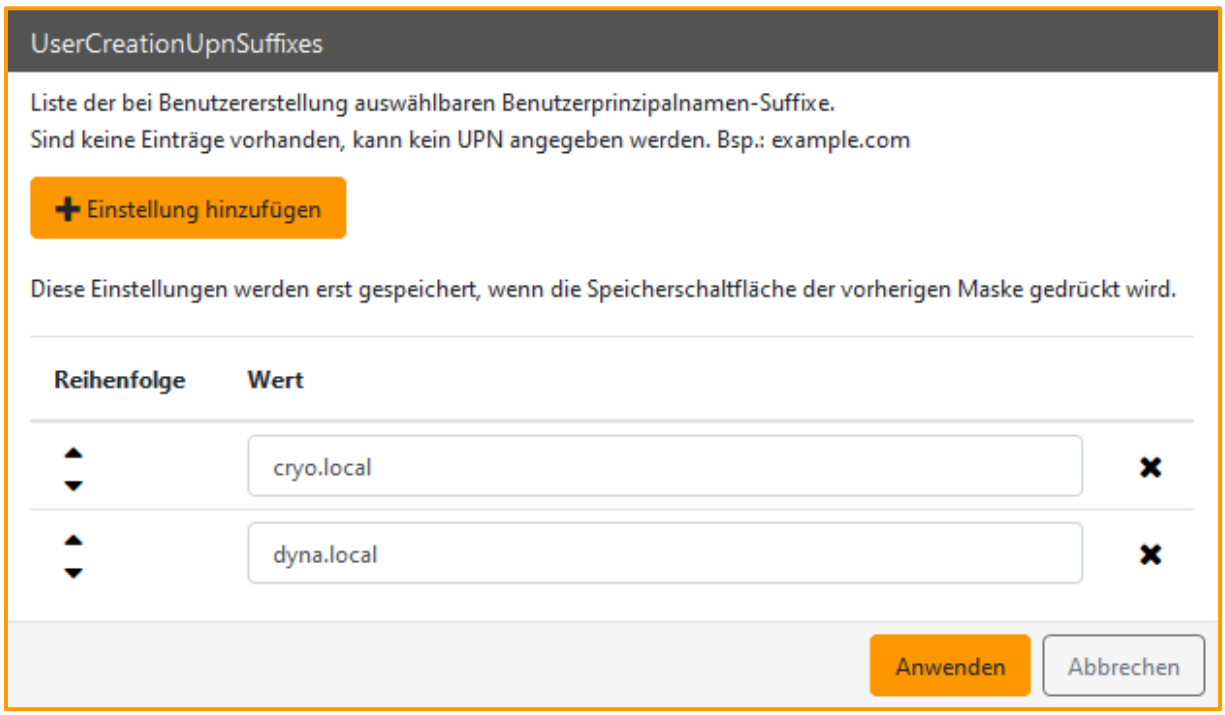
Beim Anlegen neuer Benutzer können Sie automatisch ein Zufallspasswort generieren lassen. Dieses Setting gibt die Länge des zu generierenden Passwortes vor.

### 12.7.1.35 UserCreationScript

Nach der Erstellung eines neuen Benutzerkontos kann ein PowerShell-Skript ausgeführt werden. Geben Sie hier entweder das Skript selbst oder eine Skript-Datei an. Access Manager stellt dabei Variablen zur Verfügung, die im PowerShell Skript verwendet werden können. Diese sind im Editor-Fenster aufgeführt. Bitte beachten Sie die Hinweise für die technische Unterstützung von PowerShell-Skripten im Kapitel 12.2.

### 12.7.1.36 UserCreationUpnSuffixes

Diese Option dient dazu, die bei der Benutzererstellung auswählbaren Suffixe der Benutzerprinzipalnamen (UPN) vor zu konfigurieren. Über das Symbol wird ein Dialog geöffnet, in dem Sie der Liste Benutzerprinzipalnamen-Suffixe hinzufügen oder entfernen können.



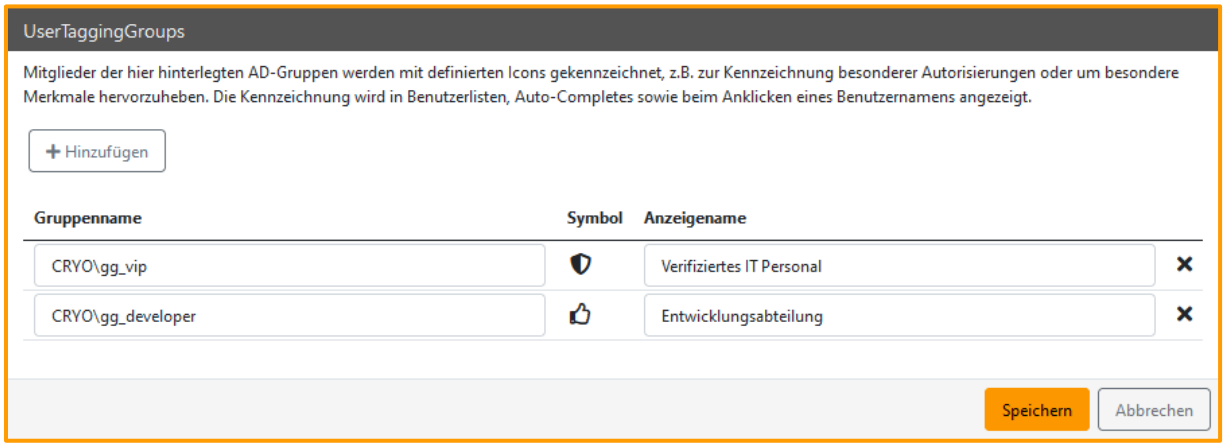

Sind in dieser Liste keine Einträge vorhanden, ist die Option um einen UPN anzugeben nicht vorhanden.

#### 12.7.1.37 UserProfilesDefaultSelfServiceEnabled

Analog zu den entsprechenden Optionen für Verzeichnisse und SharePoint Sites bestimmt diese Einstellung, ob neu erstellte Benutzerprofile standardmäßig für die Beantragung sichtbar sind.

#### 12.7.1.38 UserTaggingGroups

Hier können Sie eine Liste von AD-Gruppen angeben mit einem gewünschten Symbol und einer Beschreibung. Benutzer, die in einer solchen AD-Gruppe Mitglied sind, werden mit dem entsprechenden Symbol gekennzeichnet. Ist ein Benutzer in mehreren Gruppen Mitglied, werden auch die weiteren Symbole angezeigt.



### 12.7.2 Modul „3rd Party Management"

#### 12.7.2.1 ClusterThirdPartyManagementNodesInTrees

Wenn aktiviert, werden alle Elementsammlungen / Elemente unter einem Elementsammlungs-Knoten zusammengefasst. Somit lassen sich alle Elementsammlungseinträge mit einem einzigen Klick auf den Knoten ein- und ausblenden. Diese Gruppierung wird im Management Portal an allen Stellen angewendet, die diese Ressourcen-Typen in einer Liste anzeigen. Die Bezeichnung des Knotens kann über die Einstellung ClusterThirdPartyManagementNodesLabel angepasst werden.

#### 12.7.2.2 ClusterThirdPartyManagementNodesLabel

Geben Sie hier den Namen des o.g. Knotens an.

#### 12.7.2.3 ThirdPartyDefaultSelfServiceEnabled

Standardeinstellung für die Option *Im Self Service anzeigen* beim Anlegen neuer Elemente.

#### 12.7.2.4 ThirdPartyItemAdGroupDescription

Namensvorlage für das Beschreibungsfeld der vom Access Manager erzeugten AD-Gruppen. Diese Beschreibung wird nicht für vorhandene AD-Gruppen verwendet, sondern nur, wenn der AM eine neue AD-Gruppe erzeugt.

### 12.7.3 Modul „Fileserver Management"

#### 12.7.3.1 AdGroupDescription

Namensvorlage für das Beschreibungsfeld der vom Access Manager erzeugten AD-Gruppen. Der Platzhalter {0} wird durch den vollständigen UNC-Pfad ersetzt und der Platzhalter {1} durch die Rechte, die von dieser Gruppe im Dateisystem gewährt werden.

#### 12.7.3.2 AllowMissingFolderRenamingInDatabaseByOwners

Wenn die Aufgabe *InitializeFolderStructureScan* bei der Überprüfung einen verwalteten Ordner nicht findet, wird dieser Ordner im Verzeichnisbaum entsprechend markiert und der Administrator hat die Möglichkeit, diesen Ordner entweder aus dem Access Manager zu entfernen (wenn er sicher ist, dass der Ordner z.B. von außen gelöscht wurde) oder – im Falle einer einfachen Umbenennung – einen anderen Ordner auszuwählen, bei dem es sich um den gesuchten handelt. Diese letztere Möglichkeit kann den Verzeichnisbesitzern mit dieser Option ebenfalls zur Verfügung gestellt werden (siehe Kapitel 4.3.2.4).

#### 12.7.3.3 ClusterFolderManagementNodesInTrees

Wenn aktiviert, werden alle Server / Shares unter einem Verzeichnis-Knoten zusammengefasst. Somit lassen sich alle Servereinträge mit einem einzigen Klick auf den Knoten ein- und ausblenden. Diese Gruppierung wird im Management Portal an allen Stellen angewendet, die diese Ressourcen-Typen in einer Liste anzeigen. Die Bezeichnung des Knotens kann über die Einstellung ClusterFolderManagementNodesLabel angepasst werden.

#### 12.7.3.4 ClusterFolderManagementNodesLabel

Geben Sie hier den Namen des o.g. Knotens an.

#### 12.7.3.5 DefaultBrowseGroupForShares

Vorgeschlagene Browse-Gruppe, wenn ein neues Share eingebunden wird.

#### 12.7.3.6 DefaultCleanUpPeriodInDays

Standardeinstellung für die Anzahl der Tage, die eine Datei unbenutzt bleiben kann, bevor sie durch die Aufgabe "XChangeCleanUp" gelöscht wird.

#### 12.7.3.7 DefaultInheritRights

Standardeinstellung für die Option *Berechtigungen erben* beim Anlegen neuer Berechtigungsverzeichnisse.

#### 12.7.3.8 DefaultSelfServiceEnabled

Standardeinstellung für die Option *Sichtbarkeit im Self Service Portal* beim Anlegen neuer Berechtigungsverzeichnisse.

#### 12.7.3.9 FileserverDefaultPermissionIsWrite

Ist diese Option gesetzt, wird bei der manuellen Vergabe von Dateisystemrechten standardmäßig das Schreibrecht vorgeschlagen, sonst das Leserecht.

#### 12.7.3.10 FolderNameBlacklist

In dieser Liste können Sie komplette Verzeichnisse (UNC-Pfad Notation) oder Verzeichnisteile angeben, die bei einem Verzeichnis-Scan (siehe auch Kapitel 10.6.2.1) bei der weiteren Verarbeitung ignoriert und im Verzeichnisbaum nicht mehr angezeigt werden sollen. Wird ein kompletter Pfad angegeben (z.B. \\filer01\share\folder-01\), so wird nur dieser Pfad (inklusive seiner Unterverzeichnisse) ausgeschlossen. Geben Sie stattdessen nur einen Namensteil an (z.B. \folder-02\), so werden alle Verzeichnisse, die diesen Namensteil enthalten, ausgeschlossen, also etwa \\filer01\share\folder-02\, \\filer01\share\folders\folder-02\, \\filer02\sharename\folder-02\.

**Bitte beachten Sie:**

- Es muss immer ein führender und endender Backslash (\) verwendet werden.
- Alle Pfadangaben beachten die Groß-/Kleinschreibung, d.h. \folder\ wirkt nicht auf ein Verzeichnis „Folder“, nur auf „folder“.
- Die Funktion wirkt nur auf *nicht* verwaltete Verzeichnisse. Berechtigungsverzeichnisse können nicht ignoriert werden, ebenso wie nicht verwaltete Verzeichnisse, unter denen Berechtigungsverzeichnisse existieren.

#### 12.7.3.11 IncludeShareNameInSharePermissionGroups

Anhand dieser Einstellung kann festgelegt werden, ob der Sharename oder die numerische ID des Shares in die Namen der von Access Manager angelegten AD-Shareberechtigungsgruppen eingefügt wird. Eine Änderung dieser Einstellung wirkt sich nicht auf bereits bestehende Shares aus.

#### 12.7.3.12 MaxNestedFolderDepthSSP

Die maximale Verschachtelungstiefe von Berechtigungsverzeichnissen, die im Management Portal von Anwendern angefragt oder vom Besitzer angelegt werden können. Setzen Sie diesen Wert auf '0', um die Verschachtelung zu verhindern. Ein Wert größer als '99' deaktiviert diese Überprüfung. Ein Wert von '1' bedeutet beispielsweise, dass noch ein Berechtigungsverzeichnis unterhalb eines bestehenden Berechtigungsverzeichnisses beantragt werden kann.

#### 12.7.3.13 MaxTokenSize

Die maximal erlaubte Größe eines Kerberos-Tokens. Diese Einstellung wird nur innerhalb des Access Managers verwendet, um Konflikte in der Funktion "MovePermissionsToInferiorLevel" zu vermeiden. Der Wert sollte etwas kleiner als die tatsächliche maximale Token-Größe im AD sein.

#### 12.7.3.14 OwnershipTakeoverAuditOnNewShares

Standardvorgabe für den *Besitzübernahme Modus* (Kapitel 8.2.1.2) im Zusammenspiel mit der Option *OwnershipTakeoverOnNewShares* (Kapitel 12.7.3.16). Hierdurch wird die Protokollierung der Besitzübernahme durch den Access Manager im Dateisystem aktiviert.

#### 12.7.3.15 OwnershipTakeoverAuditUseFullTextSearch

Diese Option wird im Zusammenhang mit der zuvor genannten verwendet und benutzt intern eine Volltextsuche auf der Datenbank, wenn ein Benutzer den Bericht *Besitzübernahme einer Ressource nach Verzeichnis* ausführt und über den Button *Ressource suchen* nach einem Verzeichnispfad sucht. Die Verwendung der Volltextsuche empfiehlt sich, wenn im System sehr viele Dateien (über eine Million) auditiert wurden. Nach Aktivierung der Option müssen Sie einmalig ein Suchindex durch das Zahnrad-Symbol erstellen lassen.

Technisch bedingt unterscheidet sich das Suchverhalten nach auditierten Verzeichnissen für den Anwender bei Verwendung des Reports: Bei aktivierter Volltextsuche werden gesuchte Pfadnamensteile nur jeweils am Beginn eines Verzeichnisnamens gefunden. Ohne Volltextsuche werden sie auch innerhalb der Verzeichnisnamen gefunden.

---

*Technische Voraussetzung für die Verwendung der Volltextsuche ist das optionale Paket zur Volltextsuche auf dem Datenbankserver.*

---

#### 12.7.3.16 OwnershipTakeoverOnNewShares

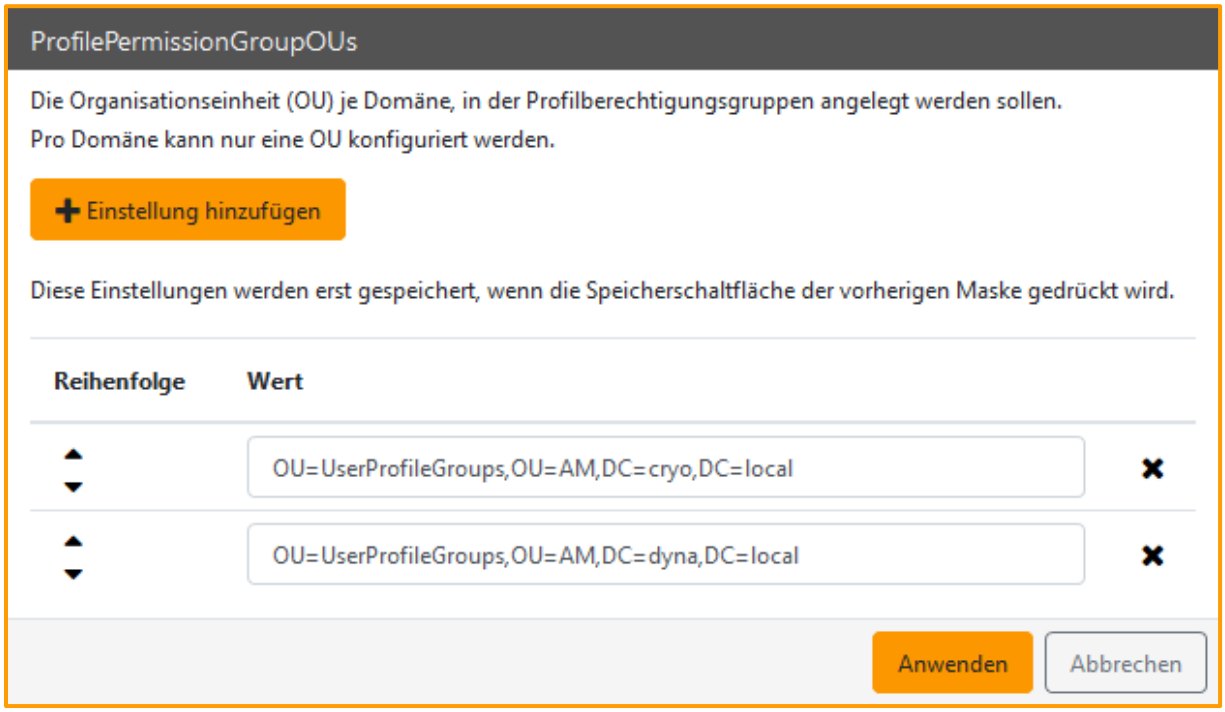
Standardvorgabe für den *Besitzübernahme Modus* (Kapitel 8.2.1.2) im Zusammenspiel mit der Option *OwnershipTakeoverAuditOnNewShares* (Kapitel 12.7.3.14). Hierdurch wird die Besitzübernahme durch den Access Manager im Dateisystem aktiviert.

#### 12.7.3.17 ProfilePermissionGroupNamingPatternGlobal, ProfilePermissionGroupNamingPatternLocal

Werden für Profile eigene AD-Gruppen verwendet (siehe vorige Einstellung), legen diese beiden Einstellungen fest, nach welchem Namensschema die zu erstellenden Gruppen benannt werden. Der Parameter {0} wird dabei durch die Domäne ersetzt, in der der Fileserver des berechtigten Verzeichnisses steht. Parameter {1} ist ein Zähler, der automatisch für jede neue Profilberechtigungsgruppe inkrementiert wird. Um eindeutige Gruppennamen im AD zu gewährleisten, sind beide Parameter zwingend erforderlich.

#### 12.7.3.18 ProfilePermissionGroupOUs

Wenn Sie Benutzerprofilgruppen für die Berechtigungsvergabe verwenden, regelt diese Einstellung, in welcher OU sie gespeichert werden. Geben Sie für jede Domäne, in der durch den Access Manager verwaltete Fileserver liegen, genau eine OU an.




Wenn der Profiladministrator später ein Benutzerprofil auf das Verzeichnis eines Servers in der Domäne CRYO berechtigt, wird das System entsprechende Profilgruppen in der OU dieser Domäne erzeugen; kommt noch ein weiteres Verzeichnis von einem Server in der Domäne DYNA hinzu, werden in der zugehörigen anderen Domänen-OU ebenfalls Profilgruppen angelegt. Profilmitglieder (Benutzerkonten) werden dann entsprechend ihrer Domänenzugehörigkeit in der lokalen bzw. globalen Profilgruppe der jeweiligen Domänen-OU eingetragen.

### 12.7.3.19 ProfilePermissionGroupsEnabled

Diese Option entscheidet bei der Berechtigungsvergabe durch *Profile* über die Verwendung von eigens für die Benutzerprofile erstellten AD-Gruppen als Standardverfahren (im Gegensatz zum bisherigen Verfahren über Verzeichnisberechtigungsgruppen). Weitere Informationen zu diesen Verfahren finden Sie im Kapitel 12.3.

Alle Benutzerprofile, die nach der Umschaltung dieser Option erstellt werden, folgen der eingestellten Berechtigungstechnik. Zuvor erstellte Profile funktionieren weiterhin nach der alten Technik und werden mit einem entsprechenden Hinweis versehen und können, falls gewünscht, manuell auf die neue Logik umgestellt werden. Diese Umstellung wirkt sich jeweils auch auf die angewandte Technik bei bereits vorhandenen Berechtigungen aus. Dadurch ist für verschiedene Profile der gleichzeitige Einsatz beider Techniken möglich. Der Profiladministrator erhält bei der Verwaltung der Profile einen Hinweis, wenn ein Profil nicht nach dem hier eingestellten Standardverfahren arbeitet. Die Einstellungen für das Benennungsschema der Profil-AD-Gruppen werden im Folgenden erklärt. Die Gruppen werden erzeugt, sobald ein Benutzerprofil auf mindestens einem Verzeichnis berechtigt wird. Wo die AD-Gruppen gespeichert werden, regelt die Einstellung *ProfilePermissionGroupOUs*.

Wird ein Benutzerprofil vom Profiladministrator gelöscht, werden die zugehörigen Profilgruppen in der AD automatisch ohne Nachfrage ebenfalls gelöscht, nachdem sie auf den betroffenen Verzeichnissen nicht mehr berechtigt sind.

---

*Profilgruppen sollten nicht außerhalb des Access Manager für eigene Zwecke verwendet werden.*

---

**Sonderfall bei der Verwendung einer Klassifizierung mit der Option *Gruppe autorisierte Benutzer*:**

Wie am Ende von Kapitel 7.2 beschrieben, kommt es mit Profilgruppen zu unterschiedlichen Verzeichnisberechtigungen ggü. deren Nicht-Verwendung, wenn in einem Profil mindestens ein Verzeichnis enthalten ist, welches die möglichen zu berechtigenden Benutzer auf Basis einer Klassifizierung mit einer autorisierten Nutzergruppe einschränkt.

### 12.7.3.20 RegexFolderNameValidation

Validierungsregel für neue Verzeichnisnamen. Zur Anpassung an eigene Erfordernisse empfehlen wir Kenntnisse über Reguläre Ausdrücke.

Sollen bspw. zusätzlich Leerzeichen und deutsche Umlaute erlaubt werden sowie eine Namenslänge zwischen 2 und 30 Zeichen, verwenden Sie diesen Ausdruck:

```
^[A-Za-zÄÖÜäöüß0-9-_]([ ]?[A-Za-zÄÖÜäöüß0-9-_]){1,29}$
```

### 12.7.3.21 RegexFolderNameValidationText, RegexFolderNameValidationText_DE

Der englische und deutsche Fehlertext, der angezeigt wird, falls die Validierung eines Verzeichnisnamens fehlschlägt.

#### 12.7.3.22 ResponsiblesInfoFileName

Der Name der Info-Datei, die im Elternverzeichnis eines Berechtigungsverzeichnisses abgelegt wird und die Verantwortlichen der Rechtezuweisung enthält. Gibt es mehr als ein Berechtigungsverzeichnis im Elternverzeichnis (d.h. mehrere Berechtigungsverzeichnisse liegen parallel zueinander auf derselben Ebene), werden die jeweiligen Verzeichnis-Informationen in der angegebenen Datei zusammengefasst.

#### 12.7.3.23 RetainADGroupsAfterRightsFolderRevocation

Falls diese Option aktiviert ist, wird die Zuordnung von AD-Gruppen im Dateisystem beibehalten, nachdem einem Verzeichnis der Berechtigungsverzeichnisstatus entzogen wurde.

#### 12.7.3.24 SkipDirectoriesWithReparsePoints

Das Aktivieren dieser Option verhindert, dass die Aufgabe MaintainAccessPermissions (incl. sub-objects) (siehe Kapitel 10.6.2.3) sog. Junctions / ReparsePoints, die auf ein anderes Verzeichnis verweist, folgt. Dadurch wird der Problemfall vermieden, dass die Prüfung in eine Endlosschleife läuft, wenn versehentlich Junctions im Kreis auf sich selbst verweisen.

## 12.7.4 Modul „SharePoint Management“

### 12.7.4.1 ClusterSharePointManagementNodesInTrees

Wenn aktiviert, werden alle SiteCollections / Sites unter einem SharePoint-Knoten zusammengefasst. Somit lassen sich alle SharePoint-Einträge mit einem einzigen Klick auf den Knoten ein- und ausblenden. Diese Gruppierung wird im Management Portal an allen Stellen angewendet, die diese Ressourcen-Typen in einer Liste anzeigen. Die Bezeichnung des Knotens kann über die Einstellung ClusterSharePointManagementNodesLabel angepasst werden.

### 12.7.4.2 ClusterSharePointManagementNodesLabel

Geben Sie hier den Namen des o.g. Knotens an.

### 12.7.4.3 SharePointDefaultPermission

Mit dieser Option wird bei der manuellen Vergabe von SharePoint-Rechten standardmäßig das eingegebene Recht, z.B. *write*, vorgeschlagen.

### 12.7.4.4 SharePointDefaultSelfServiceEnabled

Standardeinstellung für die Option *Im Self Service anzeigen* beim Anlegen neuer verwalteter Sites.

### 12.7.4.5 SharePointGroupDescription

Namensvorlage für das Beschreibungsfeld der vom Access Manager erzeugten SharePoint-Gruppen. Der Platzhalter {0} wird durch die vollständige URL ersetzt und der Platzhalter {1} durch die Rechte, die von dieser Gruppe in SharePoint gewährt werden.

### 12.7.4.6 SharePointOnlineDomainMap

Ordnet NETBIOS-Namen zu DNS-Namen zu, um Benutzer-IDs in ein SharePoint Online kompatibles Format zu übersetzen. Konfigurieren Sie beispielsweise DOMAIN:mydomain.onmicrosoft.com, so wird DOMAIN\user.name zu user.name@mydomain.onmicrosoft.com. Mehrere NETBIOS:DNS-Paare können mit ";" getrennt konfiguriert werden. Bitte beachten Sie, dass nur eine 1:1 Zuordnung erlaubt ist. Das bedeutet, Sie können den gleichen NETBIOS-Namen nicht mehreren verschiedenen DNS-Namen zuordnen oder anders herum.

### 12.7.4.7 SharePointSiteNameValidationRegEx

Validierungsregel für Namen von neuen / umbenannten SharePoint-Sites. Wird nicht verwendet beim Anlegen einer neuen Website-Sammlung.

## 12.7.5 Modul „Fileserver Accounting“

### 12.7.5.1 CostCenterLdapFilter

LDAP-Filterausdruck zur Ermittlung der relevanten Einträge aus dem Verzeichnis.

### 12.7.5.2 CostCenterLdapPass

Passwort für den LDAP-Zugriff.

### 12.7.5.3 CostCenterLdapProperty

LDAP-Eigenschaft, die den Kostenstellennamen enthält.

### 12.7.5.4 CostCenterLdapString

Der LDAP-Server für den Import der Kostenstellen. Das Format ist LDAP://server:portnummer

### 12.7.5.5 CostCenterLdapUser

Benutzername für den LDAP-Zugriff.

### 12.7.5.6 DefaultPricingItemId

Standard-Kalkulationsposition für neue Abrechnungsverzeichnisse.

### 12.7.5.7 ExportPath

Pfad zum Ablegen der Abrechnungsdaten nach einem erfolgreichen Abrechnungslauf.

### 12.7.5.8 GroupExportData

Die Vorlage für die Exportdatei der gruppenbezogenen Abrechnungsdaten. Vom Access Manager bereitgestellte Variablen beginnen mit einem Dollar-Zeichen ($). Jede Spalte wird mit einem Semikolon von der nächsten getrennt.

### 12.7.5.9 NoChargeBelow

Keine Inrechnungstellung der Kosten, wenn der berechnete Betrag unterhalb dieses Werts liegt (in €).

### 12.7.5.10 UserExportData

Vorlage für die Exportdatei der benutzerbezogenen Abrechnungsdaten. Vom Access Manager bereitgestellte Variablen beginnen mit einem Dollar-Zeichen ($). Jede Spalte wird mit einem Semikolon von der nächsten getrennt.

### 12.7.6 Modul „Password Reset“

Da dieses Modul auch unabhängig von Access Manager verwendet werden kann, wird die Funktionalität in einem eigenen Handbuch beschrieben. Für die Einbindung in AM existieren diese Parameter:

#### 12.7.6.1 PasswordResetApiKey

Der Autorisierungsschlüssel des Produkts AMPR, mit dem sich der Access Manager legitimiert. Dieser Schlüssel wird vom AMPR zur Verfügung gestellt.

#### 12.7.6.2 PasswordResetApiTimeoutMs

Wartezeit für Anfragen an die AMPR-Schnittstelle in Millisekunden.

#### 12.7.6.3 PasswordResetClientUrl

Die Adresse, unter der die Webseite des AMPR angezeigt wird. Diese wird in die Anzeige des Access Manager integriert.

#### 12.7.6.4 PasswordResetServerUrl

Die Adresse der AMPR Programmierschnittstelle (API).

### 12.7.7 Modul „Easy Desktop“

Dieses Modul erweitert die Beantragungsfunktionalität auf die Client-Rechner der Anwender und muss dort installiert werden. Zur Verwendung existiert ein eigenes Handbuch. Für die Konfiguration auf AM-Seite existieren diese Parameter:

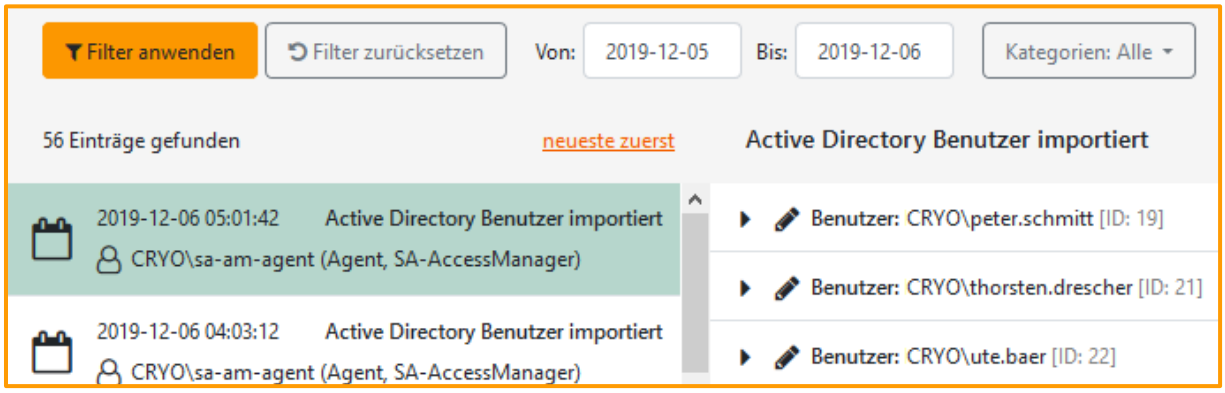
#### 12.7.7.1 EasyDesktopEnabled

Hiermit kann die Funktion zur Beantragung von Rechten und Verzeichnissen auf dem Client generell ein- und ausgeschaltet werden.

#### 12.7.7.2 EasyDesktopManualPath

Ruft der Anwender im Easy Desktop Kontextmenü den Punkt „Hilfe“ auf, wird die hier spezifizierte Ressource geöffnet. Es kann sich dabei um einen beliebigen Typ handeln (Webadresse, Textdokument, Video etc.), es sollte jedoch sichergestellt werden, dass die Adresse vom Client erreichbar ist.

# 12.8 Audit


Die Seite *Audit* bietet eine mehrstufige Auflistung aller im Access Manager durchgeführten Aktionen. Hier können Sie im Detail nachvollziehen, welche Aktivitäten zu welchem Zeitpunkt ausgeführt wurden, wer sie veranlasst hat und welche Objekte betroffen waren. Zur Steigerung der Übersicht und zum schnellen Finden bestimmter Informationen stehen Ihnen Filter und Sortierung zur Verfügung.

Der Aufbau der Seite untergliedert sich in drei Bereiche:

- Oben: Filtereinstellungen
- Links: Liste der durchgeführten Aktivitäten
- Rechts: Details einer ausgewählten Aktivität

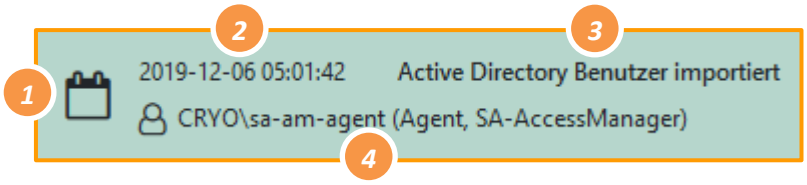
## 12.8.1 Filtereinstellungen

Die Filterzeile bietet die Möglichkeit die anzuzeigenden Aktivitäten auf einen Zeitraum einzuschränken (Von-Bis Angaben). Da alle Aktivitäten einer bestimmten Kategorie zugeordnet sind, lassen sich die einzelnen Kategorien an- und abwählen (DropDown-Liste *Kategorien*). Nach Einstellung der gewünschten Kriterien klicken Sie den Button *Filter anwenden*.

Mit dem Button *Filter zurücksetzen* werden alle Filtereinstellungen wieder auf die Standardwerte gesetzt, d.h. der Zeitraum umfasst nur den gestrigen Tag und alle Kategorien werden aktiviert.

### 12.8.2 Liste der Aktivitäten

Alle Aktivitäten, die den eingestellten Filterkriterien entsprechen, werden in diesem Bereich aufgeführt. Jeder Eintrag zeigt dabei folgende Informationen an:

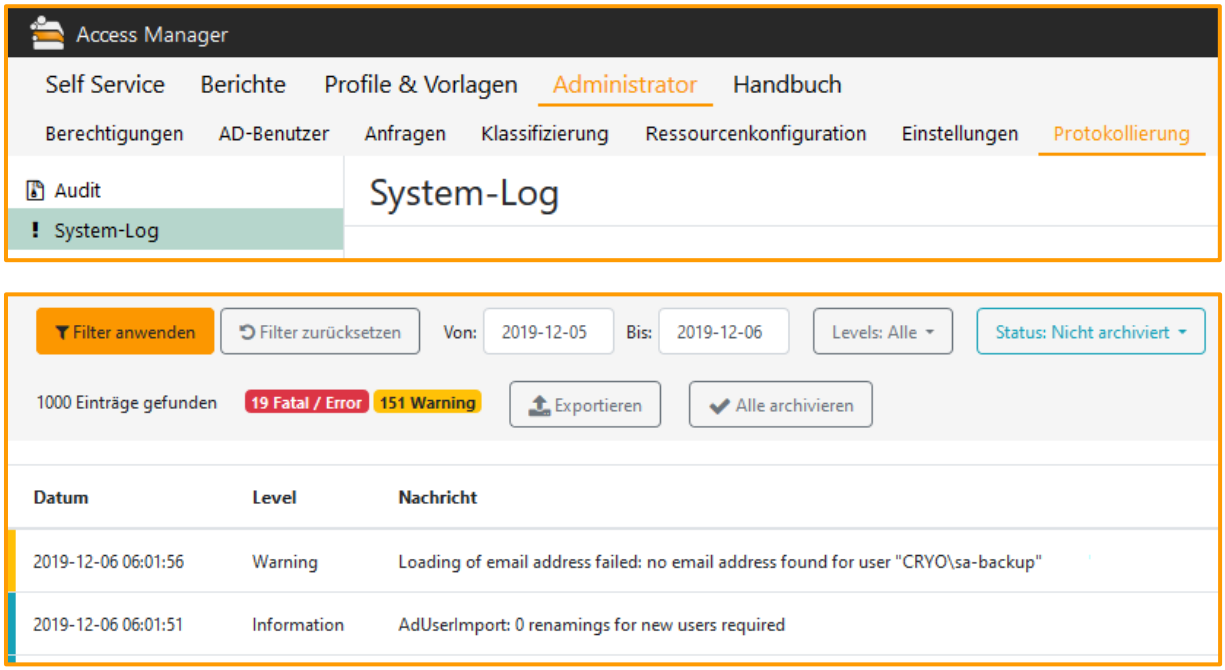



1) Das Symbol zeigt an, ob die Aktivität manuell durch eine Benutzeraktion oder automatisch durch eine geplante Aufgabe ausgelöst wurde.
2) Datum und Uhrzeit (Weltzeit, UTC) der Aktivität.
3) Die Kategorie der Aktivität.
4) Das Benutzerkonto, welches die Aktivität ausgelöst hat.

### 12.8.3 Details der Aktivitäten

Dieser Bereich enthält eine Liste aller Objekte, die von der zuvor ausgewählten Aktivität betroffen waren. Jedes Objekt lässt sich anklicken und erweitert dann die Anzeige um eine Tabelle, welche für die veränderten Objekteigenschaften den neuen und alten Wert enthalten.

# 12.9 Error Logging




Auf der Seite *System-Log* werden alle Fehler und Meldungen des Systems mit Zeitstempel, Kritikalität und Beschreibung aufgelistet.

Eine Meldung kann *Archiviert* werden, indem Sie ihre Checkbox anklicken. Dadurch verschwindet sie sofort aus der Anzeige, kann aber über die Auswahl des *Status: Archiviert* wieder angezeigt werden. Die Schaltfläche *Alle archivieren* markiert auf Nachfrage alle für die aktuellen Filtereinstellungen gefundenen Einträge.

Mithilfe der Schaltfläche *Exportieren* erstellen Sie eine CSV Datei mit den für die aktuellen Filtereinstellungen gefundenen Einträge. Bei Problemen können Sie diese Datei dem Support-Mitarbeiter der BAYOONET AG zur Verfügung stellen.

---

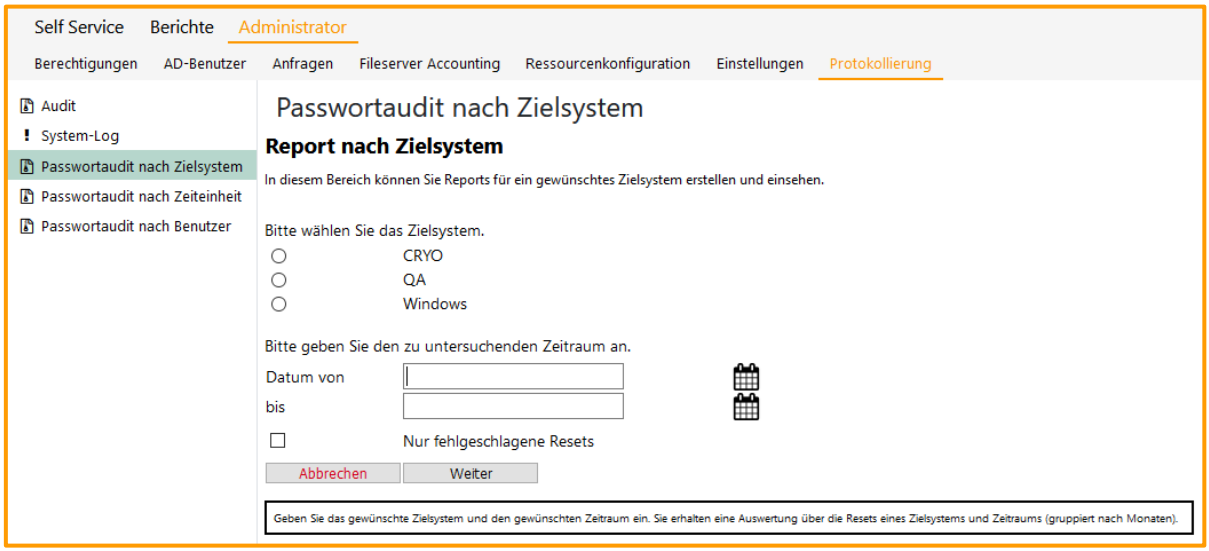
*Bitte beachten Sie, dass die Fehler-Datei vertrauliche Daten Ihres Unternehmens enthalten kann.*

---

## 12.10 Passwort Audit

Setzen Sie das zusätzliche Produkt AMPR ein und haben Sie die *AMPR-Rolle Administrator*, stehen Ihnen im Administrator-Bereich *Protokollierung* zusätzliche Auditierungsmöglichkeiten zur Verfügung. Sie können sich hier Berichte über alle Passwort-bezogenen Aktivitäten für einen einstellbaren Zeitraum ausgeben lassen. Das Audit umfasst die Fokussierung auf:

- Passwortaudit nach Zielsystem
- Passwortaudit nach Zeiteinheit
- Passwortaudit nach Benutzer




*Diese Menüpunkte stellen die Funktionen des Programms AMPR zur Verfügung.*
*Eine Beschreibung aller Funktionen finden Sie im zugehörigen AMPR-Handbuch.*

# 13 Anpassungsmöglichkeiten der Oberfläche

Access Manager bietet die Möglichkeit die Benutzungsoberfläche den eigenen Wünschen anzupassen.

Die Gestaltung der Oberfläche ist mit etablierten Web-Technologien wie HTML, CSS und JavaScript umgesetzt und bietet die Möglichkeit, den vorhandenen Stil zu überschreiben. Kenntnisse im Umgang mit den genannten Technologien sind dafür Voraussetzung. Auf Wunsch kann die BAYOONET AG beauftragt werden, solche Anpassungen für Sie durchzuführen bzw. Sie bei der Umsetzung zu unterstützen.

*Bitte beachten Sie, dass kundenseitige Anpassungen nicht vom Support abgedeckt sind und immer auf eigene Verantwortung erfolgen. Es kann nicht garantiert werden, dass Ihre Anpassungen nach einem System-Update noch funktionieren; ggf. muss der Code an die neue Version angepasst werden.*

## 13.1 Dateien und Speicherorte

Oberflächenänderungen für das Management Portal werden auf dem AM-Server im Installationsverzeichnis des IIS vorgenommen. Haben Sie bei der Installation das Standard-Installationsverzeichnis beibehalten, lautet das lokale Verzeichnis auf dem Server

`C:\inetpub\wwwroot\AccessManager\ssp\wwwroot`

Hier befindet sich das Verzeichnis `Customization` und darin eine Textdatei namens `custom.css` für die grafischen Überschreibungen sowie eine `custom.js`, mit der eigener JavaScript-Code injiziert werden kann. Diese Dateien können mit einem einfachen Texteditor bearbeitet werden.

Für eigene Ressourcen wie etwa ein Firmen-Logo existiert ein weiteres Verzeichnis, `Images`, unterhalb von `Customization`.

Die folgenden Abschnitte beschreiben einige Beispiele, wie die Datei `custom.css` zu bearbeiten ist um etwa das Access Manager Logo durch ein eigenes Firmen-Logo zu ersetzen oder bestimmte Masken auszublenden.

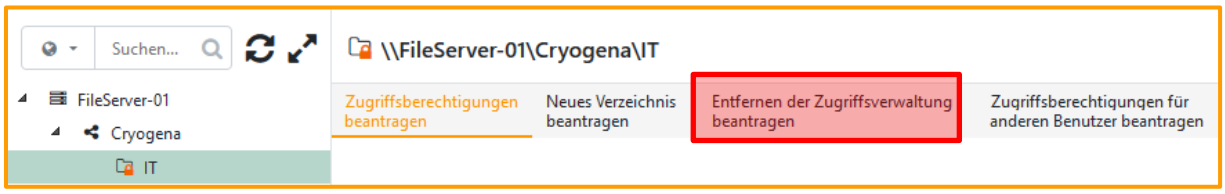
## 13.2 Eigenes Firmenlogo

Das Logo wird immer mit einer Höhe von 22 Pixel dargestellt, die Breite wird im Seitenverhältnis dazu skaliert. Um die Dateigröße möglichst klein und damit auch die Ladezeit der Webseite kurz zu halten, empfiehlt es sich, die Bilddatei zuvor in einem Grafikprogramm auf diese Höhe herunter zu skalieren. Notieren Sie die daraus resultierende Breite. Kopieren Sie die Bilddatei (Format: *.png) z.B. mit dem Namen `company_header_logo.png` in das Images-Verzeichnis und tragen Sie folgendes in die `custom.css` ein:

```
.main-header-logo {
  background-image:url(/Customization/Images/company_header_logo.png)
!important;
  width: 77px !important;
  background-repeat: no-repeat;
  background-size: contain;
}
```

Ersetzen Sie die rot markierte Zahl (77) durch die zuvor notierte Bildbreite. Die Einheit „px“ ist erforderlich und muss wie in dem Beispiel direkt auf die eingetragene Zahl folgen.

## 13.3 Ausblenden einzelner Anzeige-Elemente




Die Option *Entfernen der Zugriffsverwaltung beantragen* erscheint normalerweise beim Anwählen einer verwalteten Ressource.

Mit diesem Code wird die Option für Berechtigungs**verzeichnisse** ausgeblendet:

```
li[aria-controls="delete-folder"] {
  display:none !important;
}
```

Bei Anfragen zu **SharePoint Sites** lautet der Code wie folgt:

```
li[aria-controls="deleteSite"] {
  display:none !important;
}
```

## 13.4 Funktionserweiterung mit JavaScript

Während Sie in der Datei `custom.css` das *Aussehen* der Oberfläche anpassen, haben Sie mit der `custom.js` die Möglichkeit, *funktionale* Erweiterungen und Veränderungen zu implementieren – hierzu zählen übrigens auch Textänderungen in der Oberfläche. In dieser Datei sind bereits einige häufig benötigte Standardfunktionen vordefiniert, die Sie für Ihre Zwecke weiterverwenden können.

**Neben reinem JavaScript / ECMA-Script (Version ist Browser-abhängig) wird jQuery in der Version 3.6.0 unterstützt.**

---

*Zur sicheren Abgrenzung eigener Funktionen dient der eigene Scope „custom“. Alle Funktionen und Variablen müssen diesen verwenden. Die werkseitig ausgelieferte Datei definiert den Scope. Fügen Sie hier Ihren Custom-Code ein.*

---

Rufen Sie dann Ihre Funktionen in der `document.ready()` Funktion auf.

# 13.5 Anpassung von Berichten

## 13.5.1 Eigenes Logo

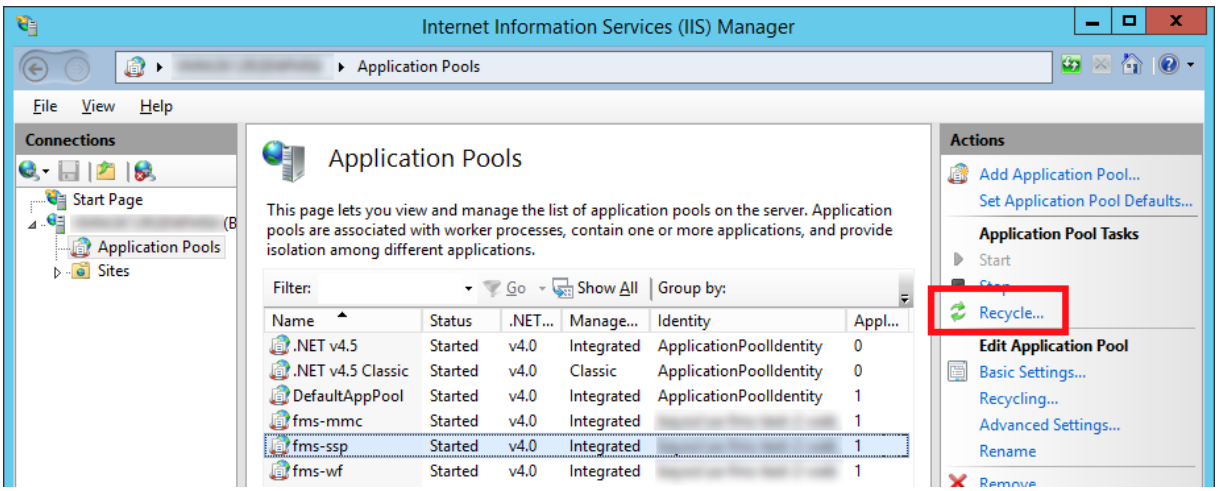
Für Berichte können Sie den standardmäßigen BAYOOSOFT Schriftzug oben rechts durch Ihr eigenes Firmenlogo ersetzen. Das Access Manager-Logo unten links kann **nicht** ersetzt werden.

Für den Austausch benötigen Sie eine Grafikdatei im PNG-Format mit dem festen Namen `report-header-logo.png`. Die beste Darstellung Ihrer Grafik erhalten Sie bei einem Seitenverhältnis von 4:1 (Breite:Höhe). Bilder mit anderem Formfaktor werden unter Beibehaltung des Seitenverhältnisses entsprechend skaliert.

Kopieren Sie Ihre so vorbereitete Datei auf dem AM-Server in das Verzeichnis:

`C:\inetpub\wwwroot\AccessManager\ssp\wwwroot\Customization\Images`

Das Logo steht in allen Berichten zur Verfügung, nachdem Sie den Application Pool *fms-ssp* im IIS des AM-Servers recycled haben:




## 13.5.2 Anpassung von Farben, Schriftarten, Layout

Eine kundenseitige Anpassung des Aussehens (z.B. Schrift-, Hintergrund- und Rahmenfarben) wird zurzeit nicht unterstützt. Wenn Sie eine Anpassung benötigen, sprechen Sie unser Vertriebsteam an.

# 14 Beispiele für eigene PowerShell Skripte

PowerShell-Skripte können sehr viele verschiedene Aufgaben übernehmen, der konkrete Einsatzzweck hängt von den Kundenanforderungen ab. Sofern Sie in Ihrem Skript auf externe Systeme mit anderen Anmeldedaten zugreifen müssen, sollten Sie diese aus Sicherheitsgründen nicht unverschlüsselt im Skript hinterlegen.

*Bitte beachten Sie, dass kundenseitige Anpassungen nicht vom Support abgedeckt sind und immer auf eigene Verantwortung erfolgen. Es kann nicht garantiert werden, dass Ihre Anpassungen nach einem System-Update noch funktionieren; ggf. muss der Code an die neue Version angepasst werden.*

*Die BAYOONET AG übernimmt keine Verantwortung für Fehler, Defekte und Datenverluste, die durch den Einsatz kundeneigener Skripte entstehen.*

## 14.1 Ausführung nach Anlegen eines AD-Benutzerkontos

Dieses Beispiel zeigt eine Debug-Ausgabe in eine Log-Datei mit Prüfung der vom AM übergebenen Variablen, wenn Sie als Administrator einen neuen Benutzer im AD angelegt haben. Speichern Sie das Skript als Datei (z.B. mit dem Namen `Create-AD-User-Logging.ps1`) auf dem Agent-Server der *Default* Agent-Gruppe und rufen Sie es in den administrativen Einstellungen auf (siehe Kapitel 12.7.1.35).

```
$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
```