Grouper - Gruppenverwaltung für die Universität Ulm

Als Erweiterung des IDM bietet Grouper allen Eigentümern einer Organisationseinheit die Möglichkeit, eigenständig eigene Gruppen anzulegen und zu verwalten. Diese Gruppen stehen dann zur individuellen Rechtevergabe in diversen Zielsystemen zur Verfügung.

Den Login-Link finden Sie hier: Anmeldung

In der Zentralen Universitätsverwaltung wird Grouper für das Management der Berechtigungen der Gruppenlaufwerke O: und S: verwendet.

Ausgangssituation

Bisher wurden auf dem Fileserver der Zentralen Universitätsverwaltung (o: und s: Laufwerk) die Zugriffsberechtigungen über Gruppenmitgliedschaften und individuellen Benutzerrechten realisiert. Die Gruppen wurden vom kiz gepflegt, die individuellen Berechtigungen von den Beschäftigten der ZUV.

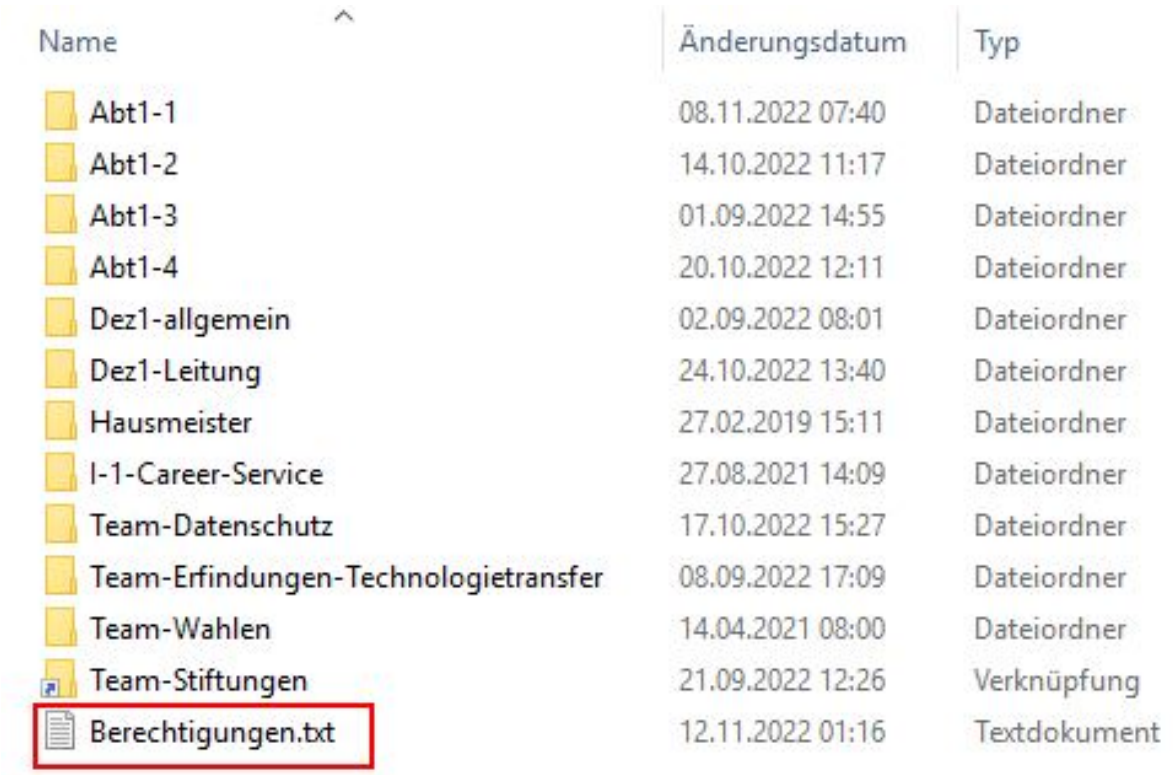
Neue Situation

Mit der Einführung von Grouper haben die Beschäftigten der ZUV selbst die Möglichkeit Gruppenmitgliedschaften zu pflegen. Zugriffsberechtigungen auf Ordner werden ausschließlich über Gruppen geregelt. Individuelle Benutzerrechte werden abgeschafft.

- Initial werden die Dezernats- und Abteilungsleitenden aus dem IDM übernommen. Alle anderen Beschäftigten müssen explizit in die Gruppen aufgenommen werden.
- Die Verwaltung der Gruppen kann an Beschäftigte der ZUV delegiert werden.
- Für jede Abteilung gibt es Ansprechpartner, die Beschäftigte in die gewünschte Gruppe aufnehmen können. Die Ansprechpartner stehen in der Datei **Berechtigungen.txt**, die auf dem File-Server auf der Ebene der Abteilungsordnern oder in den Abteilungsordnern steht.
- Für jeden dieser Ordner steht eine Gruppe in Grouper zur Verfügung.
- Neue Ordner und die dazugehörigen Gruppen können bei Bedarf über ein Ticket angefordert werden. Dazu ist nur die Dezernatsleitung berechtigt.
- In allen Ordnern, in denen eine Datei **Berechtigungen.txt** steht, gibt es nur Lese-Rechte. Nur Administratoren dürfen schreiben.
- In den Abteilungsordnern haben i.d.R die Mitglieder der Berechtigten Gruppe Schreib-Lese-Rechte. Ausnahmen, wie **o:\zuv\Allgemein\bilder**, stehen in der Datei **Berechtigungen.txt**. In diesem Fall dürfen alle lesen.
- Ordner, deren Inhalt von allen gelesen werden kann, enthalten die Datei **hier-kann-JEDER-lesen.txt**.
- Die Verwaltenden einer Gruppe sind dafür verantwortlich, dass Mitglieder, die keinen Ordner-Zugriff mehr haben dürfen, aus den entsprechenden Gruppen entfernt werden.
- Nach dem Verlassen der Universität wird ein Benutzer nach einer gewissen Zeit automatisch gelöscht. Damit erlöschen auch seine Gruppenberechtigungen.
- Bei einem Arbeitsplatzwechsel innerhalb der Universität bleibt die Gruppenmitgliedschaft erhalten! Hier muss manuell eingegriffen werden.
- Gruppenmitgliedschaften können zeitlich befristet vergeben werden. Das bietet sich bei Auszubildenden und Studentischen Hilfskräften an.

Berechtigungen für den File-Server vergeben

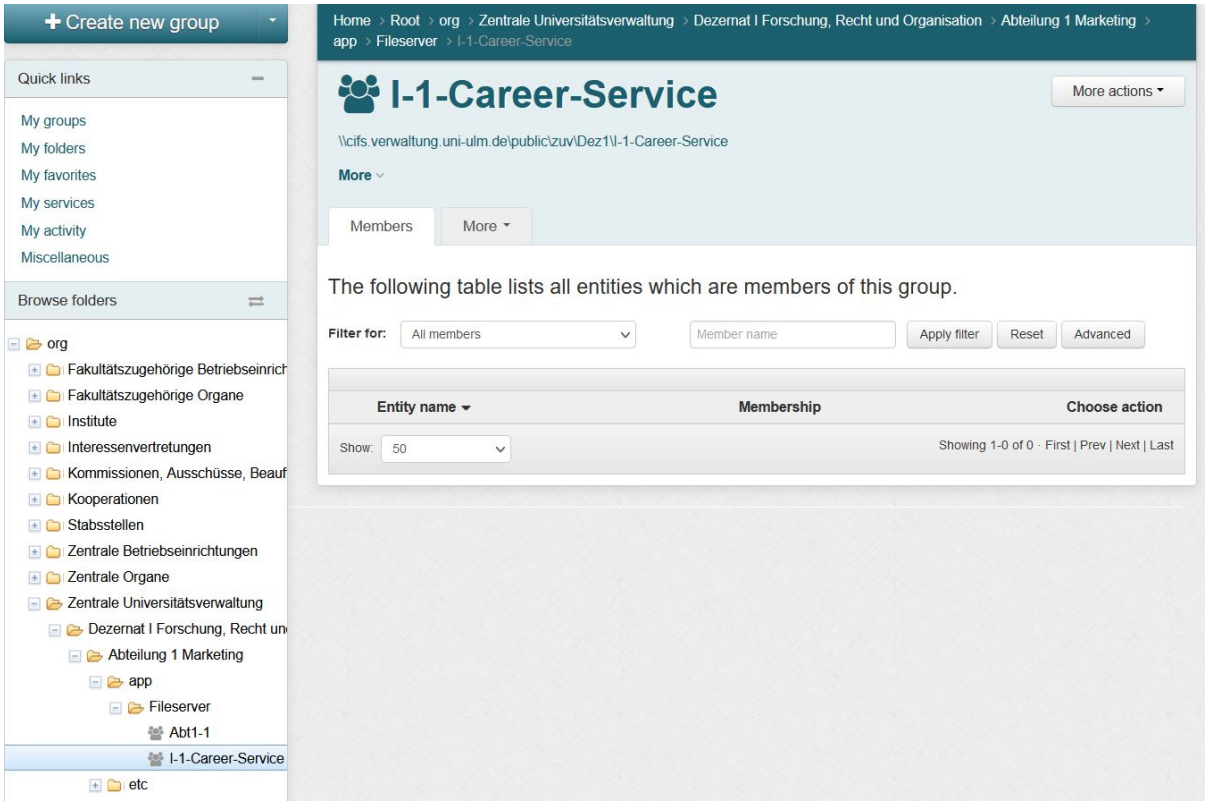
Um auf die Inhalte der Ordner unterhalb der Ebene **o:\zuv\Dez_** zugreifen zu können, ist eine Mitgliedschaft in der entsprechenden Gruppe notwendig. Nachfolgend wird beschrieben, wie Beschäftigte in Gruppen aufgenommen werden und wie die Einrichtungsleitenden (i.d.R Dezernentinnen und Dezernenten) die Gruppenverwaltung delegieren können.



Name	Änderungsdatum	Typ
Abt1-1	08.11.2022 07:40	Dateiordner
Abt1-2	14.10.2022 11:17	Dateiordner
Abt1-3	01.09.2022 14:55	Dateiordner
Abt1-4	20.10.2022 12:11	Dateiordner
Dez1-allgemein	02.09.2022 08:01	Dateiordner
Dez1-Leitung	24.10.2022 13:40	Dateiordner
Hausmeister	27.02.2019 15:11	Dateiordner
I-1-Career-Service	27.08.2021 14:09	Dateiordner
Team-Datenschutz	17.10.2022 15:27	Dateiordner
Team-Erfindungen-Technologietransfer	08.09.2022 17:09	Dateiordner
Team-Wahlen	14.04.2021 08:00	Dateiordner
Team-Stiftungen	21.09.2022 12:26	Verknüpfung
Berechtigungen.txt	12.11.2022 01:16	Textdokument

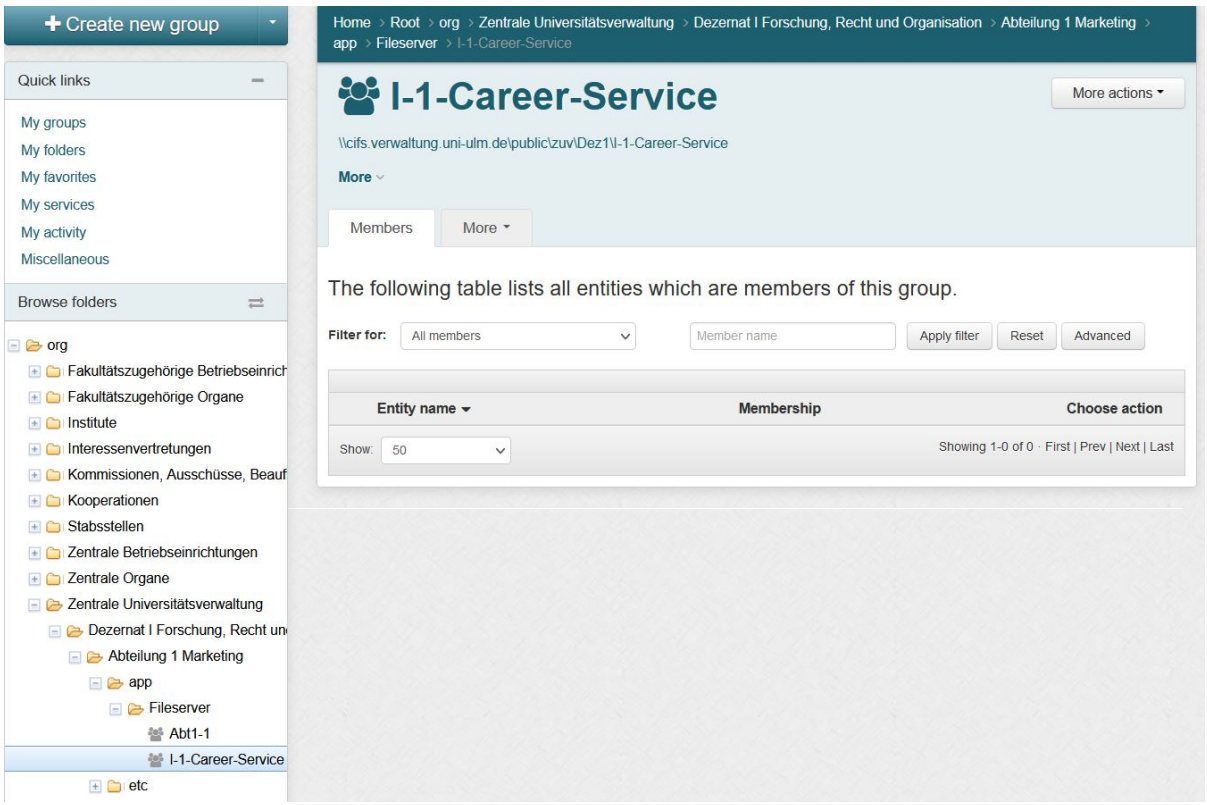
Mitglieder oder Gruppen in eine Gruppe aufnehmen

Die zur Verfügung stehenden Gruppen sind in Grouper im linken Bereich unter **org → Zentrale Universitätsverwaltung → Dezernat…→ Abteilung…→ app → Fileserver** zu finden. Die Organisationsstruktur in Grouper kann von der Ordnerstruktur auf dem File-Server abweichen. Wählen Sie Ihre Organisationseinheit und Ihre Abteilung. Hier ein Beispiel aus Dezernat I.

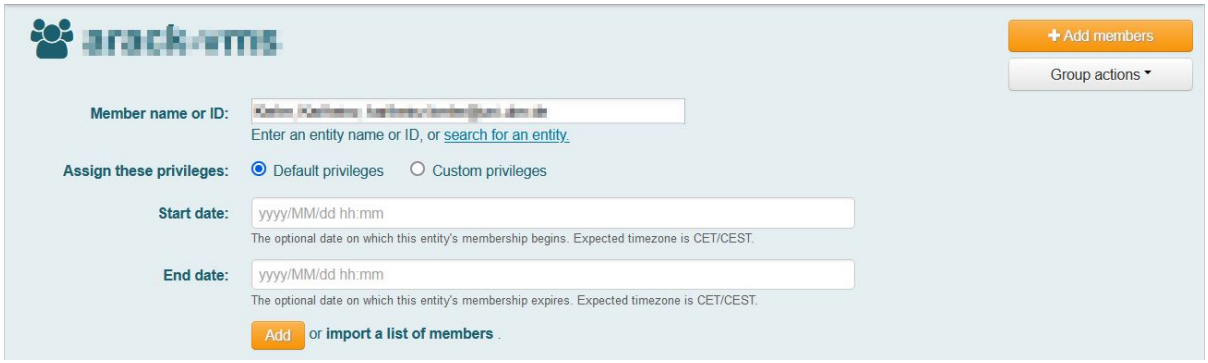


Für die Abteilung 1 des Dezernats I gibt es die Gruppen **Abt1-1** und **I-1-Career-Service**. Für alle Ordner mit beschränktem Zugriff, gibt es eine korrespondierende Gruppe in Grouper. Im Beispiel oben wäre das die Gruppe **I-1-Career-Service** die dem Ordner **\\cifs.verwaltung.uni-ulm.de\public\zuv\Dez1\I-1-Career-Service** zugeordnet ist (**\\cifs.verwaltung.uni-ulm.de\public** wird auf dem Arbeitsplatzrechners durch o: substituiert). Der Gruppe **Abt1-1** ist der Ordner **\\cifs.verwaltung.uni-ulm.de\public\zuv\Dez1\Abt1-1** zugeordnet. Alle darunterliegenden Ordner um Dateien erben die Berechtigungen.

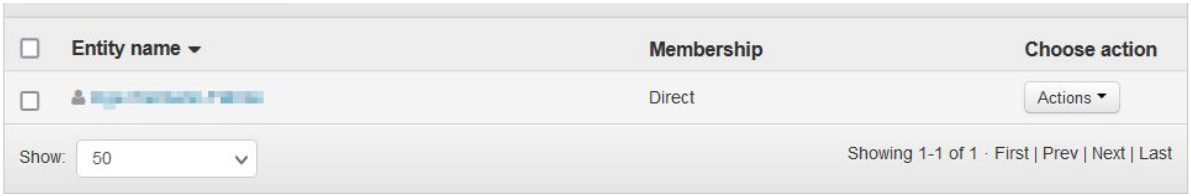
Klicken Sie auf die gewünschte Gruppe z.B. **I-1-Career-Service**



Um neue Mitglieder oder Gruppen in eine Gruppe aufzunehmen, klicken Sie auf die Schaltfläche **+Add members** . Geben Sie hinter **Member name or ID** Name oder den kiz Benutzernamen an. Eventuell werden mehrere Namen angezeigt. Es kann von Vorteil sein den kiz Benutzernamen anzugeben, da dieser eindeutig ist. Hinter **Start date** und **End date** kann Anfang und Ende des Zeitraums der Gruppenmitgliedschaft angegeben werden. Mit der Schaltfläche **Add** fügen Sie das Mitglied der Gruppe hinzu und schließen den Vorgang ab.



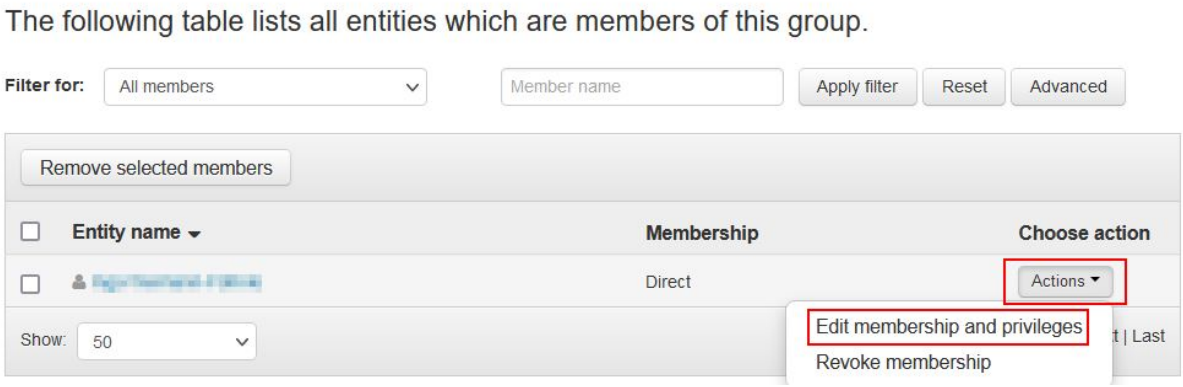
Der Name des ausgewählten Mitglieds wird in der Spalte **Entity name** angezeigt.



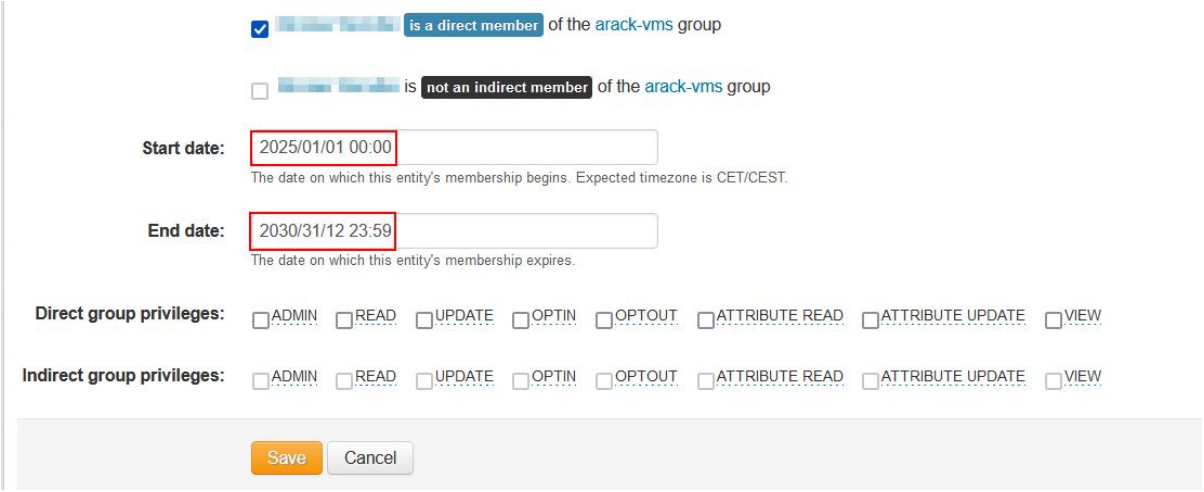
Es ist auch möglich eine Gruppe als Mitglied hinzuzufügen. Es stehen für jedes Dezernat und jede Abteilung auf Dezernatsebene passende Gruppen zur Verfügung. Diese Gruppen erhalten automatisch von den Vorsystemen ihre Daten.

Gruppenmitgliedschaft zeitlich beschränken

Auch nach dem Hinzufügen von Mitgliedern kann die Gruppenmitgliedschaft zeitlich begrenzt werden. Klicken Sie auf **Actiones** und **Edit membership and privileges**.

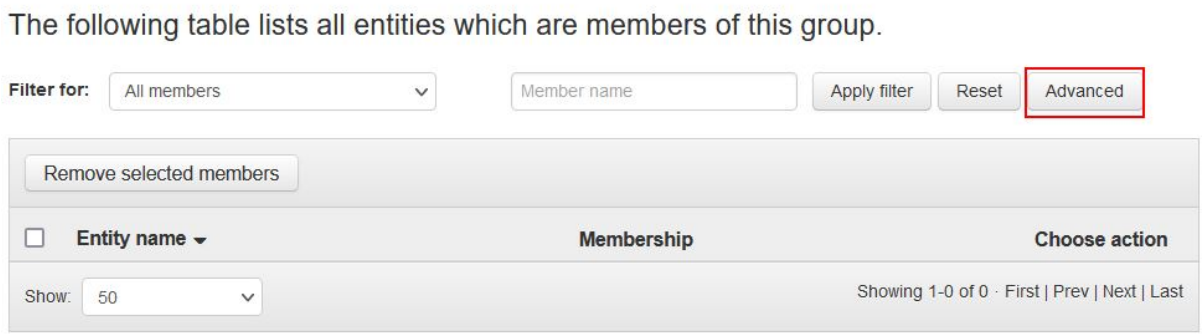


Geben Sie **Start date** und **End date** im Datumsformat **JJJJ/MM/TT HH:MM** an.

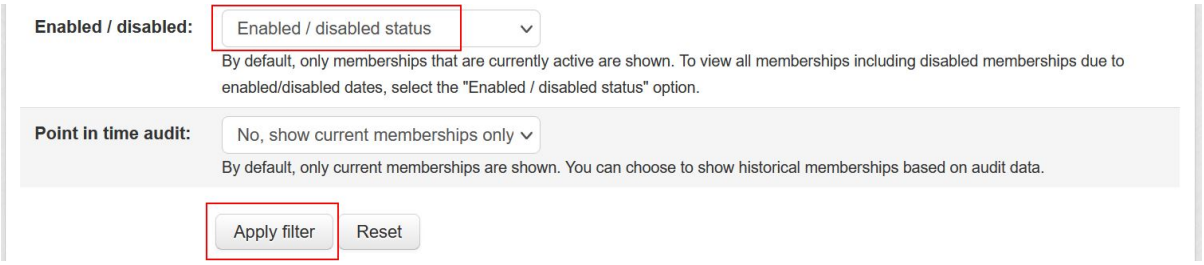


Mit **Save** werden die Angaben übernommen. In der Standardeinstellung werden nur aktive Gruppenmitglieder angezeigt. Sollte das **Start date** in der Zukunft liegen, verschwindet der Eintrag aus der Liste, taucht aber beim Erreichen das Datums wieder auf.

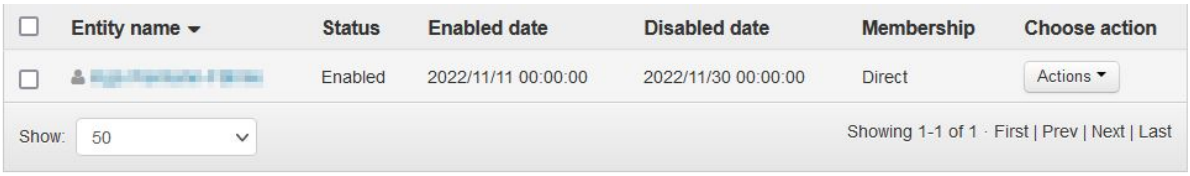
Mit einer speziellen Einstellung können auch inaktive Gruppenmitglieder eingeblendet werden. Klicken Sie dazu auf **Advanced**.



Wählen Sie dann die Einstellung **Enable /disable status**. Mit **Apply filter** wird die Einstellung übernommen und es werden auch inaktive Mitglieder angezeigt.

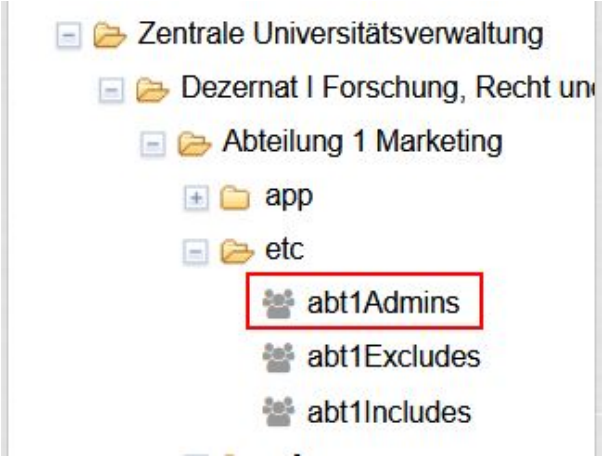


Es erscheint das Anfangs- und Endedatum der Gruppenmitgliedschaft. Diese Anzeigeeinstellung ist nicht dauerhaft.

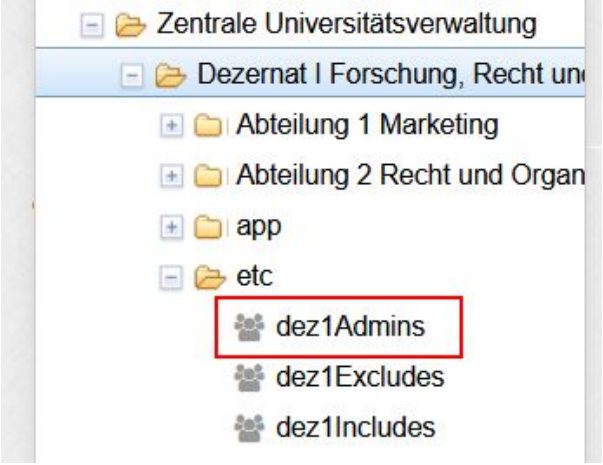


Hinzufügen von Gruppenverwaltenden

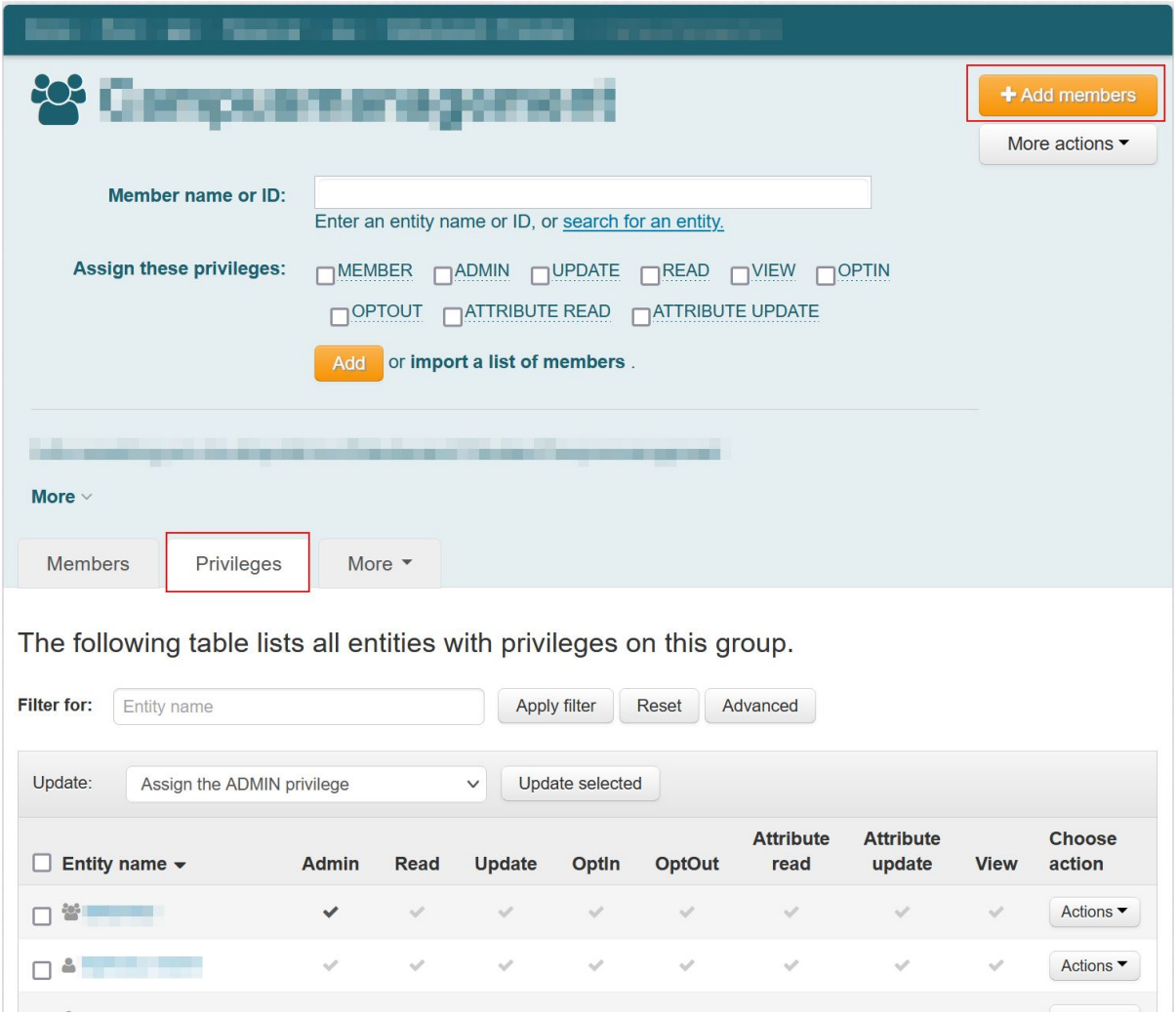
Initial werden nur die Dezernats- und Abteilungsleitenden als Gruppenverwalter aus dem IDM übernommen. Diese können weitere Gruppenverwaltende bestimmen. Dazu müssen die Dezernatsleitenden die dafür bestimmten Beschäftigten, wie oben beschrieben, in die Gruppe **abt_Admins** aufnehmen. Für _ ist die Abteilung des Dezernats einzutragen.



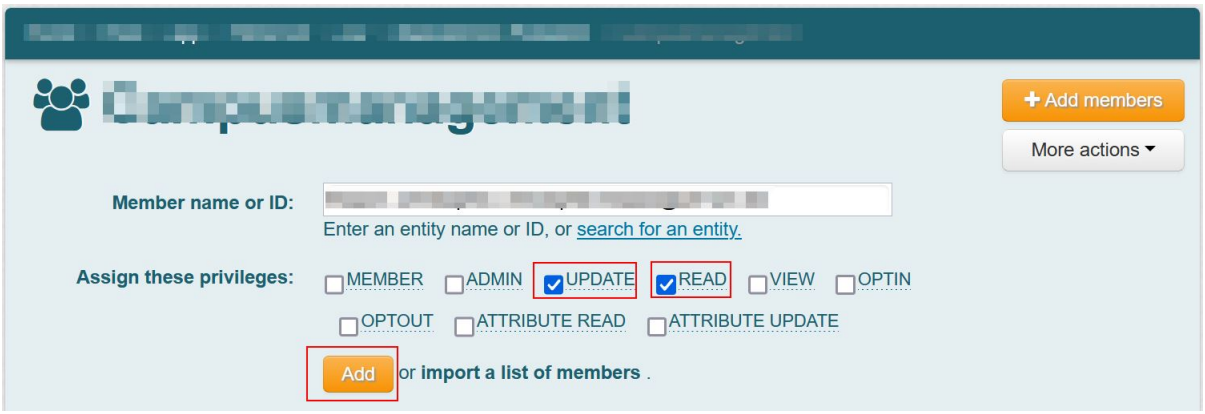
Sollen Gruppenverwaltende für alle Gruppen eines Dezernats zuständig sein, müssen die Verwaltenden auf Dezernatsebene in die Gruppe **dez_Admins** aufgenommen werden.



Es ist auch möglich Gruppenverwaltende nur für eine bestimmte Gruppe zu bestimmen. Dazu muss die Gruppe ausgewählt werden und auf die Schaltfläche **Privileges** geklickt werden. Dann **+Add members** . Geben Sie hinter **Member name or ID:** Name oder den kiz Benutzernamen an, der die Gruppe verwalten soll. Es kann auch eine Gruppe angegeben werden.



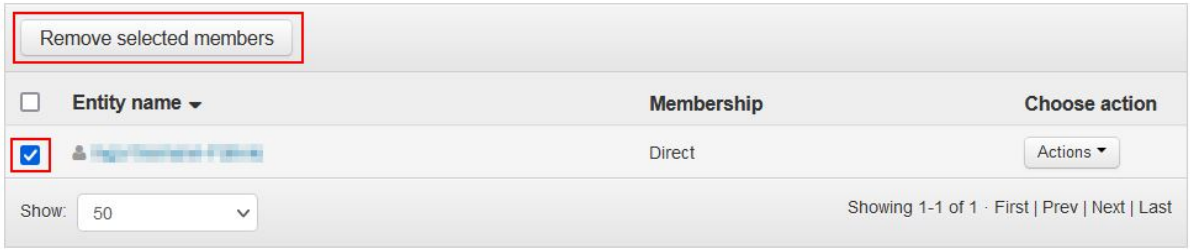
Hinter **Assign these privileges:** können die Berechtigungen ausgewählt werden. Normalerweise reichen **UPDATE** und **READ**.



Mit **Add** werden die Einstellungen übernommen.

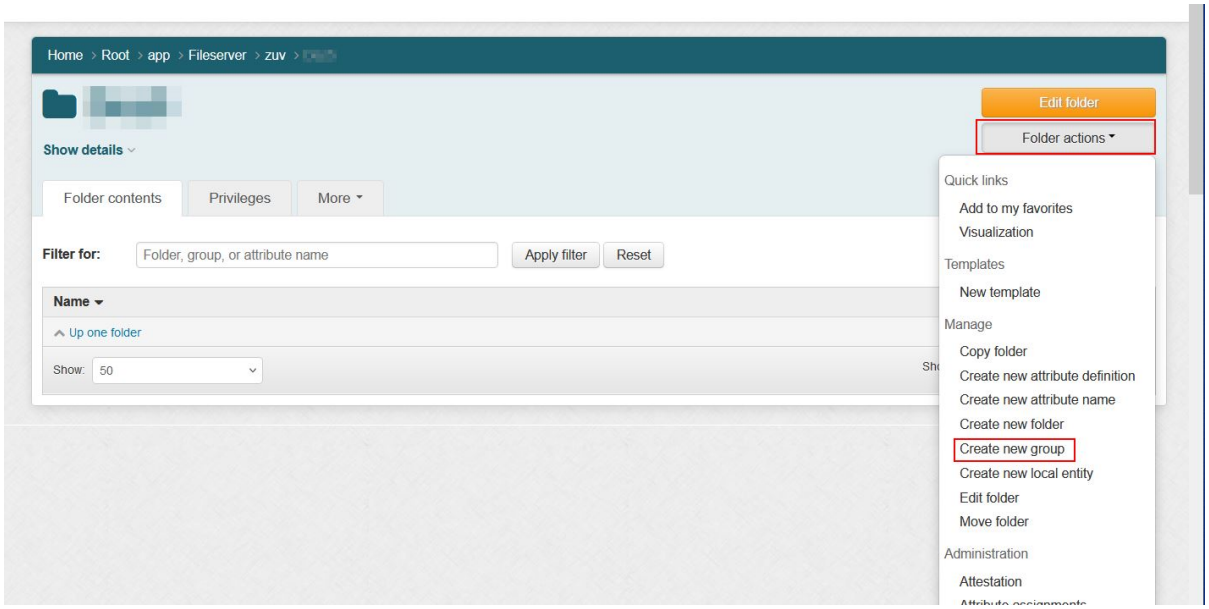
Mitglieder (können auch Gruppen sein) aus einer Gruppe entfernen

Setzen Sie dazu den Haken vor dem Namen des Mitglieds und klicken Sie **Remove selected members**.

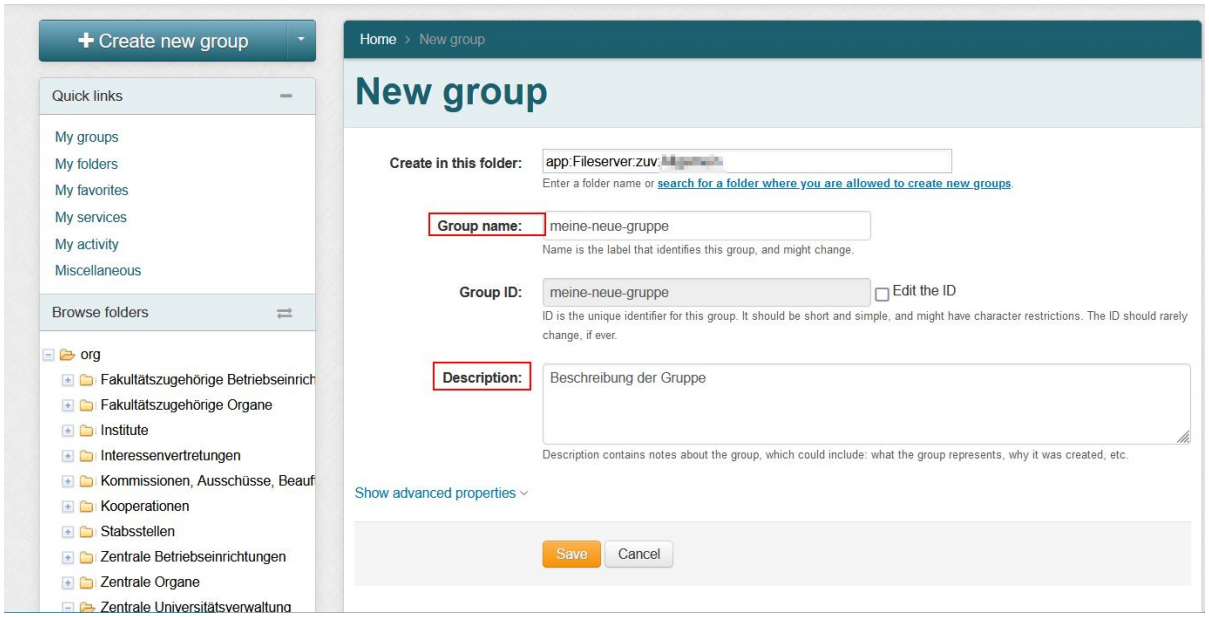


Anlegen von zusätzlichen Gruppen

Zuerst müssen Sie im linken Bereich unter **Browse folders** den Folder öffnen, unter dem Sie die neue Gruppe anlegen möchten. Klicken Sie dann **Folder actions** und **Create new Group**.



Geben Sie hinter **Group name** den Namen der neuen Gruppe an. Hinter **Description** kann eine Beschreibung der Gruppe eingetragen werden.



Mit **Save** wird der Vorgang abgeschlossen.

Online-Kalender

Für jede Grouper-Gruppe wird automatisch ein Online-Kalender angelegt. Der kann dann in SOGo oder Thunderbird abonniert werden. Dazu in SOGo auf das **+** Zeichen hinter **Abonnements** klicken und den Namen des Kalenders eingeben. Der Kalender heißt wie die Grouper-Gruppe. Die Mitglieder der Grouper-Gruppe sind die Verwalter des Kalenders. Eine Zuordnung zu einem bestimmten Benutzer gibt es hier nicht.

FAQs

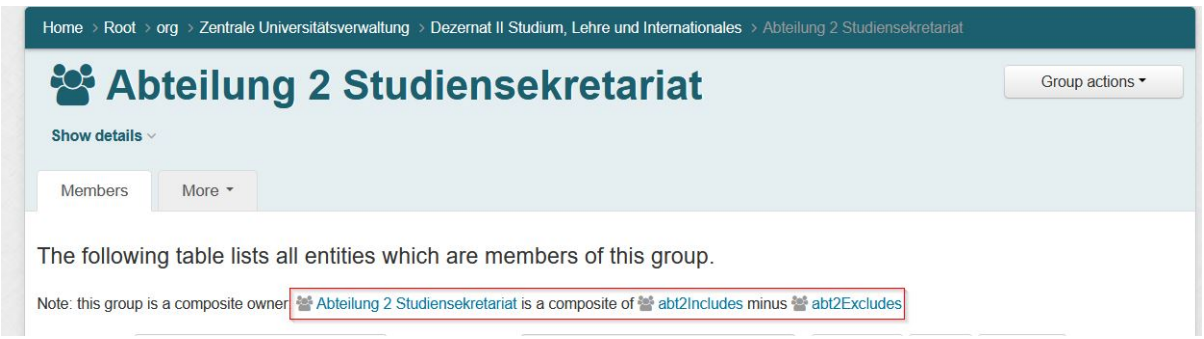
1. Kann eine Gruppe in eine Andere aufgenommen werden?
Ja, das geht. Man könnte die Gruppe **Dez1-Leitung** in alle anderen Gruppen des Dezernats I aufnehmen. Dann haben alle Mitglieder von **Dez1-Leitung** die Berechtigungen, die die Gruppen haben, in denen **Dez1-Leitung** Mitglied ist. Damit kann man vermeiden, dass neue Mitglieder die umfassenden Zugriff benötigen, in alle relevanten Gruppen einzeln aufgenommen werden müssen.

*2. Kann man die Gruppen, die unter **app → Fileserver** erscheinen, auch für andere Services wie z.B. Cloudstore verwenden?*
Nein, diese Gruppen können nur für den Fileserver verwandet werden.

*3. Was ist der Unterschied zwischen **direct** und **indirect** Member?*
Mitglieder einer Gruppe können Personen aber auch andere Gruppen sein! Ein **direct Member** ist eine Person, die Mitglied der aktuellen Gruppe ist. Ein **indirect Member** ist eine Person, die Mitglied einer anderen Gruppe ist, welche wiederum Mitglied der aktuellen Gruppe ist.

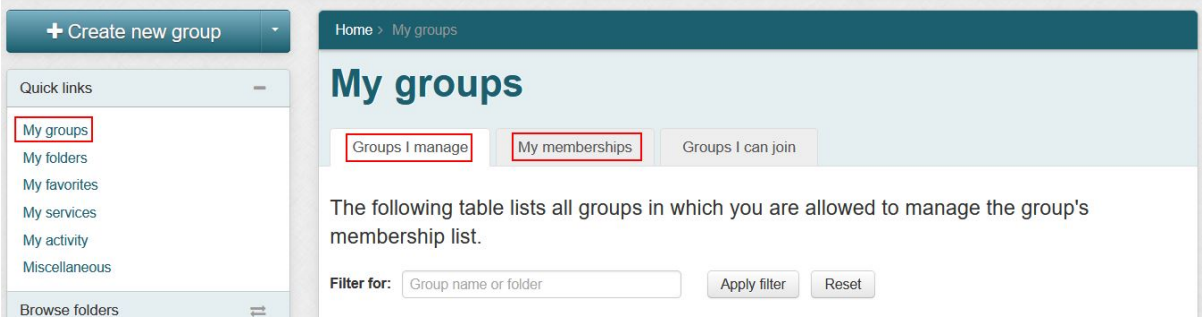
*4. Warum erscheinen manche Gruppen im **ref:** und im **org:** Zweig.*
Im Gegensatz zu **org:** können die Gruppenmitglieder einer **ref:** Gruppe in Grouper nicht bearbeitet werden.

*5.Wozu dienen die Gruppen **etc/abt_includes** und **etc/abt_excludes**?* Die Gruppe **abt_includes** wird mit Daten aus dem **ref:** Zweig gebildet. Das bedeutet, Mitglieder können hier nicht entfernt werden. Es ist in Grouper aber nicht nur möglich Benutzergruppen zu addieren, es ist auch erlaubt Differenzmengen, also Menge 1 minus Menge 2, zu bilden. Dafür dient die Gruppe **abt_excludes**. Diese Differenzmengen stehen für alle Dezernate und Abteilungen auf Dezernatsebene zur Verfügung. Hier ein Beispiel aus dem Dezernat II. Hier findet man die Gruppe **Abteilung 2 Studiensekretariat**, die gebildet wird aus **abt2Includes minus abt2Excludes**. Man kann also für diese Gruppe über **abt2Excludes** Mitglieder entfernen.



Damit wird erreicht, dass neue Beschäftige automatisch in die richtigen Gruppe kommen, aber auch bei Dienstende oder Abteilungswechsel entfernt werden.

6. Wie kann ich sehen, in welchen Gruppen ich Mitglied bin und welche Gruppen ich verwalten darf?
Klicken Sie dazu links oben unter **Quick links** auf **My Groups**. Sie erhalten dann rechts die Schaltflächen **Groups I manage** und **My memberships**. Klicken Sie auf diese Schaltflächen um zu sehen, in welchen Gruppen Sie Mitglied sind bzw. welche Gruppen Sie verwalten dürfen.



7. Wie kann ich sehen, in welchen Foldern und Gruppen ein Mitarbeitender Mitglied ist?
Geben Sie dazu rechts oben im Suchfeld den Namen oder besser den kiz-Benutzernamen der betreffenden Person ein und betätigen Sie anschließend die **Enter-Taste**. Sie erhalten eine Liste mit den Namen, die dem Suchkriterium entsprechen. Klicken Sie dann auf den gewünschten Namen. Es werden die relevanten Folder und Gruppen angezeigt. Hier werden auch Folder und Gruppen angezeigt, die nichts mit dem Fileserver zu tun haben. Gruppen, die auf den Fileserver bezogen sind, enthalten im zugehörigem Folderpfad **Fileserver**. Um das zu erkennen, bewegen Sie die Maus auf die gewünschte Gruppe. Es erscheint eine Messagebox mit dem Folderpfad.

8. Wie kann man sehen, von wem eine Gruppe bearbeitet wurde?
Auf die gewünschte Gruppe klicken. **Group actions → Audit log**

9. Kann man einen bestehenden Kalender in einen Grouper Gruppenkalender überführen?
Einfach den alten Kalender exportieren und in den neuen über Grouper erzeugten Kalender importieren. Das geht in SOGo und Thunderbird.