Konfiguration und Verwaltung

Benutzerverwaltung

Inhaltsverzeichnis

Benutzer und Gruppen

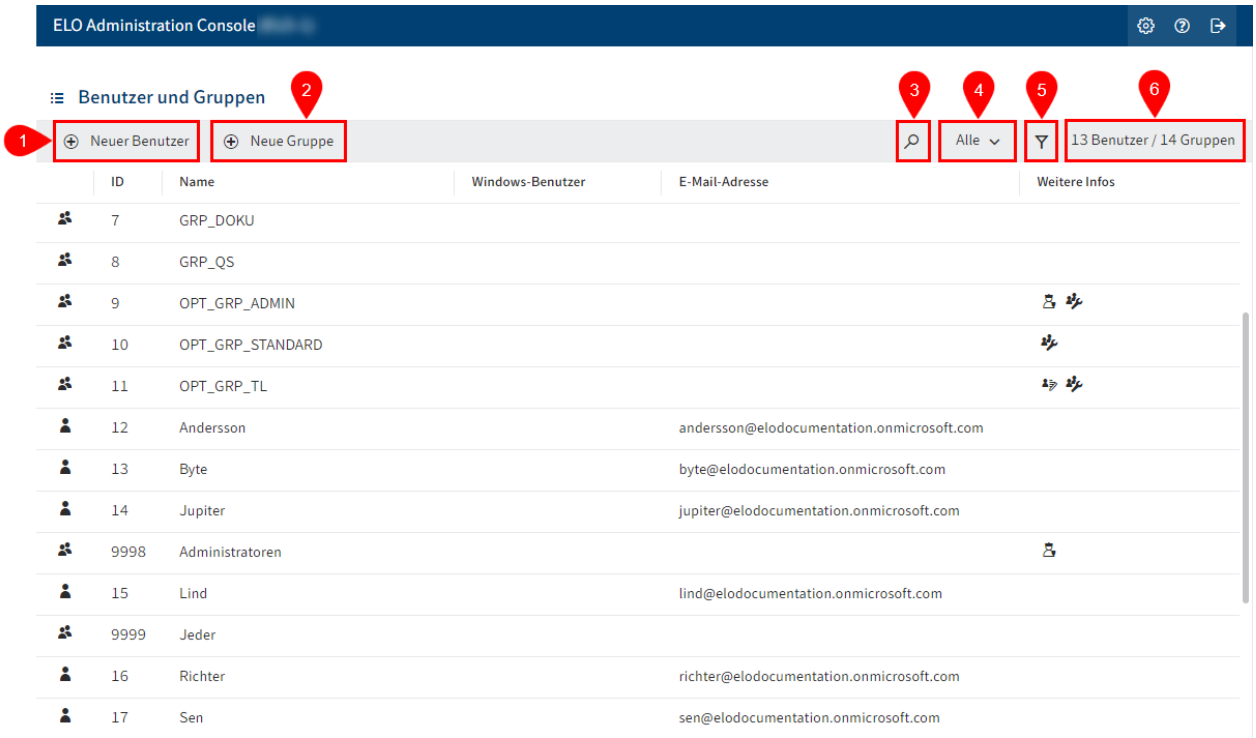
Einführung

Alle Personen, die ELO nutzen, benötigen ein entsprechendes ELO Konto.

Über Gruppen können in ELO Rechte, Berechtigungen und Grundeinstellungen verwaltet werden. Außerdem werden Gruppen in Workflows und für die Vertretungsreglung verwendet.

Konten und Gruppen können Sie in der Benutzer- und Gruppenverwaltung angelegen, konfigurieren und verwalten. Diese öffnen Sie in der ELO Administration Console über *Systemeinstellungen > Benutzer- und Gruppenverwaltung*.

Übersicht 'Benutzer und Gruppen'



Die Benutzer- und Gruppenverwaltung bietet folgende Handlungsmöglichkeiten:

1 Benutzer anlegen

2 Gruppe anlegen

3 Suche durchführen

4 Auswahl der Listenanzeige: Alle, Benutzer, Gruppen

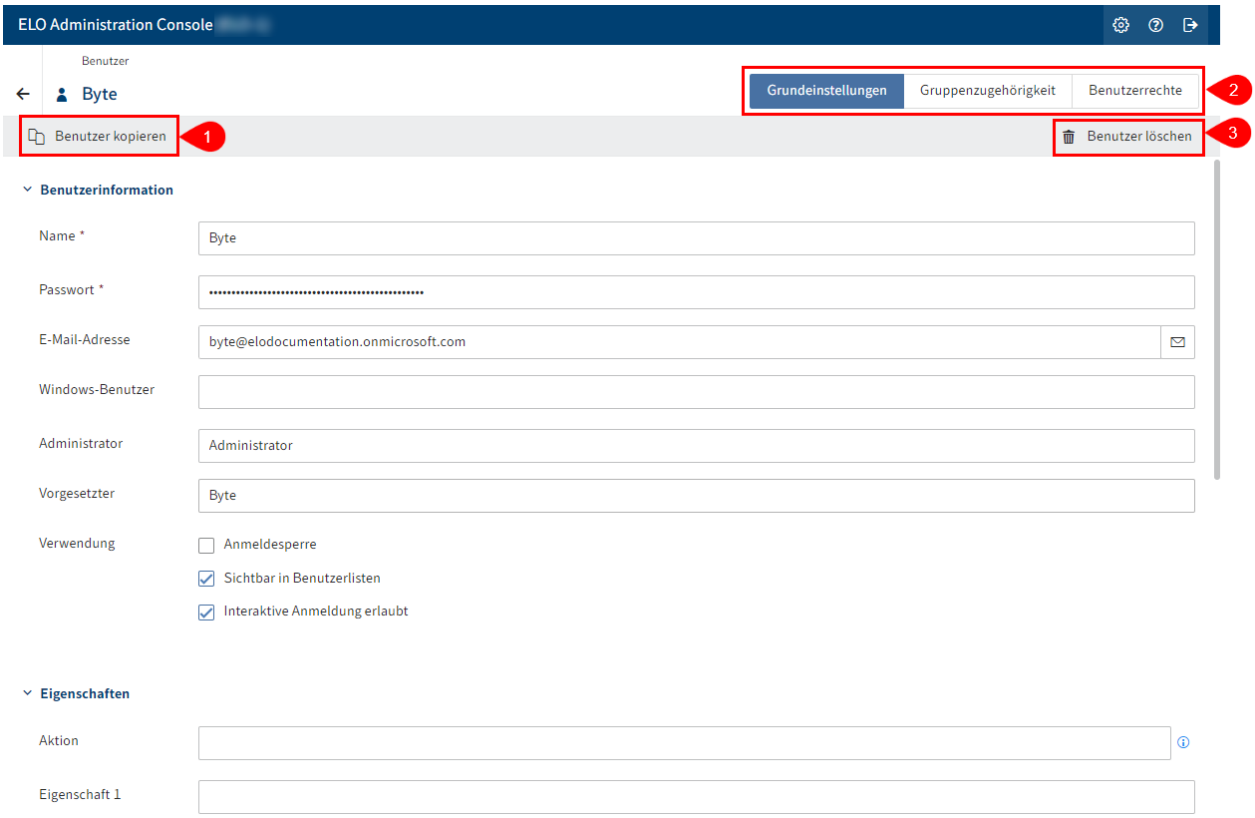
5 Filter setzen

6 Anzahl der bestehenden Benutzer und Gruppen

> **Information**

Sie können die Liste der bestehenden Benutzer und Gruppen aufsteigend oder absteigend nach den IDs, Namen oder E-Mail-Adressen sortieren, indem Sie in der ersten Tabellenzeile *ID*, *Name* oder *E-Mail-Adresse* auswählen.

Detailansicht 'Benutzer'



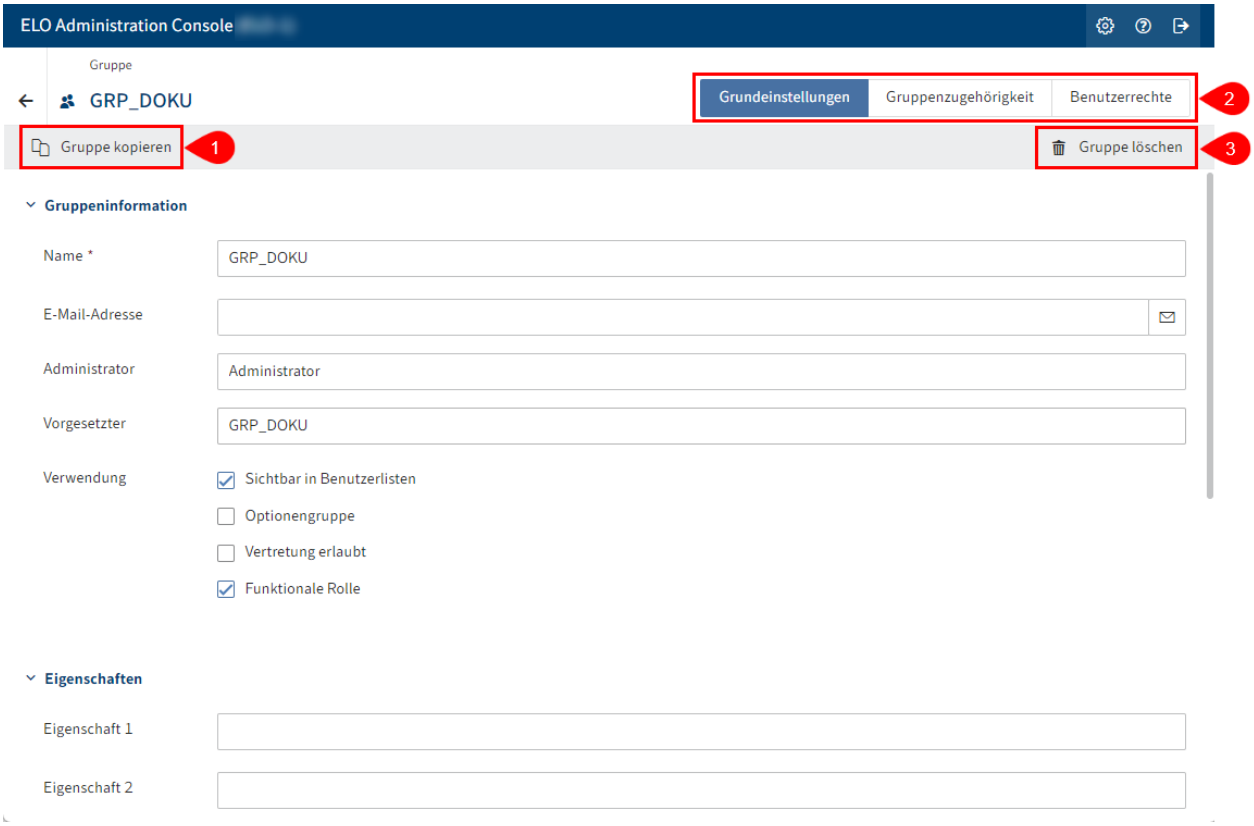
Die Detailansicht *Benutzer* bietet folgende Handlungsmöglichkeiten:

1 Benutzer kopieren: Bis auf die Felder *Name*, *E-Mail-Adresse*, *Passwort* und *Windows-Benutzer* werden alle Konfigurationen übernommen.

2 Konfiguration vornehmen: Über die Tabs Grundeinstellungen, Gruppenzugehörigkeit, Benutzerrechte

3 Benutzer löschen

Detailansicht 'Gruppe'



Die Detailansicht *Gruppe* bietet folgende Handlungsmöglichkeiten:

1 Gruppe kopieren: Bis auf die Felder *Name*, *E-Mail-Adresse* und die Mitglieder werden alle Konfigurationen übernommen.

2 Konfiguration vornehmen: Über die Tabs Grundeinstellungen, Gruppenzugehörigkeit, Benutzerrechte

3 Gruppe löschen

Benutzer

Benutzer anlegen

Um einen Benutzer anzulegen, gehen Sie folgendermaßen vor:

1. Öffnen Sie die ELO Administration Console.
2. Öffnen Sie die Benutzer- und Gruppenverwaltung (*Systemeinstellungen > Benutzer- und Gruppenverwaltung*).

3. Wählen Sie *Neuer Benutzer*.

   Der Bereich *Benutzer* erscheint.

4. Konfigurieren Sie den neuen Benutzer. Navigieren Sie dazu über die Tabs *Grundeinstellungen*, *Gruppenzugehörigkeit* und *Benutzerrechte*.

   Nähere Informationen finden Sie im nachfolgenden Abschnitt 'Konfiguration'.

5. Nachdem Sie die Konfiguration vorgenommen haben, wählen Sie *Benutzer speichern*.

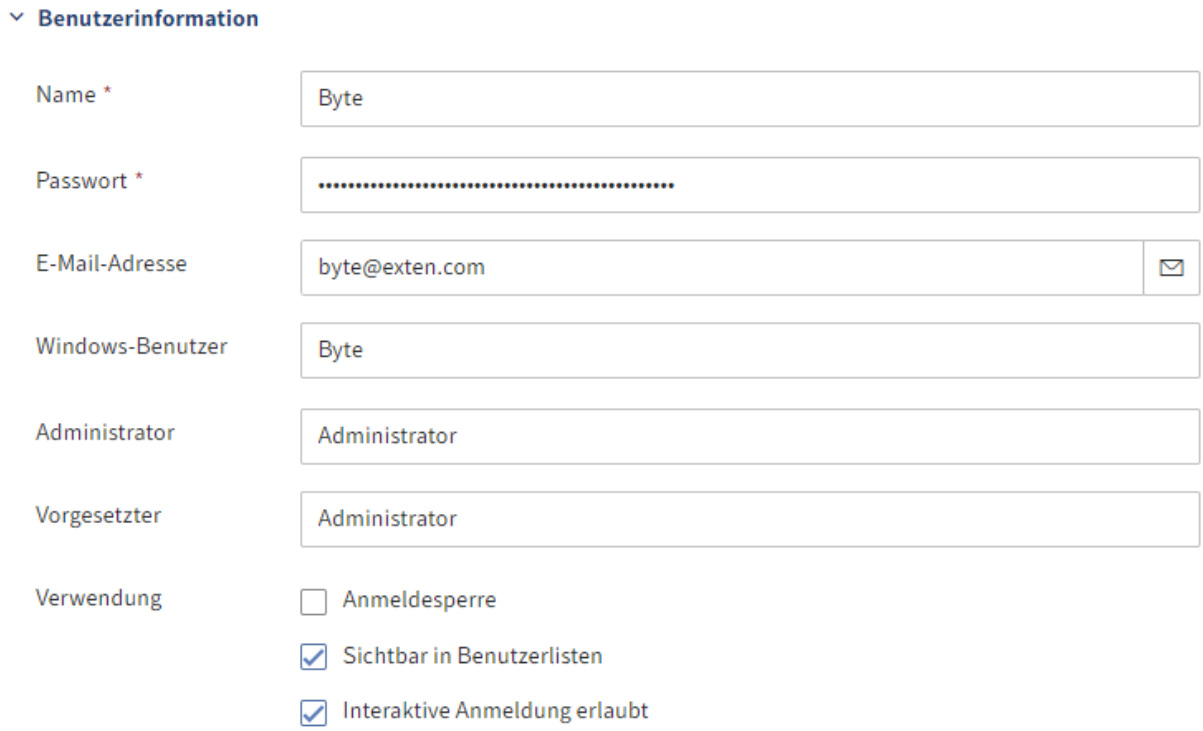
Sie haben einen neuen Benutzer angelegt.

Konfiguration

Grundeinstellungen festlegen

Im Bereich *Grundeinstellungen* legen Sie die *Benutzerinformation*, *Eigenschaften* und zusätzliche *Information* fest.

Benutzerinformation



- Name: Pflichtfeld. Kann nachträglich geändert werden.
- Passwort: Pflichtfeld. Kann nachträglich geändert werden.
- E-Mail-Adresse: Wird im Client im jeweiligen Profil angezeigt und kann in Workflows, Formularen und Scripten verwendet werden.
- Windows-Benutzer: Tragen Sie bei Bedarf den Windows-Kontonamen ein, falls beispielsweise SSO verwendet werden soll. Diese Information kann in Workflows, Formularen und Scripten verwendet werden.
- Administrator: Wird automatisch mit dem Namen des Kontos gefüllt, mit dem der neue Benutzer angelegt wird. Besitzt das anlegende Konto das Recht *Hauptadministrator*, wird das Feld *Administrator* mit dem Konto *Administrator* gefüllt. Kann nachträglich geändert werden. Legt fest, wer die Stammdaten des jeweiligen Benutzers bearbeiten darf.
- Vorgesetzter: Kann in Workflows, Formularen und Scripten verwendet werden. Wenn dieses Feld leer gelassen wird, wird der Inhalt des Feldes *Name* übernommen.
- Verwendung:
  - *Anmeldesperre*: Ist diese Option aktiviert, kann man sich mit diesem Konto nicht mehr im System anmelden. Das Konto ist weiterhin im System sichtbar. Um es auszublenden, deaktivieren Sie die Grundeinstellung *Sichtbar in Benutzerlisten*.

    > **Information**
    >
    > Diese Option ist bei dem Konto Administrator nicht verfügbar.

  - *Sichtbar in Benutzerlisten*: Ist diese Option aktiviert, erscheint das Konto in den entsprechenden Auswahllisten im ELO Client. Ist die Option deaktiviert, ist das Konto nur für die Administration sichtbar. Bereits durchgeführte Aktionen mit

diesem Konto, wie z. B. abgelegte Dokumente oder neue Dokumentversionen, bleiben jedoch weiterhin für alle im ELO Client sichtbar.

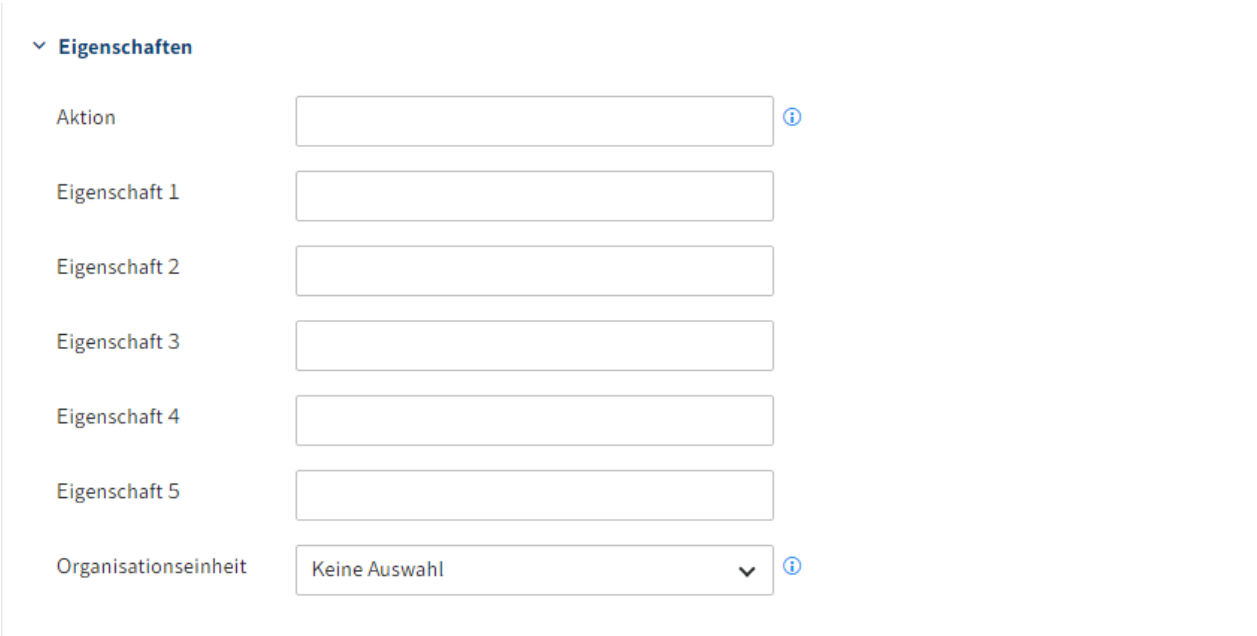
> **Information**
>
> Die Mitglieder einer Organisationseinheit sehen nur die in ihrer Organisationseinheit enthaltenen Konten.

- *Interaktive Anmeldung erlaubt*: Ist diese Option aktiviert, kann man sich mit dem Konto über den Anmeldedialog im ELO Client anmelden.

> **Beachten Sie**
>
> Diese Einstellung kann nicht vom Server überprüft werden. Sie gilt nicht als Sperre und lässt sich umgehen.

> **Information**
>
> Diese Option ist bei dem Konto Administrator nicht verfügbar.

Eigenschaften



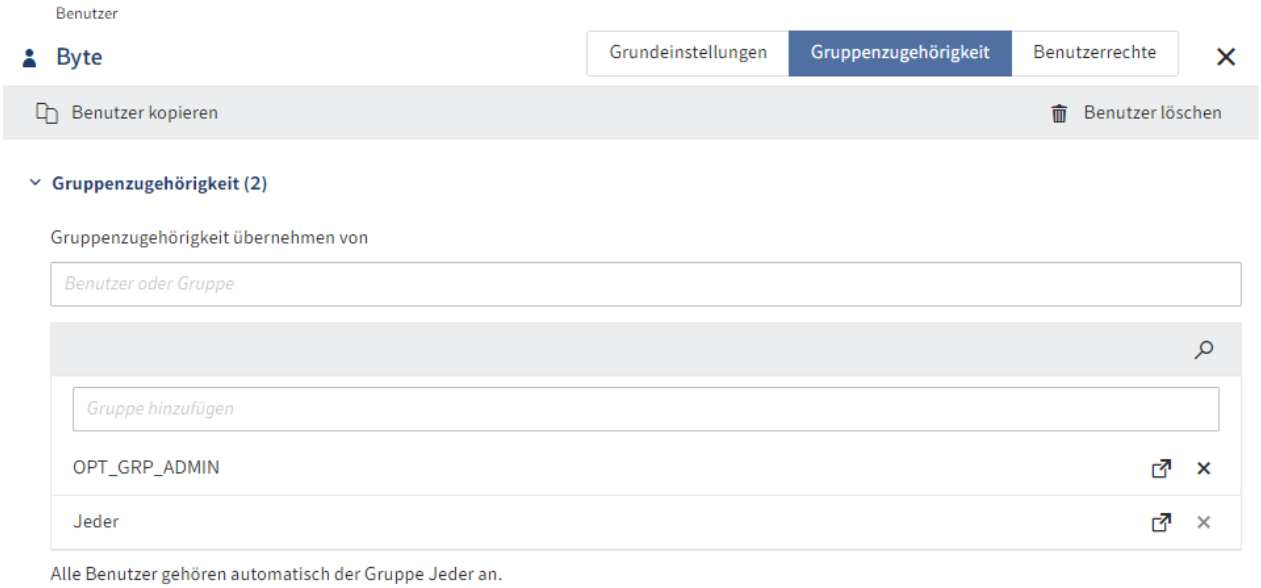
- Aktion: Hier eingetragene Kürzel wirken sich auf das Passwort aus.
  - Beispiele:
    - EX20233105: Das Passwort läuft am 31.05.2023 ab und muss dann erneuert werden.
    - PWf: Das gesetzte Passwort muss bei der ersten Anmeldung geändert werden.
    - PW: Das gesetzte Passwort kann bei der ersten Anmeldung geändert werden.
- Eigenschaft 1-5: Informationen können über Scripte ausgewertet werden.
-

Organisationseinheit: Informationen dazu finden Sie unter Konfiguration und Verwaltung > Benutzerverwaltung > Weitere Konfigurationen > Organisationseinheiten.

Information

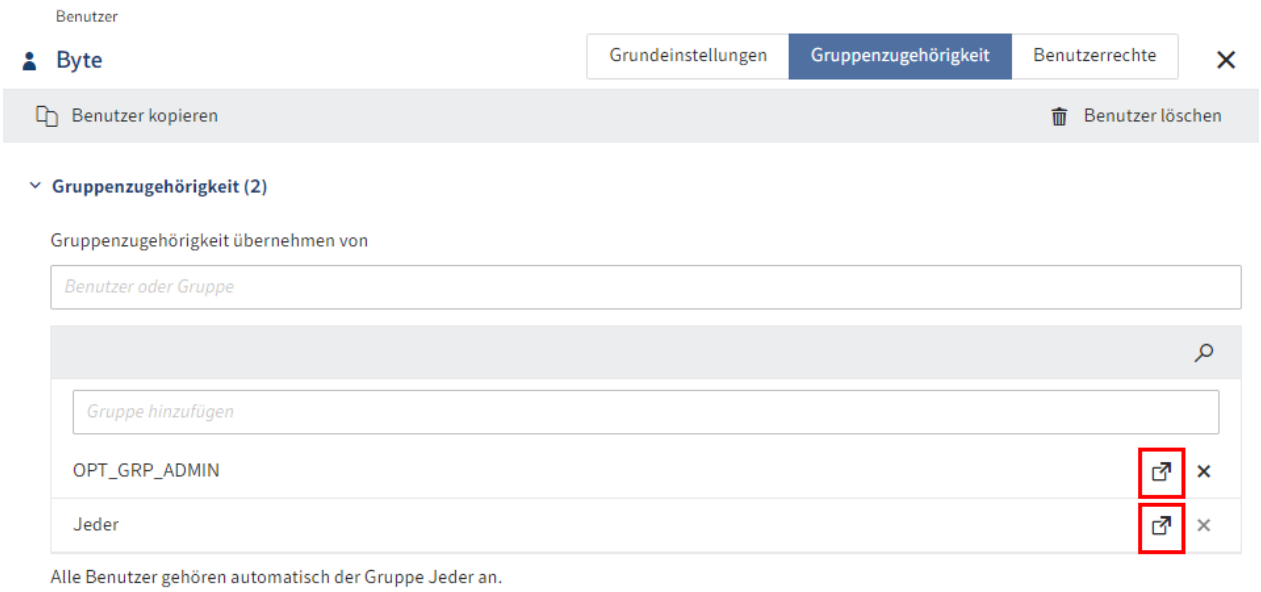
- Beschreibung: Die Eingabe darf maximal 250 Zeichen enthalten.
- Letzte vermerkte Anmeldung: Aktualisiert sich automatisch.
- Zuletzt geändert: Aktualisiert sich automatisch.
- ID: Jedes Konto erhält automatisch eine ID. Die ID kann zur Ansprache des Kontos bei anderen Funktionen verwendet werden.
- GUID: Jedes Konto erhält automatisch eine GUID. Die GUID kann zur Ansprache des Kontos bei anderen Funktionen verwendet werden.

Gruppenzugehörigkeit festlegen



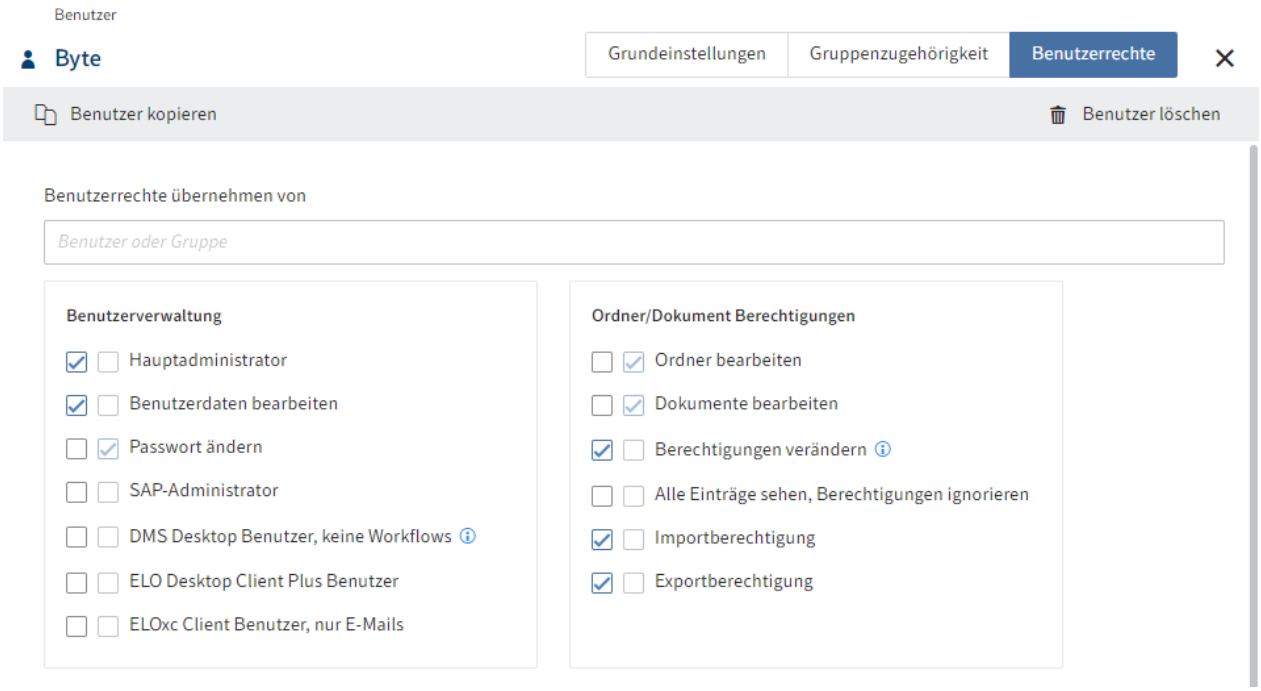
Sie können entweder bestehende Gruppenzugehörigkeiten eines anderen Benutzers oder einer Gruppe übernehmen oder bestehende Gruppen manuell hinzufügen. Sie können einen Benutzer in eine oder mehrere Gruppen aufnehmen. Die Anzahl der Gruppenzugehörigkeit dieser Gruppe wird in Klammern angezeigt. Benutzer sind immer Mitglied in der Gruppe *Jeder*.

> **Information**
>
> Tippen Sie ein Leerzeichen in eines der Eingabefelder ein, wird die gesamte Liste der vorhandenen Benutzer und Gruppen angezeigt.



Um in die Einstellungen einer zugehörigen Gruppe zu gelangen, wählen Sie das entsprechende Linksymbol. Die Einstellungen erscheinen in einem neuen Browser-Tab.

Benutzerrechte zuweisen



Es gibt drei Möglichkeiten für die Vergabe von Benutzerrechten:

- Vererbung

  Weitere Informationen dazu finden Sie unter Konfiguration und Verwaltung > Benutzerverwaltung > Rechte in ELO > Vererbung von Rechten.

- Manuelle Zuweisung

  Weitere Informationen dazu finden Sie unter Konfiguration und Verwaltung > Benutzerverwaltung > Rechte in ELO > Benutzerrechte.

- Übernehmen von einem anderen Benutzer oder einer Gruppe

> **Information**
>
> Im Idealfall werden alle Rechte über Gruppen vererbt. Das vereinfacht die Rechtevergabe und die Rechteverwaltung.

Benutzer löschen

> **Beachten Sie**
>
> Wenn Sie einen Benutzer löschen, wird dieser unwiderruflich gelöscht.

Löschen Sie keinen Benutzer, der bereits in ELO verwendet wurde. Dadurch kann es zu Inkonsistenzen kommen. In diesem Fall ist es besser, den Benutzer nicht zu löschen, sondern die Grundeinstellungen zu ändern:

1. Aktivieren Sie *Anmeldesperre aktivieren*
2.

Deaktivieren Sie *Interaktive Anmeldung erlauben*

3. Deaktivieren Sie *Sichtbar in Benutzerlisten*

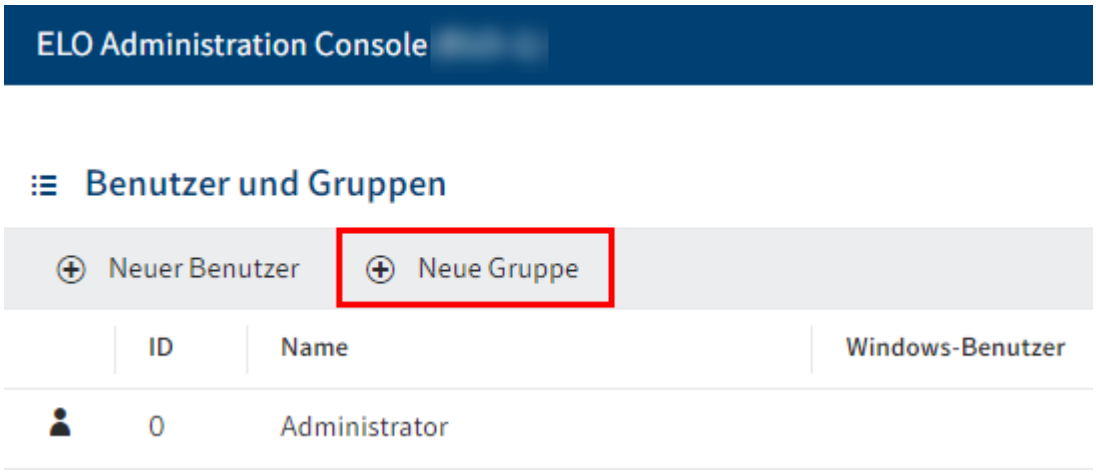
Der Benutzer kann sich nicht mehr in ELO anmelden und ist auch nicht für andere Benutzer sichtbar. Er ist in ELO nur noch im Hintergrund vorhanden. Seine bisherigen Aktionen, wie beispielsweise ein bereits verfasster Feed oder ein Eintrag in den Dokumentversionen, sind noch in ELO sichtbar.

Gruppen

Gruppe anlegen

Um eine Gruppe anzulegen, gehen Sie folgendermaßen vor:

1. Öffnen Sie die ELO Administration Console.
2. Öffnen Sie die Benutzer- und Gruppenverwaltung (*Systemeinstellungen > Benutzer- und Gruppenverwaltung*).



3. Wählen Sie *Neue Gruppe*.

   Der Bereich *Gruppe* erscheint.

4. Konfigurieren Sie die neue Gruppe. Navigieren Sie dazu über die Tabs *Grundeinstellungen*, *Gruppenzugehörigkeit* und *Benutzerrechte*.

   Nähere Informationen finden Sie im nachfolgenden Abschnitt 'Konfiguration'.

5. Nachdem Sie die Konfiguration vorgenommen haben, wählen Sie *Gruppe speichern*.

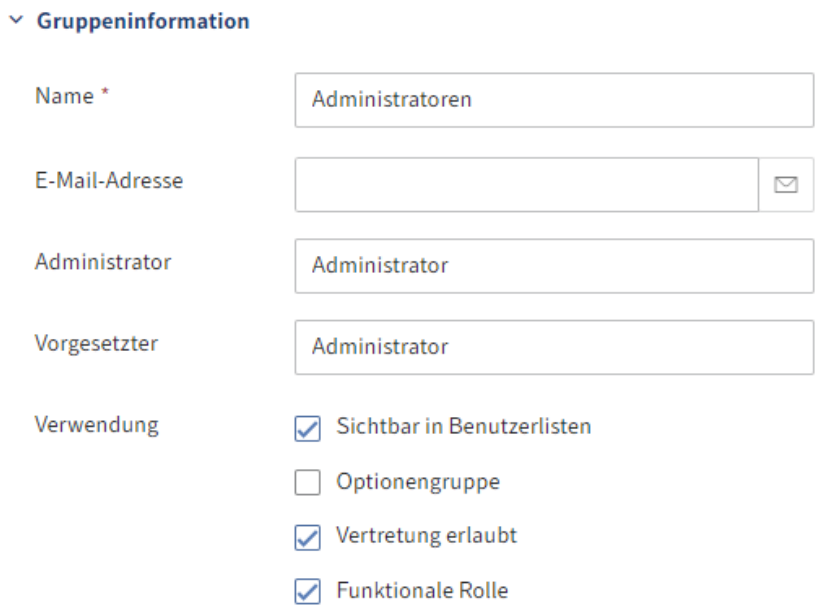
Sie haben eine neue Gruppe angelegt.

Konfiguration

Grundeinstellungen festlegen

Im Bereich *Grundeinstellungen* legen Sie die *Gruppeninformation*, *Eigenschaften* und zusätzliche *Information* fest.

Gruppeninformation



- Name: Pflichtfeld. Kann nachträglich geändert werden.
- E-Mail-Adresse: Wird im Client im jeweiligen Profil angezeigt und kann in Workflows, Formularen und Scripten verwendet werden.
- Administrator: Wird automatisch mit dem Namen des Kontos gefüllt, mit dem die neue Gruppe angelegt wird. Besitzt das anlegende Konto das Recht *Hauptadministrator*, wird das Feld *Administrator* mit dem Konto *Administrator* gefüllt. Kann nachträglich geändert werden. Legt fest, wer die Stammdaten der jeweiligen Gruppe bearbeiten darf.
- Vorgesetzter: Kann in Workflows, Formularen und Scripten verwendet werden. Wenn dieses Feld leer gelassen wird, wird der Inhalt des Feldes *Name* übernommen.
- Verwendung:
  - *Sichtbar in Benutzerlisten*: Ist diese Option aktiviert, erscheint die Gruppe in den entsprechenden Auswahllisten im ELO Client. Ist die Option deaktiviert, ist die Gruppe weiterhin in ELO vorhanden, wird aber nicht in den entsprechenden Auswahllisten im ELO Client angezeigt.
  - *Optionengruppe*: Optionengruppen werden definiert, um bestimmte *ProfileOpts* zuzuweisen. Nur diese Gruppen erscheinen in Dialogen, in denen Einstellungen für andere ELO Konten vorgenommen werden.

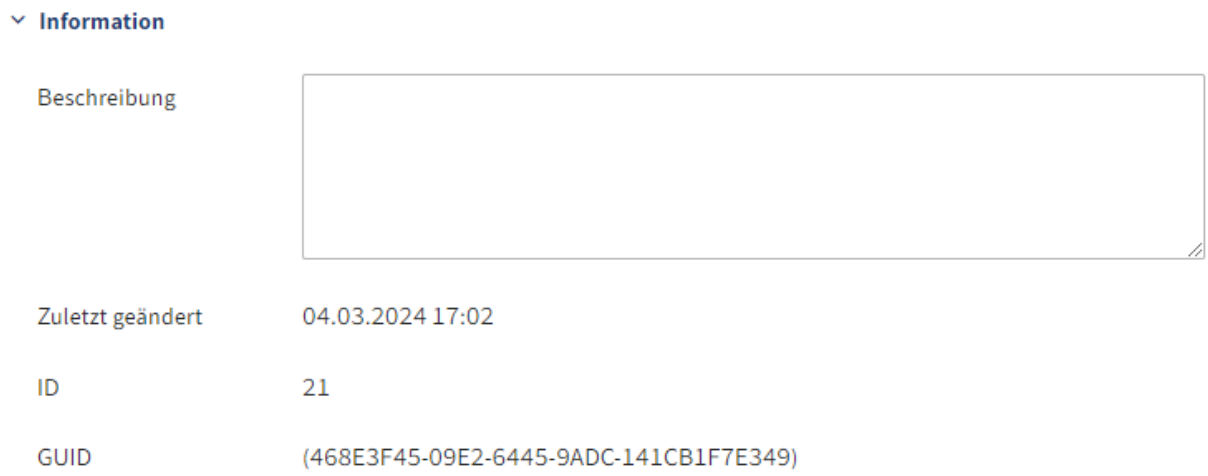
    Weitere Informationen zu Optionengruppen finden Sie unter Optionengruppen.
  - *Vertretung erlaubt*: Die Verteilung der Rechte kann über das Vertretungsmodul gesteuert werden. Bei Gruppen, deren Vertretung erlaubt ist, können die Rechte an die Vertretung übertragen werden.
  - *Funktionale Rolle*: Ist diese Option aktiviert, werden Mitglieder dieser Gruppe bei der Anmeldung gefragt, ob sie die *Funktionale Rolle* für die aktuelle Sitzung übernehmen wollen.

Das ist dann sinnvoll, wenn eine Person unterschiedliche Aufgaben in ELO zu erfüllen hat, die jeweils unterschiedliche Berechtigungen und Rechte erfordern.

Eigenschaften

- Eigenschaft 1-5: Informationen können über Scripte ausgewertet werden.
- Organisationseinheit: Informationen dazu finden Sie unter Konfiguration und Verwaltung > Benutzerverwaltung > Weitere Konfigurationen > Organisationseinheiten.

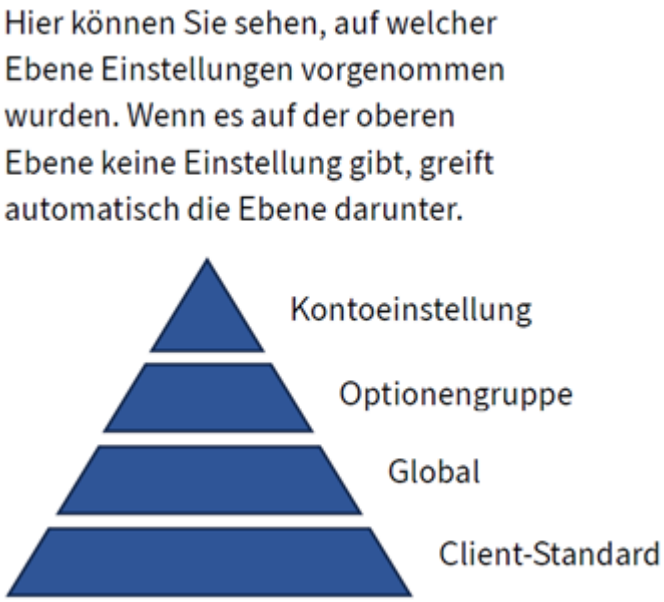
Information



- Beschreibung: Die Eingabe darf maximal 250 Zeichen enthalten.
- Zuletzt geändert: Aktualisiert sich automatisch.
- ID: Jede Gruppe erhält automatisch eine ID. Die ID kann zur Ansprache der Gruppe bei anderen Funktionen verwendet werden.
- GUID: Jede Gruppe erhält automatisch eine GUID. Die GUID kann zur Ansprache der Gruppe bei anderen Funktionen verwendet werden.

Optionengruppen

Grundsätzlich werden bei einem Konto individuelle Optionen verwendet. Wenn es diese nicht gibt, werden die Optionen für die Optionengruppen verwendet. Wenn diese nicht definiert wurden, wird die Optioneneinstellung der Gruppe *Jeder* verwendet. Wenn hier nichts definiert wird, gibt es einen ELO Standardwert (*company default setting* oder Client-Standard).



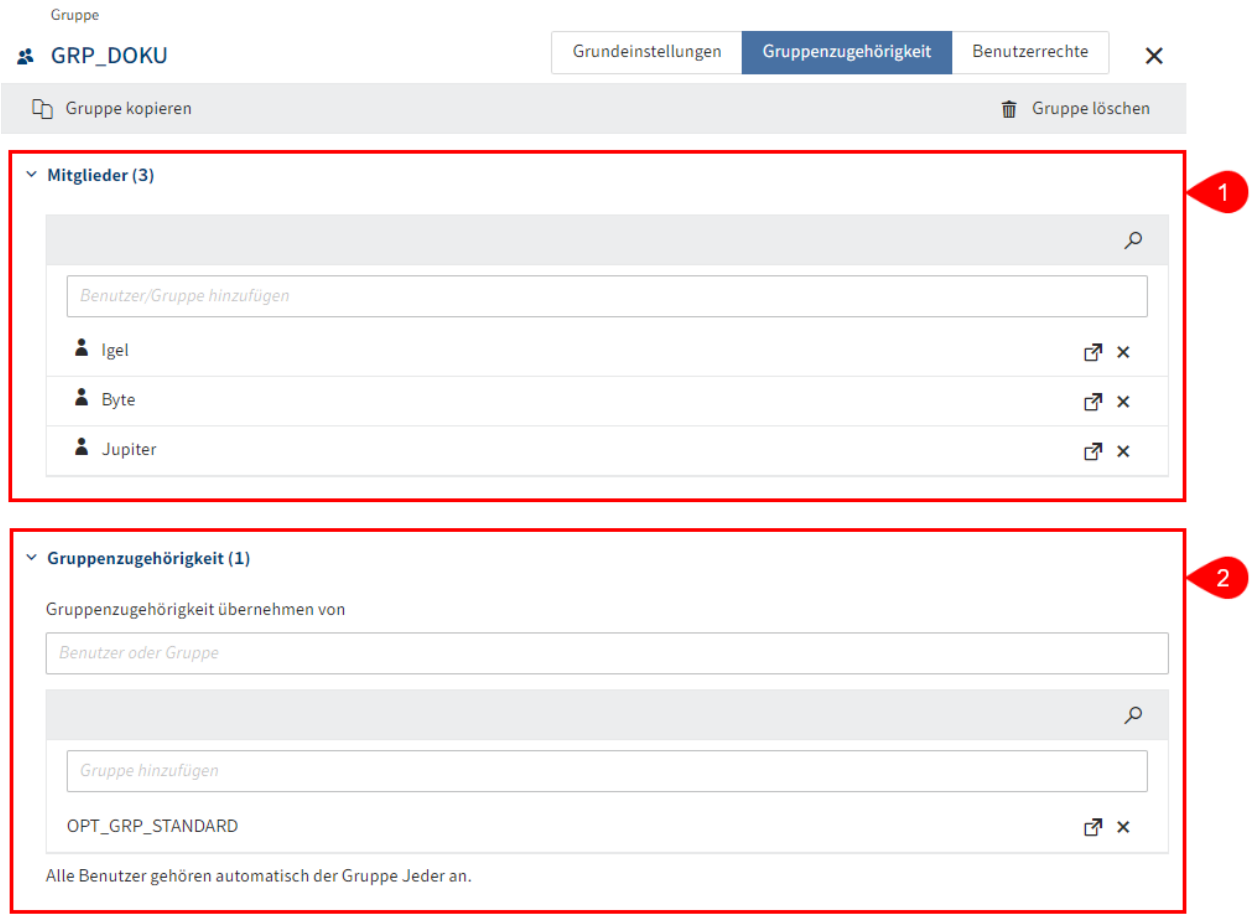
Über diese Gruppen können Sie kontrollieren, wer welche Funktionen in welchem Zusammenhang zur Verfügung gestellt bekommt.

Sie können hierüber steuern, wer gewisse ELO Funktionen nur über die rechte Maustaste, nur über die Symbole der Multifunktionsleiste, beides gleichzeitig oder in gewissen Bereichen der Software überhaupt nicht zur Verfügung gestellt bekommt. Auch Scripte und deren Ausführung sowie Icons können hier pro Optionengruppe gesteuert werden.

Das ist vor allem für ELO Arbeitsplätze mit speziellen Aufgabenbereichen sinnvoll. So lassen sich ELO Arbeitsplätze übersichtlicher gestalten und Fehlbedienungen ausschließen.

> **Beachten Sie**
>
> Ein ELO Konto sollte nur in einer Optionengruppe vorhanden sein. Mitgliedschaften in mehreren Optionengruppen können dazu führen, dass Einstellungen miteinander konkurrieren.

Gruppenzugehörigkeit festlegen

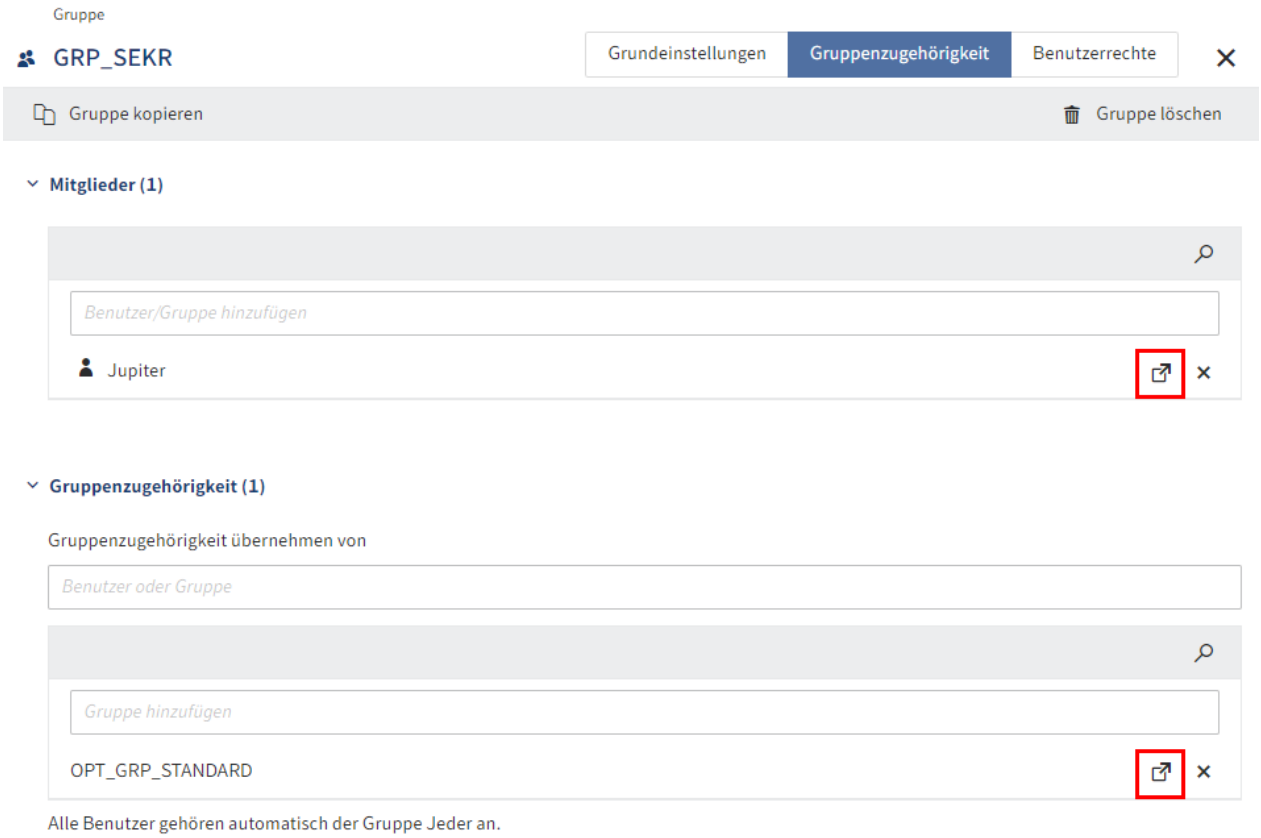


1 Mitglieder: Bestehende Benutzer oder Gruppen als Mitglieder hinzufügen. Die Anzahl der Mitglieder dieser Gruppe wird in Klammern angezeigt.

2 Gruppenzugehörigkeit: Bestehende Gruppenzugehörigkeiten anderer Gruppen oder Benutzer übernehmen oder bestehende Gruppen manuell hinzufügen. Die Anzahl der Gruppenzugehörigkeit dieser Gruppe wird in Klammern angezeigt.

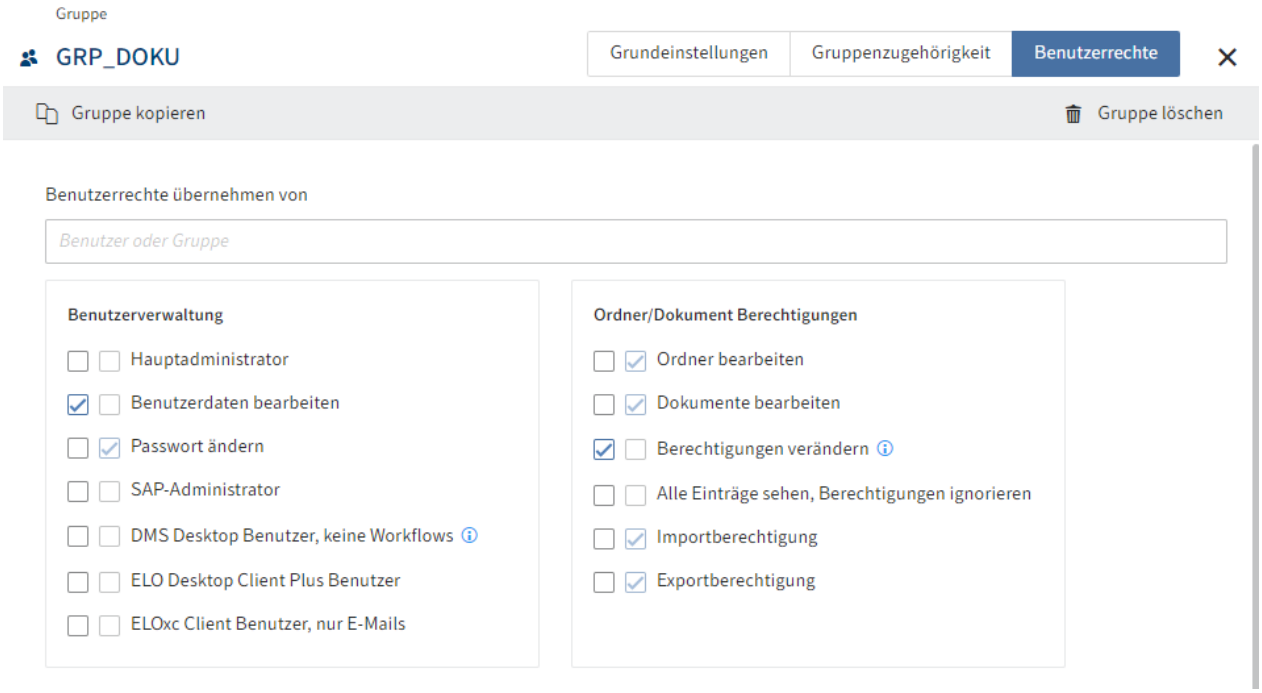
> **Information**
>
> Gruppen können in andere Gruppen aufgenommen werden. Dadurch lassen sich komplexe Kombinationen von Rechteeinstellungen und Berechtigungskonzepte realisieren.

> **Information**
>
> Tippen Sie ein Leerzeichen in eines der Eingabefelder ein, wird die gesamte Liste der vorhandenen Benutzer und Gruppen angezeigt.



Um in die Einstellungen eines Mitglieds oder einer zugehörigen Gruppe zu gelangen, wählen Sie das entsprechende Linksymbol. Die Einstellungen erscheinen in einem neuen Browser-Tab.

Benutzerrechte zuweisen



Es gibt drei Möglichkeiten für die Vergabe von Benutzerrechten:

- Vererbung

Weitere Informationen dazu finden Sie unter Konfiguration und Verwaltung > Benutzerverwaltung > Rechte in ELO > Vererbung von Rechten.

- Manuelle Zuweisung

  Weitere Informationen dazu finden Sie unter Konfiguration und Verwaltung > Benutzerverwaltung > Rechte in ELO > Benutzerrechte.

- Übernehmen von einer anderen Gruppe oder einem Benutzer

> **Information**
>
> Im Idealfall werden alle Rechte über Gruppen vererbt. Das vereinfacht die Rechtevergabe und die Rechteverwaltung.

Gruppe löschen

> **Beachten Sie**
>
> Wenn Sie eine Gruppe löschen, wird diese unwiderruflich gelöscht.

Löschen Sie keine Gruppe, die bereits in ELO verwendet wurde. Dadurch kann es zu Inkonsistenzen kommen. In diesem Fall ist es besser, die Gruppe nicht zu löschen, sondern die Grundeinstellungen zu ändern:

- Deaktivieren Sie *Sichtbar in Benutzerlisten*

Die Gruppe ist in ELO nur noch im Hintergrund vorhanden. Dennoch bleibt die Rechtevergabe über die Gruppe bestehen und bisherige Aktionen mit dieser Gruppe, wie beispielsweise Beteiligungen an Workflows, sind noch in ELO sichtbar.

Weitere Konfigurationen

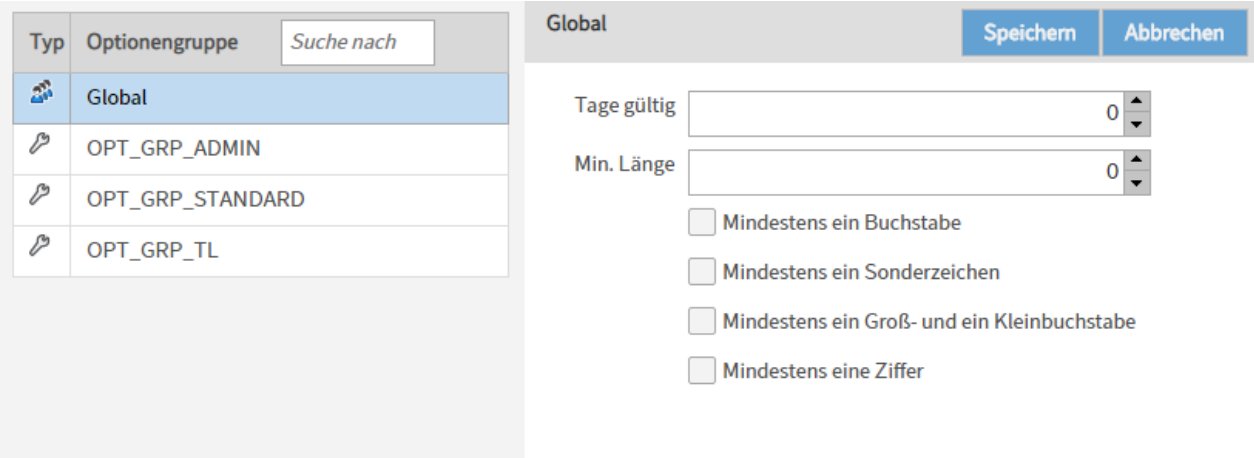
Einführung

Weitere Konfigurationen für die Administration der Benutzerverwaltung sind:

- Das Festlegen von Passwortregeln
- Zugang sperren
- Organisationseinheiten

Passwortregeln

Im Bereich *Passwortregeln* (*Wartung > Passwortregeln*) legen Sie die Regeln für die Einstellungen zur Passwortsicherheit fest.



Tage gültig: Legen Sie die Gültigkeitsdauer des Passwortes fest.

Min. Länge: Legen Sie die minimale Länge für Passwörter in ELO fest.

> **Information**
>
> Je mehr verschiedene Zeichen und Sonderzeichen verwendet werden, desto sicherer ist das verwendete Passwort. Legen Sie fest, welche Zeichen in dem Passwort verwendet werden müssen.

Zugang sperren

Über den Menüpunkt *Zugang sperren* (*Weitere > Zugang sperren*) können Sie festlegen, dass nur Mitglieder der ausgewählten Gruppe Zugriff auf ELO haben.

Repository zugänglich für Gruppe: Sobald Sie in diesem Feld anfangen zu tippen, schlägt Ihnen ELO passende Gruppen vor. Wählen Sie eine Gruppe aus und bestätigen Sie die Auswahl mit *Speichern*. Das jeweilige Repository ist dann nur noch für Mitglieder dieser Gruppe zugänglich.

Beachten Sie

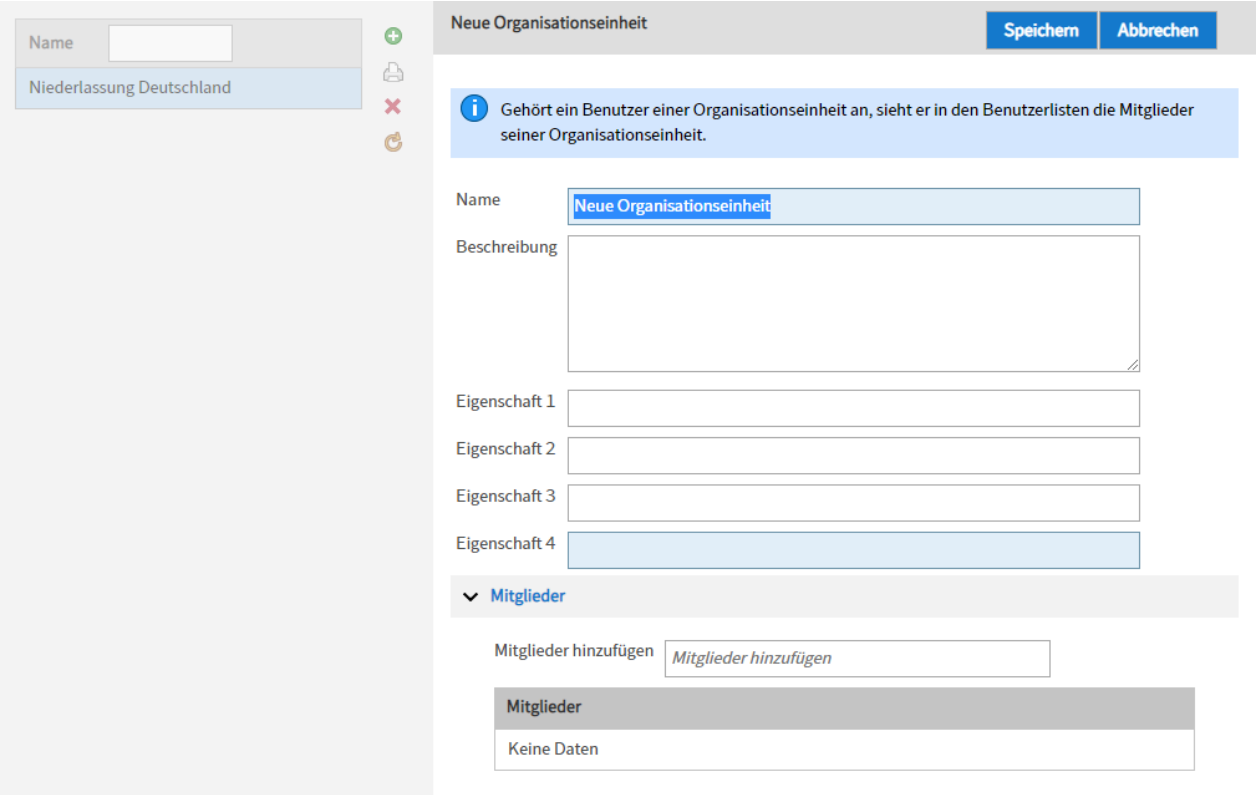
Eine Anmeldung mit Konten, die über das Benutzerrecht *Hauptadministrator* verfügen, ist jederzeit möglich. Personen, die bereits angemeldet sind, können ELO weiterhin nutzen, bis sie sich abmelden.

Information

Um das Repository wieder für alle Konten freizugeben, verwenden Sie die Gruppe *Jeder*.

Organisationseinheiten

Die Organisationseinheiten öffnen Sie in der ELO Administration Console über *Systemeinstellungen > Organisationseinheiten*.



Organisationseinheiten dienen zur Einteilung und strikten Trennung von Konten.

Die Mitglieder einer Organisationseinheit sehen nur die in ihrer Organisationseinheit enthaltenen Konten.

Dies kann beispielsweise bei sehr großen Unternehmen sinnvoll sein, wenn die Niederlassungen in verschiedenen Ländern nicht direkt zusammenarbeiten. Ein Konto oder eine Gruppe kann nur einer Organisationseinheit angehören. Die Zugehörigkeit zu einer Organisationseinheit kann über Gruppen vererbt werden.

> **Information**
>
> Verschiedene Organisationseinheiten sollten keine namensgleichen Konten verwalten.
>
> Beispiel: Drei verschiedene Organisationseinheiten sollten nicht alle das Konto *Admin* enthalten.

Rechte in ELO

Einführung

Diese Dokumentation behandelt die Rechte und Rechtevergabe in ELO.

Durch die Rechtevergabe in ELO wird festgelegt, welche Aktionen grundsätzlich in ELO ausgeführt werden dürfen. Die Rechte werden in der ELO Administration Console vergeben.

Rechte gelten grundsätzlich in ELO. Zusätzlich gibt es Berechtigungen für die einzelnen Einträge und Elemente in ELO. Welche Aktionen dann tatsächlich auf einem Eintrag oder Element durchgeführt werden dürfen, ergibt sich aus der Kombination von Berechtigungen und Rechten.

Beispiele:

1. Sie haben das Benutzerrecht *Dokumente löschen*, das Ihnen generell erlaubt, Dokumente in ELO zu löschen. Für ein bestimmtes Dokument haben Sie jedoch nur die Berechtigung *Sehen (R)*. Sie können dieses Dokument trotz des generellen Rechts nicht löschen, da Sie die Berechtigung zum Löschen für genau dieses Dokument nicht haben.

2. Sie haben für ein bestimmtes Dokument die Berechtigungen *Sehen (R)* und *Löschen (D)*. Jedoch haben Sie nicht das Benutzerrecht *Dokumente löschen*. Sie können dieses Dokument trotz der gesetzten Berechtigungen nicht löschen, da Sie das Recht nicht besitzen und somit generell keine Dokumente im System löschen dürfen.

Weitere Informationen finden Sie in den nachfolgenden Abschnitten:

- Benutzerrechte
- Vererbung von Rechten
- Rechtevergabe in den ELO Spaces
- Konfiguration

Verwandtes Thema

Berechtigungen in ELO: Durch die Vergabe der Berechtigungen wird festgelegt, wer welche Aktionen auf einem bestimmten Eintrag oder Element in ELO durchführen darf. Informationen zu den Berechtigungen in ELO finden Sie unter Konfiguration und Verwaltung > Benutzerverwaltung > Berechtigungen in ELO.

Benutzerrechte

Die Benutzerrechte können Sie in der Konfiguration der Benutzer und Gruppen verwalten.

> **Information**
>
> Im Idealfall werden alle Rechte über Gruppen vererbt. Das vereinfacht die Rechtevergabe und die Rechteverwaltung.

Rechte zur Benutzerverwaltung

Hauptadministrator (FLAG_ADMIN)

Dieses Recht wird benötigt, um globale Einstellungen vorzunehmen.

Besitzen Sie das Recht *Hauptadministrator*, können Sie alle Benutzer und Gruppen sehen, auch wenn bei diesen die Option *Sichtbar in Benutzerlisten* deaktiviert ist. Besitzen Sie zusätzlich das Recht *Benutzerdaten bearbeiten*, können Sie alle Benutzer und Gruppen administrieren.

Das Recht *Hauptadministrator* ermöglicht, die Berechtigungen der obersten Ebene des Repositorys zu verändern: Um die Berechtigungen und Optionen der obersten Ebenen zu ändern, müssen Sie den Dialog *Berechtigungen setzen* öffnen, dies geht nur mit dem Recht *Hauptadministrator*. Um die Berechtigungen tatsächlich zu ändern, brauchen Sie aber das Recht *Berechtigungen verändern*, also benötigen Sie hier beide Rechte.

Mit dem Recht *Hauptadministrator* dürfen Sie folgende Aktionen in ELO durchführen:

- Einträge dauerhaft entfernen, auch wenn Sie die Rechte *Ordner löschen*, *Dokumente löschen*, *Nicht änderbare Dokumente löschen* und *Versionen löschen* nicht besitzen
- Eine Sperre für alle Einträge entfernen, nicht nur für die selbst gesperrten Einträge
- Vertretung für alle Benutzer einsetzen
- Ansichten und Anzeigeprofile für alle Benutzer verwalten
- Masken löschen
-

Anmeldung beim Administrationsmodus oder bei geschlossenem Repository

Weitere Informationen finden Sie unter Rechte in ELO > Konfiguration > Notwendige Rechte für die Bereiche der ELO Administration Console.

Benutzerdaten bearbeiten (FLAG_SUBADMIN)

Mit dem Recht *Benutzerdaten bearbeiten* dürfen Sie folgende Aktionen in ELO durchführen:

- Benutzer und Gruppen anlegen. Gruppen und andere Benutzer können nur mit den gleichen (oder weniger) Rechten ausgestattet werden.
- Benutzer und Gruppen administrieren, wenn Sie im Feld *Administrator* des jeweiligen Benutzers bzw. der Gruppe eingetragen sind oder Sie zusätzlich das Recht *Hauptadministrator* besitzen. Ist im Feld *Administrator* eine Gruppe eingetragen, können alle Mitglieder dieser Gruppe den entsprechenden Benutzer oder die Gruppe administrieren, wenn die administrierende Gruppe zusätzlich das Recht *Hauptadministrator* besitzt.
- Sie können nur Gruppen zuweisen, in denen Sie als *Administrator* eingetragen sind oder wenn Sie zusätzlich das Recht *Hauptadministrator* besitzen.
- Eigene Benutzerdaten verwalten, wenn Sie selbst als *Administrator* in der Benutzerverwaltung eingetragen sind oder zusätzlich das Recht *Hauptadministrator* besitzen.
- Im ELO Java Client können *Vertretungsregelungen für andere* mit diesem Recht für die selbst administrierten Benutzer eingestellt werden, auch wenn diese Benutzer nicht *Sichtbar in Benutzerlisten* sind.

> **Information**
>
> Nur Benutzer mit den Rechten *Hauptadministrator* und *Benutzerdaten bearbeiten* können alle Benutzer und Gruppen sehen und administrieren.

Passwort ändern (FLAG_CHANGEPW)

Mit diesem Recht darf das eigene Passwort für die Anmeldung im System geändert werden.

SAP-Administrator (FLAG_SAPADMIN)

Dieses Recht dient zur Anbindung von ELO an SAP mittels ELO Suite for SAP ArchiveLink® und ermöglicht die Verwaltung der Ablagemaske, die die Schnittstelle zu SAP betrifft. Die Ablagemaske für SAP-verwaltete Dokumente ist für alle sichtbar, kann aber nur bearbeitet werden, wenn man dieses Recht besitzt.

DMS Desktop Benutzer, keine Workflows (FLAG2_IS_DMS_DESKTOP_USER)

Ist diese Option gesetzt, stehen keinerlei Workflow-Funktionen zur Verfügung. Folgende Funktionen sind betroffen:

- Ad-hoc-Workflow
- Fristverlängerung Workflow
- Übersicht Workflows
- Workflow abgeben
-

Workflow annehmen
- Workflow anzeigen
- Workflow delegieren
- Workflow starten
- Workflow weiterleiten
- Workflow zurückgeben
- Workflow zurückstellen
- Workflows zum Eintrag
- Workflow-Vorlagen bearbeiten
- Zurückstellung löschen

> **Beachten Sie**
>
> Dieses Recht ist eine Einschränkung und überschreibt alle anderen Rechte, die es zu Workflows gibt. Ist dieses Recht gesetzt, können alle Funktionen und Rollen, die Workflows betreffen, nicht verwendet werden, egal ob die einzelnen Rechte direkt eingestellt oder vererbt werden. Auch zugewiesene Workflow-Aufgaben können nicht bearbeitet werden. Hintergrund ist, dass im ELO DMS Desktop keine Workflows inbegriffen sind.

ELO Desktop Client Plus Benutzer (FLAG2_DESKTOP_CLIENT_PLUS)

Dieses Recht öffnet den ELO Desktop Client im erweiterten Modus mit einigen Funktionalitäten zu Aufgaben und dem Vollclient-Darstellungsmodus.

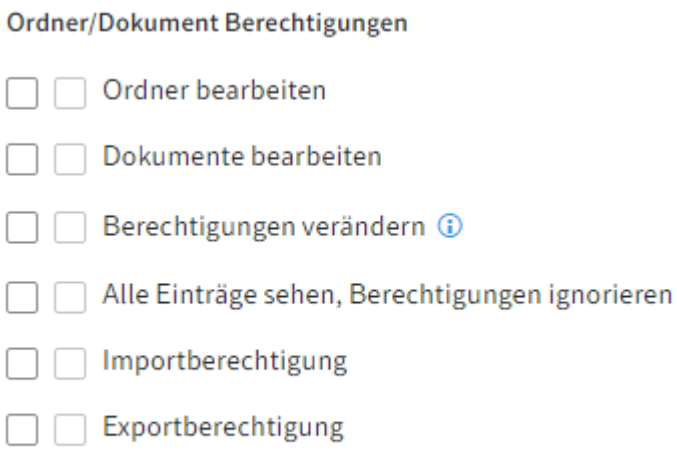
> **Beachten Sie**
>
> Dieses Recht schränkt die Funktionalitäten ein.

ELOxc Client Benutzer, nur E-Mails (FLAG2_LIMITED_CLIENT)

Dieses Recht öffnet den Client for Microsoft Outlook im ELOxc for Microsoft EWS-Modus, eingeschränkt auf die Dateiformate (EML, MSG und VCF), die von Microsoft Outlook geöffnet werden können. Alle anderen Formate sind nicht zugänglich.

> **Beachten Sie**
>
> Dieses Recht schränkt die Funktionalitäten ein.

Rechte zu Ordner/Dokument Berechtigungen



Ordner bearbeiten (FLAG_EDITSTRUCTURE)

Dieses Recht erlaubt das Bearbeiten und Anlegen von Strukturen in Ordnern.

Dokumente bearbeiten (FLAG_EDITDOCS)

Dieses Recht erlaubt das Bearbeiten von Dokumenten. Dazu gehört:

- Laden neuer Versionen
- Aus- und Einchecken
- Dateien einfügen
- Dokumente aus Vorlagen
- Dateianbindungen hinzufügen und löschen
- In Volltext aufnehmen
- Aus Volltext entfernen
- Signatur erstellen

Die Metadaten von Dokumenten können nur geändert werden, wenn das Recht vorhanden ist. Ohne dieses Recht öffnen sich die Metadaten im Read-only-Modus.

Berechtigungen verändern (FLAG_EDITACL)

Dieses Recht erlaubt das Bearbeiten der Berechtigungen von Einträgen (Dokumente und Ordner) in ELO.

> **Information**
>
> Um die Berechtigungen der Einträge verändern zu können, wird grundsätzlich das Recht *Ordner bearbeiten* oder *Dokumente bearbeiten* benötigt. Zusätzlich benötigt man bei den einzelnen Einträgen die Berechtigung *Berechtigungen setzen* (P).

Bei der Ablage im Client hat man in jedem Fall die Möglichkeit, die Rechte einzustellen, da man auch die vollen Rechte an der Datei besitzt. Das Benutzerrecht bezieht sich auf das nachträgliche Bearbeiten der Berechtigungen.

Dieses Recht betrifft nicht die Berechtigungseinstellungen in der ELO Administration Console oder in der Konfiguration des ELO Java Clients. Wenn man z. B. Stempel oder Masken bearbeiten kann, kann man auch deren Berechtigungen bearbeiten, ohne dass dieses Benutzerrecht geprüft wird.

Alle Einträge sehen, Berechtigungen ignorieren (FLAG_IGNOREACL)

Dieses Recht beinhaltet, dass alle Dokumente und Ordner angezeigt werden, auch wenn sie für das jeweilige Konto eigentlich gesperrt sind. Es hebt alle vorhandenen Objektberechtigungen auf. Wer dieses Recht besitzt, hat volle Berechtigungen auf alle ELO Einträge.

Der einzige Weg, Dokumente vor Konten zu schützen, die dieses Benutzerrecht besitzen, ist es, sie zu verschlüsseln.

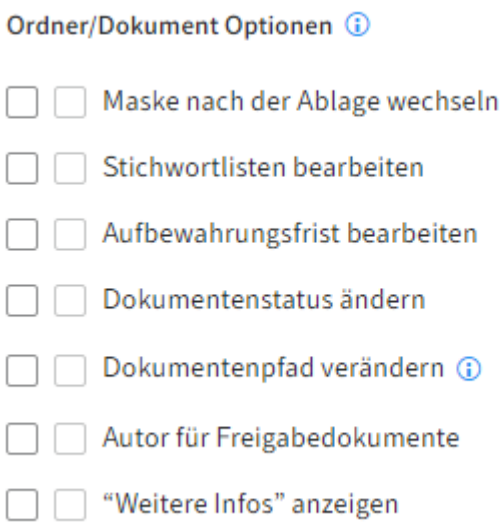
Importberechtigung (FLAG_IMPORT)

Dieses Recht erlaubt den Import eines Exportdatensatzes in das Repository. Alle Daten werden importiert, die in dem Datensatz vorhanden sind, unabhängig von den Objektberechtigungen. Es werden also auch die Daten importiert, für die das Konto keine Berechtigung besitzt. Diese Daten sind über dieses Konto anschließend nicht sichtbar.

Exportberechtigung (FLAG_EXPORT)

Dieses Recht erlaubt, einen Exportdatensatz zu erstellen. Man kann nur die Einträge und Dokumente exportieren, für die man die entsprechenden Berechtigungen hat.

Rechte zu Ordner/Dokument Optionen



Information

> Die Rechte in dieser Gruppe (außer *Dokumentenpfad verändern*) sind nur wirksam, wenn auch das Recht *Ordner bearbeiten* beziehungsweise *Dokumente bearbeiten* vorhanden ist.

Maske nach Ablage wechseln (FLAG_CHANGEMASK)

Mit diesem Recht kann man einem bereits abgelegten Dokument nachträglich eine andere Maske zuweisen. Hierbei ist zu beachten, dass beim Maskenwechsel Metadaten verloren gehen können. Voraussetzung ist, dass das Recht *Ordner bearbeiten* beziehungsweise *Dokumenten bearbeiten*, je nach Eintrag, vorhanden ist.

Stichwortlisten bearbeiten (FLAG_EDITSWL)

Mit diesem Recht kann man die Stichwortlisten bearbeiten. Man kann neue Einträge hinzufügen, verändern und auch löschen. Ohne dieses Benutzerrecht kann man – auch wenn man das Recht *Masken und Felder bearbeiten* hat – die Stichwortlisten in der Verwaltung der Masken in der ELO Administration Console nicht bearbeiten.

Voraussetzung im Client ist, dass das Recht *Ordner bearbeiten* beziehungsweise *Dokumente bearbeiten*, je nach Eintrag, vorhanden ist.

Aufbewahrungsfrist bearbeiten (FLAG_EDITDUEDATE)

Mit diesem Recht darf die Aufbewahrungsfrist von Dokumenten gesetzt und verlängert werden (Datum darf nur weiter in die Zukunft verschoben werden). Ist das Recht nicht gesetzt, ist das entsprechende Feld in dem Dialog *Metadaten* deaktiviert.

Voraussetzung ist, dass das Recht *Ordner bearbeiten* beziehungsweise *Dokumente bearbeiten*, je nach Eintrag, vorhanden ist.

Dokumentenstatus ändern (FLAG_CHANGEREV)

Dieses Recht erlaubt, den Dokumentenstatus im Dialog *Metadaten* über den Reiter *Optionen* von Dokumenten einzustellen:

- Keine Versionskontrolle
- Versionskontrolle eingeschaltet
- Keine Änderung möglich

Voraussetzung ist, dass das Recht *Dokumente bearbeiten* vorhanden ist.

Dokumentenpfad verändern (FLAG_CHANGEPATH)

Mit diesem Recht kann man die Auswahlliste für den Dokumentenpfad in den Optionen bei den Dokumenten verwenden und diesen für ein bestimmtes Dokument ändern. Das ist nur bei der Eingabe der Metadaten in der Postbox möglich. Wenn ein Dokument schon abgelegt wurde, wird diese Auswahlliste für immer inaktiv. Nachträglich kann man nur mit der Funktion *Dokumentendateien verschieben* und mit dem Recht *Hauptadministrator* die Dokumente auf einen anderen Pfad verschieben.

Mit diesem Recht kann man nicht neue Dokumentenpfade anlegen und deren Definition ändern. Um die Dokumentenpfade zu bearbeiten, anzulegen und zuzuweisen benötigt man das Recht *Hauptadministrator*.

Autor für Freigabedokumente (FLAG_AUTHOR)

Dieses Recht erlaubt, die Checkbox *Freigabedokument* zu aktivieren oder zu deaktivieren und Freigabedokumente zu bearbeiten: Für den Autor besteht die Möglichkeit, vorhergehende Versionen eines Dokuments weiterhin zu bearbeiten. Beim Auschecken wird ein Auswahldialog über alle Dokumentversionen angezeigt. Beim Einchecken wird die alte Arbeitsversion beibehalten. Die Arbeitsversion (= freigegebene Version) darf nur ein Autor für Freigabedokumente ändern.

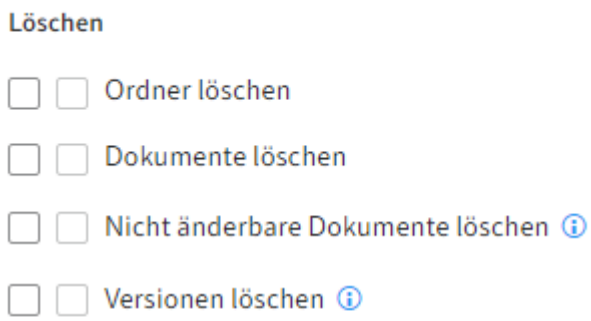
Voraussetzung ist, dass das Recht *Dokumente bearbeiten* vorhanden ist.

"Weitere Infos" anzeigen (FLAG2_SHOW_EXTRA_INFO)

Dieses Recht legt fest, ob man im Dialog *Metadaten* den Tab *Weitere Infos* sehen kann.

Voraussetzung ist, dass das Recht *Ordner bearbeiten* beziehungsweise *Dokumente bearbeiten*, je nach Eintrag, vorhanden ist.

Rechte zum Löschen



Ordner löschen (FLAG_DELSTRUC)

Dieses Recht legt fest, ob man Ordner löschen darf.

Dokumente löschen (FLAG_DELDOC)

Dieses Recht legt fest, ob man Dokumente löschen darf.

Nicht änderbare Dokumente löschen (FLAG_DELREADONLY)

Mit diesem Recht kann man Dokumente löschen, die mit dem Dokumentenstatus *Keine Änderung möglich* abgelegt oder zu diesem Status geändert wurden.

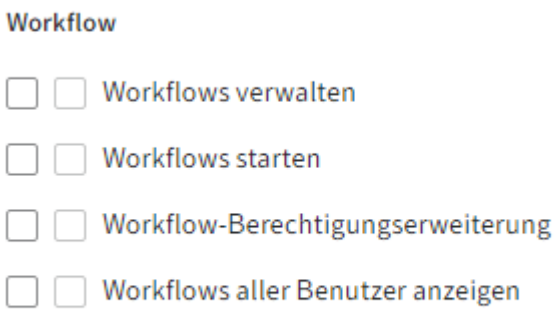
Voraussetzung ist, dass das Recht *Dokumente löschen* vorhanden ist.

Versionen löschen (FLAG_DELVERSION)

Mit diesem Recht kann man einzelne Versionen aus der Versionsverwaltung eines Dokuments löschen.

Im ELO Java Client kann man bei der aktivierten Funktion *Gelöschte Einträge einblenden* die gelöschten Versionen eines Dokuments im Dialog *Dokumentversionen* sehen.

Rechte zu Workflows



Workflows verwalten (FLAG_EDITWF)

Zur Verwaltung der Workflows gehören:

- Workflow-Vorlagen und Formulare erstellen
- Bestehende aktive Workflows vorzeitig beenden
- Erledigte und vorzeitig beendete Workflows dauerhaft entfernen
- Bei der Teilnahme an Workflows nachfolgende Knoten bearbeiten

Workflows starten (FLAG_STARTWF)

Mit diesem Recht kann man Workflows starten. Folgende Funktionen sind betroffen:

- Ad-hoc-Workflow
- Übersicht Workflows
- Workflow starten
- Workflows zum Eintrag

Man benötigt dieses Recht auch, um Workflows bei der Ablage von Einträgen mit einer Maske mit einem hinterlegten Workflow zu starten. Hat man dieses Recht nicht, dann kann man zwar Dokumente mit dieser Maske ablegen, aber es startet kein Workflow.

Dieses Recht wird auch geprüft, um überhaupt die *Übersicht Workflows* und die *Workflows zum Eintrag* in der Multifunktionsleiste im ELO Client aktiv zu bekommen. So kann man sich einen Überblick über alle Workflows verschaffen, an denen man direkt oder indirekt über eine Gruppe beteiligt ist.

Workflow-Berechtigungserweiterung (FLAG2_EXTEND_WORKFLOW_RIGHTS)

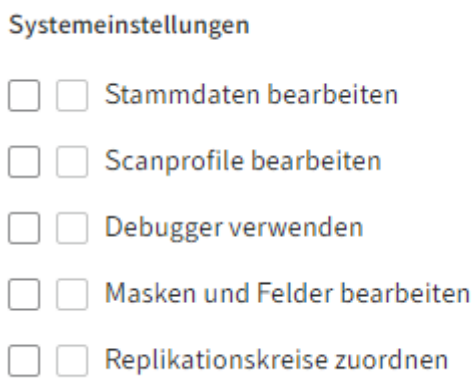
Ist dieses Recht gesetzt, erhält man ein temporäres Leserecht für den im aktiven Workflowknoten befindlichen Eintrag. Lesen des Dokuments ist dann nur im Aufgabenbereich möglich und auch nur solange das Dokument an einen selbst oder an eine Gruppe, deren Mitglied man ist, gerichtet ist. Zusätzlich kann über einen Eintrag in der Datenbank-Tabelle *ProfileOpts* gesteuert werden, inwieweit noch weitere Berechtigungen temporärer oder dauerhafter Natur vergeben werden.

Dieses Recht kann nicht (auch nicht temporär) andere Benutzerrechte ersetzen. Das Recht betrifft Dokumente und Ordner, aber nicht Masken.

Workflows aller Benutzer anzeigen (FLAG2_WF_CONTROLLER)

Das Recht erlaubt es, alle aktiven Workflows zu sehen und nicht nur diejenigen, an denen man beteiligt ist.

Rechte zu Systemeinstellungen



Stammdaten bearbeiten (FLAG_EDITCONFIG)

Mit diesem Recht hat man Zugriff auf die Verwaltung der *Eintragstypen* (Icons und Bezeichnungen für Ordner und Dokumente), *Schriftfarben* und *Stempel*.

Scanprofile bearbeiten (FLAG_EDITSCAN)

Die Aktivierung dieser Funktion berechtigt dazu, die Einstellungen für die Scanparameter und *Scanprofile* für sich selbst zu verändern. Mit dem Recht *Hauptadministrator* ist man auch dazu berechtigt, die globalen *Scanprofile* und die Scanparameter für andere Konten zu verändern und zu verwalten.

Debugger verwenden (FLAG_EDITSCRIPT)

Im ELO Java Client kann man mit diesem Recht über den Tastaturbefehl STRG + ALT + D den JavaScript-Debugger öffnen.

> **Information**
>
> Scripte werden in ELO wie Dokumente verwaltet. Um Scripte bearbeiten zu dürfen, muss man die entsprechenden Berechtigungen besitzen.

Masken und Felder bearbeiten (FLAG_EDITMASK)

Mit diesem Recht darf man neue Masken anlegen und bestehende Masken verändern.

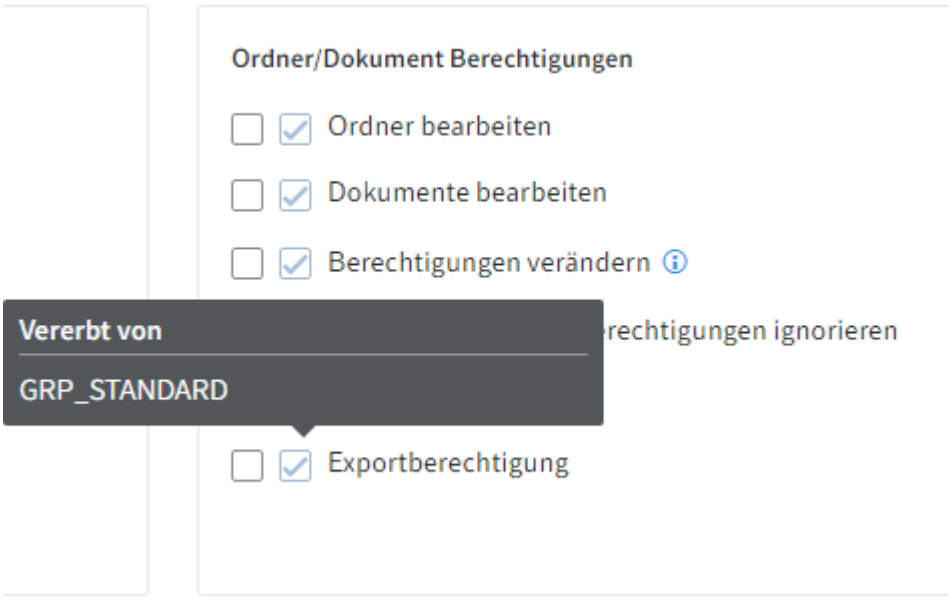
Wenn die Stichwortlisten in den Masken bearbeitet werden müssen, benötigt man zusätzlich das Recht *Stichwortlisten bearbeiten*.

Replikationskreise zuordnen (FLAG_EDITREPL)

Dieses Recht benötigt man, um Daten eines Repositorys Replikationskreisen zuordnen zu dürfen. Replikationskreise werden von ELO Replication benötigt, um Abgleichmengen feststellen zu können.

Vererbung von Rechten

Vor den Benutzerrechten befinden sich jeweils zwei Checkboxen. Die Checkboxen links beziehen sich jeweils auf die individuellen Rechte des Kontos oder der Gruppe. Die Checkboxen rechts beziehen sich auf die von den Gruppenzugehörigkeiten übernommenen Rechte. Beim Mouseover über eine der Checkboxen rechts erscheint ein Tooltip mit der Information, woher das jeweilige Recht geerbt wurde.



Information

Im Idealfall werden alle Rechte über Gruppen vererbt. Das vereinfacht die Rechtevergabe und die Rechteverwaltung.

Rechtevergabe in den ELO Spaces

Die Rechte für die Team- und Workspaces in ELO werden über die zugewiesenen Rollen festgelegt.

Teamspace

Sie können einer Rolle die folgenden besonderen Teamspace-Rechte zuweisen:

- Rollen bearbeiten: Bearbeiten und Anlegen von Rollen im Teamspace, unabhängig davon, ob der Teamspace selbst bearbeitet werden darf.
- Teamspace bearbeiten: Änderungen an einem Teamspace vornehmen. Zusätzlich kann man die Rollenzuweisung von Mitgliedern des Teamspace ändern und neue Mitglieder hinzufügen.
- Teamspace löschen: Kann nur aktiviert werden, wenn auch *Teamspace bearbeiten* aktiviert ist.

Weitere Informationen zu den Rollen im Teamspace finden Sie unter ELO Pakete > ELO Teamspaces > Rollen festlegen.

Workspace

Sie können einer Rolle die folgenden besonderen Workspace-Rechte zuweisen:

- Workspace bearbeiten: Änderungen an einem Workspace vornehmen. Zusätzlich kann man die Rollenzuweisung von Mitgliedern des Workspace ändern und neue Mitglieder hinzufügen.
- Rollen bearbeiten: Bearbeiten und Anlegen von Rollen im Workspace. Kann nur aktiviert werden, wenn auch *Workspace bearbeiten* aktiviert ist.
- Workspace löschen: Kann nur aktiviert werden, wenn auch *Workspace bearbeiten* aktiviert ist.

Weitere Informationen zu den Rollen im Workspace finden Sie unter ELO Pakete > ELO Workspaces > Rollen festlegen.

Konfiguration

Notwendige Rechte für die Bereiche der ELO Administration Console

Systemeinstellungen

Administrationsbereiche	Rechte
Benutzer- und Gruppenverwaltung	Benutzerdaten bearbeiten, Hauptadministrator
	Mit dem Recht *Hauptadministrator* kann man ALLE Benutzer und Gruppen administrieren, nicht nur diejenigen, bei denen man als Administrator gesetzt ist.
Organisationseinheiten	Hauptadministrator
	Als Administrator von einem Benutzer (mit dem Recht *Benutzerdaten bearbeiten*), kann man diesen Benutzer einer vorhandenen Organisationseinheit zuweisen, als Hauptadministrator hat man Zugriff auf den Bereich *Organisationseinheiten*.
Masken	Masken und Felder bearbeiten
	Man benötigt separat das Recht *Stichwortlisten bearbeiten*, um auch die Stichwortlisten darin bearbeiten zu können, und das Recht *Hauptadministrator*, um Masken zu löschen oder nachträglich deren Daten als Tabelle zu speichern.
Feldvorlagen	Masken bearbeiten
Stichwortlisten	Stichwortlisten bearbeiten
Eintragstypen	Stammdaten bearbeiten
Dokumentenpfade	Hauptadministrator
Standard-Dokumentenpfade	Hauptadministrator
Verschlüsselungskreise	Hauptadministrator
ELO Online-Hilfe-URL	Hauptadministrator
Stempel	Stammdaten bearbeiten
ELO Forms Services-URL	Hauptadministrator
ELO Analytics-URL	
Repository-Eigenschaften	Hauptadministrator
Schriftfarben	Stammdaten bearbeiten

Wartung

Administrationsbereiche	Rechte
Administrationsmodus	Hauptadministrator
Reportoptionen	Hauptadministrator
Reporteinträge löschen	Hauptadministrator
Löschen und entfernen	Hauptadministrator

Administrationsbereiche	Rechte
Backup-Tasks	Hauptadministrator
Passwortregeln	Hauptadministrator
Dokumentdateien verschieben	Hauptadministrator

Servermodule

Administrationsbereiche	Rechte
ELO Automation Services	Hauptadministrator
Backup-Profile	Hauptadministrator
Volltextdienst	Hauptadministrator
Passwort erstellen	Hauptadministrator
ELO Transport	Hauptadministrator
Konfigurationsdateien	Hauptadministrator
Formulardesigner	Workflows verwalten
ELOxc	*Keine Prüfung in der ELO Administration Console. Die Prüfung übernimmt ELOxc selbst.*

Systeminformationen

Administrationsbereiche	Rechte
Administrationsordner	Hauptadministrator
Serverinformationen	Hauptadministrator
Angemeldete Benutzer	Hauptadministrator
Statistik	Hauptadministrator
Lizenzübersicht	Hauptadministrator
Lizenzreport	Hauptadministrator
Log-Dateien	Hauptadministrator
Monitoring	Hauptadministrator
Checksummen prüfen	Hauptadministrator

Weitere

Administrationsbereiche	Rechte
LDAP-Import	Hauptadministrator
Zugang sperren	Hauptadministrator

Verschlüsselung von Dokumenten

In Systemen ist eine Methode enthalten, Dokumente zu verschlüsseln. Diese Dokumente sind auf Betriebssystemebene verschlüsselt, können nur mithilfe eines Passwortes geöffnet werden und bieten auch auf Datensicherungen höchste Sicherheit vor Lesbarkeit durch Unbefugte.

In ELO können Dokumente aus vertraulichen oder anderen Gründen besonders schützenswerter Inhalte zusätzlich zu den ACL-Berechtigungseinstellungen noch verschlüsselt werden. Damit sind Dokumente auch auf dem Betriebssystem wirksam gegen Administratoren geschützt.

In ELO wird seit Version 12 mit AES-256 (Advanced Encryption Standard) verschlüsselt, einer symmetrischen Verschlüsselungsmethode, die mit Blockverschlüsselung arbeitet. Mehr als 16 Verschlüsselungskreise sind nun verfügbar. Die Ver- und Entschlüsselung findet auf Serverseite statt.

Bereits verschlüsselte Dokumente verbleiben im alten Verschlüsselungsmodus. Beide Verschlüsselungsverfahren werden in der Datenbank gekennzeichnet und in einem Kompatibilitätsmodus nebeneinander betrieben.

Eine Verschlüsselung kann mit ELO Funktionen nur beim Eintritt in das ELO Repository erfolgen. Dokumente in der Postbox lagern dort immer unverschlüsselt, bis sie letztendlich ins Repository verschoben werden. Eine nachträgliche Verschlüsselung schon in ELO befindlicher Dokumente ist über ELO Funktionen nicht vorgesehen und in der Regel auch nicht sinnvoll, denn sobald im Repository abgelegt, sind Dokumente gegebenenfalls auf einem Spiegelpfad, auf revisionssicheren Medien und eventuell auch schon unverschlüsselt in verschiedenen Backup-Systemen verteilt.

Verschlüsselung kann nur von Personen eingerichtet werden, die das Recht *Hauptadministrator* besitzen. Wer den Verschlüsselungskreis und das dazugehörige Verschlüsselungspasswort kennt, kann die Verschlüsselung einsetzen. Ein Verschlüsselungskreis ist also nicht zwingend an eine einzelne Person gebunden, er kann auch für Gruppen verwendet werden.

Die mit AES-256 neu verschlüsselten Dokumente können in den Volltext aufgenommen werden. Dafür muss ein Systembenutzer eingerichtet werden, der den Zugriff auf die verschlüsselten Dokumente realisiert. Die verschlüsselten Dokumente können, müssen aber nicht in der Volltextdatenbank berücksichtigt werden.

Die Verschlüsselungskreise sind nicht mit dem Konzept der Schlüssel zu verwechseln, die mit der Version 10 abgekündigt wurden.

Weitere Informationen zur Verschlüsselung finden Sie unter Konfiguration und Verwaltung > Systemverwaltung > Ordner & Dokumente > Verschlüsselungskreise.

Berechtigungen in ELO

Einführung

In ELO werden Berechtigungen für jeden Eintrag und jedes Element vergeben. Dadurch wird festgelegt, wer welche Aktionen auf einem bestimmten Eintrag oder Element in ELO durchführen darf. Diese Berechtigungen werden in den Metadaten im Tab *Berechtigungen* vergeben.

Dabei handelt es sich um folgende Berechtigungen:

- R (Read)
- W (Write)
- D (Delete)
- E (Edit)
- L (List)
- P (Permissions)

Berechtigungen gelten für die einzelnen Einträge und Elemente in ELO. Rechte gelten grundsätzlich in ELO. Welche Aktionen dann tatsächlich auf einem Eintrag oder Element durchgeführt werden dürfen, ergibt sich aus der Kombination von Berechtigungen und Rechten.

Beispiele:

1. Sie haben das Benutzerrecht *Dokumente löschen*, das Ihnen generell erlaubt, Dokumente in ELO zu löschen. Für ein bestimmtes Dokument haben Sie jedoch nur die Berechtigung *Sehen (R)*. Sie können dieses Dokument trotz des generellen Rechts nicht löschen, da Sie die Berechtigung zum Löschen für genau dieses Dokument nicht haben.

2. Sie haben für ein bestimmtes Dokument die Berechtigungen *Sehen (R)* und *Löschen (D)*. Jedoch haben Sie nicht das Benutzerrecht *Dokumente löschen*. Sie können dieses Dokument trotz der gesetzten Berechtigungen nicht löschen, da Sie das Recht nicht besitzen und somit generell keine Dokumente im System löschen dürfen.

Weitere Informationen zu den Berechtigungen finden Sie in den nachfolgenden Abschnitten:

- Allgemeine Berechtigungen
- Weitere Berechtigungen

Verwandtes Thema

Rechte in ELO: Durch die Vergabe der Benutzerrechte wird festgelegt, welche Aktionen grundsätzlich in ELO ausgeführt werden dürfen. Informationen zu den Rechten in ELO finden Sie unter Konfiguration und Verwaltung > Benutzerverwaltung > Rechte in ELO.

Allgemeine Berechtigungen

Die Berechtigungen für Einträge und Elemente in ELO unterscheiden sich je nach Kontext.

In den folgenden Abschnitten finden Sie die Berechtigungen für die einzelnen Einträge und Elemente:

- Dokumente
- Ordner
- Randnotizen
- Anmerkungen (z. B. Stempel, Haftnotizen)
- Masken
- Workflow-Vorlagen
- Workflows
- ELO Spaces

Dokumente

Berechtigung	Beschreibung
Sehen (R)	Dokumente und Metadaten sehen, Anmerkungen und Randnotizen hinzufügen
Metadaten ändern (W)	
Löschen (D)	Dokumente als gelöscht markieren. Nur Personen mit administrativen Rechten können Dokumente endgültig löschen. Informationen dazu finden Sie unter Konfiguration und Verwaltung > Systemverwaltung > Ordner und Dokumente > Löschen und entfernen.
Bearbeiten (E)	Dokumente bearbeiten, z. B. einchecken, auschecken, neue Version laden, Arbeitsversion ändern
<Liste bearbeiten> (L)	Wirkt sich nicht auf Dokumente aus
Berechtigungen setzen (P)	Berechtigungen ändern (setzen, bearbeiten, löschen)

Ordner

Berechtigung	Beschreibung
Sehen (R)	Ordner und Metadaten sehen, Randnotizen hinzufügen
Metadaten ändern (W)	
Löschen (D)	Ordner als gelöscht markieren, wenn auch Untereinträge gelöscht werden dürfen oder der Ordner leer ist. Nur Personen mit administrativen Rechten können Ordner endgültig löschen. Informationen dazu finden Sie unter Konfiguration und Verwaltung > Systemverwaltung > Ordner und Dokumente > Löschen und entfernen.
<Bearbeiten> (E)	Wirkt sich nicht auf Ordner aus, ist aber wichtig für die Vererbung der Berechtigungen auf darin enthaltene Dokumente.

Berechtigung	Beschreibung
Liste bearbeiten (L)	Inhalt des Ordners verändern, z. B. Dokumente darin erstellen, verschieben, kopieren oder entfernen, Referenz einfügen oder löschen.
Berechtigungen setzen (P)	Berechtigungen ändern (setzen, bearbeiten, löschen)

Randnotizen

Es gibt drei verschiedene Arten von Randnotizen.

Allgemeine Randnotiz

Alle, die die Berechtigung *Sehen* für den Eintrag haben, können diese Randnotizen erstellen und sehen. Besitzt man ausschließlich die Berechtigung *Sehen* für den Eintrag, kann man nur allgemeine Randnotizen bearbeiten und löschen, die man selbst erstellt hat. Besitzt man zusätzlich die Berechtigung *Metadaten ändern* für den Eintrag, kann man alle Randnotizen bearbeiten und löschen.

Persönliche Randnotiz

Alle, die die Berechtigung *Sehen* für den Eintrag haben, können diese Randnotizen für sich selbst erstellen, bearbeiten und löschen. Keine andere Person kann diese Randnotizen sehen.

> **Information**
>
> Hauptadministratoren können persönliche Randnotizen von anderen Benutzern ebenfalls nicht sehen.

Permanente Randnotiz

Alle, die die Berechtigung *Sehen* für den Eintrag haben, können diese Randnotizen erstellen und sehen. Es ist nicht möglich, permanente Randnotizen nachträglich zu bearbeiten oder zu löschen.

> **Beachten Sie**
>
> Hauptadministratoren können permanente Randnotizen ebenfalls nicht nachträglich bearbeiten oder löschen.

Anmerkungen

Es gibt Anmerkungen mit und ohne Text.

Die Anmerkungen mit Text umfassen Haftnotizen, Textnotizen, Textstempel. Die Anmerkungen ohne Text umfassen Freihandmarker, Rechteckmarkierung, horizontaler Marker und Durchstreichen sowie Schwärzung und Bildstempel.

> **Information**

Da sich die Eigenschaften von Stempeln ein wenig von den anderen Anmerkungen unterscheiden, werden diese im Folgenden gesondert aufgeführt.

Die folgende Tabelle gilt für die oben aufgeführten Anmerkungen (außer Stempel):

Berechtigung	Beschreibung
Sehen (R)	Anmerkungen erstellen, selbst erstellte Anmerkungen bearbeiten und löschen
Ändern (W)	Anmerkungen mit Text: Textinhalt bearbeiten und formatieren, Position merken, Position merken, Größe ändern; Anmerkungen ohne Text: Eigenschaften ändern (Farbe, Strichdicke)
Löschen (D)	
Verschieben (E)	Position der Anmerkung auf dem Dokument ändern
<Liste bearbeiten> (L)	Wirkt sich nicht auf Anmerkungen aus
Berechtigungen setzen (P)	Berechtigungen ändern

Information

Die Anmerkungen mit und ohne Text unterscheiden sich in Bezug auf die Berechtigungen lediglich bei der Berechtigung *W (Write)*.

Stempel

Im Folgenden wird zwischen dem Stempel als Werkzeug und dem Stempelabdruck unterschieden.

Werkzeug 'Stempel'

Das Werkzeug *Stempel* wird mittels *ProfileOpts* für einen bestimmten Benutzer, eine Optionengruppe oder global definiert. Stempel können in der ELO Administration Console und im ELO Java Client erstellt und verwaltet werden. Im ELO Java Client ist jedoch nur die Konfiguration der eigenen Stempel möglich. Die definierten Stempel erscheinen in der Stempelliste der entsprechenden Benutzer. Damit ein Benutzer das Werkzeug *Stempel* verwenden kann, muss diesem mindestens ein Stempel von der Administration zugewiesen sein. Ansonsten kann dieser auch keine Stempel im ELO Java Client für sich selbst definieren.

Erstellt ein Benutzer im ELO Java Client einen Stempel, erscheint dieser Stempel in der Stempelliste des Benutzers und kann nur von diesem verwendet werden. Selbst erstellte Stempel können vom Benutzer im ELO Java Client im Werkzeug *Stempel* und von der Administration in der ELO Administration Console verwaltet werden. Um benutzer- oder gruppenspezifische Stempel in der ELO Administration Console zu konfigurieren, muss die Administration den entsprechenden Benutzer oder die Gruppe über die Schaltfläche *Benutzer auswählen* wählen. Im Standard ist die Gruppe *Jeder* ausgewählt.

Stempelabdruck

Berechtigung	Beschreibung
Sehen (R)	Stempelabdruck auf Dokument sehen, Position merken
Ändern (W)	Größe ändern
Löschen (D)	
Verschieben (E)	Position ändern
<Liste bearbeiten> (L)	Wirkt sich nicht auf den Stempelabdruck aus
Berechtigungen setzen (P)	Berechtigungen ändern

> **Information**
>
> Für einen Stempelabdruck gelten immer die Berechtigungen, die während des Anbringens auf dem Dokument eingestellt sind. Nachträglich geänderte Berechtigungen wirken sich nicht auf bereits angebrachte Stempelabdrücke aus, sondern nur auf die, die nach der Änderung neu angebracht werden.

Masken und Felder

Masken

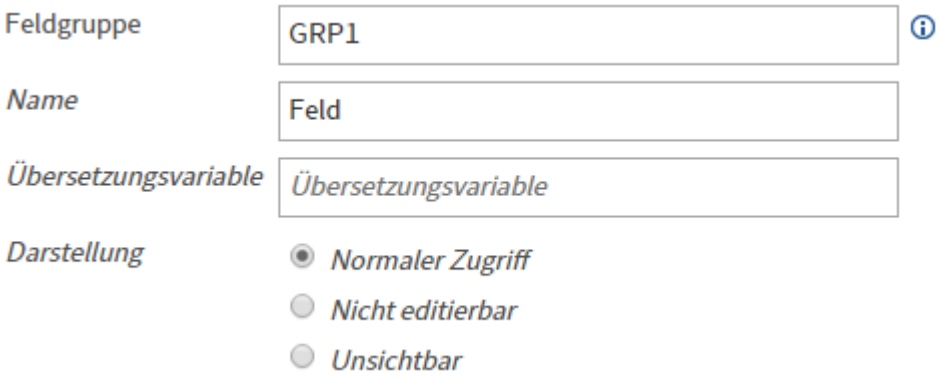
Die Berechtigungen für Masken können nur in der ELO Administration Console gesetzt werden.

Berechtigung	Beschreibung
Metadaten sehen (R)	Masken im Dialog *Metadaten* sehen, Metadaten im Read-only-Modus sehen
Metadaten ändern (W)	Einträge ablegen und Metadaten eingeben (auch Erstablage). Haben Sie die übergeordnete *W*-Berechtigung der Maske nicht, können Sie die Metadaten der Einträge nicht ändern. Auch bei einer vorhandenen *W*-Berechtigung beim Eintrag öffnet sich der Dialog im Read-only-Modus. Um die Metadaten eines damit abgelegten Eintrags danach zu verändern, benötigen Sie zusätzlich die *W*-Berechtigung auf dem Eintrag.
Maske löschen (D)	Diese Berechtigung wird nicht geprüft. Um Masken in der ELO Administration Console löschen zu können, benötigen Sie das Benutzerrecht *Hauptadministrator*.
Maske bearbeiten (E)	Diese Berechtigung wird nicht geprüft.

Felder

Über die *Darstellung* der Felder wird grundsätzlich bestimmt, ob das Feld manuell befüllt werden kann (*Normaler Zugriff*), nur gesehen werden kann (*Nicht editierbar*) oder auf/in der Benutzeroberfläche nicht gesehen werden kann (*Unsichtbar*).

Diese Eigenschaft des Feldes ist übergeordnet. Eine feine Gliederung des *Normalen Zugriffs* kann über die Berechtigungen geregelt werden.



Berechtigung	Beschreibung
Sehen (R)	Das Feld sehen, Zusammenarbeit mit der Darstellung (Normaler Zugriff/-Schreibgeschützt/Unsichtbar) berücksichtigen
Schreiben (W)	Das Feld ausfüllen, Zusammenarbeit mit der Darstellung (Normaler Zugriff/Schreibgeschützt/Unsichtbar) berücksichtigen
<Löschen> (D)	Wirkt sich nicht auf Felder aus
<Bearbeiten> (E)	Wirkt sich nicht auf Felder aus
<Listen> (L)	Wirkt sich nicht auf Felder aus
<Berechtigungen> (P)	Wirkt sich nicht auf Felder aus

Workflow-Vorlagen

Berechtigung	Beschreibung
Sehen (R)	Vorlage sehen, Workflow damit starten
Ändern (W)	Vorlage bearbeiten, neue Version der Vorlage erstellen
Dauerhaft entfernen (D)	
<Bearbeiten> (E)	Wirkt sich nicht auf Workflow-Vorlagen aus
<Liste bearbeiten> (L)	Wirkt sich nicht auf Workflow-Vorlagen aus
Berechtigungen setzen (P)	Berechtigungen ändern

Workflows

Die Berechtigungen für Workflows können Sie in der jeweiligen Workflow-Vorlage festlegen, indem Sie den Startknoten markieren und in den Workflow-Einstellungen im Bereich *Allgemein* den Button *Berechtigungen* wählen.

Berechtigung	Beschreibung
Sehen (R)	Workflow (als Prozess) sehen
Ändern (W)	Workflow nach Start ändern
Dauerhaft entfernen (D)	
Beenden (E)	Der Workflow wird nicht gelöscht und ist im ELO Java Client im Dialog *Übersicht Workflows* über den Zustand *erledigt* einsehbar.

Berechtigung	Beschreibung
<Liste bearbeiten> (L)	*Keine Auswirkung auf Workflows*
Berechtigungen setzen (P)	Berechtigungen ändern

> Die Berechtigungen für die Workflows greifen nur, wenn das Konto die entsprechenden Benutzerrechte für Workflows besitzt. Weitere Informationen zu den Benutzerrechten für Workflows finden Sie unter Konfiguration und Verwaltung > Benutzerverwaltung > Rechte in ELO > Benutzerrechte > Rechte zu Workflows.

ELO Spaces

Die Berechtigungen für die Inhalte von Team- und Workspaces in ELO werden über die zugewiesenen Rollen festgelegt.

Sie können einer Rolle folgende Standard-Berechtigungen für Inhalte in Team- und Workspaces zuweisen:

Berechtigung	Beschreibung
Sehen (R)	Eintrag sehen
Metadaten ändern (W)	Metadaten des Eintrags bearbeiten
Löschen (D)	Eintrag löschen
Bearbeiten (E) (nur Dokumente)	Ausgewählten Eintrag bearbeiten, d. h. Arbeitsversion ändern und neue Version laden
Liste bearbeiten (L) (nur Ordner)	Inhalt des Ordners verändern, z. B. Dokumente in diesem Ordner erstellen, aus diesem Ordner verschieben oder entfernen
Berechtigungen setzen (P)	Berechtigungen für den ausgewählten Ordner ändern

> Die eingestellten Berechtigungen greifen nur, wenn das Konto die entsprechenden Benutzerrechte besitzt.

Zusätzlich können Sie im Client Berechtigungsoptionen für Einträge setzen, die in einem Team- oder Workspace erstellt wurden. Nähere Informationen dazu finden Sie in der Dokumentation zum ELO Java Client.

Weitere Berechtigungen

Die Begriffe *Vorgängerrechte* und *Eigentümerrechte* sind historisch bedingt. Es handelt sich hierbei um Berechtigungen.

Vorgängerrechte

Die Vorgängerrechte sind die Berechtigungen, die bei einem Element vererbt werden. Ordner haben andere Ordner oder Dokumente als Untereinträge. Die Dokumente haben Dateianbindungen und Notizen als Untereinträge.

Beispiel: Nur die Gruppe *Personal* hat die Berechtigungen für ein Dokument. Für die Notizen darin hat die Gruppe *Jeder* die Berechtigungen. Da aber nur die Gruppe *Personal* Zugriff auf das Dokument hat, kann nicht *Jeder* die Notiz im Dokument sehen, sondern nur diejenigen, die auch für das Dokument die Leseberechtigung haben.

Hat ein Benutzer oder eine Gruppe Berechtigungen für ein Dokument, aber keine Berechtigungen für dessen gesamten Ablagepfad, wird das Dokument nach einer Suche oder Verlinkung in der Trefferliste angezeigt.

Eigentümerrechte

Die Eigentümerrechte sind Platzhalter, die mit dem Benutzer ersetzt werden, der

- einen Ordner angelegt hat
- ein Dokument abgelegt hat
- einen Stempelabdruck oder eine sonstige Anmerkung auf einem Dokument angebracht hat
- einen Workflow gestartet hat

Jeder

In einem gut eingerichteten ELO Repository sollte es nur wenige Einträge geben, bei denen Vollzugriff für *Jeder* erlaubt ist.

Sie können Ihr Repository dahingehend überprüfen, dass Sie den Administratoren ein dynamisches Register einrichten, in dem alle Objekte angezeigt werden, die Vollzugriff *Jeder* erlauben. Richten Sie dazu einen Ordner mit folgender Zeile im Zusatztext ein:

```
!+ objekte where objacl='75PYJA' and objstatus=0
```

> **Beachten Sie**
>
> Die Gruppe *Jeder* benötigt Leseberechtigung für persönliche Ordner, damit einige Services darauf zugreifen können. Wird die Leseberechtigung für *Jeder* entfernt, können beispielsweise andere Benutzer die Profilseite dieses Benutzers nicht mehr sehen.

Konzept für die Rechte- und Berechtigungsvergabe

Einführung

Bei dem folgenden Konzept für die Rechte- und Berechtigungsvergabe handelt es sich lediglich um eine Empfehlung.

Grundsätzlich gibt es in ELO die Möglichkeit, Benutzer und Gruppen mit Benutzerrechten zu versehen. Losgelöst davon können Berechtigungen für einzelne Einträge und Elemente vergeben werden. Ziel der Rechte- und Berechtigungsvergabe ist es, den Personen so viel Zugriff wie nötig und so wenig wie möglich auf Einträge und Informationen zur Verfügung zu stellen.

Die Rechte- und Berechtigungsvergabe kann direkt über den Benutzer erfolgen – dies ist aber in den meisten Fällen wenig zielführend. Sinnvoller ist es, Benutzer mit denselben Rechten in Gruppen zu organisieren und die Rechte sowie Berechtigungen auf Basis dieser Gruppen zu vergeben.

In dieser Dokumentation wird ein sinnvoller Aufbau der Gruppen für die Rechte- und Berechtigungsvergabe dargestellt. Die Intention ist, den Aufbau so einfach wie möglich zu gestalten, um ihn problemlos später in ELO umsetzen zu können.

Die Rechte und Berechtigungen in ELO sollten den Aufgaben der Personen im Unternehmen entsprechen. Folgende Fragen sollte man dabei im Blick haben:

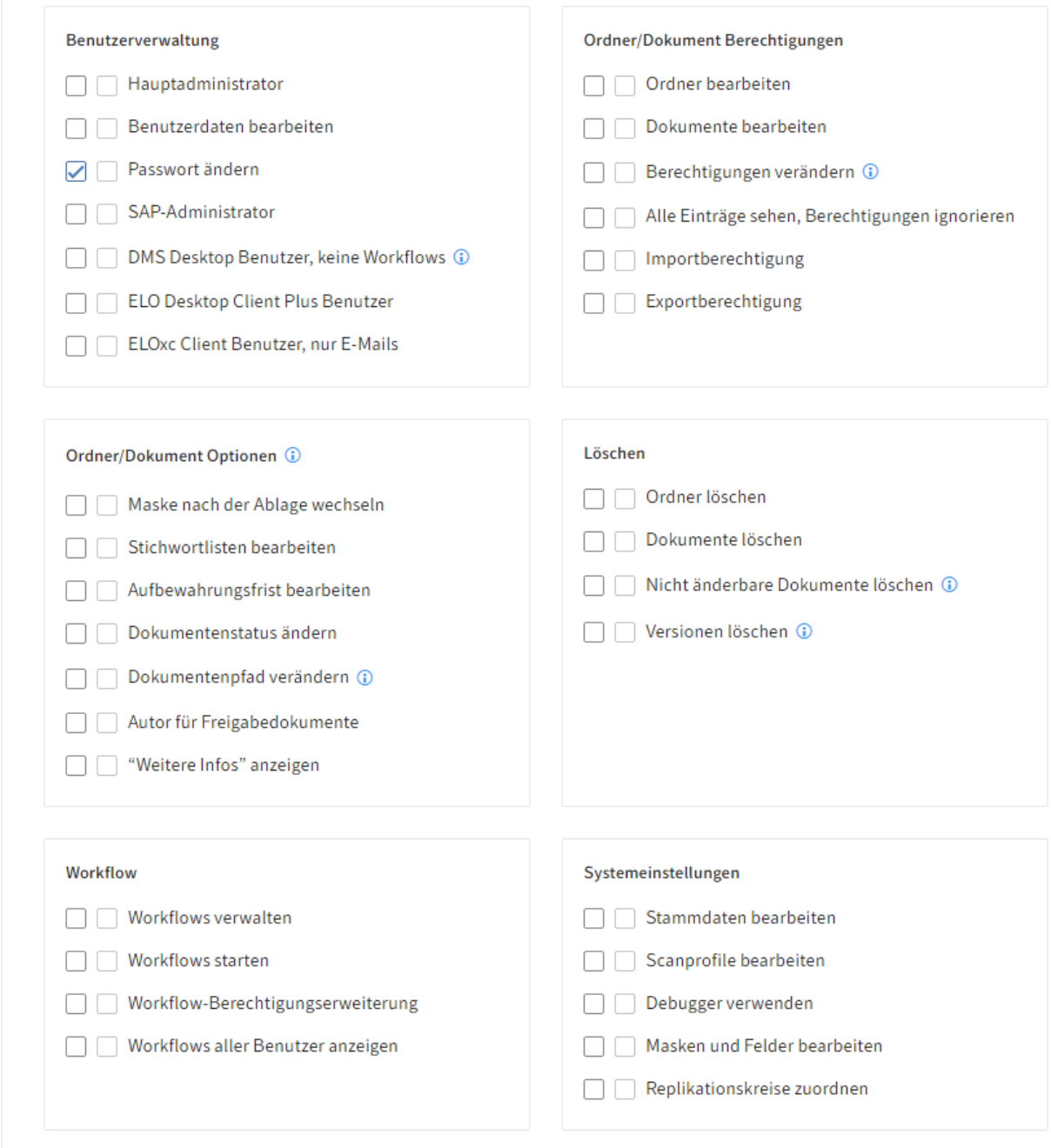
- Welche Aufgaben hat die Person im Unternehmen?
- In welchen Abteilungen des Unternehmens ist die Person tätig?
- Welche Informationen und Dokumente benötigt die Person, um ihre Aufgaben im Unternehmen zu erfüllen?

Vergabe der Benutzerrechte

Zu der ersten Frage nach den Aufgaben des Mitarbeiters im Unternehmen kann man mit der Vergabe der Benutzerrechte reagieren. Je nachdem, welche Art von Tätigkeiten mit den Daten und Dokumenten im ELO Repository gemacht werden, kann man über unterschiedliche Gruppen die Benutzerrechte vergeben. In unserem Beispiel für ein Rechtekonzept unterscheiden wir fünf verschiedene Benutzerrechtegruppen.

ELO View-User

Die Mitglieder dieser Gruppe dürfen Ordner und Dokumente nur anzeigen und gegebenenfalls Anmerkungen und Randnotizen anbringen oder Feed-Beiträge schreiben. Sie dürfen weder Änderungen an den Metadaten durchführen noch das Dokument selbst in irgendeiner Art und Weise bearbeiten oder löschen. Die Personen recherchieren im Repository, bringen aber selbst keine Inhalte ein.



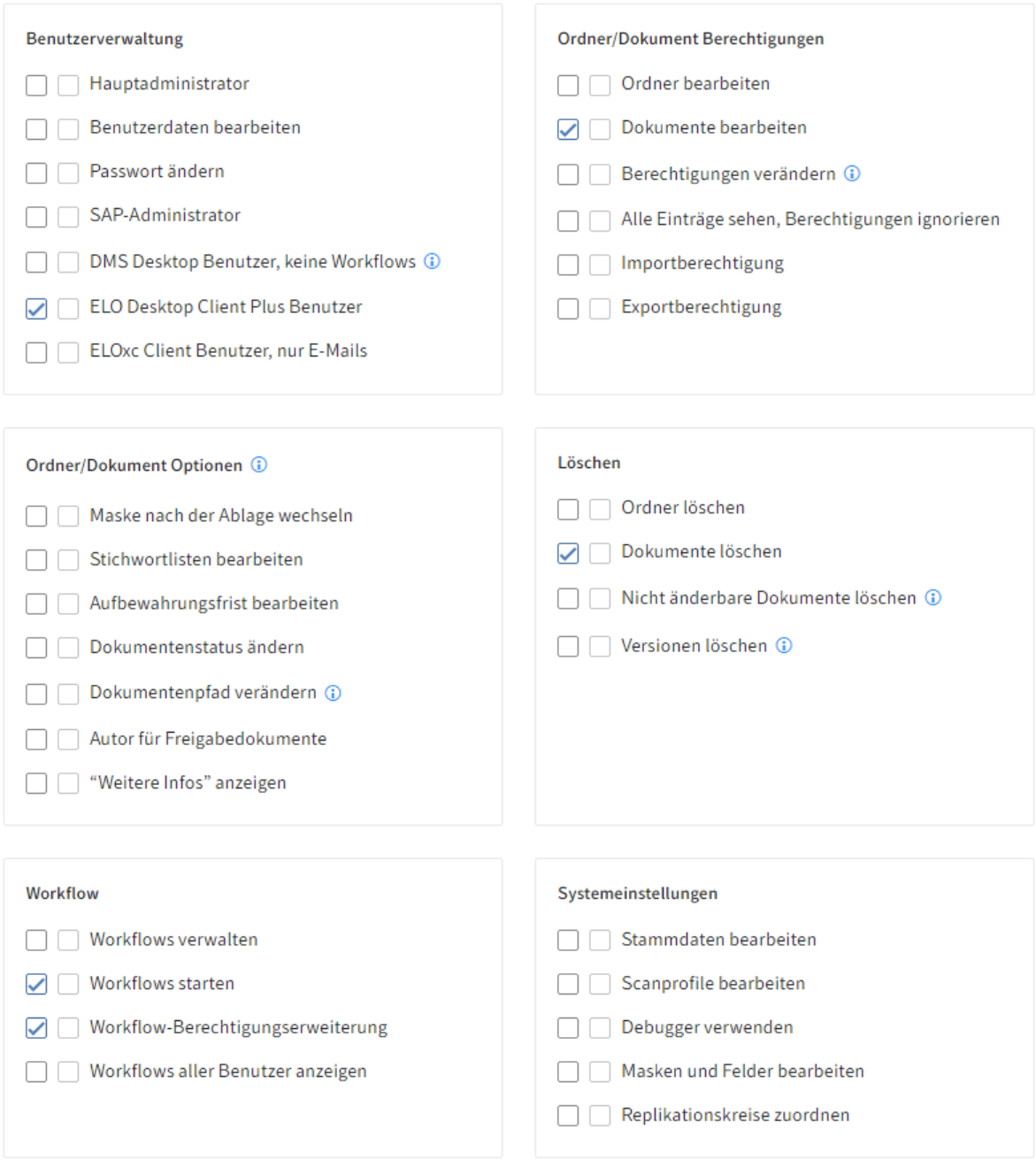
Die Rollengruppe ELO_ViewUsers (minimale Rechte) kann folgendes Recht haben:

- Passwort ändern

ELO Standard-User

Die Mitglieder dieser Gruppe haben bereits erweiterte Rechte, die das Bearbeiten von Dokumenten und Metadaten ermöglichen. Je nach Rechtevergabe, dürfen sie Dokumente und Ordner ändern oder löschen, Metadaten ändern, drucken und exportieren, Workflows starten und bearbeiten.

Diese Personen haben typischerweise die Aufgabe, neue Dokumente in ELO einzubringen und/oder diese entsprechend zu bearbeiten.



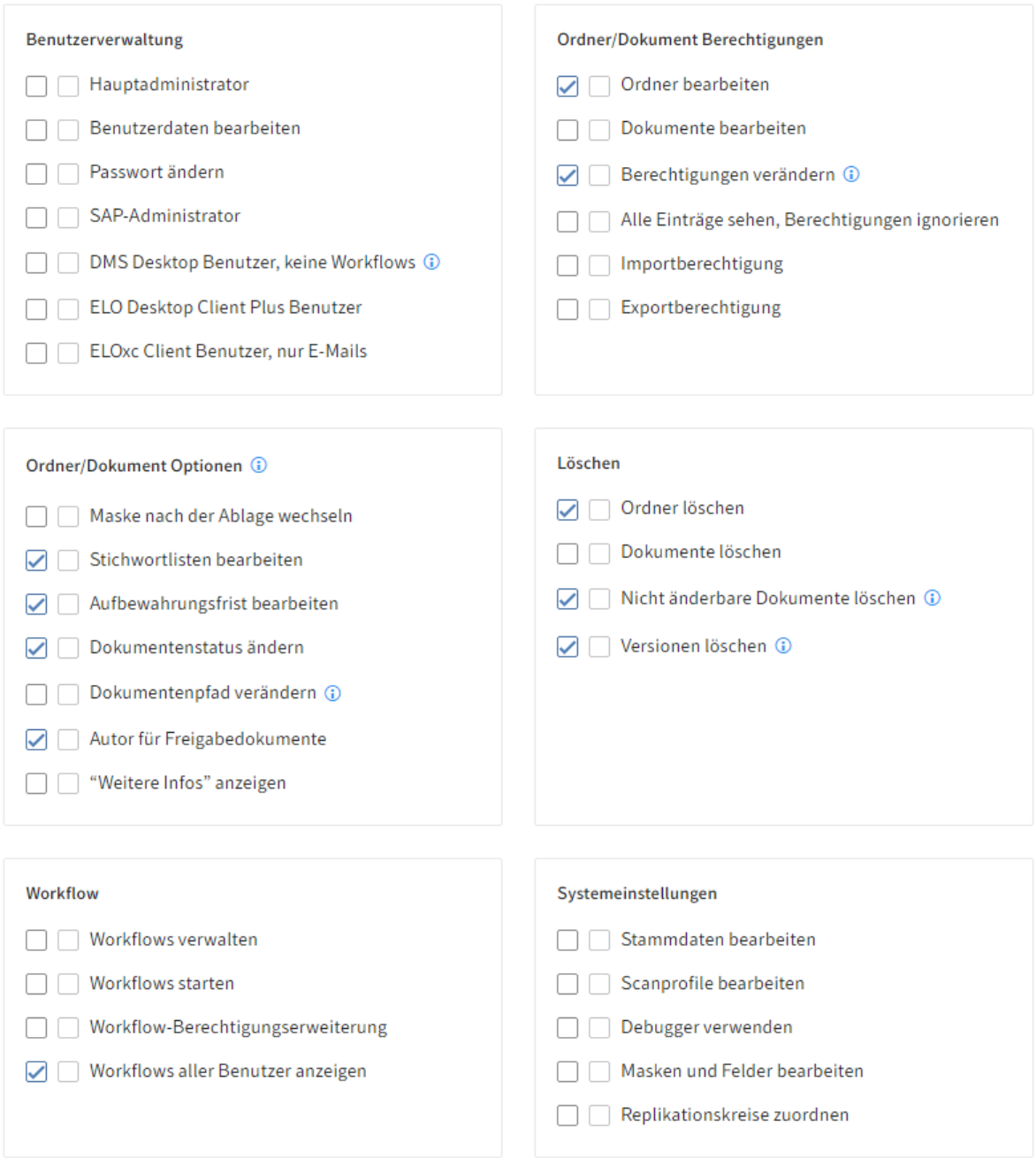
Die Rollengruppe ELO_StandardUsers (Grundrechte für die Bearbeitung von Dokumenten) kann folgende Rechte haben:

- ELO Desktop Client Plus Benutzer
- Dokumente bearbeiten
- Dokumente löschen
- Workflows starten
- Workflow-Berechtigungserweiterung

Der ELO Power-User

Die Mitglieder dieser Gruppe sind fachlich und administrativ für mehr Aufgaben in ELO berechtigt. Typischerweise bearbeiten sie die Ordnerstruktur in ELO und deren Berechtigungskonzept. Sie setzen die Struktur im Repository mit statischen oder dynamischen Ordnern um, oder mit Standardregistern, die von anderen Personen verwendet werden können.

Sie können Dokumente und auch die Optionen von Dokumenten bearbeiten, Verfallsdatum und Dokumentenstatus verändern. Sie können nicht veränderbare Dokumente und auch Versionen löschen. Sie können den Stand von Workflows kontrollieren, an denen sie nicht beteiligt sind.



Die Rollengruppe ELO_PowerUsers (Erweiterte Rechte und Bearbeitung von Ordnerstruktur) kann folgende Rechte haben:

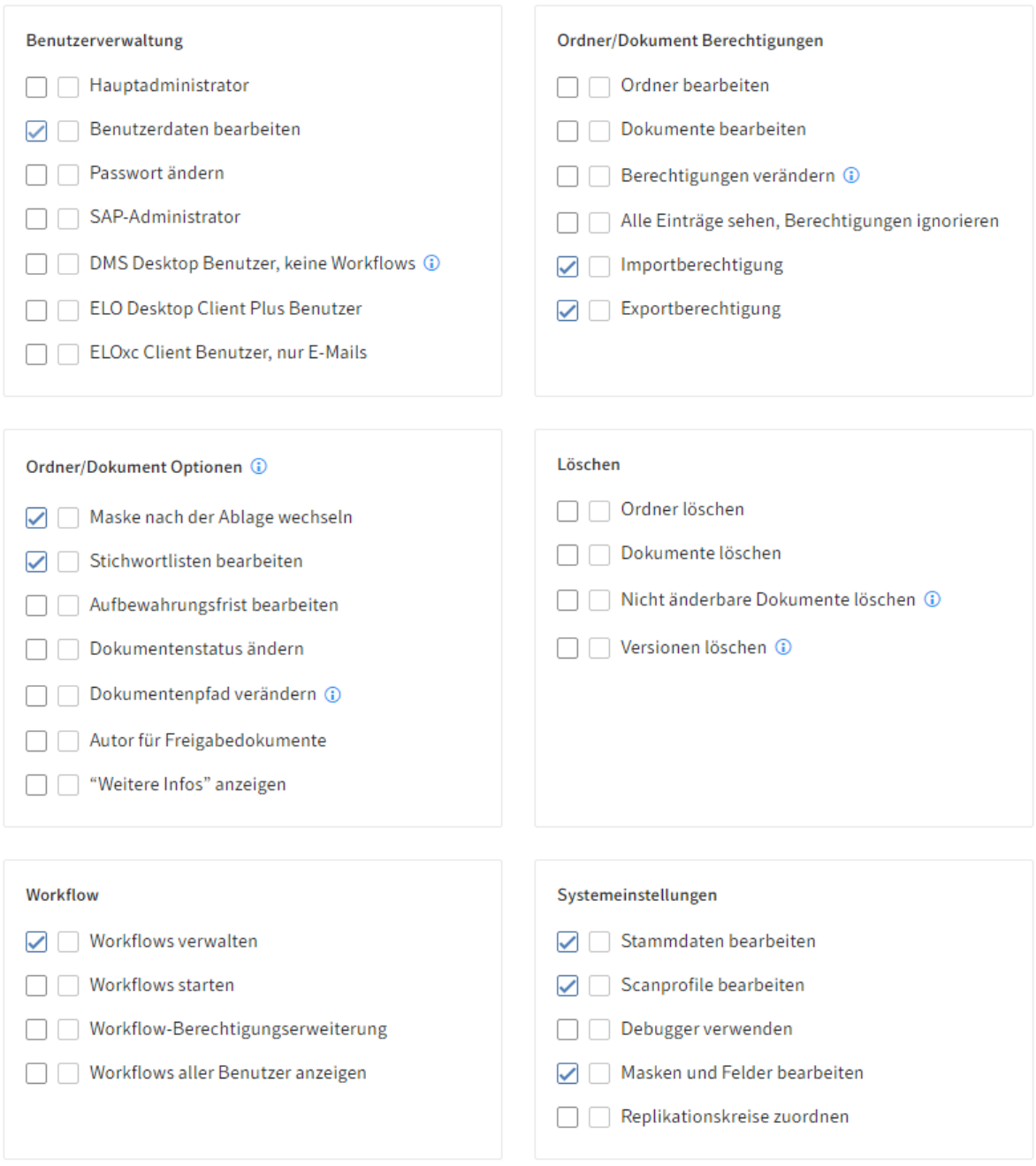
- Ordner bearbeiten
- Ordner löschen
- Berechtigungen verändern
- Stichwortlisten bearbeiten
- Aufbewahrungsfrist bearbeiten
- Autor für Freigabedokumente
- Versionen löschen
- Workflows aller Benutzer anzeigen (Kontrollieren)
-

Nicht änderbare Dokumente löschen
- Dokumentenstatus ändern

Der ELO Fachadministrator

Die Mitglieder dieser Gruppe können Einstellungen im Repository für eigens administrierte Benutzer vornehmen und deren Vertretungen verwalten. Sie werden meistens als Administrator ihrer eigenen Abteilung eingesetzt. Sie kennen interne Prozesse und erstellen die nötigen Workflow-Vorlagen. Sie wissen, welche Daten bei der Ablage festgehalten werden müssen und definieren die nötigen Masken und Stichwortlisten. Sie können Stempel erstellen und Schriftfarben bearbeiten.

Der ELO Fachadministrator ist also weniger für die Bearbeitung und das Arbeiten mit Dokumenten verantwortlich. Er sorgt für Struktur, Prozesse und die notwendige Pflege des Repositorys und führt Überwachungsaufgaben durch.



Die Rollengruppe ELO_FachAdministratoren (Einstellungen im Repository) kann folgende Rechte haben:

- Importberechtigung
- Exportberechtigung
- Masken und Felder bearbeiten
- Stichwortlisten bearbeiten
- Maske nach der Ablage wechseln
- Stammdaten bearbeiten
- Workflows verwalten
- Benutzerdaten bearbeiten (nur die selbst administrierten)
- Scanprofile bearbeiten

Der ELO Administrator

Die Mitglieder dieser Gruppe können Einstellungen in der Konfiguration, Scanprofile und Vertretung sowie Benutzerdaten für alle anderen Benutzer verwalten. Sie können Organisationseinheiten verwalten, Replikationskreise zuordnen, Sperren entfernen und Dokumentdateien im Dateisystem verwalten, verschieben, in einem Backup sichern oder dauerhaft entfernen.

ELO Administratoren arbeiten nicht produktiv mit Ordnern oder Dokumenten im Repository, sondern führen in der Regel ausschließlich administrative Tätigkeiten durch.

Benutzerverwaltung

- [x] Hauptadministrator
- [x] Benutzerdaten bearbeiten
- [ ] Passwort ändern
- [x] SAP-Administrator
- [ ] DMS Desktop Benutzer, keine Workflows
- [ ] ELO Desktop Client Plus Benutzer
- [ ] ELOxc Client Benutzer, nur E-Mails

Ordner/Dokument Berechtigungen

- [ ] Ordner bearbeiten
- [ ] Dokumente bearbeiten
- [ ] Berechtigungen verändern
- [ ] Alle Einträge sehen, Berechtigungen ignorieren
- [ ] Importberechtigung
- [ ] Exportberechtigung

Ordner/Dokument Optionen

- [ ] Maske nach der Ablage wechseln
- [ ] Stichwortlisten bearbeiten
- [ ] Aufbewahrungsfrist bearbeiten
- [ ] Dokumentenstatus ändern
- [x] Dokumentenpfad verändern
- [ ] Autor für Freigabedokumente
- [x] “Weitere Infos” anzeigen

Löschen

- [ ] Ordner löschen
- [ ] Dokumente löschen
- [ ] Nicht änderbare Dokumente löschen
- [ ] Versionen löschen

Workflow

- [ ] Workflows verwalten
- [ ] Workflows starten
- [ ] Workflow-Berechtigungserweiterung
- [ ] Workflows aller Benutzer anzeigen

Systemeinstellungen

- [ ] Stammdaten bearbeiten
- [x] Scanprofile bearbeiten
- [x] Debugger verwenden
- [ ] Masken und Felder bearbeiten
- [x] Replikationskreise zuordnen

Gruppen- und Berechtigungskonzept

Es ist sinnvoll, Funktionen und Berechtigungen in Gruppen zusammenzufassen.

Um die unterschiedlichen Bereiche im Repository mit unterschiedlichen Berechtigungen zu versehen, bietet es sich an, hierfür spezifische Bereichsgruppen zu bilden. Im folgenden Beispiel wird erläutert, wie so eine Vergabe der Rechte über Gruppen und UND-Gruppen aufgestellt werden könnte.

Vergabe der Rechte über Gruppen

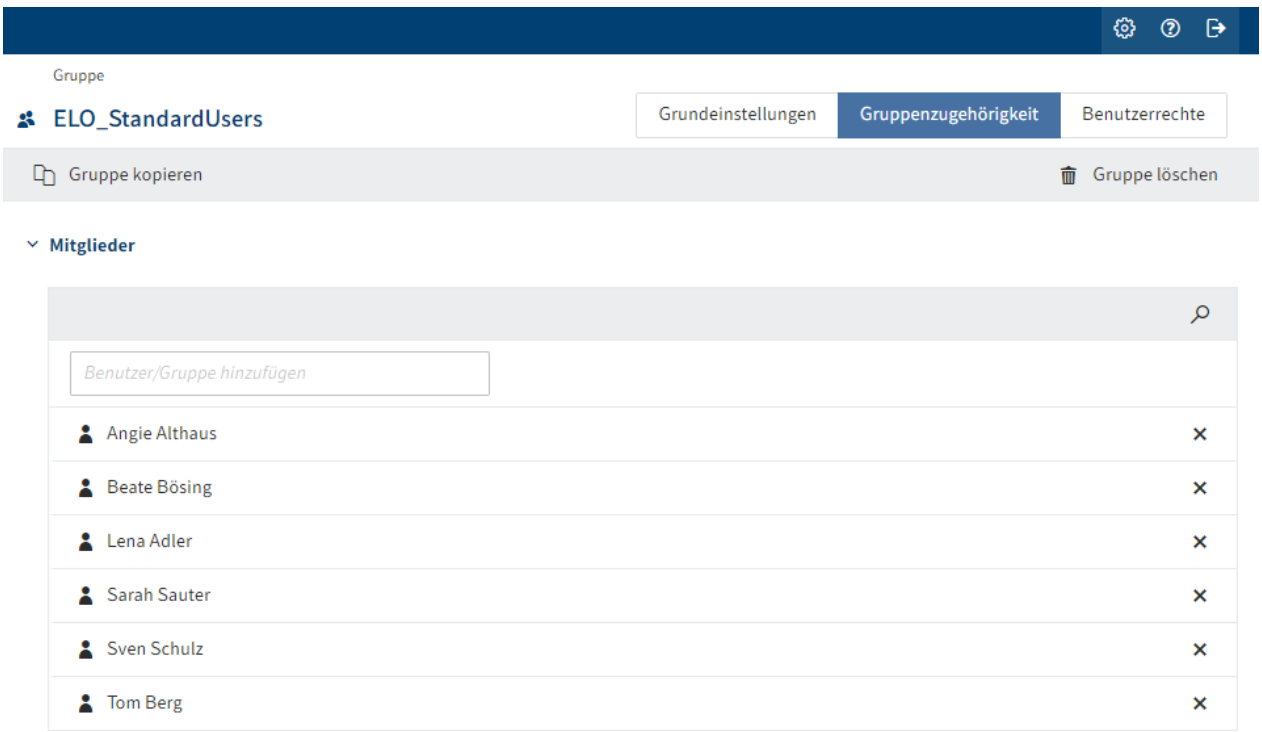
Die Firma Mustermann besteht aus den Abteilungen Personal, Produktion und Logistik. Für die verschiedenen Abteilungen sind unterschiedliche Berechtigungen im Repository vorgesehen.

Die Zugehörigkeit zu den verschiedenen Bereichen im Repository regelt auch die Berechtigungen auf die im Repository befindlichen Dokumente. In unserem Beispiel dürfen die Mitglieder der Abteilung Personal auf alle Dokumente im Bereich Personal zugreifen, die Mitglieder der Abteilung Produktion auf den Bereich Produktion und die Mitglieder der Abteilung Logistik auf den Bereich Logistik. Daher werden die Gruppen auch entsprechend der Firmenbereiche angelegt.

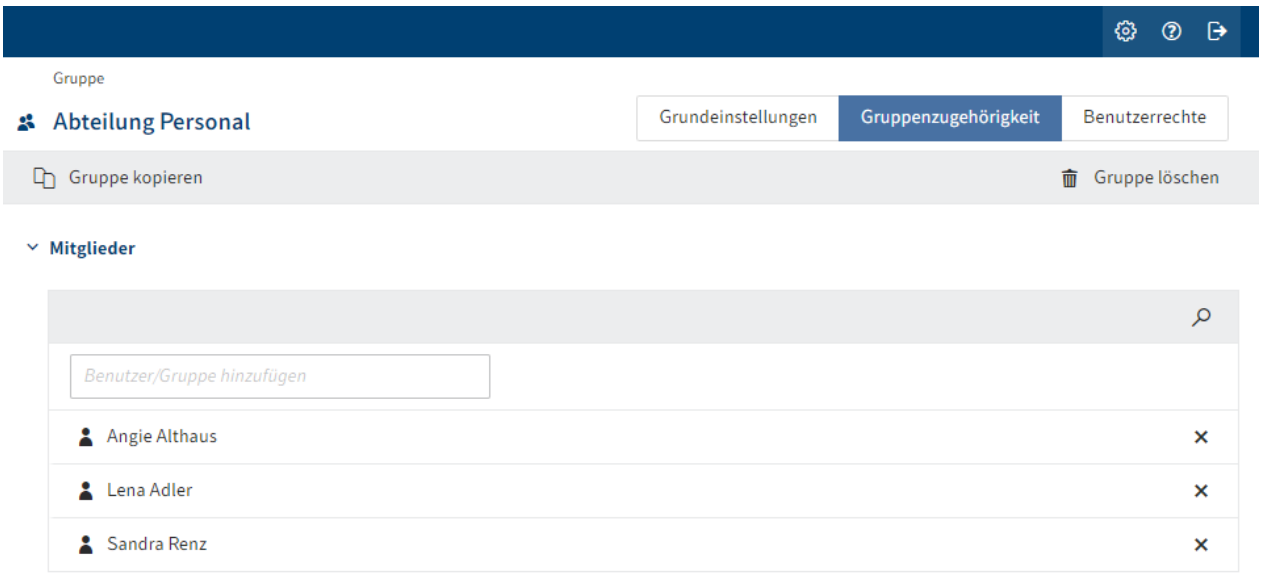
Die Gruppen, über die die Benutzerrechte vergeben werden, auch als Rollengruppen bezeichnet, werden mit den Gruppen der Abteilungszugehörigkeit kombiniert.

Die Benutzerrechte sollten immer an Gruppen geknüpft werden, nicht an den einzelnen Benutzer. Die Rechtevergabe kann somit einfach und transparent erfolgen, überwacht und verwaltet werden.

In der Gruppe ELO_StandardUsers in unserer Beispielfirma haben wir folgende Mitglieder:

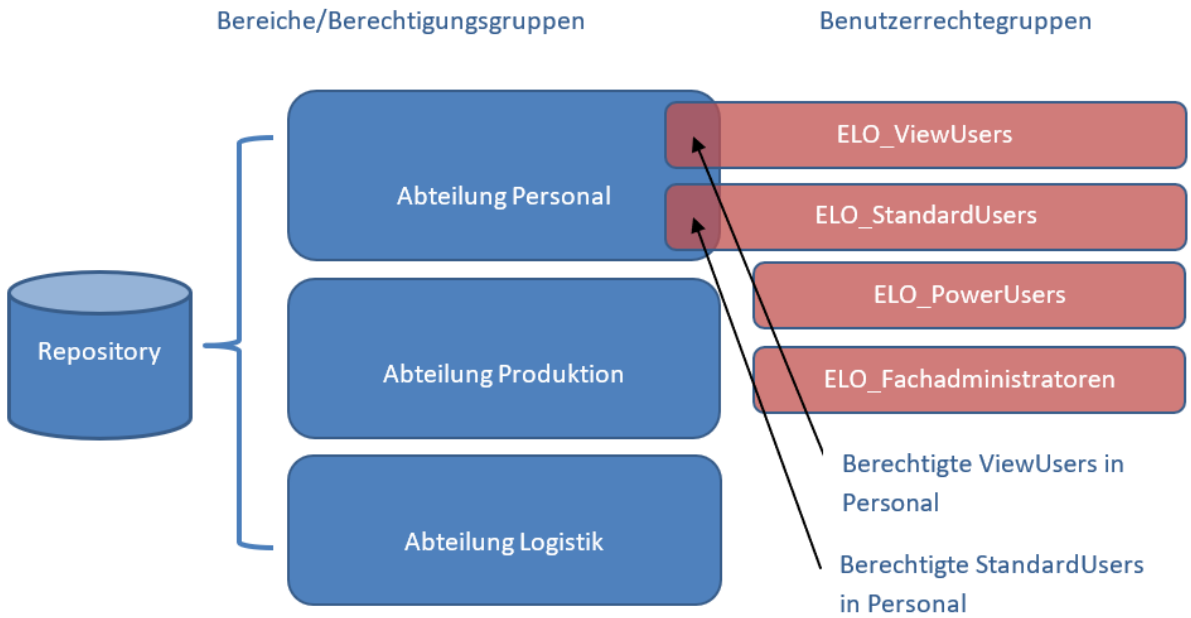


In der Rollengruppe *Abteilung Personal* haben wir folgende Mitglieder. Nur diese werden im Bereich *Personal* auf Dokumente zugreifen können.



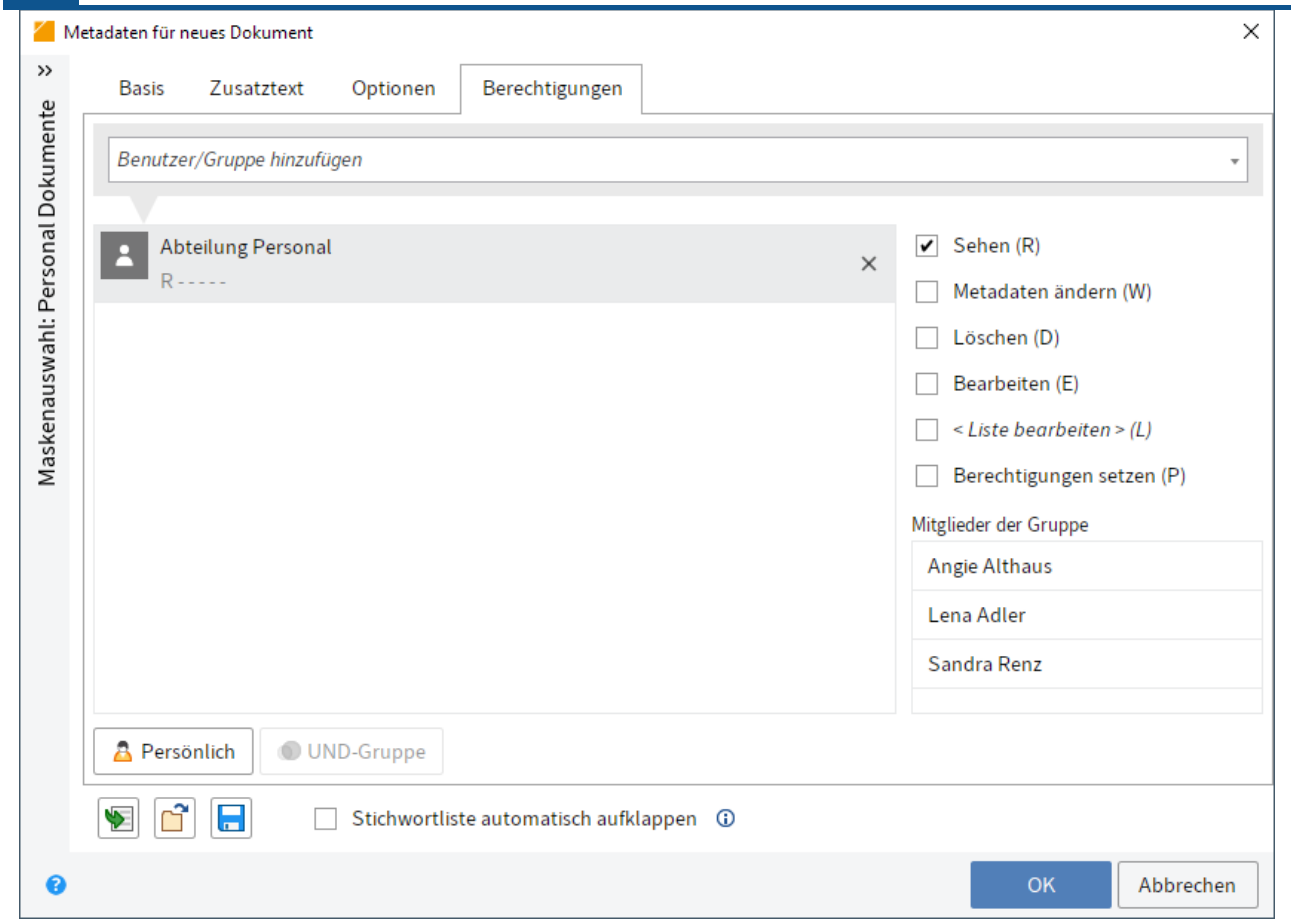
Verwendung von UND-Gruppen

Das nachfolgende Schaubild soll die Berechtigungsvergabe innerhalb der Personalabteilung verdeutlichen.

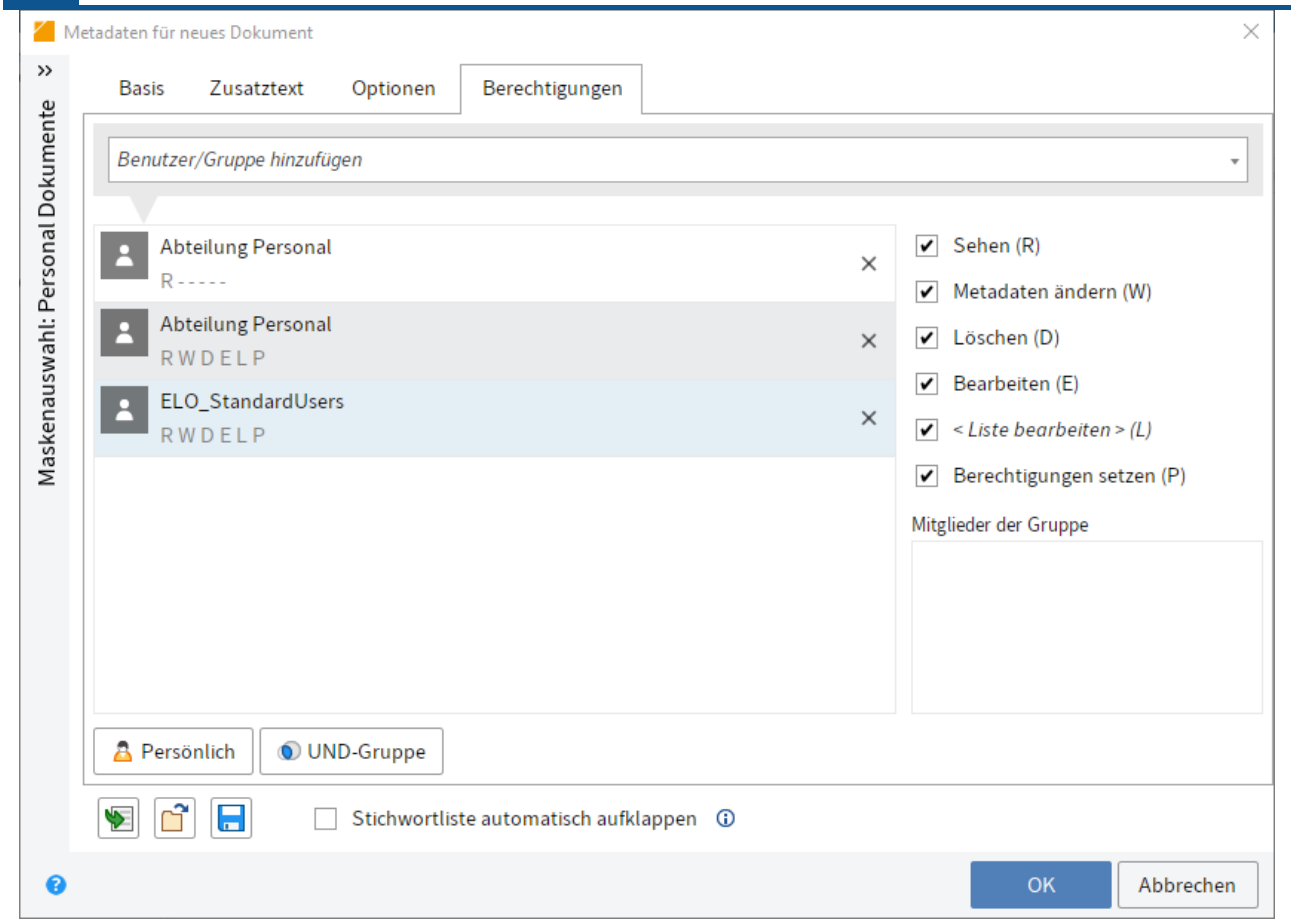


Nun können wir die Berechtigungen auf Dokumente und Ordner im Bereich *Personal* mittels einer UND-Gruppe bestimmen: So gelten die Berechtigungen für die Mitglieder, die sowohl in der Gruppe *Abteilung Personal* als auch in der Gruppe *ELO_StandardUsers* sind (in diesem Beispiel Lena Adler und Angie Althaus).

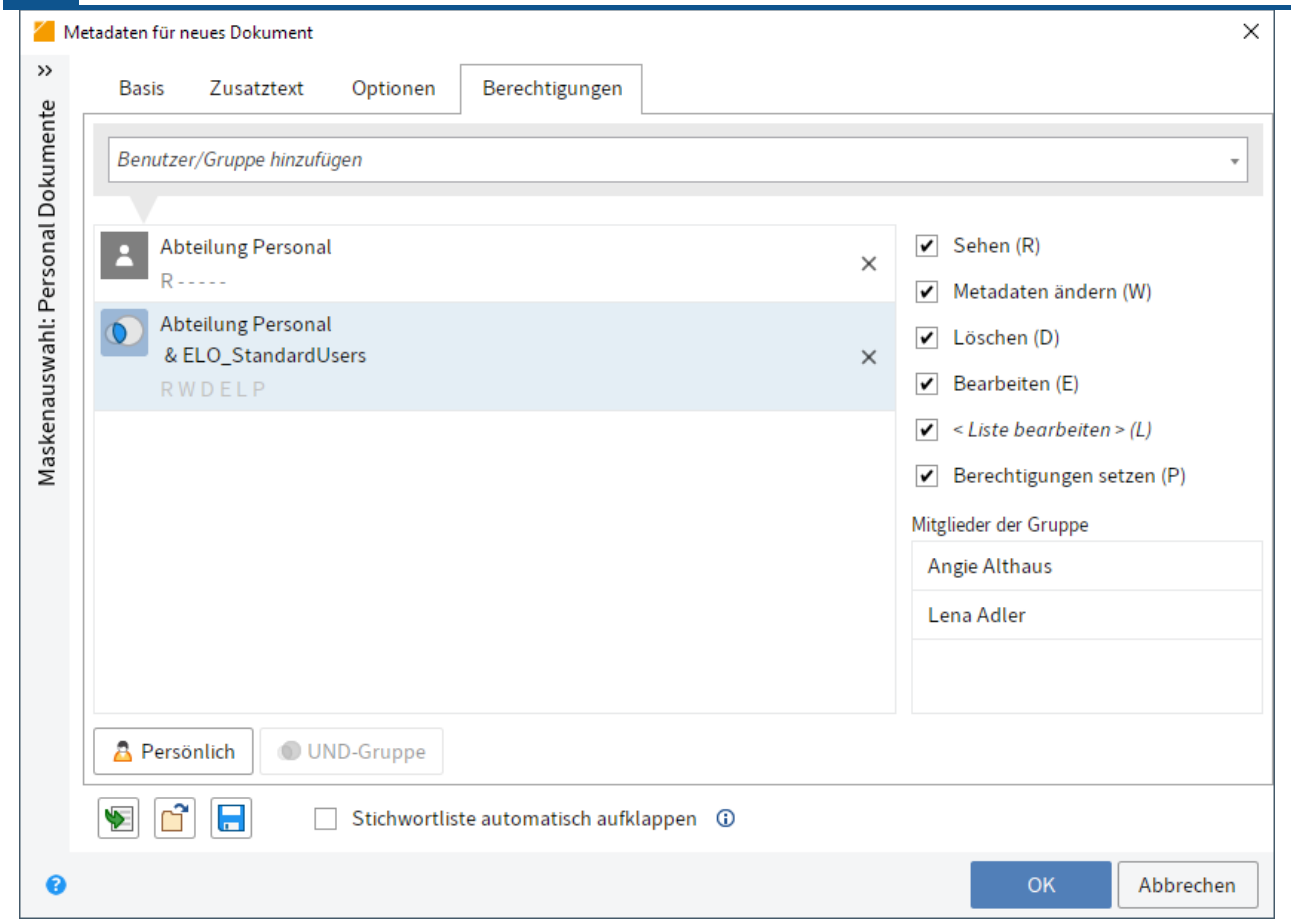
So kann man beispielsweise bei einem Personaldokument bestimmen, dass alle Mitglieder der Abteilung *Personal* das Dokument sehen können.



Um sicherzustellen, dass nur die *ELO_StandardUsers* in der Gruppe *Abteilung Personal* Vollzugriff auf dieses Dokument haben, bilden wir eine UND-Gruppe. Eine UND-Gruppe bildet die Schnittmenge der ausgewählten Gruppen.

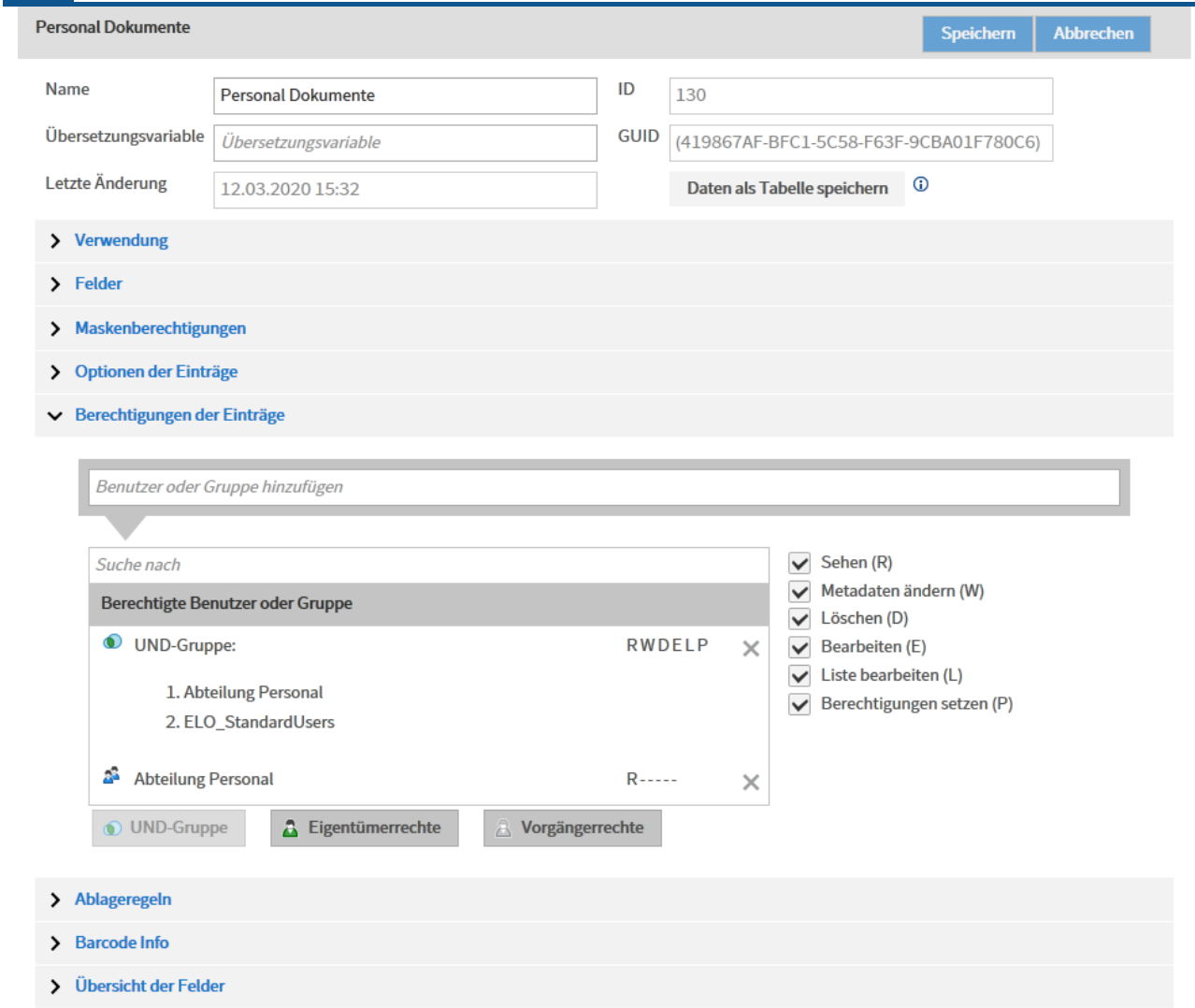


In diesem Beispiel haben die Mitglieder der UND-Gruppe Vollzugriff auf dieses Dokument. ELO zeigt an, um welche Personen es sich in diesem Beispiel handelt.



Vergabe der Berechtigungen über Masken

Um sicherzustellen, dass die Personaldokumente nur von berechtigten Personen bearbeitet werden können, empfiehlt es sich, diese Berechtigungen über die Maske zu definieren und nicht bei den einzelnen Einträgen im Repository.


Personal Dokumente
Speichern
Abbrechen
Name
Personal Dokumente
ID
130
Übersetzungsvariable
Übersetzungsvariable
GUID
(419867AF-BFC1-5C58-F63F-9CBA01F780C6)
Letzte Änderung
12.03.2020 15:32
Daten als Tabelle speichern
Verwendung
Felder
Maskenberechtigungen
Optionen der Einträge
Berechtigungen der Einträge
Benutzer oder Gruppe hinzufügen
Suche nach
Berechtigte Benutzer oder Gruppe
UND-Gruppe:
RWDELP
1. Abteilung Personal
2. ELO_StandardUsers
Abteilung Personal
R-----
Sehen (R)
Metadaten ändern (W)
Löschen (D)
Bearbeiten (E)
Liste bearbeiten (L)
Berechtigungen setzen (P)
UND-Gruppe
Eigentümerrechte
Vorgängerrechte
Ablageregeln
Barcode Info
Übersicht der Felder

LDAP

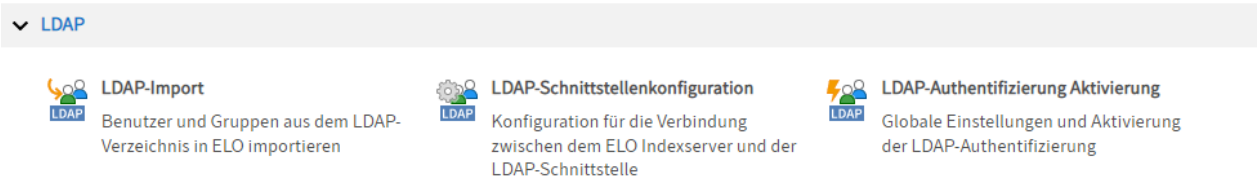
Einführung

Mithilfe des Lightweight Directory Access Protocol (LDAP) können Benutzer und Gruppen aus einem Active Directory (AD) ins ELO System übernommen werden. Dies erfolgt über den LDAP-Import.

Damit der LDAP-Import erfolgen kann, muss die Verbindung zwischen LDAP und der ELO LDAP-Schnittstelle hergestellt und konfiguriert werden.

Außerdem muss die LDAP-Authentifizierung aktiviert sein, damit sich Benutzer mit den im Active Directory hinterlegten Daten bei ELO anmelden können.

Die Menüpunkte finden Sie in der ELO Administration Console unter *LDAP*.



Die Benutzerverwaltung wird im LDAP-Verzeichnis in einer Baumstruktur verwaltet. Dabei wird ein eindeutiger Name innerhalb des LDAP-Verzeichnisses, der `distinguished name` (DN), als eindeutiger Schlüssel verwendet. Ein Beispiel für einen DN ist `cn=John Doe,ou=people,dc=comy,dc=org`. Hier setzt sich der DN aus drei Teilen zusammen, dem `common name` (CN), der `organizational unit` (OU) und der `domain component` (DC). Mit der Kombination OU/DC werden unterschiedliche Zweige innerhalb der LDAP-Baumstruktur referenziert. Der DC dient zum Adressieren der obersten Ebene unter dem Wurzelknoten des LDAP-Verzeichnisses. In der Regel wird hier die Internetdomain der Firma nachgebildet. Ebenfalls direkt unter dem Wurzelknoten befinden sich die Schemadaten. Im LDAP-Schema werden die möglichen Attribute vorgegeben und im LDAP-Eintrag, der über den DN aufgelöst wird, sind die entsprechenden Werte zu diesen Eigenschaften hinterlegt.

> **Beachten Sie**
>
> Verwenden Sie im Active Directory (AD) kein ; (Semikolon) in Gruppen- und Benutzernamen.

LDAP-Schnittstellenkonfiguration

In der ELO Administration Console bearbeiten Sie über den Menüpunkt *LDAP-Schnittstellenkonfiguration* die Konfigurationsdatei *ldap.json* bezüglich der Verbindungsdaten, der Auswahl der Benutzer und der Attributzuweisung. Die Datei *ldap.json* wird im Repository unter folgendem Pfad gespeichert:

Administration // IndexServer Scripting Base // _ALL // ldap.json

Information

Pfadänderungen sind in folgenden Fällen möglich:

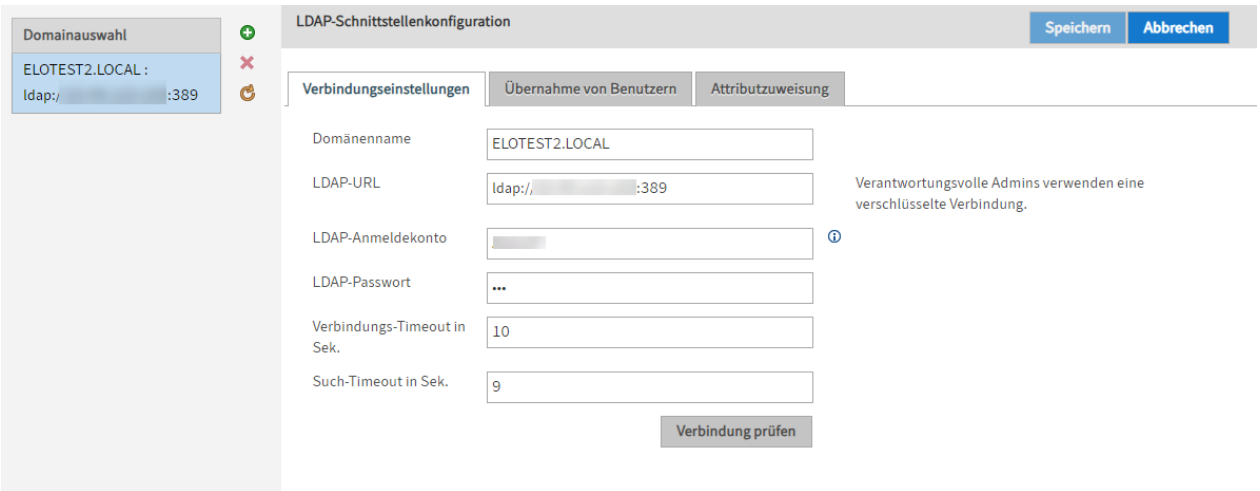
- Möchten Sie für einen ELO Indexserver eine spezielle Konfiguration vornehmen, kopieren Sie die Datei in das Verzeichnis des jeweiligen ELO Indexservers und passen Sie die Datei dort an.
- Möchten Sie unterschiedliche Konfigurationen für verschiedene ELO Indexserver vornehmen, benötigen Sie für jeden ELO Indexserver eine eigene Datei.

Die Konfiguration bezieht sich auf ein einzelnes Repository. Wird die Konfiguration über die ELO Administration Console bearbeitet, muss der ELO Indexserver des Repositorys neu gestartet werden. Falls es mehrere ELO Indexserver gibt, müssen alle neu gestartet werden.

Beachten Sie

Das Konto *ELO Service* (oder das jeweils verwendete Dienstkonto) sollte nicht über LDAP authentifiziert werden. Dadurch sind die serverseitigen ELO Anwendungen unabhängig von der LDAP-Konfiguration. Ansonsten kann das Deaktivieren der LDAP-Verbindung dazu führen, dass die ELO Anwendungen nicht mehr starten. Eine Aktivierung der LDAP-Anbindung ist dann nicht mehr über die ELO Administration Console möglich.

Auch administrative Konten sollten nicht über LDAP authentifiziert werden.



Sie können Einstellungen für mehrere Domänen vornehmen.

Im Bereich *Domainauswahl* sehen Sie die vorhandenen Domänen.

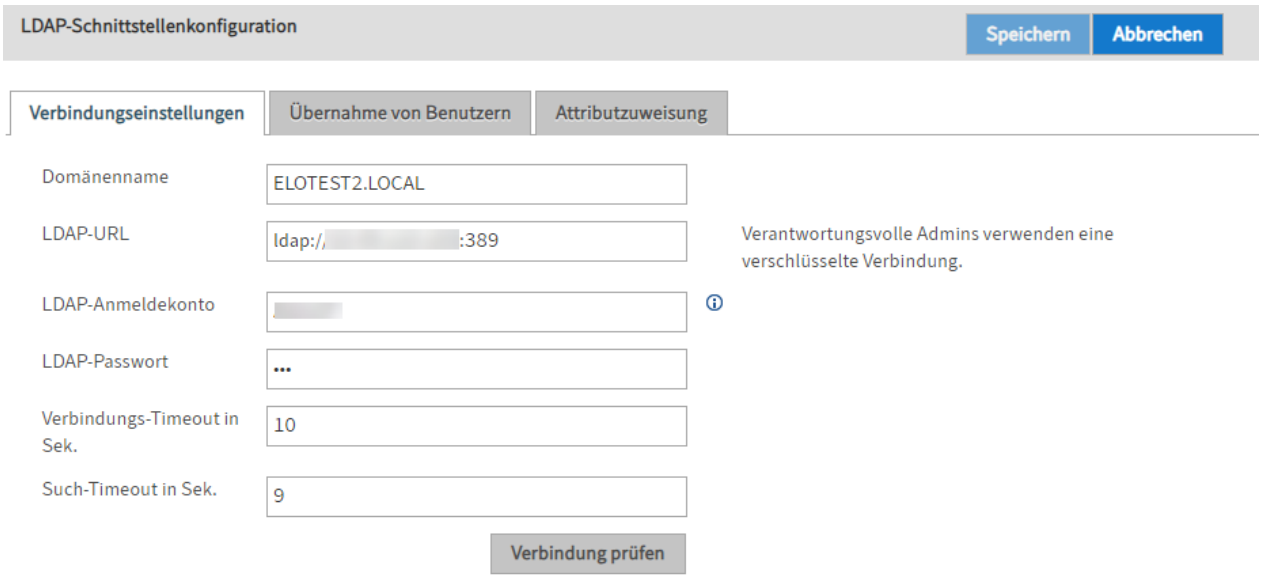
Hinzufügen (grünes Plussymbol): Einstellungen für eine Domäne hinzufügen

Löschen (rotes X-Symbol): Einstellungen für eine Domäne löschen

Daten erneut vom Server abrufen (gelbes Kreispfeilsymbol): Bereich *Domainauswahl* aktualisieren

> **Information**
>
> Bei Verbindungsproblemen kann die Log-Datei des ELO Indexservers auf *debug* umgestellt werden. Dies vereinfacht die Fehlersuche.

Verbindungseinstellungen



Domänenname: Geben Sie in dieser Option den DNS-Namen oder die IP-Adresse der Domäne an. Die Einstellung wird verwendet, wenn aus dem `sAMAccountName` der `userPrincipalName` gebildet wird.

LDAP-URL: Über die Eingaben im Feld *LDAP-URL* wird die Verbindung zum LDAP-Server über TCP bestimmt.

LDAP-Anmeldekonto: Für SSO wird ein technisches Konto benötigt, unter dessen Anmeldung der vom SSO-Mechanismus übergebene Kontoname (in der Regel `sAMAccountName`) im LDAP gesucht werden kann. Geben Sie einen `userPrincipalName` an.

> **Beachten Sie**
>
> Das Konto muss ausreichende Rechte haben, um die Benutzerattribute und Gruppenzugehörigkeiten zu lesen.

> **Beachten Sie**

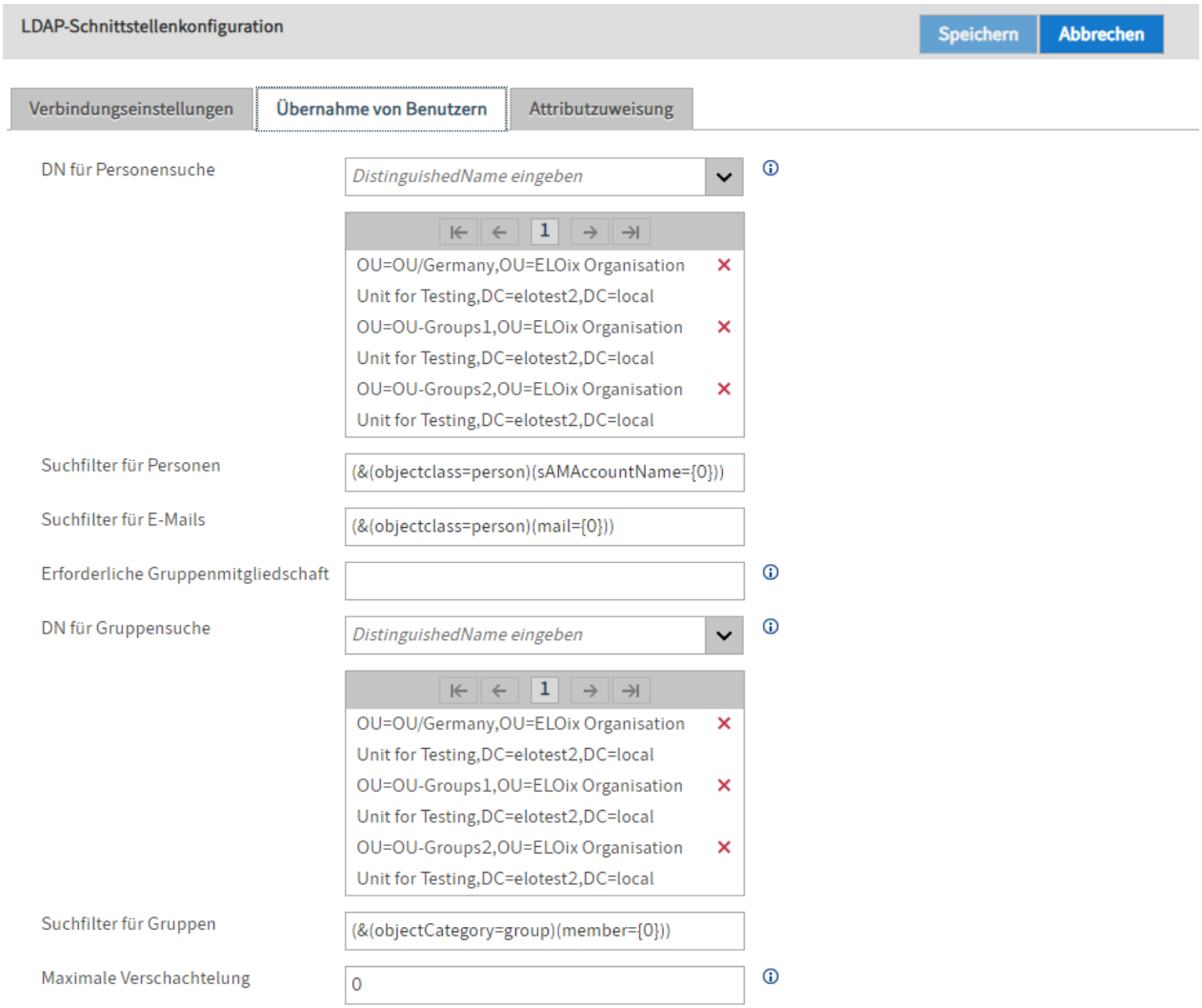
Bei der Verwendung von Kerberos: Trennen Sie das Kerberos-Konto und das LDAP-Anmeldekonto. Das Kerberos-Konto muss nicht in ELO existieren.

LDAP-Passwort: In das Feld *LDAP-Passwort* kann das unverschlüsselte Kennwort des LDAP-Anmeldekontos eingetragen werden. Der ELO Indexserver speichert es beim Neustart verschlüsselt.

Verbindungs-Timout in Sek.: Die LDAP-Schnittstelle bricht nach dieser Anzahl von Sekunden einen Verbindungsaufbau zum LDAP-Server ab. Anschließend wird der nächste Server in der Liste probiert.

Such-Timeout in Sek.: Bei einer Suche nach Benutzern oder Gruppen wird dieser Timeout-Wert an den LDAP-Server übergeben.

Übernahme von Benutzern



DN für Personensuche: Über dieses Feld geben Sie an, in welchen Zweigen des LDAP-Verzeichnisses nach Benutzern gesucht werden soll.

Beachten Sie

Die Liste darf nicht leer sein.

> Geben Sie auch nicht zu viele Zweige an. Je mehr Zweige Sie angeben, desto ungenauer wird die Suche.

Suchfilter für Personen: Die Suche nach Benutzern kann mit diesem Filter eingegrenzt werden.

Suchfilter für E-Mails: Bei einer ersten Anmeldung mit E-Mail-Adresse wird der Benutzer über diesen Filter im LDAP-Verzeichnis gesucht.

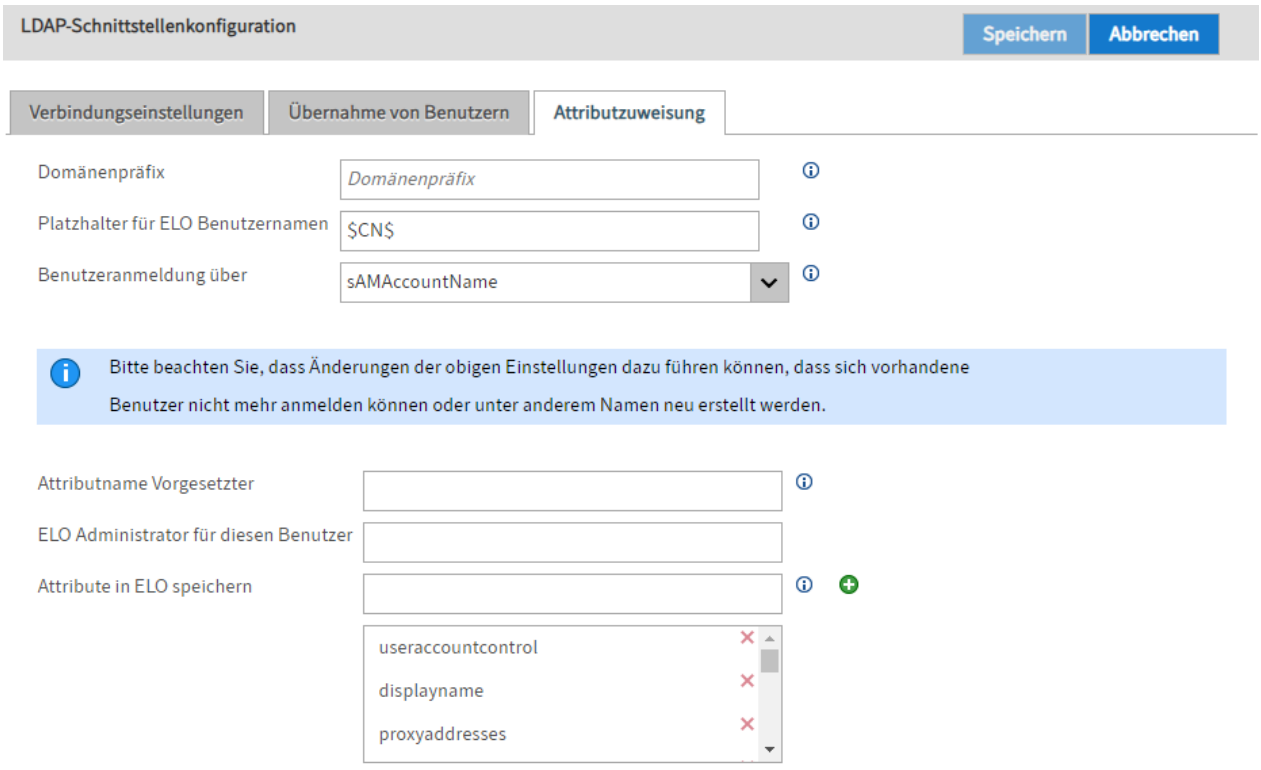
Erforderliche Gruppenmitgliedschaft: Über dieses Feld kann die Anmeldung auf die Benutzer beschränkt werden, die Mitglied einer bestimmten Gruppe im LDAP-Verzeichnis sind. Die Angabe ist als Common Name vorzunehmen.

DN für Gruppensuche: Über dieses Feld geben Sie an, in welchen Zweigen des LDAP-Verzeichnisses die Gruppen liegen müssen, die für den Gruppenabgleich infrage kommen. Ist die Liste leer, gehen alle Gruppen des Benutzers in den Gruppenabgleich ein.

Suchfilter für Gruppen: Die Suche nach den Gruppen eines Benutzers kann mit diesem Filter eingegrenzt werden.

Maximale Verschachtelung: Über dieses Feld kann die Tiefe der Gruppe-in-Gruppe-Beziehung angeben werden. Dies bezieht sich auf das Sammeln von Benutzergruppen für den Gruppenabgleich.

Attributzuweisung



Domänenpräfix: Das Domänenpräfix ist erforderlich, wenn mehrere Domänen konfiguriert werden und zum ELO Benutzer der `sAMAccountName` als Windows-Benutzer geführt wird. Das Domänenpräfix muss mit einem Trennzeichen abgeschlossen werden. Dadurch wird das Präfix vom Benutzernamen separiert. Es sollte vorzugsweise ein Backslash verwendet werden.

Information

Wenn SSO genutzt werden soll, muss das Domänenpräfix mit dem „kurzen“ (NetBIOS) Domänennamen übereinstimmen.

Das für SSO passende Domänenpräfix finden Sie (auf dem Client-Computer) in der Umgebungsvariablen `USERDOMAIN`. Für SSO mit Domänenpräfix muss in der Datei *config.xml* des ELO Indexservers die Option `"ntlm.domainUserFormat"` gesetzt werden. Wird im Feld *Benutzeranmeldung über* die Option `sAMAccountName` gewählt und ein Domänenpräfix definiert, enthält der Windows-Benutzer den Account-Namen mit vorangestelltem Domänenpräfix.

Beispiel:

- `sAMAccountName` = fritzfrei
- Domänenpräfix = ELO\
- Windows-Benutzer = ELO\fritzfrei

Platzhalter für ELO Benutzernamen: Aus verschiedenen LDAP-Attributen des Benutzers kann der Benutzername für ELO zusammengestellt werden. Hierfür kann ein Formatausdruck mit Platzhaltern angegeben werden. Die Platzhalter sind in $-Zeichen eingerahmt und entsprechen den LDAP-Attributnamen.

Benutzeranmeldung über: Über das Drop-down-Menü *Benutzeranmeldung über* wählen Sie aus, ob für die Eigenschaft *Windows-Benutzer* (siehe ELO Benutzerverwaltung) der `sAMAccountName`, der `userPrincipalName` oder die `UID` verwendet werden soll.

Beachten Sie

Die im Feld *Benutzeranmeldung über* gewählte Einstellung muss zu den Einstellungen im Feld *Suchfilter für Personen* (Tab *Übernahme von Benutzern*) passen. Achten Sie auf korrekte Groß-/Kleinschreibung.

Auch die Schreibung von Umlauten sollte identisch zwischen Active Directory und ELO Benutzernamen sein.

Dabei ist zu beachten, dass die ELO Administration Console auf die nachfolgenden vier Attribute auf der LDAP-Seite prüft. Die ELO Administration Console verwendet das erste gesetzte Attribut für den Namen.

```
LdapServerFactory.CONST.USERINFO.DISPLAY_NAME,
LdapServerFactory.CONST.USERINFO.CN,
LdapServerFactory.CONST.USERINFO.SAM_ACCOUNT_NAME
LdapServerFactory.CONST.USERINFO.DISTINGUISHED_NAME
```

Information

Für manche Umgebungen ist eine individuelle Konfiguration notwendig. Das Feld lässt eine freie Eingabe von Werten zu.

Attributname Vorgesetzter: Über dieses Feld legen Sie fest, aus welchem Attribut der Vorgesetzte des ELO Benutzers ermittelt wird. Üblicherweise wird das Attribut `$manager$` verwendet.

> **Beachten Sie**
>
> Der Vorgesetzte muss bereits in ELO angelegt sein.

ELO Administrator für diesen Benutzer: Für Benutzer, die über die LDAP-Schnittstelle erstellt werden, kann über das Feld *ELO Administrator für diesen Benutzer* festgelegt werden, welcher ELO Benutzer als Administrator zugewiesen wird. Die Angabe kann als ID, GUID oder ELO Benutzername erfolgen.

Attribute in ELO speichern: Über dieses Feld legen Sie fest, welche Attribute aus dem LDAP in ELO übertragen werden sollen.

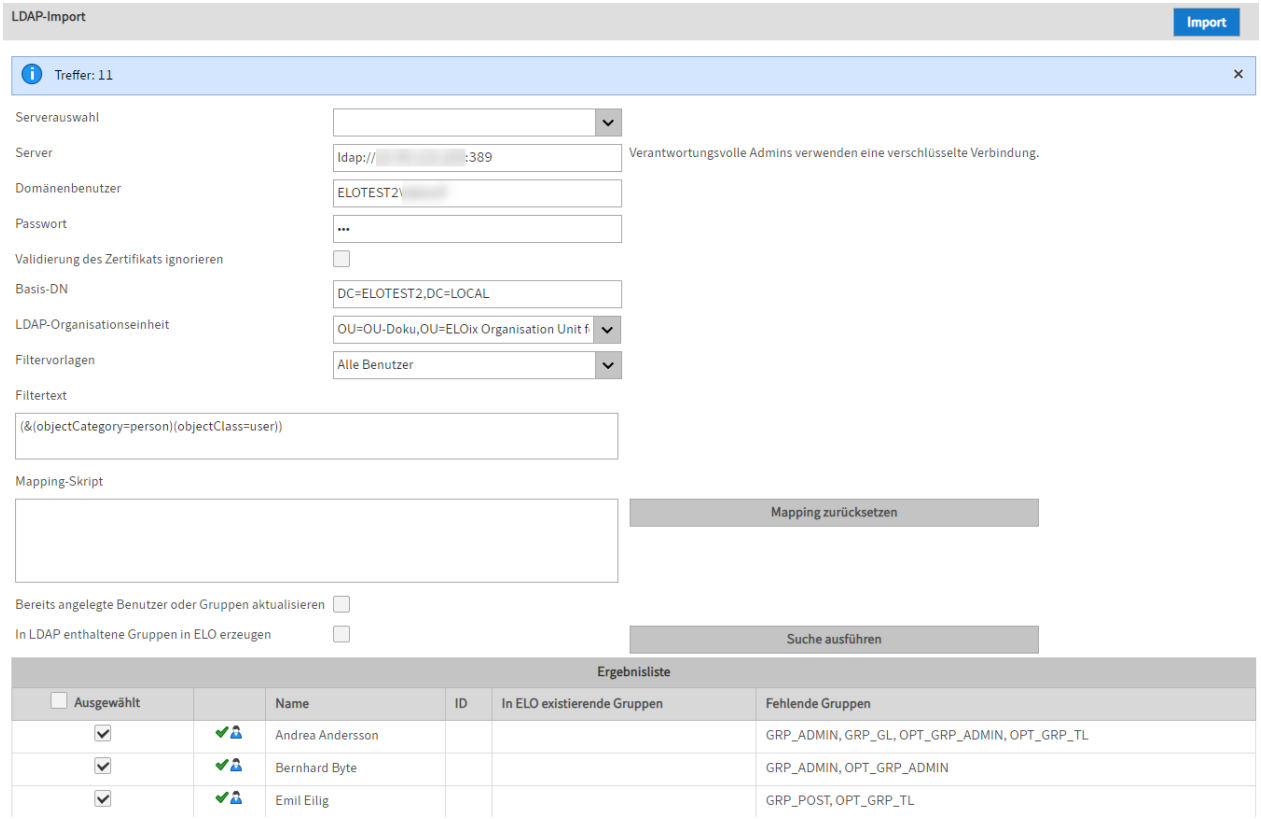
Um ein Attribut hinzuzufügen, tragen Sie den Namen des Attributs in das Feld ein. Klicken Sie anschließend auf *Hinzufügen* (grünes Plussymbol).

Um ein Attribut zu entfernen, klicken Sie auf das jeweilige X-Symbol in der Liste der Attribute.

> **Information**
>
> Pflichtattribute können nicht gelöscht werden. Das X-Symbol ist in diesem Fall ausgegraut.

LDAP-Import

Mit dem LDAP-Import können Sie Benutzer und Gruppen aus einem Active Directory (AD) in das ELO System übernehmen.



- Serverauswahl: Die ELO Administration Console versucht automatisch mögliche LDAP-Server zu finden. Ist dieses Auswahlfeld leer, wird in der Domäne kein Server gefunden. Dies kann beispielsweise bei einer VPN-Verbindung der Fall sein.
- Server: Hier wird der Server zur LDAP-Verbindung eingetragen. Hier kann auch die IP-Adresse, der Port oder das Protokoll eingetragen werden.

  `BNF: Server ::=[ldap|ldaps]://[Servername|IP-Adresse]:Port`

> **Beachten Sie**
>
> Verwenden Sie eine verschlüsselte Verbindung, in diesem Fall also LDAP via SSL (LDAPS).

- Domänen-Benutzer und Passwort: Die Anmeldedaten bestehen aus dem Namen und dem Passwort.
- Validierung des Zertifikats ignorieren: Die Validierung des Zertifikats kann im Bedarfsfall auch ignoriert werden.
- Basis-DN und LDAP-Organisationseinheit: Mit diesen Einträgen wird der korrekte Zweig im LDAP-Verzeichnis ausgewählt.
-

Filtervorlagen und Filtertext: Einige LDAP-Filterausdrücke werden in der Auswahlliste vorgegeben und in den Filtertext zum freien Bearbeiten übernommen.

- Mapping-Skript: Erlaubt ein zusätzliches Bearbeiten der Daten als JavaScript-Code.

  Nähere Informationen finden Sie im nachfolgenden Abschnitt *Das Mapping-Skript*.

- Mapping zurücksetzen: Löscht den Text aus dem Mapping-Skriptfeld.
- Bereits angelegte Benutzer oder Gruppen aktualisieren: Wenn der Name zu einem bereits vorhandenen Eintrag aufgelöst werden kann, wird dieser Eintrag nur mit gesetztem Häkchen erneut bearbeitet.

> **Beachten Sie**
>
> LDAP Gruppen werden nur bei der Anmeldung der Benutzer ausgelesen und angewendet.

- In LDAP enthaltene Gruppen in ELO erzeugen: Legt auch Gruppen mit an, die noch nicht in ELO vorhanden sind.
- Suche ausführen: Führt die Suche aus und zeigt die Ergebnisse an.
- Ergebnisliste: Zeigt die Liste der zu importierenden Einträge an. Alle gültigen Einträge sind auch gleich selektiert. Wenn bei der Überprüfung ungültige Daten erkannt wurden, werden diese nicht selektiert sein und der Hinweis auf den Verstoß ist als Tooltip hinterlegt.

Das Mapping-Skript

Es gibt ein vorgegebenes Mapping von Standard LDAP-Attributen auf ELO-Attribute. Um eine flexiblere Anpassung zu ermöglichen, kann man in das Eingabefeld JavaScript-Code einfügen. Dieser wird in einen Code-Rahmen eingebettet und für jeden Datensatz der LDAP-Suche ausgeführt.

Der ELO Indexserver hat eine Datenstruktur für die Benutzer und Gruppen: das UserInfo-Objekt. Dieses wird in der Entwickler-Dokumentation des ELO Indexservers ausführlich beschrieben. Der Zugriff im Mapping-Skript kann über den Variablennamen elo erfolgen.

Standard-Mapping

- elo.type
  - Anhand der LDAP `ObjectClass=person`
  - Wenn die Klasse vorhanden ist, wird ein Benutzer erzeugt, sonst eine Gruppe.
- elo.name
  - Anhand der LDAP-Attributen `displayName`, `cn`, `sAMAccounName` und `distinguishedName`
  - Das zuerst gefunden LDAP-Attribut wird als Name gesetzt.
- `elo.userProps[UserInfoC.PROP_NAME_OS]`
  - Der Wert des LDAP-Attribut `sAMAccountName` wird übernommen.
- `elo.userProps[UserInfoC.PROP_NAME_EMAIL]`
  - Der Wert des LDAP-Attributs `mail` wird übernommen.
- `elo.superiorId`
  -

Das LDAP-Attribut `manager` wird ausgewertet.

- Wenn das `manager`-Attribut auf einen existierenden ELO Benutzer verweist, wird dessen ID als Vorgesetzter eingetragen.
- `elo.id`
  - Wenn der Name auf einen gültigen ELO Benutzer verweist, wird diese ID hier als ID eingetragen. Sonst -1 für einen neuen Benutzer.

JavaScript-Code-Rahmen

In der Log-Stufe debug wird das erzeugte Script im Logfile ausgegeben.

```
// rhino compatible modus on java 8 (nashorn)
load('nashorn:mozilla_compat.js')
// editable basic javascript mapping function Version 1.0
importPackage(Packages.de.elo.ix.client)
importClass(Packages.de.elo.ldap.LdapImportException)
function extractDN(v){
try{
var vv=v.substring(3,v.indexOf('=', 3))
return vv.substring(0,vv.lastIndexOf(','))
}
catch(e){}
}
function map(ixc, elo, ldap, userNames){
%% Hier wird der Text aus der Oberfläche für das Feld Mapping-Skript ausgegeben. %%
}
```

Wenn die ELO Administration Console unter Java 8 gestartet wurde, wird der Rhino-Kompatibilitätsmodus eingebunden.

```
public interface LdapImportMapping {
  public void map( de.elo.ix.client.IXConnection ixc, de.elo.ix.client.UserInfo userInfo,
                   javax.naming.directory.Attributes attributes,
                   Map<String, de.elo.ix.client.UserName> userNames );
}
```

Der Zugriff auf den JavaScript-Rahmen erfolgt über das Java Interface `LdapImportMapping`. In der Map wird der ELO-Namen in Kleinbuchstaben als Schlüssel auf das `UserName`-Objekt verwendet.

Beispiele

- Ein Datensatz kann ausgeschlossen werden, indem die elo.id=0 gesetzt wird.

```
if (elo.name.startsWith('_')){
elo.id=0
}
```

-

Da JavaScript-Code verwendet werden kann, ist es auch möglich, über den Mechanismus der Fehlermeldung auf der Oberfläche Ausgaben zum Testen anzeigen zu lassen.

```
throw ldap.get('mail').getClass()
```

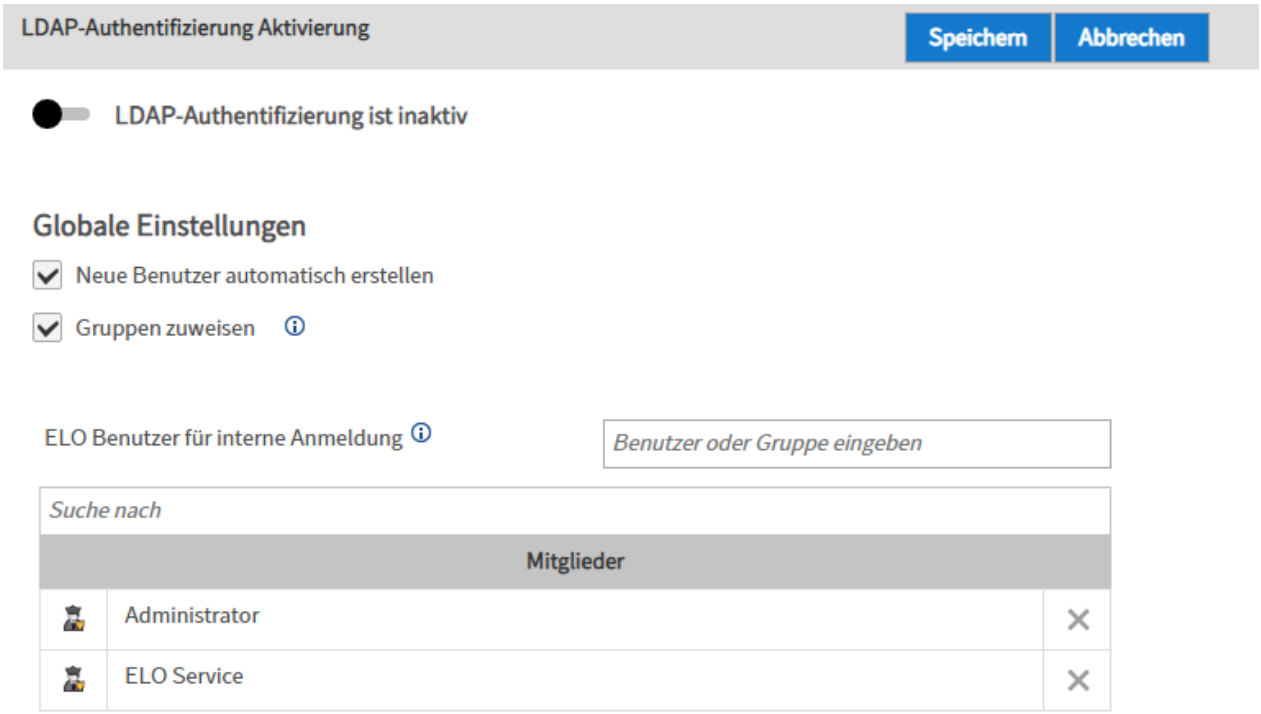
oder auch

```
throw userNames['administrator'].id
```

- Ein kleines Beispiel zeigt, wie unter Überprüfung des `mail`-Attributes Elemente ausgeschlossen werden können und der Anzeigename für die verbleibenden Benutzer gesetzt wird.

```
var emailRegex = /^[\w._-]+[+]?[\w._-]+@[\w.-]+\.[a-zA-Z]{2,6}$/
var lMail = ldap.get('mail')
if (lMail){
    lMail = lMail.get()
    if(emailRegex.test(lMail)){
        elo.name += ' ('+lMail.split('@').pop()+')'
        // gültige Mail -> den Anzeigename anpassen.
    }
}else{
    elo.id=0
    // ungültige Mail -> ausschließen
}
```

LDAP-Authentifizierung Aktivierung



LDAP-Authentifizierung ist inaktiv/LDAP-Authentifizierung ist aktiv: Mit diesem Schalter aktivieren oder deaktivieren Sie die LDAP-Authentifizierung.

Neue Benutzer automatisch erstellen: Ist die Option *Neue Benutzer automatisch erstellen* aktiviert, wird ein Benutzer nach der Anmeldung automatisch im ELO angelegt, sofern er noch nicht existiert.

> **Information**
>
> Die erstmalige Anmeldung, d. h. der Benutzer existiert noch nicht im ELO, muss über einen der folgenden Werte erfolgen:
>
> - `sAMAccountName`, `userPrincipalName` oder `mail` für Active Directory
> - `UID` oder `mail` für OpenLDAP

Gruppen zuweisen: Ist die Option *Gruppen zuweisen* aktiviert, werden Benutzer automatisch den passenden LDAP-Gruppen zugewiesen. Dafür müssen die Gruppen in ELO angelegt sein und die Namen müssen den Namen der Gruppen im LDAP entsprechen.

> **Beachten Sie**
>
> LDAP-Gruppen werden nur bei der Anmeldung der Benutzer ausgelesen und angewendet.

ELO Benutzer für interne Anmeldung: Hier legen Sie fest, welche ELO Benutzer/Gruppen sich nicht über LDAP authentifizieren sollen. Diese Benutzer/Gruppen können sich direkt an ELO anmelden.