Rechte in ELO

[Stand: 25.06.2019 | Programmversion: 12.00.000]

In diesem Dokument wird erklärt, wie die Rechte in ELO funktionieren. Die folgenden Einstellungen, Berechtigungen und Benutzerrechte gelten für die Version 12.

Wir sind bemüht, Ihnen eine möglichst übereinstimmende Dokumentation zu unseren Produkten zu liefern. Da wir aber unsere Module ständig weiterentwickeln und parallel auch mehrere Versionen herstellen, verändern sich Programmzustände sehr schnell. Kleinere Darstellungsfehler in der Dokumentation sind daher hin und wieder unvermeidbar. Hierfür bitten wir um Ihr Verständnis.

Inhalt

1 Einführung 4
1.1 Allgemeines 4
1.2 Glossar 4
2 Benutzerrechte 6
2.1 Grundeinstellungen, Rechte und „einschränkende“ Rechte 6
2.1.1 Grundeinstellungen für Benutzer 6
2.1.2 Grundeinstellungen für Gruppen 6
2.2 Rechte zur Benutzerverwaltung 8
2.2.1 Hauptadministrator (FLAG_ADMIN) 8
2.2.2 Benutzerdaten bearbeiten (FLAG_SUBADMIN) 8
2.2.3 Passwort ändern (FLAG_CHANGEPW) 9
2.2.4 SAP-Administrator (FLAG_SAPADMIN) 9
2.2.5 DMS Desktop Benutzer, keine Workflows (FLAG2_IS_DMS_DESKTOP_USER) 9
2.2.6 ELOxc Client Benutzer, nur E-Mails (FLAG2_LIMITED_CLIENT) 10
2.3 Rechte zu Ordner/Dokument Berechtigungen 10
2.3.1 Ordner bearbeiten (FLAG_EDITSTRUCTURE) 10
2.3.2 Dokumente bearbeiten (FLAG_EDITDOCS) 10
2.3.3 Berechtigungen verändern (FLAG_EDITACL) 11
2.3.4 Alle Einträge sehen, Berechtigungen ignorieren (FLAG_IGNOREACL) 11
2.3.5 Importberechtigung (FLAG_IMPORT) 11

2.3.6 Exportberechtigung (FLAG_EXPORT) 11
2.4 Rechte zu Ordner/Dokument Optionen 12
2.4.1 Maskenwechsel im Archiv (FLAG_CHANGEMASK) 12
2.4.2 Stichwortlisten bearbeiten (FLAG_EDITSWL) 12
2.4.3 Aufbewahrungsfrist bearbeiten (FLAG_EDITDUEDATE) 12
2.4.4 Dokumentenstatus ändern (FLAG_CHANGEREV) 12
2.4.5 Dokumentenpfad verändern (FLAG_CHANGEPATH) 13
2.4.6 Autor für Freigabedokumente (FLAG_AUTHOR) 13
2.4.7 „Weitere Infos“ anzeigen (FLAG2_SHOW_EXTRA_INFO) 13
2.5 Rechte zum Löschen 13
2.5.1 Ordner löschen (FLAG_DELSTRUC) 13
2.5.2 Dokumente löschen (FLAG_DELDOC) 13
2.5.3 Nicht änderbare Dokumente löschen (FLAG_DELREADONLY) 13
2.5.4 Versionen löschen (FLAG_DELVERSION) 14
2.6 Rechte zu Workflows 14
2.6.1 Workflows verwalten (FLAG_EDITWF) 14
2.6.2 Workflows starten (FLAG_STARTWF) 14
2.6.3 Workflow-Berechtigungserweiterung (FLAG2_EXTEND_WORKFLOW_RIGHTS) 15
2.6.4 Workflows aller Benutzer anzeigen (FLAG2_WF_CONTROLLER) 15
2.7 Rechte zu Systemeinstellungen 15
2.7.1 Stammdaten bearbeiten (FLAG_EDITCONFIG) 15
2.7.2 Scanprofile bearbeiten (FLAG_EDITSCAN) 15
2.7.3 Debugger verwenden (FLAG_EDITSCRIPT) 15
2.7.4 Verschlagwortungsmasken bearbeiten (FLAG_EDITMASK) 15
2.7.5 Replikationskreise bearbeiten (FLAG_EDITREPL) 16
2.8 Rechte zu ELO Analytics 16
2.8.1 Suchen verwalten (Discover) (FLAG2_ANALYTICS_DISCOVER) 16
2.8.2 Visualisierungen verwalten (FLAG2_ANALYTICS_VISUALIZE) 16
2.8.3 Dashboards verwalten (FLAG2_ANALYTICS_DASHBOARD_EDIT) 16
2.8.4 Dashboards anzeigen (FLAG2_ANALYTICS_DASHBOARD_VIEW) 16
3 Berechtigungen 17
3.1 Dokumente 17

3.2 Ordner ... 18
3.3 Randnotizen ... 18
3.3.1 Allgemeine Randnotiz ... 18
3.3.2 Persönliche Randnotiz ... 19
3.3.3 Permanente Randnotiz ... 19
3.4 Anmerkungen (mit Text) ... 19
3.5 Anmerkungen (ohne Text) ... 19
3.6 Stempel ... 20
3.6.1 Werkzeug Stempel ... 20
3.6.2 Stempelabdruck (wie Anmerkungen mit und ohne Text) ... 20
3.7 Verschlagwortungsmasken ... 21
3.7.1 Indexfelder ... 22
3.8 Workflow-Vorlagen ... 24
3.9 Workflows ... 24
3.10 Sonstige Rechte ... 25
3.10.1 Vorgängerrechte ... 25
3.10.2 Eigentümerrechte ... 26
3.10.3 Jeder ... 26
3.10.4 Workflow-Teilnehmer ... 26
4 Verschlüsselung ... 27
5 Konfiguration ... 28
5.1.1 Notwendige Rechte für die Bereiche der ELO Administration Console ... 28
5.1.2 Konfiguration für andere ... 31
5.1.3 Konfigurationskreise ... 31
5.1.4 Benutzergruppen und vererbte Rechte ... 32
5.1.5 Vertretungen ... 33
5.1.6 Berechtigung in Mein ELO/Feed ... 33

1 Einführung

1.1 Allgemeines

Grundsätzlich gibt es in ELO die Möglichkeit, die einzelnen Benutzer und Gruppen mit Benutzerrechten zu versehen. Diese kann man auch als „Werkzeuge" verstehen, die die Benutzer zu allgemeinen Aktionen im Archiv befähigen. Aber auch die einzelnen Einträge und Elemente sind in ELO mit Zugriffsrechten zu versehen, womit sich im Detail der Zugriff auf Daten und Information im System verfeinert einstellen lässt.

In der Praxis geht es darum, den Zugriff auf Information durch Unbefugte zu verhindern und die Veränderbarkeit der Daten so zu regeln, dass eine größtmögliche Balance zwischen Schutz und Arbeitsmöglichkeiten besteht. Diese Methoden stehen im System hierfür zur Verfügung:

- Benutzerrechte
- Berechtigungen
- Verschlüsselung

1.2 Glossar

Begriff	Definition
Benutzerrechte	Allgemeine Einstellungen, die darüber entscheiden, ob ein Benutzer bestimmte Funktionen (z.B. Benutzerdaten bearbeiten, Dokumente löschen) grundsätzlich in ELO ausführen darf.
Berechtigungen	Legen fest, welche Zugriffsrechte (z.B. lesen, löschen) Benutzer auf bestimmte/einzelne Objekte haben.
Zugriffsrechte	Haben je nach Kontext unterschiedliche Auswirkung, bezogen auf *Read*, *Write*, *Delete*, *Edit*, *List* (RWDEL).
Eigentümerrechte	Ein Platzhalter, bei dem, je nach Kontext, die Zugriffsrechte an den Benutzer vergeben werden, der einen Eintrag abgelegt hat, einen Workflow gestartet oder eine Anmerkung auf einem Dokument angebracht hat.
Persönlich	Diese Schaltfläche entfernt alle vorhandenen Zugriffsrechte aus einem Element und vergibt dem angemeldeten Benutzer alle Zugriffsrechte.

Vorgängerrechte	Ein Platzhalter, bei dem, je nach Kontext, die Zugriffsrechte des übergeordneten Elements übertragen werden.
Workflow-Teilnehmer	Ein Benutzer, der aktiv an einem ELO Workflow beteiligt ist.

2 Benutzerrechte

2.1 Grundeinstellungen, Rechte und „einschränkende“ Rechte

Grundeinstellungen können nicht vererbt werden. Aus diesem Grund wurden Sie auch nicht mehr als Rechte angelegt wie in vergangenen Versionen, sondern als Grundeinstellung, die bei jedem Benutzer individuell einstellbar sind. Gruppen und Benutzer haben teilweise unterschiedliche Grundeinstellungen.

2.1.1 Grundeinstellungen für Benutzer

2.1.1.1 Anmeldesperre aktivieren

Wenn bei einem Benutzer das Recht *Anmeldesperre aktivieren* gesetzt wird, kann sich dieser Benutzer nicht mehr im System anmelden. Das Benutzerkonto ist im System komplett gesperrt. Das bedeutet aber nicht, wie manchmal erwartet, dass gesperrte Benutzer nicht mehr im System sichtbar sind. Hierfür ist es notwendig, die Grundeinstellung *Sichtbar in Benutzerlisten* zu deaktivieren.

2.1.1.2 Sichtbar in Benutzerlisten

Ist diese Option aktiviert, erscheint der Benutzer in den Dialogen im ELO Client. Ist die Option deaktiviert, ist der Benutzer weiterhin als Benutzer in ELO vorhanden, er wird aber nicht in den Dialogen mit Benutzer-Auswahllisten angezeigt, die für normale Benutzer zugänglich sind. Die Sichtbarkeitseinstellungen eines Benutzers für andere kann auch über die Organisationseinheiten geregelt werden. Grundsätzlich können Benutzer, wenn sie in einer Organisationseinheit sind, nur Benutzer aus der eigener Organisationseinheit sehen.

Benutzer ohne aktivierte Grundeinstellung *Sichtbar in Benutzerlisten* können weiterhin als Feldwert in Tabellen und Übersichten sichtbar sein. Zum Beispiel als Feldwert in „Abgelegt von“ in den von den Benutzern abgelegten Dokumente, oder als Indexfeldwert in einem Benutzerfeld.

In der ELO Administration Console dürfen Benutzer mit den Rechten *Hauptadministrator* und *Benutzerdaten bearbeiten* Benutzer auch sehen, die sonst in den Clients nicht *Sichtbar in Benutzerlisten* sind. Das gilt auch für Administrationsaufgaben (Konfiguration, Workflows, Vertretung, Berechtigungen setzen…) im Client.

2.1.1.3 Interaktive Anmeldung erlauben

Ist diese Option aktiviert, kann sich der Benutzer über das Anmeldedialog im ELO Client anmelden.

2.1.2 Grundeinstellungen für Gruppen

2.1.2.1 Sichtbar in Benutzerlisten

Diese Option wirkt sich bei Gruppen identisch wie bei den Benutzer aus.

2.1.2.2 Optionengruppe

Optionengruppen werden definiert, um bestimmte *ProfileOpts* zuzuweisen. Nur diese Gruppen erscheinen in Dialogen, in denen Einstellungen für andere Benutzer vorgenommen werden.

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

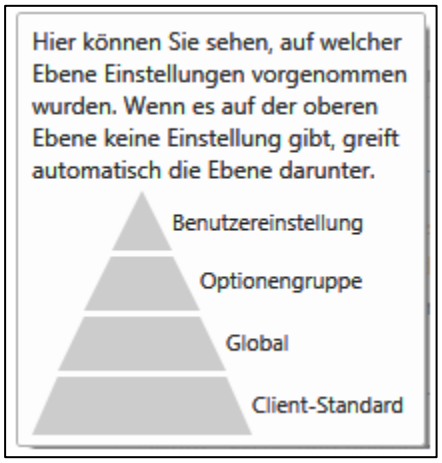


Abb. 1: Ebenenkonzept der Konfiguration

Über diese Gruppen können wir kontrollieren, welcher Benutzer welche Funktionen in welchem Zusammenhang zur Verfügung gestellt bekommt.

Wir können hierüber steuern, wer gewisse ELO Funktionen nur über die rechte Maustaste oder nur über die Symbole der Multifunktionsleiste oder beides gleichzeitig oder in gewissen Bereichen der Software überhaupt nicht zur Verfügung gestellt bekommt. Auch Skripte und deren Ausführung und 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 Benutzer sollte nur einmal in einer Optionengruppe vorhanden sein, da Mehrfachmitgliedschaften in einer Optionengruppe dazu führen können, dass Einstellungen vorgenommen wurden, die sich gegenseitig konkurrieren.

2.1.2.3 Vertretung erlaubt

Über diese ab ELO 12 hinzugefügte Eigenschaft können Sie die Verteilung der Rechte über das neue Vertretungsmodul steuern. Bei Gruppen, bei denen die Vertretung erlaubt ist, können die Rechte an Vertreter übertragen werden.

2.2 Rechte zur Benutzerverwaltung

2.2.1 Hauptadministrator (FLAG_ADMIN)

Dieses Recht wird benötigt, um globale Einstellungen vorzunehmen.

Wenn man beispielsweise das Recht *Benutzerdaten bearbeiten* besitzt, kann man mit dem **zusätzlichen** Recht *Hauptadministrator* **alle** Benutzer administrieren, nicht nur diejenigen, bei denen man als Administrator eingestellt ist. Benutzer mit dem Recht *Hauptadministrator* können weiterhin alle Benutzer sehen, auch die, die nicht *Sichtbar in Benutzerlisten* sind.

Das Recht *Hauptadministrator* ermöglicht, die Berechtigungen der obersten Archivebene zu verändern: Um die Rechte und Optionen der obersten Archivebenen zu ändern, muss man den *Berechtigungen setzen*-Dialog öffnen, dies geht nur mit dem Recht *Hauptadministrator*. Um die Berechtigungen tatsächlich zu ändern, braucht man aber *Berechtigungen ändern,* also benötigt man hier beide Rechte.

Mit dem Recht *Hauptadministrator* kann man:

- Einträge **dauerhaft entfernen**, auch wenn man die Rechte *Ordner löschen*, *Dokumente löschen*, *Versionen löschen* und *Nicht änderbare Dokumente löschen* nicht hat.
- Eine **Sperre entfernen** kann ein Hauptadministrator für alle Einträge, nicht nur für die selbst gesperrten Einträge.
- **Vertreter einsetzen**, für andere Benutzer
- **Ansichten** und **Vorschauprofile verwalten,** auch für andere Benutzer
- Verschlagwortungsmasken löschen
- Anmeldung beim Administrationsmodus oder bei geschlossenen Archiven

Lesen Sie dazu auch das Kapitel *5.1.1 Notwendige Rechte für die Bereiche der ELO Administration Console.*

2.2.2 Benutzerdaten bearbeiten (FLAG_SUBADMIN)

Dieses Recht erlaubt dem Benutzer, selbst andere Benutzer anzulegen und zu verwalten. Dabei können neue Benutzer nur mit den gleichen (oder weniger) Rechten ausgestattet werden.

Das Recht wird benötigt, wenn ein Benutzer als „Administrator" für andere Benutzer eingetragen ist. Nur dann kann er diese über die Benutzerverwaltung administrieren. Die Benutzerdaten dürfen aber nur vom Administrator des jeweiligen Benutzers gesehen und bearbeitet werden. Man kann als Administrator eine Gruppe eintragen. Dann können alle Benutzer mit dem Recht *Benutzerdaten bearbeiten* in dieser Gruppe diesen Benutzer oder Gruppe administrieren. Nur Benutzer mit den Rechten *Hauptadministrator* **und** *Benutzerdaten bearbeiten* können **alle** Benutzer sehen und administrieren. Eigene Benutzerdaten verwalten darf man nur, wenn man das Recht *Hauptadministrator* hat, oder aber selbst als Administrator in der Benutzerverwaltung eingetragen ist.

Vertretungsregelungen für andere können mit diesem Recht für die selbst administrierten Benutzer eingestellt werden, auch wenn diese Benutzer **nicht** *Sichtbar in Benutzerlisten* sind.

2.2.3 Passwort ändern (FLAG_CHANGEPW)

Dieses Recht erlaubt einem Benutzer, sein eigenes Passwort für das Anmelden in dem System zu ändern.

2.2.4 SAP-Administrator (FLAG_SAPADMIN)

Dieses Recht dient zur Anbindung von ELO an SAP mittels ELO Archive Link for SAP und ermöglicht die Verwaltung der Ablagemaske, die die Schnittstelle zu SAP betrifft. Die Ablagemaske für SAP-verwaltete Dokumente ist für alle sichtbar, aber nur von Benutzern mit diesem Recht zur Bearbeitung.

2.2.5 DMS Desktop Benutzer, keine Workflows (FLAG2_IS_DMS_DESKTOP_USER)

Ist diese Option gesetzt, stehen keinerlei Workflow-Funktionen zur Verfügung, betroffene Funktionen sind:

- 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 kein „Recht“, sondern eine Einschränkung und überschreibt alle andere Rechte, die es zu Workflows gibt. Wenn ein Benutzer dieses „Recht“ erhält, kann er all die Funktionen und Rollen, die Workflows betreffen, nicht verwenden, egal ob die einzelnen Rechte bei einem Benutzer direkt oder vererbt werden. Er kann auch ihm zugewiesene Workflow-Aufgaben nicht bearbeiten. Hintergrund ist, dass im ELO DMS Desktop keine Workflows inbegriffen sind.

2.2.6 ELOxc Client Benutzer, nur E-Mails (FLAG2_LIMITED_CLIENT)

Dieses Recht öffnet den Client for Microsoft Outlook in 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 ist kein „Recht“, es schränkt die Funktionalitäten ein.

2.3 Rechte zu Ordner/Dokument Berechtigungen

2.3.1 Ordner bearbeiten (FLAG_EDITSTRUCTURE)

Diese Option erlaubt es dem Benutzer, die Aktenstruktur (Schränke, Ordner oder Register) zu bearbeiten oder neu anzulegen.

Das Recht *Ordner bearbeiten* allein erlaubt nur das Anlegen neuer Ordner. In vorherigen Versionen war es so, dass das Anlegen eines neuen Dokuments als Veränderung des Ordners angesehen wurde. Das führte dazu, dass man zum Anlegen neuer Dokumente nicht nur das Recht *Dokumente bearbeiten,* sondern zusätzlich auch immer das Recht *Ordner bearbeiten* benötigte.

In der Version 11 wird das Einfügen des Dokuments nicht mehr als Veränderung des Ordners betrachtet. Ein Benutzer, der nur das Recht *Dokumente bearbeiten* hat, aber nicht das Recht *Ordner bearbeiten*, soll also neue Dokumente anlegen können.

2.3.2 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 Verschlagwortung von Dokumenten kann nur geändert werden, wenn das Recht vorhanden ist. Ohne dieses Recht öffnet sich die Verschlagwortung in Read-only-Modus.

2.3.3 Berechtigungen verändern (FLAG_EDITACL)

Erlaubt dem Benutzer, die Berechtigungen der Einträge (Dokumente und Ordner) im Archiv zu ändern.

> **Information**: Um die Berechtigungen der Einträge verändern zu können, braucht man grundsätzlich das Recht *Ordner bearbeiten* bzw. *Dokumente bearbeiten*. Ab ELO 12 benötigt man zusätzlich bei den einzelnen Einträgen das Zugriffsrecht *Berechtigungen setzen* (P).

Der Benutzer hat bei der Ablage im ELO Java Client in jedem Fall die Möglichkeit, die Rechte einzustellen, da er 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 der Benutzer die Stempel, Verschlagwortungsmasken usw. bearbeiten kann, kann er auch deren Berechtigungen bearbeiten, ohne dass dieses Benutzerrecht geprüft wird.

2.3.4 Alle Einträge sehen, Berechtigungen ignorieren (FLAG_IGNOREACL)

Dieses Recht beinhaltet, dass alle Dokumente und Ordner angezeigt werden, auch wenn sie für den jeweiligen Benutzer eigentlich verschlossen sind. Es hebt alle vorhandenen Objektberechtigungen auf. Wer dieses Recht besitzt, hat volle Berechtigungen auf alle ELO Einträge.

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

2.3.5 Importberechtigung (FLAG_IMPORT)

Dieses Recht erlaubt den Import eines Exportdatensatzes in das Archiv. Alle Daten werden importiert, die in dem Datensatz vorhanden sind, unabhängig von den Objektberechtigungen. Es werden also auch die Daten importiert, auf die der Benutzer im Archiv keine Berechtigung hat. Diese Daten sind für ihn anschließend nicht sichtbar.

2.3.6 Exportberechtigung (FLAG_EXPORT)

Dieses Recht erlaubt dem Benutzer, einen Exportdatensatz zu erstellen. Er kann nur die Einträge und Dokumente exportieren, auf die er im Archiv die Zugriffsberechtigung hat.

2.4 Rechte zu Ordner/Dokument Optionen



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

2.4.1 Maskenwechsel im Archiv (FLAG_CHANGEMASK)

Mit diesem Recht kann der Benutzer einem bereits verschlagworteten Dokument nachträglich eine andere Verschlagwortungsmaske zuweisen. Hierbei ist zu beachten, dass beim Maskenwechsel Verschlagwortungsinformationen verloren gehen können. Voraussetzung ist, dass das Recht *Ordner bearbeiten* bzw. *Dokumenten bearbeiten*, je nach Eintrag, vorhanden ist.

2.4.2 Stichwortlisten bearbeiten (FLAG_EDITSWL)

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

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

2.4.3 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 der Verschlagwortung deaktiviert.

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

2.4.4 Dokumentenstatus ändern (FLAG_CHANGEREV)

Mit diesem Recht kann der Benutzer den Dokumentenstatus über den Reiter *Optionen* in der Verschlagwortung von Dokumenten einstellen:

- Keine Versionskontrolle
- Versionskontrolle eingeschaltet
- Keine Änderung möglich

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

2.4.5 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 Verschlagwortung 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*.

2.4.6 Autor für Freigabedokumente (FLAG_AUTHOR)

Dieses Recht erlaubt das Kontrollkästchen *Freigabedokument* zu setzen 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 *Dokumenten bearbeiten* vorhanden ist.

2.4.7 „Weitere Infos“ anzeigen (FLAG2_SHOW_EXTRA_INFO)

Dieses Recht legt fest, ob der Benutzer den Tab *Weitere Infos* innerhalb der Verschlagwortung sehen kann. Voraussetzung ist, dass das Recht *Ordner bearbeiten* bzw. *Dokumente bearbeiten*, je nach Eintrag, vorhanden ist.

2.5 Rechte zum Löschen

2.5.1 Ordner löschen (FLAG_DELSTRUC)

Dieses Recht legt fest, ob ein Benutzer Ordner löschen darf.

2.5.2 Dokumente löschen (FLAG_DELDOC)

Dieses Recht legt fest, ob ein Benutzer Dokumente löschen darf.

2.5.3 Nicht änderbare Dokumente löschen (FLAG_DELREADONLY)

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

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

2.5.4 Versionen löschen (FLAG_DELVERSION)

Mit diesem Recht kann der Benutzer einzelne Versionen aus der Versionsverwaltung eines Dokuments löschen. *bearbeiten* vorhanden ist.ist.

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

2.6 Rechte zu Workflows

2.6.1 Workflows verwalten (FLAG_EDITWF)

Mit diesem Recht Zur Verwaltung der Workflows gehören:

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

2.6.2 Workflows starten (FLAG_STARTWF)

Mit diesem Recht kann ein Benutzer Workflows starten. Betroffene Funktionen:

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

Er benötigt dieses Recht auch, um Workflows bei der Ablage von Einträgen mit einer Verschlagwortungsmaske mit einem hinterlegten Workflow zu starten. Hat er dieses Recht nicht, dann kann er 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 Java Client aktiv zu bekommen. So kann der Benutzer sich einen Überblick über alle Workflows verschaffen, an denen er direkt oder indirekt über eine Gruppe beteiligt ist.

2.6.3 Workflow-Berechtigungserweiterung (FLAG2_EXTEND_WORKFLOW_RIGHTS)

Ist das Recht gesetzt, wird dem Benutzer ein temporäres Leserecht für den im aktiven Workflowknoten befindlichen Eintrag zugeteilt. 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. Ist das Recht gesetzt, wird dem Benutzer ein temporäres Leserecht für den im Workflow befindlichen Eintrag zugeteilt. 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 wirkt auf Dokumente und Ordner, nicht auf Verschlagwortungsmasken.

2.6.4 Workflows aller Benutzer anzeigen (FLAG2_WF_CONTROLLER)

Das Recht erlaubt einem Benutzer, alle aktiven Workflows zu sehen und nicht nur diejenige, an denen er beteiligt ist.

2.7 Rechte zu Systemeinstellungen

2.7.1 Stammdaten bearbeiten (FLAG_EDITCONFIG)

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

2.7.2 Scanprofile bearbeiten (FLAG_EDITSCAN)

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

2.7.3 Debugger verwenden (FLAG_EDITSCRIPT)

Skripte sind normale Dokumente im Archiv. Das heißt, um Skripte bearbeiten zu dürfen, muss man die entsprechenden Zugriffsrechte auf die einzelnen zu bearbeitenden Skripte besitzen. Im ELO Java Client kann man mit diesem Recht über den Tastaturbefehl STRG + Alt + D den JavaScript-Debugger öffnen.

2.7.4 Verschlagwortungsmasken bearbeiten (FLAG_EDITMASK)

Mit diesem Recht darf der Benutzer neue Verschlagwortungsmasken anlegen und bestehende verändern.

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

2.7.5 Replikationskreise bearbeiten (FLAG_EDITREPL)

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

2.8 Rechte zu ELO Analytics

2.8.1 Suchen verwalten (Discover) (FLAG2_ANALYTICS_DISCOVER)

Mit diesem Recht können Sie die Abfragen auf die Lucene-Datenbank erstellen und konfigurieren. Die Abfragen sind die Grundlage für die Auswertungen der Daten aus dem ELO Archiv.

2.8.2 Visualisierungen verwalten (FLAG2_ANALYTICS_VISUALIZE)

Mit diesem Recht können Sie die Visualisierung für die Suchergebnisse aus der Lucene-Datenbank festlegen.

2.8.3 Dashboards verwalten (FLAG2_ANALYTICS_DASHBOARD_EDIT)

Mit diesem Recht können Sie die Dashboards verwalten. Auf den Dashboards werden die Suchergebnisse den gewünschten Visualisierungen zugewiesen.

2.8.4 Dashboards anzeigen (FLAG2_ANALYTICS_DASHBOARD_VIEW)

Mit diesem Recht können Sie die fertig konfigurierten Dashboards anzeigen. Sie haben nur das Recht, die Auswertungsergebnisse anzusehen.

3 Berechtigungen

Mit ELO 12 steht für ELO Objekte im Archiv das neues Recht *Berechtigungen setzen* (P) zur Verfügung. Dieses Recht regelt die Steuerung der Berechtigungsänderungen eines ELO Objektes im Archiv. Hat ein ELO Benutzer dieses Recht auf einem ELO Objekt, kann er die Berechtigungen anpassen.

3.1 Dokumente

Zugriffsrecht	Bezeichnung ab 10.0	Berechtigt zu
R (Read) *<Lesen>*	Sehen (R)	Dokument und Verschlagwortung sehen, Berechtigungen sehen, Notizen hinzufügen
W (Write) *<Schreiben>*	Verschlagwortung ändern (W)	Verschlagwortung ändern, bzw. beim Einchecken einer neuen Version, das Datum anpassen.
D (Delete) *<Löschen>*	Löschen (D)	Dokument als gelöscht markieren
E (Edit) *<Bearbeiten>*	Bearbeiten (E)	Dokumentdatei ändern, Auschecken, Einchecken, Neue Version laden, Arbeitsversion ändern
L (List) *<Listen>*	*Keine Auswirkung auf Dokumente im ELO Java Client*	
P (Permissions) *<Berechtigungen>*	Berechtigungen setzen (P)	Berechtigungen ändern

3.2 Ordner

Zugriffsrecht	Bezeichnung ab 10.0	Berechtigt zu
R (Read) *<Lesen>*	Sehen (R)	Ordner sehen im Baumansicht, Randnotizen hinzufügen
W (Write) *<Schreiben>*	Verschlagwortung ändern (W)	Verschlagwortung bearbeiten
D (Delete) *<Löschen>*	Löschen (D)	Ordner als gelöscht markieren (nur wenn auch Untereinträge gelöscht werden können oder der Ordner leer ist)
E (Edit) *<Bearbeiten>*	*Keine Auswirkung auf Ordner, wichtig aber für die Vererbung der Rechte auf die darin enthaltene Dokumente*	Obwohl Ordner ausgecheckt werden können und damit alle enthaltenen Dokumente auf der ersten Ebene unterhalb des Ordners mit dem Recht *Bearbeiten*, wird dieses Recht bei Ordnern nicht ausgewertet.
L (List) *<Listen>*	Liste bearbeiten	Inhalt des Ordners bearbeiten: Neue Dokumente darin einfügen, verschieben, kopieren oder entfernen. Referenz einfügen oder löschen.
P (Permissions) *<Berechtigungen>*	Berechtigungen setzen (P)	Berechtigungen ändern

3.3 Randnotizen

Die Randnotizen sind seit Langem in den ELO Systemen vorhanden. Ihnen liegt ein anderes Konzept als bei den Zugriffsrechten zugrunde, was die Sichtbarkeit und die Möglichkeiten, diese zu verändern, betrifft.

3.3.1 Allgemeine Randnotiz

Diese Randnotizen können vom jedem, der den Eintrag sehen kann, angelegt, bearbeitet und gelöscht werden. Wenn man nur das Recht *Lesen* auf dem Dokument hat, kann man nur allgemeine Randnotizen löschen, die man selbst angebracht hat.

3.3.2 Persönliche Randnotiz

Der Benutzer, der das Leserecht auf dem Eintrag hat, kann diese Randnotizen für sich selbst anlegen, bearbeiten oder löschen. Sonst kann keiner diese Randnotizen sehen.

3.3.3 Permanente Randnotiz

Jeder, der den Eintrag sehen kann, kann auch die darauf angebrachten permanenten Randnotizen sehen, aber nicht nachträglich ändern oder löschen.

3.4 Anmerkungen (mit Text)

Die Anmerkungen mit Text umfassen Haftnotizen, Textnotizen, Textstempel.

Zugriffsrecht	Bezeichnung	Berechtigt zu
R (Read) *<Lesen>*	Sehen (R)	Anmerkung auf dem Dokument betrachten
W (Write) *<Schreiben>*	Ändern (W)	Textinhalt bearbeiten und formatieren, Position merken, Positionsmarke einfügen (nicht bei Textstempel), Größe ändern
D (Delete) *<Löschen>*	Löschen (D)	Löschen
E (Edit) *<Bearbeiten>*	Verschieben (E)	Position der Anmerkung auf dem Dokument ändern
L (List) *<Listen>*	*Keine Auswirkung auf Anmerkungen*	
P (Permissions) *<Berechtigungen>*	Berechtigungen setzen (P)	Berechtigungen ändern

3.5 Anmerkungen (ohne Text)

Die Anmerkungen ohne Text umfassen Freihandmarker, Rechteckmarkierung, horizontaler Marker und Durchstreicher, Schwärzung und Bildstempel.

Zugriffsrecht	Bezeichnung	Berechtigt zu
R (Read) *<Lesen>*	Sehen (R)	Anmerkung auf dem Dokument betrachten
W (Write) *<Schreiben>*	Ändern (W)	Eigenschaften ändern (Farbe, Strichdicke)
D (Delete) *<Löschen>*	Löschen (D)	Löschen
E (Edit) *<Bearbeiten>*	Verschieben (E)	Position der Anmerkung auf dem Dokument ändern
L (List) *<Listen>*	*Keine Auswirkung auf Anmerkungen*	
P (Permissions) *<Berechtigungen>*	Berechtigungen setzen (P)	Berechtigungen ändern

3.6 Stempel

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

3.6.1 Werkzeug Stempel

Das Werkzeug „Stempel" wird mittels *ProfileOpts* für einen bestimmten Benutzer, Optionengruppe oder Global definiert. Das setzt den definierten Stempel in der Liste der verfügbaren Stempel für die entsprechenden Benutzer. Hat man für einen Benutzer keinen Stempel entweder speziell für ihn oder für eine Gruppe, zu der er gehört, kann dieser Benutzer das Werkzeug „Stempel" nicht verwenden. Er kann auch keine Stempel im ELO Java Client für sich selbst definieren.

3.6.2 Stempelabdruck (wie Anmerkungen mit und ohne Text)

Zugriffsrecht	Bezeichnung	Berechtigt zu
R (Read) *<Lesen>*	Sehen (R)	Stempelabdruck auf dem Dokument betrachten
W (Write) *<Schreiben>*	Ändern (W)	Größe ändern beim Textstempel, Position merken

D (Delete) *<Löschen>*	Löschen (D)	Stempelabdruck löschen
E (Edit) *<Bearbeiten>*	Verschieben (E)	Position auf Dokument ändern
L (List) *<Listen>*	*Keine Auswirkung auf Stempel*	
P (Permissions) *<Berechtigungen>*	Berechtigungen setzen (P)	Berechtigungen ändern

3.7 Verschlagwortungsmasken

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

Zugriffsrecht	Bezeichnung	Berechtigt zu
R (Read) *<Lesen>*	Verschlagwortung sehen (R)	Maske in der Maskenliste im Verschlagwortungsdialog sehen, Verschlagwortung im Read-only-Modus sehen. Die Maske kann zwar ausgewählt werden, aber erst mit dem W-Recht kann die Verschlagwortung ausgefüllt und der Dialog mit „Speichern“ verlassen werden.

W (Write) *<Schreiben>*	Verschlagwortung ändern (W)	Einträge ablegen/verschlagworten (auch Erstablage). Haben Sie das übergeordnete W-Recht der Maske nicht, können Sie die Verschlagwortung der Einträge nicht ändern. Auch bei einem vorhandenen W-Recht beim Eintrag öffnet sich der Dialog im Read-only-Modus. Um die Verschlagwortung eines damit abgelegten Eintrags danach zu verändern, benötigen Sie zusätzlich das W-Recht auf dem Eintrag.
D (Delete) *<Löschen>*	Maske löschen (D)	Dieses Recht wurde in der Vergangenheit im ELO Windows Client geprüft und ist aus historischen Gründen noch vorhanden. Aktuell wird es nicht geprüft. Um Masken in der ELO Administration Console löschen zu können wird das Benutzerrecht *Hauptadministrator* geprüft.
E (Edit) *<Bearbeiten>*	Maske bearbeiten (E)	Dieses Recht wurde in der Vergangenheit im ELO Windows Client geprüft und ist aus historischen Gründen noch vorhanden. Aktuell wird es nicht geprüft.
L (List) *<Listen>*	*Keine Auswirkung auf Verschlagwortungsmasken*	
P (Permissions) *<Berechtigungen>*	*Keine Auswirkung auf Verschlagwortungsmasken*	

3.7.1 Indexfelder

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

Diese Eigenschaft des Indexfeldes ist übergeordnet. Eine feine Gliederung des „Normalen Zugriffs“ kann über die Zugriffsrechte geregelt werden.



Abb. 2: Darstellung der Indexfelder bei der ELO Administration Console, Indexfelder

Zugriffsrecht	Bezeichnung	Berechtigt zu
R (Read) *<Lesen>*	Sehen (R)	Das Indexfeld sehen, Zusammenarbeit mit der Darstellung (Normaler Zugriff/Schreib-geschützt/Unsichtbar) berücksichtigen
W (Write) *<Schreiben>*	Schreiben (W)	Das Indexfeld ausfüllen, Zusammenarbeit mit der Darstellung (Normaler Zugriff/Schreib-geschützt/Unsichtbar) berücksichtigen
D (Delete) *<Löschen>*	*Keine Auswirkung auf Indexfelder*	
E (Edit) *<Bearbeiten>*	*Keine Auswirkung auf Indexfelder*	
L (List) *<Listen>*	*Keine Auswirkung auf Indexfelder*	
P (Permissions) *<Berechtigungen>*	*Keine Auswirkung auf Indexfelder*	

3.8 Workflow-Vorlagen

Zugriffsrecht	Bezeichnung	Berechtigt zu
R (Read) *<Lesen>*	Sehen (R)	Sehen, Workflow damit starten
W (Write) *<Schreiben>*	Ändern (W)	Vorlage bearbeiten, neue Version der Vorlage erstellen
D (Delete) *<Löschen>*	Löschen (D)	Vorlage löschen
E (Edit) *<Bearbeiten>*	*Keine Auswirkung auf Workflow-Vorlagen*	
L (List) *<Listen>*	*Keine Auswirkung auf Workflow-Vorlagen*	
P (Permissions) *<Berechtigungen>*	Berechtigungen setzen (P)	Berechtigungen ändern

3.9 Workflows

Ab ELO 11 können Sie die Zugriffsrechte auf den einzelnen Workflows als Prozess bestimmen. Sind keine Berechtigungen für den Workflow beim Design der Workflow-Vorlage vorgesehen, gilt der Standard, der bis ELO 10 den Zugriff auf die Workflows bestimmt hat: Benutzer mit dem Benutzerrecht „Workflows aller Benutzer anzeigen" können den Workflow sehen (R-Recht). Benutzer mit dem Benutzerrecht „Workflows verwalten" können den Workflow sehen, nach Start ändern, dauerhaft entfernen und beenden (die Rechte R W D E). Das L-Recht hat keine Auswirkung auf die Workflows.

Sind keine Berechtigungen zu einem Workflow hinterlegt, verhält sich alles wie in ELO 9 und ELO 10:

- Das Benutzerrecht „Workflows verwalten" (FLAG_EDITWF) erhält R W D E L
- Das Benutzerrecht „Workflows aller Benutzer anzeigen" (FLAG2_WF_CONTROLLER) erhält R

Mit Berechtigungen wird Folgendes geprüft:

- „Workflow sehen" (R) benötigt das entweder das Zugriffsrecht „Sehen" (R) oder das Benutzerrecht „Workflows aller Benutzer anzeigen" (FLAG2_WF_CONTROLLER) oder der Benutzer muss in einem aktiven Workflowknoten eingetragen sein.

- „Workflow ändern“ (W) benötigt das Zugriffsrecht „Schreiben“ (W) und „Workflows verwalten“ (FLAG_EDITWF).
- „Workflow löschen“ (D) benötigt das Zugriffsrecht „Löschen“ (D) und „Workflows verwalten“ (FLAG_EDITWF).
- „Workflow beenden“ (E) benötigt das Zugriffsrecht „Bearbeiten“ € und „Workflows verwalten“ (FLAG_EDITWF).

Zugriffsrecht	Bezeichnung	Berechtigt zu
R (Read) *<Lesen>*	Workflow sehen (R)	Workflow (als Prozess) sehen
W (Write) *<Schreiben>*	Workflow nach Start ändern (W)	Workflow nach Start ändern
D (Delete) *<Löschen>*	Workflow dauerhaft entfernen (D)	Workflow dauerhaft entfernen
E (Edit) *<Bearbeiten>*	Workflow beenden (E)	
L (List) *<Listen>*	*Keine Auswirkung auf Workflows*	
P (Permissions) *<Berechtigungen>*	Berechtigungen setzen (P)	Berechtigungen ändern

3.10 Sonstige Rechte

3.10.1 Vorgängerrechte

Hierarchie der Elemente für die Berücksichtigung der Vorgängerrechte und der Rechte, die bei einem Element vererbt werden. Ordner haben andere Ordner oder Dokumente als Untereinträge. Die Dokumente haben Dateianbindungen und Notizen als Untereinträge.

Beispiel: Ein Dokument hat die Berechtigungen nur für eine Gruppe und die Notizen darin haben die Berechtigungen für *Jeder*. Hier ist die Einschränkung der Rechte auf dem Dokument entscheidend, also nicht *Jeder* wird die Notiz sehen können, nur diejenigen, die auch auf das Dokument Leserecht haben.

Hat ein Benutzer Rechte auf einem Dokument, aber keine Zugriffsrechte auf dessen gesamten Ablagepfad, wird das Dokument nach einer Suche oder Verlinkung in der Trefferliste angezeigt.

3.10.2 Eigentümerrechte

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

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

3.10.3 Jeder

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

Sie können Ihr Archiv 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 ein, mit folgender Zeile im Zusatztext:

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

3.10.4 Workflow-Teilnehmer

Mit der Einführung von Berechtigungen für Workflows entsteht der Bedarf, diesen Platzhalter einzuführen. So können bei den Workflows die Teilnehmer des Workflows speziell berechtigt werden. Dieser Platzhalter wird dann in jedem Workflow mit den Gruppen und Benutzer ersetzt, die an den Workflow in egal welcher Knoten teilnehmen.

4 Verschlüsselung

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

Die Verschlüsselung in ELO wurde zur Version 12 überarbeitet. Es wird 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 Archiv erfolgen. Dokumente in der Postbox lagern dort immer unverschlüsselt, bis sie letztendlich ins Archiv verschoben werden. Eine nachträgliche Verschlüsselung schon im ELO Archiv befindlicher Dokumente ist über ELO Funktionen nicht vorgesehen und normalerweise auch nicht sinnvoll, denn sobald im Archiv angekommen, 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 wurde.

5 Konfiguration

5.1.1 Notwendige Rechte für die Bereiche der ELO Administration Console

Administrationsbereiche	Rechte
Systemeinstellungen	
Benutzerverwaltung	Benutzerdaten bearbeiten, Hauptadministrator (Mit dem Recht *Hauptadministrator* kann man **ALLE** Benutzer administrieren, nicht nur diejenigen, bei dem 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)
Verschlagwortungsmasken	Verschlagwortungsmasken 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)
Indexfeldvorlagen	Verschlagwortungsmasken 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	
Archivkennung	Hauptadministrator
Schriftfarben	Stammdaten bearbeiten

Administrationsbereiche	Rechte
Wartung	
Administrationsmodus	Hauptadministrator
Reportoptionen	Hauptadministrator
Reporteinträge löschen	Hauptadministrator
Löschen und entfernen	Hauptadministrator
Backup-Tasks	Hauptadministrator
Passwortregeln	Hauptadministrator
Dokumentdateien verschieben	Hauptadministrator

Administrationsbereiche	Rechte
Servermodule	
ELO Automation Services	Hauptadministrator
Backup-Profile	Hauptadministrator

Volltextdienst	Hauptadministrator
Passwort erstellen	Hauptadministrator
ELO Transport	Hauptadministrator
Konfigurationsdateien	Hauptadministrator
Formulardesigner	Workflows verwalten
ELOxc for Microsoft EWS	*Keine Prüfung in der ELO Administration Console! Prüfung übernimmt die ELOxc Console selbst.*

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

Administrationsbereiche	Rechte

Weitere	
LDAP-Import	Hauptadministrator
Archiv schließen	Hauptadministrator

5.1.2 Konfiguration für andere

Als Benutzer mit dem Recht *Hauptadministrator* kann man für andere Benutzer und für Optionengruppen Einstellungen vornehmen. Ab der Version 10.1 ist es für Benutzer mit dem Recht *Benutzerdaten bearbeiten* auch für die eigens administrierten Benutzer möglich.

5.1.3 Konfigurationskreise

Es gibt Optionen, die für Benutzer zugänglich sein müssen: Die User Experience verbessert sich dadurch, dass er Kontrolle über Aussehen oder Funktionen hat. Andere Optionen erfordern aber Fachkenntnisse, die nur Administratoren haben.

Die Konfigurationskreise, die man aus dem Web Client kennt, entstehen aus dem Bedürfnis, die Sichtbarkeit und Zugriffsmöglichkeiten auf die Konfiguration für bestimmte Benutzer einzugrenzen bzw. ermöglichen.

Jede Einstellung wird dabei in sogenannten Konfigurationskreisen organisiert. Benutzer sehen in ihrer eigenen Konfiguration nur Einstellungen von Gruppen, die ihnen zugeordnet wurden, was es beispielsweise ermöglicht, administrative oder komplizierte Einstellungen vor Benutzer zu verstecken. Aus Transparenzgründen wird dem Administrator die Farbe des Konfigurationskreises ebenfalls angezeigt.

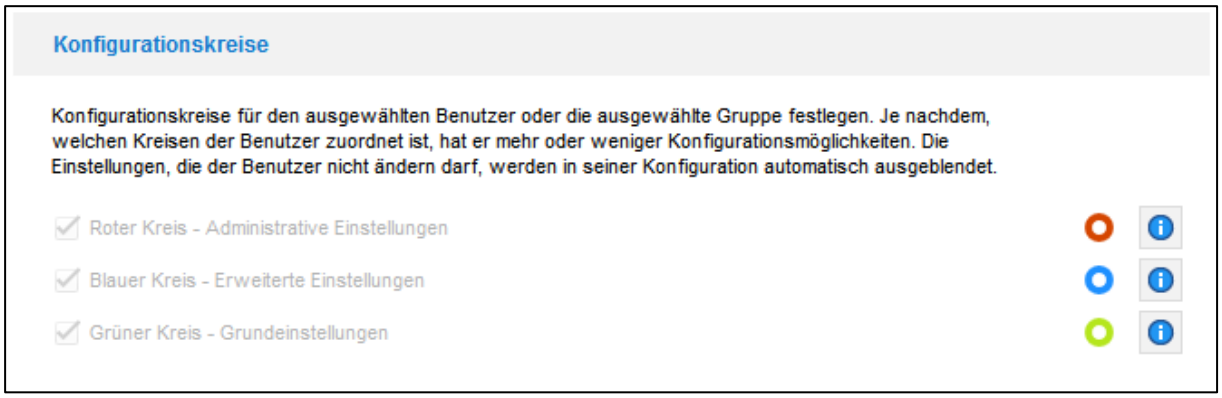


Abb. 3: Konfiguration ELO Web Client - Konfigurationskreise

5.1.3.1 Roter Kreis - Administrative Einstellungen

Die Zugehörigkeit zum roten Kreis bestimmt, ob ein Benutzer administrative Einstellungen vornehmen darf. Diese Einstellungen sind sehr technisch und nur für Experten geeignet. Bedenken Sie, dass diese Einstellung für den Standard dynamisch ermittelt wird und hier wegen der Administrationsrechte als *true* angezeigt. Benutzer, die dem roten Kreis zugewiesene Optionen sehen dürfen, dürfen auch Optionen in den beiden anderen Kreisen sehen. Dies ist Administratoren vorbehalten.

5.1.3.2 Blauer Kreis - Erweiterte Einstellungen

Die Zugehörigkeit zum blauen Kreis bestimmt, ob ein Benutzer erweiterte Einstellungen vornehmen darf. Diese Einstellungen sind nur für fortgeschrittene Benutzer geeignet, die sich gut mit ELO auskennen. Benutzer, die dem blauen Kreis zugewiesene Optionen sehen dürfen, dürfen auch Optionen in dem grünen Kreis sehen.

5.1.3.3 Grüner Kreis - Grundeinstellungen

Jeder Benutzer darf die Einstellungen, die mit einem grünen Kreis gekennzeichnet sind, nach seinen persönlichen Vorlieben verändern. Benutzer, die dem grünen Kreis zugewiesene Optionen sehen dürfen, dürfen keine weiteren Optionen sehen.

5.1.4 Benutzergruppen und vererbte Rechte

Bis auf die Grundeinstellungen können alle Benutzerrechte über die Gruppen auf deren Mitglieder vererbt werden. Die ELO Administration Console zeigt beim Mouseover über die rechte Kontrollkästchen-Spalte, von welcher Gruppe das entsprechende Benutzerrecht geerbt wurden. Es wird auch empfohlen, die Vergabe der Rechte über die Gruppen-Vererbung und nicht über die direkte Vergabe an die einzelnen Benutzer vorzunehmen.

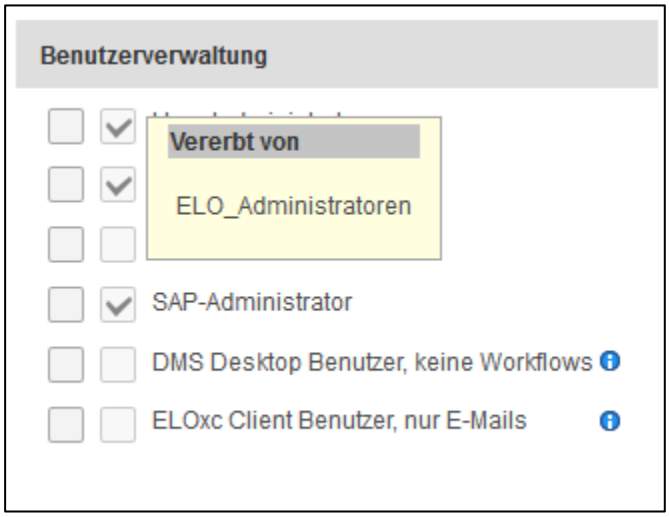


Abb. 4: Benutzerverwaltung: Vererbte Rechte im Mouseover

5.1.5 Vertretungen

Vertreterregelungen können ab der Version 12 mit Gruppenrechten organisiert werden. Damit ist die Vertreterregelung besser an die Abteilungsstruktur in den Unternehmen anpassbar.

Dabei wird festgelegt, welche Gruppen an die Vertreter übergeben werden.

Welche Berechtigungen ein Vertreter durch die Vertretung bekommt, wird über Gruppen eingestellt.

Der Benutzer kann zum Einstellen einer Vertretung aus einer Liste seiner **Gruppenzugehörigkeiten** auswählen, für welche Gruppen der Vertreter berechtigt werden soll.

Es stehen hier nur Gruppen zur Auswahl, welche die Eigenschaft **Vertretung erlaubt** gesetzt haben. Diese Eigenschaft ist neu und muss in der Benutzerverwaltung eingebaut werden. Im Standard ist die Eigenschaft nicht gesetzt.

Überlegen Sie sich vor allem aus Datenschutzgründen genau, welche Gruppen für eine Vertretung geeignet sind und geben Sie diese dann gezielt frei.

Der Vertreter erhält dann folgende mit der Gruppe zusammenhängenden Rechte:

- Benutzerrechte
- Zugriffsrechte auf Archiveinträge, Notizen, Workflows, Feed-Beiträge usw. (jegliche Elemente mit entsprechenden ACL-Berechtigungen für die Gruppe)
- Gruppenaufgaben, unabhängig davon, ob diese noch nicht angenommen sind, oder von dem zu vertretenden Benutzer angenommen wurden
- Erwähnungen der Gruppe. Diese Beiträge erscheinen dann im „Mein ELO“-Bereich des Vertreters

5.1.6 Berechtigung in Mein ELO/Feed

Die Sichtbarkeit der Einträge im Feed können eingeschränkt werden, wenn dazu noch keine Kommentare verfasst worden sind.

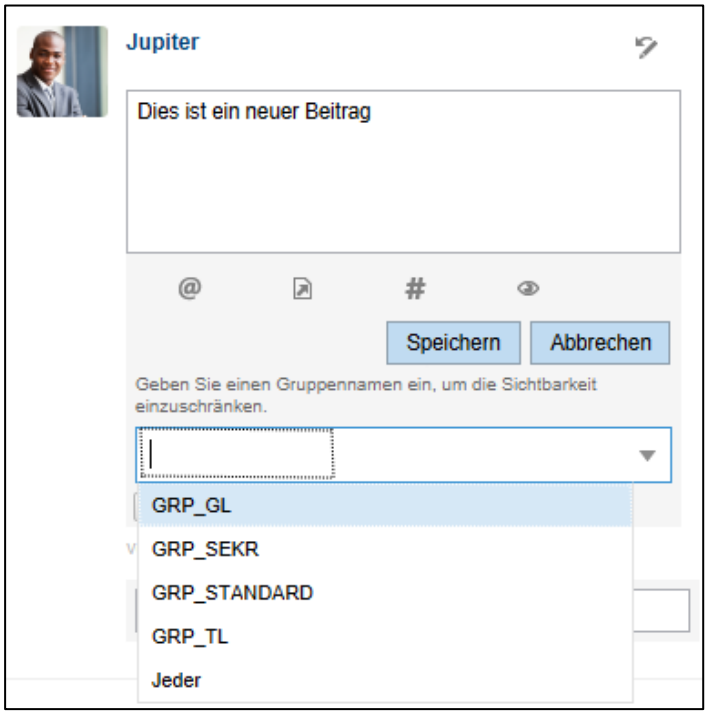


Abb. 5: Änderung der Sichtbarkeit eines Beitrags im ELO Feed

Administration Console, Rechte 29
Alle Einträge sehen, Berechtigungen ignorieren 11
Analytics 16
Anmeldesperre aktivieren 6
Anmerkungen, Berechtigungen 20
Autor für Freigabedokumente 13
Benutzerdaten bearbeiten 9
Benutzerrechte 4, 6
Berechtigungen 4, 18
Berechtigungen verändern 11
Dashboards anzeigen 17
Dashboards verwalten 16
DMS Desktop Benutzer, keine Workflows 9
Dokumente bearbeiten 11
Dokumente löschen 14
Dokumente, Berechtigungen 18
Dokumentenpfad verändern 13
Dokumentenstatus ändern 13
Eigentümerrechte 4
Eigentümerrechte, Berechtigungen setzen 27
ELOxc Client Benutzer, nur E-Mails 10
Exportberechtigung 12
Feed, Berechtigungen 34
FLAG_ADMIN 8
FLAG_AUTHOR 13
FLAG_CHANGEMASK 12
FLAG_CHANGEPATH 13
FLAG_CHANGEPW 9
FLAG_CHANGEREV 13
FLAG_DELDOC 14
FLAG_DELREADONLY 14
FLAG_DELSTRUC 14
FLAG_DELVERSION 14
FLAG_EDITACL 11
FLAG_EDITCONFIG 15
FLAG_EDITDOCS 11
FLAG_EDITDUEDATE 12
FLAG_EDITMASK 16
FLAG_EDITSCAN 16
FLAG_EDITSTRUCTURE 10
FLAG_EDITSWL 12
FLAG_EDITWF 14
FLAG_EXPORT 12
FLAG_IGNOREACL 11
FLAG_IMPORT 12
FLAG_SAPADMIN 9
FLAG_STARTWF 14
FLAG_SUBADMIN 9
FLAG2_ANALYTICS_DASHBOARD_EDIT 16
FLAG2_ANALYTICS_DASHBOARD_VIEW 17
FLAG2_ANALYTICS_DISCOVER 16
FLAG2_ANALYTICS_VISUALIZE 16
FLAG2_EXTEND_WORKFLOW_RIGHTS 15
FLAG2_IS_DMS_DESKTOP_USER 9
FLAG2_LIMITED_CLIENT 10
FLAG2_SHOW_EXTRA_INFO 13
Grundeinstellungen, Rechte und „einschränkende“ Rechte 6
Hauptadministrator 8
Importberechtigung 12
Interaktive Anmeldung erlauben 6
Jeder, Berechtigungen setzen 27
Konfigurationskreise 32
Maskenwechsel im Archiv 12
Mein ELO, Berechtigungen 34
Nicht änderbare Dokumente löschen 14
Optionengruppe 7
Ordner bearbeiten 10
Ordner löschen 14
Ordner, Berechtigungen 19
Passwort ändern 9
Randnotizen, Berechtigungen 19
Rechte zu Ordner/Dokument Berechtigungen 10
Rechte zu Ordner/Dokument Optionen 12
Rechte zu Systemeinstellungen 15
Rechte zu Workflows 14
Rechte zum Löschen 14
Rechte zur Benutzerverwaltung 8
SAP-Administrator 9
Scannereinstellungen und Profile verändern 16
Sichtbar in Benutzerlisten 6, 7
Stammdaten bearbeiten 15
Stempel, Berechtigungen 21
Stichwortlisten bearbeiten 12
Suchen verwalten 16
Verfallsdatum bearbeiten 12
Verschlagwortungsmasken bearbeiten 16
Verschlagwortungsmasken, Berechtigungen 22
Verschlüsselung 28
Verschlüsselungskreis 28
Versionen löschen 14
Visualisierungen verwalten 16
Vorgängerrechte 5
Vorgängerrechte, Berechtigungen setzen 26
Weitere Infos anzeigen 13
Workflow-Berechtigungserweiterung 15
Workflows 25
Workflows starten 14
Workflows verwalten 14
Zugriffsrechte 4