



Configuration and administration

User administration



Table of contents

Users and groups	3
Introduction	3
User	6
Groups	14
Other configurations	21
Introduction	21
Password rules	22
Block access	23
Organizational units	24
Rights in ELO	25
Introduction	25
User rights	26
Inheriting rights	36
Assign permissions in ELO Spaces	37
Configuration	39
Permissions in ELO	42
Introduction	42
General permissions	43
Other permissions	49
Concept for assigning rights and permissions	50
Introduction	50
Assigning user rights	51
Groups and permissions concept	59
LDAP	65
Introduction	65
LDAP interface configuration	66
LDAP import	73
Enable LDAP authentication	77

Users and groups

Introduction

Everyone who uses ELO needs a corresponding ELO account.

Groups can be used to manage permissions and basic settings in ELO. Groups are also used in workflows and for substitution rules.

You can create, configure, and manage users and groups in the user and group manager. You will find it in the ELO Administration Console under *System settings > User and group manager*.

'Users and groups' overview

ID	Name	Windows users	E-mail address	Additional information
0	Administrator			
1	ELO Service	eloservice		
2	GRP_ADMIN			
3	GRP_POST			
4	GRP_SALES			
5	GRP_SECR			
6	GRP_STANDARD			
7	OPT_GRP_ADMIN			
8	OPT_GRP_STANDARD			
9	PubSec.Registratur			
10	sol.pubsec.admin.FilingPlan			

The user and group manager offers the following actions:

- 1 Create user
- 2 Create group
- 3 Perform search
- 4 List selection: All, users, groups
- 5 Define filter
- 6 Number of existing users and groups

Information

You can sort the list of existing users and groups in ascending or descending order according to IDs, names, or e-mail addresses by selecting *ID*, *Name*, or *E-mail address* in the first line of the table.

'User' detailed view

The screenshot displays the 'User' detailed view for a user named 'Byte'. The interface includes a top navigation bar with settings, help, and share icons. Below the user name, there are three tabs: 'Basic settings' (highlighted with callout 2), 'Group membership', and 'User rights'. A left sidebar contains a 'Copy user' button (highlighted with callout 1) and a 'Delete user' button (highlighted with callout 3). The main content area is divided into two sections: 'User information' and 'Properties'. The 'User information' section contains fields for Name (Byte), Password (masked), E-mail address (brent.byte@mail.local), Windows user (Brent Byte), Administrator (Administrator), and Supervisor (Administrator). The 'Usage' section includes checkboxes for 'Lock account' (unchecked), 'Visible in user lists' (checked), and 'Interactive logon allowed' (checked). The 'Properties' section contains an 'Action' field.

The *User* detailed view offers the following actions:

1 Copy user: All configurations are applied, with the exception of the *Name*, *E-mail address*, *Password*, and *Windows user* fields.

2 Perform configuration: Via the Basic settings, Group membership, and User rights tabs

3Delete user

'Group' detailed view

The screenshot shows the 'Group' detailed view for 'GRP_SALES'. At the top, there is a dark blue header bar with icons for settings, help, and sharing. Below the header, the group name 'GRP_SALES' is displayed with a group icon. To the right of the group name are three tabs: 'Basic settings' (highlighted with a red box and labeled '2'), 'Group membership', and 'User rights'. Below the tabs is a horizontal bar with two buttons: 'Copy group' (highlighted with a red box and labeled '1') and 'Delete group' (highlighted with a red box and labeled '3'). The main content area is divided into two sections: 'Group information' and 'Properties'. The 'Group information' section contains fields for 'Name *' (GRP_SALES), 'E-mail address' (empty), 'Administrator' (Administrator), 'Supervisor' (GRP_SALES), and 'Usage' (checkboxes for 'Visible in user lists', 'Option group', 'Substitution allowed', and 'Functional role'). The 'Properties' section contains two empty text input fields labeled '1 property' and '2 property'.

The *Group* detailed view offers the following actions:

1 Copy group: All configurations are applied, with the exception of the *Name* and *E-mail address* field as well as the members.

2 Perform configuration: Via the Basic settings, Group membership, and User rights tabs

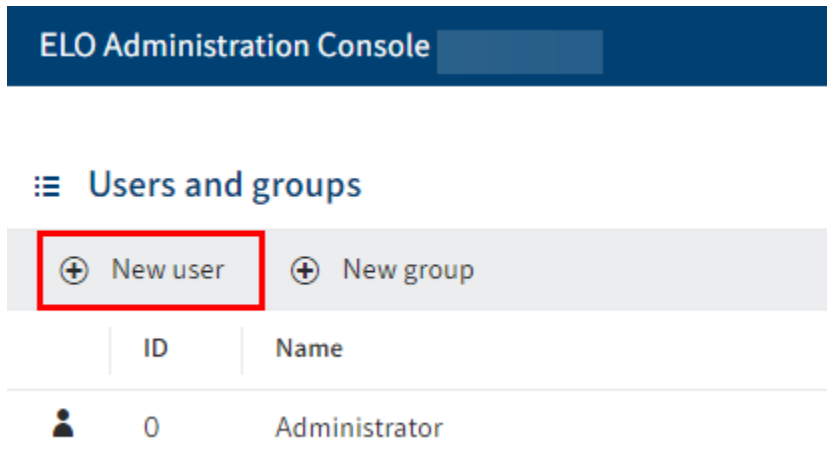
3 Delete group

User

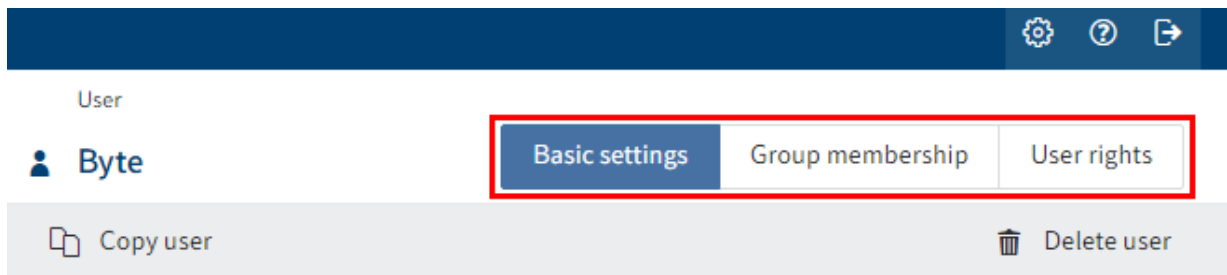
Create user

To create a user, proceed as follows:

1. Open the ELO Administration Console.
2. Open the user manager (*System settings > User and group manager*).



3. Select *New user*.



The *User* screen opens.

4. Configure the new user. Navigate to the *Basic settings*, *Group membership*, and *User rights* tabs to do so.

For more information, refer to the following section 'Configuration'.

5. Once you are finished with configuration, select *Save user* to save.

You created a new user.


Configuration

Define basic settings

In the *Basic settings* area, you define the settings for *User information*, *Properties*, and additional *Information*.

User information

▼ User information

Name *	<input type="text" value="Byte"/>
Password *	<input type="password" value="....."/>
E-mail address	<input type="text" value="byte@exten.com"/> 
Windows user	<input type="text" value="Byte"/>
Administrator	<input type="text" value="Administrator"/>
Supervisor	<input type="text" value="Administrator"/>
Usage	<input type="checkbox"/> Lock account <input checked="" type="checkbox"/> Visible in user lists <input checked="" type="checkbox"/> Interactive logon allowed

- Name: Mandatory field. This can be changed later.
- Password: Mandatory field. This can be changed later.
- E-mail address: Displayed in the user profile in the client and can be used in workflows, forms, and scripts.
- Windows user: Enter the Windows user name if required, e.g. if you are using SSO. This information can be used in workflows, forms, and scripts.
- Administrator: The user who creates the new user is automatically entered. If this user has the *Main administrator* right, the *Administrator* user is entered in the *Administrator* field. This can be changed later. Determines who may edit the master data of the user.
- Supervisor: Can be used in workflows, forms, and scripts. If this field is left blank, the content of the *Name* field is used.
- Use:
 - *Lock account*: If this option is enabled, this user will no longer be able to log on to the system. The user is still visible in the system. To hide these accounts, disable the option *Visible in user lists*.

Information

This option is not available to the Administrator.

- *Visible in user lists*: If this option is enabled, the group will show up in the corresponding selection lists in the ELO client. If this option is disabled, only administrators can see this user. Any actions already performed by this user, for example filed documents or new document versions, still remain visible to everyone in the ELO client.

Information

The members of an organizational unit only see the users within their own organizational unit.

- *Interactive logon allowed*: This option enables the user to log on to the ELO client.




Please note

This setting cannot be checked by the server. It is not considered a lock and can be bypassed.

Information

This option is not available to the Administrator.

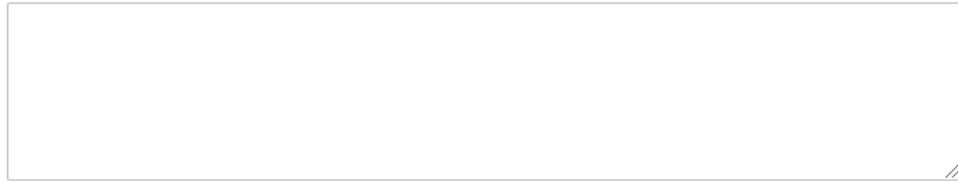
Properties**▼ Properties**

Action	<input type="text"/>	
1 property	<input type="text"/>	
2 property	<input type="text"/>	
3 property	<input type="text"/>	
4 property	<input type="text"/>	
5 property	<input type="text"/>	
Organizational unit	<div>None </div>	

- Action: Codes entered here have an effect on the password.
 - Examples:
 - EX20233105: The password expires on May 31, 2023, after which it has to be renewed.
 - PWf: The user must change their password when they log on for the first time.
 - PW: The user can change their password when they log on for the first time.
- Property 1-5: Information can be evaluated using scripts.
- Organizational unit: You will find relevant information under Configuration and administration > User administration > Additional configurations > Organizational units.

Information▼ **Information**

Description



Last recorded logon 29.09.2023 02:00

Last changed on 27.11.2023 13:38


ID 18

GUID (5CBD539D-5E00-0CAD-C899-41BE7D1A2618)



- Description: The entry can have a maximum of 250 characters.
- Last recorded logon: Is updated automatically.
- Last changed on: Is updated automatically.
- ID: Each account is automatically assigned an ID, which can be used to address the account in other functions.
- GUID: Each account is automatically assigned a GUID. The GUID can be used to address the account in other functions.

Define group membership

User




 **Byte**

Basic settings **Group membership** User rights

 Copy user  Delete user

▼ **Group membership (2)**

Copy group membership from

	
<input type="text" value="Add group"/>	
Accounting	
Everyone	

All users automatically belong to the Everyone group.


You can either inherit the group memberships from another user or group or manually add existing groups. You can add a user to one or more groups. Users are always members of the *Everyone* group.

Information



If you type a space in an input field, the entire list of available users and groups will be displayed.

Assign user rights

User

 **Byte**

Basic settings Group membership **User rights**

 Copy user  Delete user

Copy user rights from

User manager

- ☒ ☐ Main administrator
- ☒ ☐ Edit user data
- ☐ ☒ Change password
- ☐ ☐ SAP administrator
- ☐ ☐ DMS Desktop user, no workflows ⓘ
- ☐ ☐ ELO Desktop Client Plus user
- ☐ ☐ ELOxc Client user, e-mails only

Folder/document permissions

- ☐ ☒ Edit folders
- ☐ ☒ Edit documents
- ☒ ☐ Edit permissions ⓘ
- ☐ ☐ View all entries, ignore permissions
- ☒ ☐ Import permission
- ☒ ☐ Export permission

There are three options for assigning user rights:

- Inheritance

You will find more information under Configuration and administration > User administration > Rights in ELO > Inheriting rights.

- Manual assignment

You will find more information under Configuration and administration > User administration > Rights in ELO > User rights.

- Inheriting from another user or a group

Information

Ideally, all rights are inherited through groups. This makes it easier to assign and manage rights.

Delete user

Please note

When you delete a user, they are deleted permanently.

Do not delete any users that have already been used in ELO. This can lead to inconsistencies. In this case, it is better to change the basic settings of the user instead of deleting the user:

1. Enable *Lock account*
2. Disable *Allow interactive logon*
3. Disable *Visible in user lists*

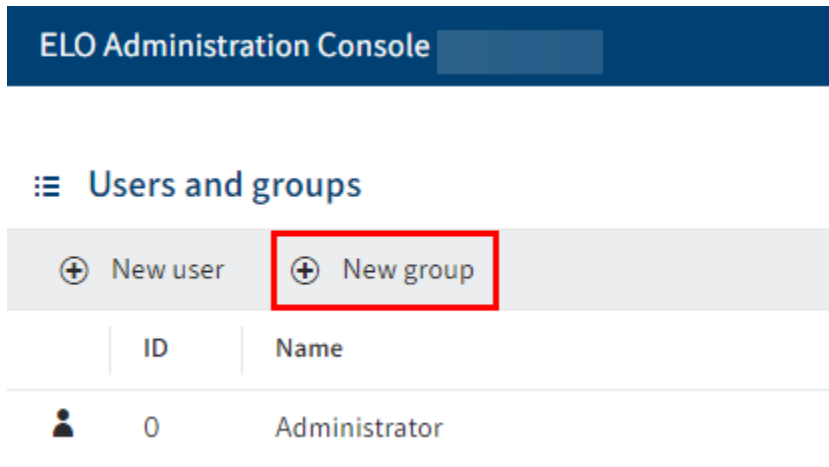
The user can no longer log on to ELO and is not visible to other users. They now only exist in the background in ELO. Their previous actions, for example feed posts or entries in the document versions, are still visible in ELO.

Groups

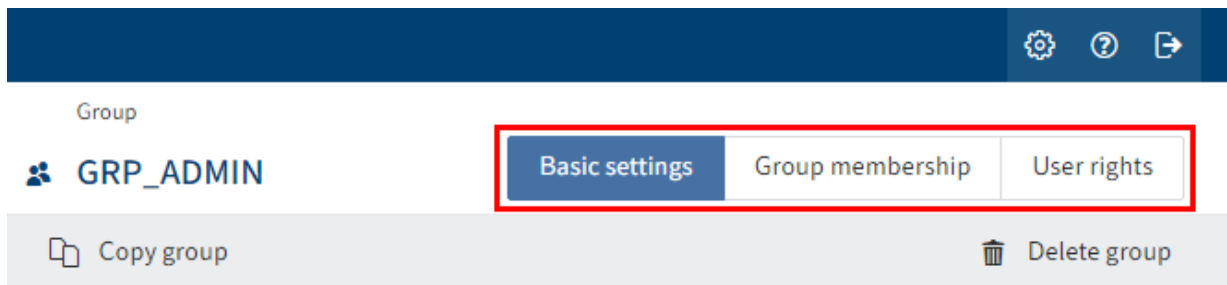
Create group

To create a group, proceed as follows:

1. Open the ELO Administration Console.
2. Open the group manager (*System settings > User and group manager*).



3. Select *New group*.



The *Group* area opens.

4. Configure the new group. Navigate to the *Basic settings*, *Group membership*, and *User rights* tabs to do so.

For more information, refer to the following section 'Configuration'.

5. Once you are finished with configuration, select *Save group* to save it.

You have created a new group.


Configuration

Define basic settings

In the *Basic settings* area, you define the *Group information*, *Properties*, and additional *Information*.

Group information

▼ Group information

Name *	<input type="text" value="Administrators"/>	
E-mail address	<input type="text"/>	
Administrator	<input type="text" value="Administrator"/>	
Supervisor	<input type="text" value="Administrator"/>	
Usage	<input checked="" type="checkbox"/> Visible in user lists <input type="checkbox"/> Option group <input checked="" type="checkbox"/> Substitution allowed <input checked="" type="checkbox"/> Functional role	

- Name: Mandatory field. This can be changed later.
- E-mail address: Displayed in the user profile in the client and can be used in workflows, forms, and scripts.
- Administrator: The name of the account used to create the new group is automatically entered. If this user has the *Main administrator* right, the *Administrator* user is entered in the *Administrator* field. This can be changed later. Determines who may edit the master data of the group.
- Supervisor: Can be used in workflows, forms, and scripts. If this field is left blank, the content of the *Name* field is used.
- Use:
 - *Visible in user lists*: If this option is enabled, the group will show up in the corresponding selection lists in the ELO client. If the option is disabled, the group still exists in ELO, but it is not shown in the corresponding selection lists in the ELO client.
 - *Option group*: Option groups are defined for the purpose of assigning specific *ProfileOpts*. Only these groups show up in dialog boxes where settings are made for other ELO accounts.

For more information on option groups, refer to Option groups.

- *Substitution allowed*: You can control how rights are distributed via the substitution module. For groups that have the substitution right, rights can be transferred to substitutes.
- *Functional role*: If this option is enabled, members of this group are asked during logon whether they want to assume the *functional role* for the current session.

This option makes sense if a user has to perform different tasks in ELO that require different permissions and rights.

Properties

▼ Properties

1 property

2 property

3 property

4 property

5 property

Organizational unit

 ▼ ⓘ

- Property 1-5: Information can be evaluated using scripts.
- Organizational unit: You will find relevant information under Configuration and administration > User administration > Additional configurations > Organizational units.

Information▼ **Information**

Description

Last changed on 25.10.2023 14:05

ID 75

GUID (468E3F45-09E2-6445-9ADC-141CB1F7E349)

- Description: The entry can have a maximum of 250 characters.
- Last changed on: Is updated automatically.
- ID: Each group is automatically assigned an ID, which can be used to address the group in other functions.
- GUID: Each group is automatically assigned a GUID. The GUID can be used to address the group in other functions.

Option groups

User-specific options are generally assigned to a user. However, group options are applied if there are no user-specific options. If these have not been defined, then the settings for the *Everyone* group are applied. If settings have not been defined for this group, there is also an ELO default value (*company default setting*).

Here you can see the level at which settings have been made. If no settings have been made at the top level, the settings for the level below that automatically apply.



These groups allow you to control who has access to specific functions.

You can define which users can execute ELO functions from the context menu, or only from the ribbon buttons, or both at once, and can even block access to parts of the software. It is also possible to control scripts and script functions as well as icons for each option group.

This is practical for ELO workstations with special areas of responsibility, in order to improve usability and to prevent incorrect usage.

Please note

An ELO user should only be a member of one option group. Memberships in multiple option groups can result in conflicting settings.

Define group membership

Group

Administrators

Basic settings Group membership User rights

Copy group Delete group

Members (2)

Add user/group

Administrator	x
Byte	x

Group membership (2)

Copy group membership from User or group

Add group

GRP_ADMIN	x
HR Department	x

All users automatically belong to the Everyone group.

1 Members: Add existing users or groups as members

2 Group membership: Inherit existing group memberships from other groups or users or manually add existing groups

Information

Groups can be incorporated into other groups. This allows you to implement complex combinations of rights settings and permissions concepts.

Information

If you type a space in an input field, the entire list of available users and groups will be displayed.

Assign user rights

Group

HR department

Basic settings | Group membership | **User rights**

Copy group | Delete group

Copy user rights from

User manager

- ☐ Main administrator
- ☒ Edit user data
- ☐ ☒ Change password
- ☐ SAP administrator
- ☐ DMS Desktop user, no workflows ⓘ
- ☐ ELO Desktop Client Plus user
- ☐ ELOxc Client user, e-mails only

Folder/document permissions

- ☐ Edit folders
- ☐ Edit documents
- ☒ Edit permissions ⓘ
- ☐ View all entries, ignore permissions
- ☐ Import permission
- ☐ Export permission

There are three options for assigning user rights:

- Inheritance

You will find more information under Configuration and administration > User administration > Rights in ELO > Inheriting rights.

- Manual assignment

You will find more information under Configuration and administration > User administration > Rights in ELO > User rights.

- Inheriting from another group or user

Information

Ideally, all rights are inherited through groups. This makes it easier to assign and manage rights.

Delete group

Please note

When you delete a group, it is deleted permanently.

Do not delete any groups that have already been used in ELO. This can lead to inconsistencies. In this case, it is better to change the basic settings of the group instead of deleting the group:

- Disable *Visible in user lists*

The group now only exists in the background in ELO. The rights assigned via the group are maintained and previous actions with this group, such as participation in workflows, are still visible in ELO.

Other configurations



Introduction

Additional configurations for the user manager:

- Set password rules
- Block access
- Organizational units

Password rules

In the *Password rules* area (*Maintenance > Password rules*), you define the password security settings.

Type	Option group	Search for
	Global	
	OPT_GRP_STANDARD	

Global Save Cancel

Days valid

Min. length

☐ At least one letter

☐ At least one special character

☐ At least one uppercase and one lowercase letter

☐ At least one number

Days valid: Define the number of days that passwords are valid.

Min. length: Define the minimum length for passwords in ELO.

Information

The more characters and special characters are used, the more secure the password is. You can define which characters must be used in the password.

Block access

Under *Block access* (*Others > Block access*), you can restrict access to ELO based on membership of a selected group.



Block access

Save Cancel

Access for group GRP_SALES ⓘ

Access for group: ELO suggests possible groups as soon as you start typing in this field. Select a group and click *Save* to confirm your selection. The respective repository can then only be accessed by members of this group.

Please note

Users with the *Main administrator* right can log on at any time. Users who are already logged on can continue to use ELO until they log off.

Information

To grant all users access to the repository, use the *Everyone* group.

Organizational units

Open the organizational units in the ELO Administration Console under *System settings > Organizational units*.

The screenshot shows the 'New organizational unit' form. On the left, there is a sidebar with a 'Name' field and a 'No data' message. The main form area has a title bar 'New organizational unit' with 'Save' and 'Cancel' buttons. Below the title bar is an information box stating: 'If users belong to an organizational unit, they see the members of that organizational unit in the user lists.' The form contains the following fields:

- Name:** A text input field containing 'New organizational unit'.
- Description:** A large text area.
- Property 1, Property 2, Property 3, Property 4:** Four text input fields.
- Members:** A section with a dropdown arrow and the label 'Members'. Below it is an 'Add members' button and a table with the header 'Members' and one row containing 'No data'.

Organizational units provide a way to classify users.

The members of an organizational unit only see the users within their own organizational unit.

This can be useful at big companies, e.g. if the branches in different countries do not work together directly. A user or a group can only belong to one organizational unit. Membership to an organizational unit can be inherited through groups.

Information

The same user should not be a member of different organizational units.

Example: Three different organizational units should not all contain the user *Admin*.

Rights in ELO

Introduction

This documentation discusses the rights in ELO and assigning them.

Rights are assigned in ELO to determine which actions may be performed within the system. Rights are assigned in the ELO Administration Console.

Rights apply across the board in ELO. There are also permissions to individual entries and elements in ELO. The actions that may actually be performed on an entry or element ultimately depend on the combination of permissions and rights.

Examples:

1. You have the user right *Delete documents*, which allows you to delete documents in ELO generally. However, you only have *Read (R)* permission to a certain document. Despite the general right, you cannot delete this document, as you do not have permission to delete this specific document.
2. You have *Read (R)* and *Delete (D)* permissions to a certain document. However, you do not have the user right *Delete documents*. Despite the permissions, you cannot delete this document, as you do not have the right and therefore are unable to delete documents in the system in general.

Refer to the following sections for more information:

- User rights
- Inheriting rights
- Assign permissions in ELO Spaces
- Configuration

Related topic

Permissions in ELO: Permissions determine who may perform which actions on a specific entry or element in ELO. You will find information on permissions in ELO under Configuration and administration > User administration > Permissions in ELO.

User rights

You can manage user rights in the Users and Groups configurations.

Information

Ideally, all rights are inherited through groups. This makes it easier to assign and manage rights.

User manager rights

User manager

- ☐ ☐ Main administrator
- ☐ ☐ Edit user data
- ☐ ☐ Change password
- ☐ ☐ SAP administrator
- ☐ ☐ DMS Desktop user, no workflows ⓘ
- ☐ ☐ ELO Desktop Client Plus user
- ☐ ☐ ELOxc Client user, e-mails only

Main administrator (FLAG_ADMIN)

Administrator rights are required to make global settings.

If you have the *Main administrator* right, you can see all users and groups, even if the option *Visible in user lists* is disabled for them. If you also have the *Edit user data* right, you can administer all users and groups.

The *Main administrator* right allows you to change the permissions of the top repository level: To change the permissions and options of the top level, you need to open the *Set permissions* dialog box, which you can only do if you have the *Main administrator* right. To modify the permissions, however, you also need the *Edit permissions* right, meaning you need both rights in this case.

You can perform the following actions in ELO with the *Main administrator* right:

- Delete entries permanently, even if you do not have the rights *Delete folders*, *Delete documents*, *Delete non-modifiable documents*, and *Delete versions*
- Remove a lock on any entry made by any user
- Assign substitutes for all users
-

Manage views and view profiles for all users

- Delete metadata forms
- Log on in administration mode or when repositories are locked

You will find more information under Rights in ELO > Configuration > Necessary rights for the ELO Administration Console.

Edit user data (FLAG_SUBADMIN)

You can perform the following actions in ELO with the *Edit user data* right:

- Create users and groups. Groups and other users can only be given the same (or fewer) rights.
- Administer users and groups if you are entered in the *Administrator* field for the respective user or group, or you also have the *Main administrator* right. If a group is entered in the *Administrator* field, all members of this group can administer the corresponding users or the group if the administrating group also has the *Main administrator* right.
- You can only assign groups you are set as an *administrator* for or if you also have the *Main administrator* right.
- You can only edit your own user data if you are set as an *administrator* in the user manager or if you also have the *Main administrator* right.
- In the ELO Java Client, this right enables you to set *substitution rules for other users* that you are an administrator of, even if they are not *Visible in user lists*.

Information

Only users with *Main administrator* and *Edit user data* rights can see and administer all users and groups.

Change password (FLAG_CHANGEPW)

With this right, you can change your own password for logging on to the system.

SAP administrator (FLAG_SAPADMIN)

This right is required for enabling the link between the ELO Suite and SAP using ELO Suite for SAP ArchiveLink® and allows you to manage the metadata form associated with the interface to SAP. The metadata form for SAP-administered documents can be viewed by every user but can only be edited by users with this right.

DMS Desktop user, no workflows (FLAG2/SDMSDESKTOPUSER)

If this option is enabled, the user does not have access to workflow functions. This applies to the following functions:

- Ad hoc workflow
- Extend workflow deadline
-

Workflow overview

- Hand off workflow
- Accept workflow
- Show workflow
- Delegate workflow
- Start workflow
- Forward workflow
- Return workflow
- Postpone workflow
- Workflows for this entry
- Edit workflow templates
- Cancel postponement

Please note

This right is a restriction that supersedes all other rights associated with workflows. A user with this right is unable to use the functions and roles associated with workflows, irrespective of whether the individual rights are set or inherited by a user or not. The user is also unable to edit any workflow tasks that are assigned to them. This is because the ELO DMS Desktop does not include workflow functions.

ELO Desktop Client Plus user (FLAG2DESKTOPCLIENT_PLUS)

This right runs the ELO Desktop Client in advanced mode, with some task functionalities and the full client view mode.

Please note

This right limits what functions are available to the user.

ELOxc Client user, e-mails only (FLAG2LIMITEDCLIENT)

This right opens the ELO Client for Microsoft Outlook in ELOxc for Microsoft EWS mode, and is restricted to the file formats (EML, MSG, and VCF) that can be opened by Microsoft Outlook. No other formats are available to the user.

Please note

This right limits what functions are available to the user.

Folder/document permissions

Folder/document permissions
☐ ☐ Edit folders
☐ ☐ Edit documents
☐ ☐ Edit permissions ⓘ
☐ ☐ View all entries, ignore permissions
☐ ☐ Import permission
☐ ☐ Export permission

Edit folders (FLAG_EDITSTRUCTURE)

This right enables users to edit documents and create child folders within folders.

Edit documents (FLAG_EDITDOCS)

This right enables users to edit documents. This includes the functions:

- Load new versions
- Check files in and out
- Insert files
- Documents from templates
- Add and delete attachments
- Add to full text database
- Delete from full text database
- Create signature

Users are only able to edit document metadata if they have the corresponding right. Otherwise, the user can only open the metadata in read-only mode.

Edit permissions (FLAG_EDITACL)

This right allows users to change the permissions to entries (documents and folders) in ELO.

Information

In order to be able to modify the permissions to entries, you need the right *Edit folders* or *Edit documents*. You also need the *Set permissions* (P) permission for each individual entry.

Users have the option to configure the rights when filing entries in the client, since they have full rights to the file. The user right applies to subsequent editing of permissions.

It does not apply to the permission settings in the ELO Administration Console or the ELO Java Client configuration. If users can edit the stamp, metadata forms, etc., they can also edit their permissions without this user right being checked.

View all entries, ignore permissions (FLAG_IGNOREACL)

This right means that the user can view all documents and folders, even if the user does not have access to them. It revokes all existing object permissions. Users with this right have full access permissions to all ELO entries.

The only way to protect documents from users who possess this user right is to encrypt them.

Import permission (FLAG_IMPORT)

This right allows users to import a data set into the repository. All data available in the data set will be imported — object permissions are ignored. The user performing the action therefore also imports data that they do not have permissions to. This data will not be visible to the user.

Export permission (FLAG_EXPORT)

This right enables the user to create a data set for export. The user can only export entries and documents that they have the corresponding permissions to.

Folder/document options

Folder/document options ⓘ

- ☐ ☐ Change metadata form after filing
- ☐ ☐ Edit keyword lists
- ☐ ☐ Edit retention period
- ☐ ☐ Change document status
- ☐ ☐ Change document paths ⓘ
- ☐ ☐ Author for approval documents
- ☐ ☐ Show "Additional information" tab

Information

The rights in this group (except *Change document paths*) only apply if the user also has the *Edit folders* or *Edit documents* rights.

Change metadata form after filing (FLAG_CHANGEMASK)

This right allows the user to assign a different metadata form to a document already filed to the repository. Please note that doing this may cause metadata to be lost. This is only possible if the user also has the right *Edit folders* or *Edit documents*, depending on the entry.

Edit keyword lists (FLAG_EDITSWL)

This right enables the user to add, change, and delete entries to the keyword list. If the user does not have this right, they will not be able to edit the keyword lists in the ELO Administration Console, even if they have the right *Edit metadata forms and fields*.

This is only possible if the user also has the right *Edit folders* or *Edit documents*, depending on the entry.

Edit retention period (FLAG_EDITDUEDATE)

This right enables the user to set and extend the retention period for documents. If the user does not have this right, the corresponding field in the *Metadata* dialog box is disabled.

This is only possible if the user also has the right *Edit folders* or *Edit documents*, depending on the entry.

Change document status (FLAG_CHANGEREV)

This right enables the user to set the document status on the *Options* tab in the *Metadata* dialog box:

- Version control disabled
- Version control enabled
- Non-modifiable

This is only possible if the user also has the right *Edit documents*.

Change document paths (FLAG_CHANGEPATH)

This right gives users access to the selection list for the document path in the document options and enables them to change the path for a specific document. This is only possible when entering metadata in the Inray. If a document has already been filed, this selection list is permanently deactivated. If this is the case, you can only move documents to a different path using the *Move document files* function if you have *main administrator* rights.

This right does not allow users to create new document paths or change their definition. Editing, creating, and assigning document paths requires *main administrator* rights.

Author for approval documents (FLAG_AUTHOR)

This right allows the user to select or deselect the *Approval document* check box and edit approval documents. The author is able to continue editing previous versions of a document. When users check out documents, they are able to select all document versions. When documents are checked in, the old working version is retained. The working version (= approved version) can only be changed by authors for approval documents.

This is only possible if the user also has the right *Edit documents*.

Show "Additional information" tab (FLAG2SHOWEXTRA_INFO)

This right determines whether a user is able to see the *Additional information* tab in the *Metadata* dialog box.

This is only possible if the user also has the right *Edit folders* or *Edit documents*, depending on the entry.

Deletion rights

Delete

☐ ☐ Delete folders

☐ ☐ Delete documents

☐ ☐ Delete non-modifiable documents ⓘ

☐ ☐ Delete versions ⓘ

Delete folders (FLAG_DELSTRUC)

This right determines whether a user is able to delete folders.

Delete documents (FLAG_DELDOC)

This right determines whether a user is able to delete documents.

Delete non-modifiable documents (FLAG_DELREADONLY)

This right enables the user to delete documents that have been filed with the status *Non-modifiable* or have been awarded this status at some point.

This is only possible if the user has the right *Delete documents*.

Delete versions (FLAG_DELVERSION)

This right allows the user to delete individual versions from a document's version history.

In the ELO Java Client, the user can see the deleted versions of a document in the *Document versions* dialog box if the *Show deleted entries* function is enabled.

Workflow rights

Workflows

- ☐ ☐ Manage workflows
- ☐ ☐ Start workflows
- ☐ ☐ Extend workflow rights
- ☐ ☐ View workflows for all users

Manage workflows (FLAG_EDITWF)

This right enables users to:

- Create workflow templates and forms
- Cancel active workflows before they are completed
- Delete completed and canceled workflows permanently
- Edit successor nodes

Start workflows (FLAG_STARTWF)

This right allows a user to start workflows. This applies to the following functions:

- Ad hoc workflow
- Workflow overview
- Start workflow
- Workflows for this entry

The user also requires this right to start workflows when filing entries with a metadata form that is linked to a workflow. If the user does not have this right, the user may file documents with this metadata form but cannot start a workflow.

Without this right, the user will not be able to use the *Workflow overview* and the *Workflows for this entry* functions on the ribbon of the ELO client. The user is able to open an overview of all workflows in which the user is involved, either directly or indirectly (through group membership).

Extend workflow rights (FLAG2EXTENDWORKFLOW_RIGHTS)

Users with this right have temporary read access to the entry assigned to the active workflow node. The document can only be viewed in the Tasks work area, and only as long as the document is assigned to the user or a group that the user is a member of. In addition, an entry in the database table *ProfileOpts* gives the user the option to control whether temporary or permanent permissions are to be assigned.

This right cannot replace other user rights, even those that are temporary. The right applies to documents and folders, but not to metadata forms.

View workflows for all users (FLAG2WFCONTROLLER)

This right allows the users to see all workflows that are active and not just those workflows that the user is participating in.

System settings

System settings

- ☐ ☐ Edit master data
- ☐ ☐ Edit scan profiles
- ☐ ☐ Use debugger
- ☐ ☐ Edit metadata forms and fields
- ☐ ☐ Assign replication sets

Edit master data (FLAG_EDITCONFIG)

This right gives the user access to *entry types* (icons and names of folders and documents), *font colors*, and *stamps*.

Edit scan profiles (FLAG_EDITSCAN)

When this option is enabled, the user can change the settings for the scanner parameters and *scan profiles*. If the user also has *Main administrator* rights, they are also able to manage and edit global *scan profiles* and the scan parameters for other users.

Use debugger (FLAG_EDITSCRIPT)

If you have this right, you can open the JavaScript debugger in the ELO Java Client with the keyboard command Ctrl+Alt+D.

Information

Scripts are managed like documents in ELO. To edit scripts, you need the corresponding permissions.

Edit metadata forms and fields (FLAG_EDITMASK)

This right enables the user to create new metadata forms and modify existing ones.

If you need to edit the keyword lists in the metadata forms, then you also need the right *Edit keyword lists*.

Assign replication sets (FLAG_EDITREPL)

You require this right for assigning data to replication sets in the repository. Replication sets are needed by ELO Replication to determine data quantities.

Inheriting rights

There are two check boxes in front of the user rights. The check boxes on the left refer to the individual rights of the user or group. The check boxes on the right refer to the rights taken on by belonging to a group. If you move the mouse over one of the check boxes on the right, a tooltip appears telling you where the right was inherited from.

The screenshot shows a configuration window titled "Folder/document options" with an information icon. It contains a list of rights, each with two checkboxes. A tooltip is displayed over the right-hand checkbox for "Change document status", indicating the right is inherited from "ELO_StandardUsers".

Folder/document options ⓘ	
<input type="checkbox"/>	<input type="checkbox"/> Change metadata form after filing
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/> Change document status
<input type="checkbox"/>	<input type="checkbox"/> Change document paths ⓘ
<input type="checkbox"/>	<input type="checkbox"/> Author for approval documents
<input type="checkbox"/>	<input type="checkbox"/> Show "Additional information" tab

Information

Ideally, all rights are inherited through groups. This makes it easier to assign and manage rights.

Assign permissions in ELO Spaces

The rights for the teamspaces and workspaces in ELO are determined based on the assigned roles.

Teamspace

You can assign the following special teamspace rights to a role:

Special teamspace rights ⓘ

- ☐ Edit roles
- ☐ Edit teamspace
- ☐ Delete teamspace

- Edit roles: Edit and create roles in the teamspace, regardless of whether the teamspace itself may be edited.
- Edit teamspace: Make changes to a teamspace. They can also change the roles assigned to members in the teamspace and add new members.
- Delete teamspace: Can only be enabled if *Edit teamspace* is also enabled.

You will find more information on the roles in teamspaces under [ELO packages > ELO Teamspaces > Define roles](#).

Workspace

You can assign the following special workspace rights to a role:

Special workspace rights ⓘ

- ☐ Edit workspace
 - ☐ Edit roles
 - ☐ Delete workspace

- Edit workspace: Make changes to a workspace. They can also change the roles assigned to members in the workspace and add new members.
- Edit roles: Edit and create roles in the workspace. Can only be enabled if *Edit workspace* is also enabled.
- Delete workspace: Can only be enabled if *Edit workspace* is also enabled.

You will find more information on the roles in workspaces under [ELO packages > ELO Workspaces > Define roles](#).

Configuration

Necessary rights for the ELO Administration Console

System settings

Administration areas	Rights
User administration	<p>Edit user data, main administrator</p> <p>A user with the right <i>Main administrator</i> can administer ALL users instead of just those who that user is set as administrator of.</p>
Group manager	<p>Edit user data, main administrator</p> <p>A user with the right <i>Main administrator</i> can administer ALL groups instead of just those who that user is set as administrator of.</p>
Organizational units	<p>Main administrator</p> <p>As an administrator of a user (with the right <i>Edit user data</i>), this user can be assigned to an existing organizational unit. The Main administrator has access to the <i>Organizational units</i> section.</p>
Metadata forms	<p>Edit metadata forms and fields</p> <p>The <i>Edit keyword lists right</i> is also required to be able to edit the contained keyword lists, as well as the <i>Main administrator</i> right to delete metadata forms or save their data as a table later on.</p>
Field templates	Edit metadata forms
Keyword lists	Edit keyword lists
Entry types	Edit master data
Document paths	Main administrator
Default document paths	Main administrator
Encryption keys	Main administrator
ELO online help URL	Main administrator
Stamps	Edit master data
ELO Forms Services URL	Main administrator
ELO Analytics URL	
Repository properties	Main administrator
Font colors	Edit master data

Maintenance

Administration areas Rights

Administration mode	Main administrator
Report options	Main administrator
Delete report entries	Main administrator
Delete and remove	Main administrator
Backup tasks	Main administrator
Password rules	Main administrator
Move document files	Main administrator

Server modules

Administration areas Rights

ELO Automation Services	Main administrator
Backup profiles	Main administrator
Full text service	Main administrator
Create password	Main administrator
ELO Transport	Main administrator
Configuration files	Main administrator
Form designer	Manage workflows
ELOxc	<i>Not checked in the ELO Administration Console. The check is performed in ELOxc.</i>

System information

Administration areas Rights

Administration folder	Main administrator
Server information	Main administrator
Users in system	Main administrator
Statistics	Main administrator
License overview	Main administrator
License report	Main administrator
Log files	Main administrator
Monitoring	Main administrator
Test checksums	Main administrator

Others

Administration areas Rights

LDAP Import	Main administrator
Block access	Main administrator

Document encryption

ELO systems provide a method to encrypt documents. These documents are encrypted at the operating system level and can only be opened with a password, ensuring that documents are safeguarded against unauthorized access, even when performing data backups.

In addition to the ACL authorization settings in ELO, you can encrypt documents that contain confidential or sensitive information. This also protects documents from being viewed by administrators at the operating system level.

Starting with ELO version 12, documents are encrypted with AES-256 (Advanced Encryption Standard), a symmetric encryption method that uses block encryption. There are now more than 16 encryption keys. Encryption and decryption take place on the server side.

Documents that have already been encrypted remain in the old encryption mode. Both encryption methods are listed in the database and run simultaneously in a compatibility mode.

It is only possible to encrypt a document with ELO functions when it is filed to the ELO repository. Documents in the Inray are always stored in unencrypted format until they are moved to the repository. ELO functions are not designed to encrypt documents already in ELO, because as soon as documents are filed to the repository, the documents may be distributed in unencrypted form to a backup path, revision-controlled media, and various backup systems.

Encryption can only be configured by users with the *Main administrator* right. A user who knows the encryption key and the corresponding password is able to implement encryption. An encryption key is therefore not necessarily bound to a single person – it can also be used for groups.

Documents encrypted with AES-256 can be added to the full text database. To do this, you need to create a system user that can access the encrypted documents. You can, but do not have to, add encrypted documents to the full text database.

The encryption keys are not to be confused with the keys concept that was discontinued starting with version 10.

You will find more information on encryption under Configuration and administration > System administration > Folders and documents > Encryption keys.

Permissions in ELO

Introduction

In ELO, permissions are assigned for every entry and every element. They determine who may perform which actions on a specific entry or element in ELO. These permissions are assigned on the *Permissions* tab of the metadata.

This includes the following permissions:

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

Permissions apply to the individual entries and elements in ELO. Rights apply across the board in ELO. The actions that may actually be performed on an entry or element ultimately depend on the combination of permissions and rights.

Examples:

1. You have the user right *Delete documents*, which allows you to delete documents in ELO generally. However, you only have *Read (R)* permission to a certain document. Despite the general right, you cannot delete this document, as you do not have permission to delete this specific document.
2. You have *Read (R)* and *Delete (D)* permissions to a certain document. However, you do not have the user right *Delete documents*. Despite the permissions, you cannot delete this document, as you do not have the right and therefore are unable to delete documents in the system in general.

Refer to the following sections for more information on permissions:

- General permissions
- Other permissions

Related topic

Rights in ELO: User rights are assigned to determine which actions may be performed within ELO. You will find information on rights in ELO under Configuration and administration > User administration > Rights in ELO.

General permissions

In ELO, permissions for entries and elements may be different depending on the context.

The following sections address the permissions for the individual entries and elements.

- Documents
- Folders
- Margin notes
- Annotations (e.g. stamps, sticky notes)
- Metadata forms
- Workflow templates
- Workflows
- ELO Spaces

Documents

Permission	Description
View (R)	View documents and metadata, add annotations and margin notes
Change metadata (W)	
Delete (D)	Mark documents as deleted. Only administrators can delete documents permanently. You will find more information under Configuration and administration > System administration > Folders and documents > Delete and remove .
Edit (E)	Edit documents, e.g. check in, check out, load new version, change working version
<Edit list> (L)	Does not apply to documents
Set permissions (P)	Change permissions (set, edit, delete)

Folders

Permission	Description
View (R)	View folders and metadata, add margin notes
Change metadata (W)	
Delete (D)	Mark folder as deleted, if child entries can be deleted or the folder is empty. Only administrators can delete folders permanently. You will find more information under Configuration and administration > System administration > Folders and documents > Delete and remove .
<Edit> (E)	Does not apply to folders, but is important for inheriting permissions to the documents within folders

Permission	Description
Edit list (L)	Change folder contents, e.g. create, move, copy, or remove documents in the folder, insert or delete reference
Set permissions (P)	Change permissions (set, edit, delete)

Margin notes

There are three different types of margin notes.

General margin note

Everyone with *View* permission to the entry can create and view these margin notes. Users who only have *View* permission to the entry can only edit and delete general margin notes they've created themselves. Users who also have the permission *Change metadata* for the entry can edit and delete all margin notes.

Personal margin note

Everyone with *View* permission to the entry can create, edit, and delete these margin notes for themselves. No other users can see these margin notes.

Information

Main administrators are not able to view the personal margin notes of other users either.

Permanent margin note

Everyone with *View* permission to the entry can create and view these margin notes. It is not possible to edit or delete permanent margin notes once they have been created.

Please note

Main administrators are not able to edit or delete permanent margin notes either.

Annotations

There are annotations with and without text.

Annotations with text include sticky notes, text notes, and stamps. Annotations without text include freehand marker, rectangle marker, horizontal marker and strikethrough, the redaction tool, and image stamps.

Information

As the properties of stamps are a little different from those of the other annotations, they are discussed separately in the following.

The table below applies to the annotations listed above (except stamps):

Permission	Description
View (R)	Create annotations, edit and delete annotations created yourself
Change (W)	Annotations with text: Edit and format text, remember position, change size; Annotations without text: Modify properties (color, line width)
Delete (D)	
Move (E)	Change the position of annotations on a document
<Edit list> (L)	Does not apply to annotations
Set permissions (P)	Change permissions

Information

The only difference between annotations with and without text in terms of permissions is the *W (Write)* permission.

Stamps

In this section, we will look at stamps as a tool and their function as an applied stamp.

'Stamps' tool

Stamps are defined for a specific user, option group, or globally using *ProfileOpts*. Stamps can be created and managed in the ELO Administration Console and the ELO Java Client. In the ELO Java Client, however, you can only configure your own stamps. The defined stamps appear in the corresponding user's stamp list. To use the *Stamps* tool, the user must have been assigned at least one stamp by the administrator. Otherwise, the user is also unable to create their own stamps in the ELO Java Client.

If a user creates a stamp in the ELO Java Client, the stamp only appears in that user's stamp list and can only be used by them. Stamps that users have created themselves are available in the ELO Java Client using the *Stamps* tool and can be managed by administrators in the ELO Administration Console. To configure user- or group-specific stamps in the ELO Administration Console, the administrator must select the relevant user or group via the *Select user* button. The *Everyone* group is selected by default.

Applied stamp

Permission	Description
View (R)	View applied stamps on a document, remember position

Permission	Description
Change (W)	Change size
Delete (D)	
Move (E)	Change position
<Edit list> (L)	Does not apply to applied stamps
Set permissions (P)	Change permissions

Information

For applied stamps, the same permissions configured when applying the stamp to the document apply. Changes to permissions later on only apply to new stamps applied after the change, and not to stamps that have already been applied.

Metadata forms and fields

Metadata forms


You can only set the permissions for metadata forms in the ELO Administration Console.

Permission	Description
View metadata (R)	View metadata forms in the <i>Metadata</i> dialog box, view metadata in read-only mode
Change metadata (W)	File entries and enter metadata (also when filing initial version). If you do not have the <i>W</i> permissions for the metadata form, you cannot change the metadata of the entries. Even if you have the <i>W</i> permissions for the entry, the dialog box opens in read-only mode. To change the metadata of an entry filed with the form, you need the <i>W</i> permissions to the entry as well.
Delete form (D)	This permission is not checked. The <i>Main administrator</i> right is required to be able to delete metadata forms in the ELO Administration Console.
Edit form (E)	This permission is not checked.

Fields

In the *Display mode* field settings, you need to define whether you want to be able to enter data manually (*Normal access*), whether you want the index fields to be read-only (*Read-only*), or whether you want them to be hidden from view (*Hidden*).

This is a parent property. You can set more detailed permissions for *normal access* at the permissions level.

Field group	GRP1 
Name	Field
Translation variable	Translation variable
Display mode	<input checked="" type="radio"/> Normal access <input type="radio"/> Read-only <input type="radio"/> Hidden

Permission	Description
View (R)	View the field, reciprocal action with display mode settings (Normal access/Read-only/Hidden)
Write (W)	Complete the field, reciprocal action with display mode settings (Normal access/Read-only/Hidden)
<Delete> (D)	Does not apply to fields
<Edit> (E)	Does not apply to fields
<Lists> (L)	Does not apply to fields
<Permissions> (P)	Does not apply to fields

Workflow templates

Permission	Description
View (R)	View template, start workflow with template
Change (W)	Edit template, create new version of the template
Delete permanently (D)	
<Edit> (E)	Does not apply to workflow templates
<Edit list> (L)	Does not apply to workflow templates
Set permissions (P)	Change permissions

Workflows

You can define permissions for workflows in the respective workflow template by selecting the start node, going to the *General* area of the workflow settings, and selecting the *Permissions* button.

Permission	Description
View (R)	View workflow (as a process)
Change (W)	Change workflow after start
Delete permanently (D)	

Permission	Description
End (E)	The workflow is not deleted and can be seen in the ELO Java Client in the <i>Workflow overview</i> dialog box > status <i>Completed</i> .
<Edit list> (L)	<i>Does not affect workflows</i>
Set permissions (P)	Change permissions

The permissions for workflows only take effect if the user has the corresponding user rights for workflows. You will find more information on the user rights for workflows under Configuration and administration > User administration > Rights in ELO > User rights > Workflow rights.

ELO Spaces

The permissions for the contents of teamspaces and workspaces in ELO are determined based on the assigned roles.

You can assign the following default permissions for contents in teamspaces and workspaces to a role:

Permission	Description
View (R)	View entry
Change metadata (W)	Edit entry metadata
Delete (D)	Delete entry
Edit (E) (only documents)	Edit selected entry, i.e. change working version and load new version
Edit list (L) (only folders)	Change contents of the folder, e.g. create documents in this folder, move or remove documents from the folder
Set permissions (P)	Change permissions for the selected folder

The current permissions only take effect if the user has the corresponding user rights.

You can also set authorization options for entries that were created in a teamspace or workspace. For more information, refer to the [ELO Java Client](#) documentation.

Other permissions

The terms *parent rights* and *owner rights* exist for historical reasons. These are actually permissions.

Parent rights

The parent rights are the permissions that are inherited from an element. Child entries in a folder can either be folders or documents. Child entries in a document can either be attachments or notes.

Example: Only the *HR* group has permission to a document. The *Everyone* group has permission to the notes in the document. Because only the *HR* group has access to the document, however, only those with read permission to the document can view the notes in the document, and not *Everyone*.

If a user or group has permissions to a document but does not have permissions to the document filing path, the document will show up in the results list following a search query or if a link is created.

Owner permissions

The owner rights are placeholders for the user that

- created a folder
- filed a document
- placed a stamp or any other annotation on a document
- started a workflow

Everyone

Ideally, there should be very few entries in the ELO repository that *Everyone* has full access to.

You can check whether your repository contains such an object by having your administrator set up a dynamic folder in which all objects are displayed that permit full access to the *Everyone* group. To do so, create a folder with the following line on the Extra text tab:

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

Please note

The *Everyone* group needs read permissions to personal folders so that services can access them. If read permission for *Everyone* is removed, other users can no longer see the profile page of this user, for example.

Concept for assigning rights and permissions

Introduction

The following concept for assigning rights and permissions is merely a recommendation.

The ability to assign rights to users and groups is a standard feature of ELO. In addition to this standard feature, users can also assign permissions to individual entries and elements. The objective is to assign users as many permissions as necessary but as few as possible to give them access to entries and data.

You can assign rights and permissions at the user level but in most cases, this is not very effective. It makes more sense to organize users with the same rights into groups and to assign rights and permissions based on these groups.

This documentation presents a logical method for structuring groups for assigning rights and permissions. The intention is to keep the structure as simple as possible so that it can be implemented in ELO without any problems.

The rights and permissions in the ELO repository should correspond to the tasks of the users in the company. The following should be taken into consideration:

- What tasks do the employees have within the company?
- In what departments do the employees work?
- What information and documents do the employees need to complete their tasks within the company?

Assigning user rights

In response to the first question of what tasks the employee has in the company, we can assign user rights. Depending on what the data and documents in the ELO repository will be used for, you can assign user rights via different groups. In our example of a rights concept, we distinguish between five different groups of user rights.

ELO view users

The members of this group may only view folders and documents, apply annotations and notes, or write feed posts. They cannot make changes to the metadata, edit the document in any way, or delete it. These users can perform searches in the repository but do not enter content or file items themselves.

<p>User manager</p> <p><input type="checkbox"/> <input type="checkbox"/> Main administrator</p> <p><input type="checkbox"/> <input type="checkbox"/> Edit user data</p> <p><input checked="" type="checkbox"/> <input type="checkbox"/> Change password</p> <p><input type="checkbox"/> <input type="checkbox"/> SAP administrator</p> <p><input type="checkbox"/> <input type="checkbox"/> DMS Desktop user, no workflows ⓘ</p> <p><input type="checkbox"/> <input type="checkbox"/> ELO Desktop Client Plus user</p> <p><input type="checkbox"/> <input type="checkbox"/> ELOxc Client user, e-mails only</p>	<p>Folder/document permissions</p> <p><input type="checkbox"/> <input type="checkbox"/> Edit folders</p> <p><input type="checkbox"/> <input type="checkbox"/> Edit documents</p> <p><input type="checkbox"/> <input type="checkbox"/> Edit permissions ⓘ</p> <p><input type="checkbox"/> <input type="checkbox"/> View all entries, ignore permissions</p> <p><input type="checkbox"/> <input type="checkbox"/> Import permission</p> <p><input type="checkbox"/> <input type="checkbox"/> Export permission</p>
<p>Folder/document options ⓘ</p> <p><input type="checkbox"/> <input type="checkbox"/> Change metadata form after filing</p> <p><input type="checkbox"/> <input type="checkbox"/> Edit keyword lists</p> <p><input type="checkbox"/> <input type="checkbox"/> Edit retention period</p> <p><input type="checkbox"/> <input type="checkbox"/> Change document status</p> <p><input type="checkbox"/> <input type="checkbox"/> Change document paths ⓘ</p> <p><input type="checkbox"/> <input type="checkbox"/> Author for approval documents</p> <p><input type="checkbox"/> <input type="checkbox"/> Show "Additional information" tab</p>	<p>Delete</p> <p><input type="checkbox"/> <input type="checkbox"/> Delete folders</p> <p><input type="checkbox"/> <input type="checkbox"/> Delete documents</p> <p><input type="checkbox"/> <input type="checkbox"/> Delete non-modifiable documents ⓘ</p> <p><input type="checkbox"/> <input type="checkbox"/> Delete versions ⓘ</p>
<p>Workflows</p> <p><input type="checkbox"/> <input type="checkbox"/> Manage workflows</p> <p><input type="checkbox"/> <input type="checkbox"/> Start workflows</p> <p><input type="checkbox"/> <input type="checkbox"/> Extend workflow rights</p> <p><input type="checkbox"/> <input type="checkbox"/> View workflows for all users</p>	<p>System settings</p> <p><input type="checkbox"/> <input type="checkbox"/> Edit master data</p> <p><input type="checkbox"/> <input type="checkbox"/> Edit scan profiles</p> <p><input type="checkbox"/> <input type="checkbox"/> Use debugger</p> <p><input type="checkbox"/> <input type="checkbox"/> Edit metadata forms and fields</p> <p><input type="checkbox"/> <input type="checkbox"/> Assign replication sets</p>

The role group ELO_ViewUsers (minimal rights) can have the following right:

- Change password

ELO standard users

The members of this group have extended rights permitting them to edit documents and metadata. Depending on their rights, they can change or delete documents and folders, change, print, and export metadata, and start and edit workflows.

Typical tasks for these users are to file new documents to the ELO repository and/or to edit them.

User manager <ul style="list-style-type: none"> <input type="checkbox"/> Main administrator <input type="checkbox"/> Edit user data <input type="checkbox"/> Change password <input type="checkbox"/> SAP administrator <input type="checkbox"/> DMS Desktop user, no workflows ⓘ <input checked="" type="checkbox"/> ELO Desktop Client Plus user <input type="checkbox"/> ELOxc Client user, e-mails only 	Folder/document permissions <ul style="list-style-type: none"> <input type="checkbox"/> Edit folders <input checked="" type="checkbox"/> Edit documents <input type="checkbox"/> Edit permissions ⓘ <input type="checkbox"/> View all entries, ignore permissions <input type="checkbox"/> Import permission <input type="checkbox"/> Export permission
Folder/document options ⓘ <ul style="list-style-type: none"> <input type="checkbox"/> Change metadata form after filing <input type="checkbox"/> Edit keyword lists <input type="checkbox"/> Edit retention period <input type="checkbox"/> Change document status <input type="checkbox"/> Change document paths ⓘ <input type="checkbox"/> Author for approval documents <input type="checkbox"/> Show "Additional information" tab 	Delete <ul style="list-style-type: none"> <input type="checkbox"/> Delete folders <input checked="" type="checkbox"/> Delete documents <input type="checkbox"/> Delete non-modifiable documents ⓘ <input type="checkbox"/> Delete versions ⓘ
Workflows <ul style="list-style-type: none"> <input type="checkbox"/> Manage workflows <input checked="" type="checkbox"/> Start workflows <input checked="" type="checkbox"/> Extend workflow rights <input type="checkbox"/> View workflows for all users 	System settings <ul style="list-style-type: none"> <input type="checkbox"/> Edit master data <input type="checkbox"/> Edit scan profiles <input type="checkbox"/> Use debugger <input type="checkbox"/> Edit metadata forms and fields <input type="checkbox"/> Assign replication sets

The role group ELO_StandardUsers (basic rights for editing documents) can have the following rights:

- ELO Desktop Client Plus user
- Edit documents
- Delete documents
- Start workflows
- Extend workflow rights

ELO power users

The members of this group are authorized to do more technical and administrative tasks in ELO. Typically, they edit the folder structure in ELO and its permissions concept. They implement the repository structure with static or dynamic folders, or with default indexes that can be used by other users.

They can edit documents as well as document options or change the expiration date and document status. They can delete non-modifiable documents and versions. They can check the status of workflows they are not involved in.

User manager

- ☐ ☐ Main administrator
- ☐ ☐ Edit user data
- ☐ ☐ Change password
- ☐ ☐ SAP administrator
- ☐ ☐ DMS Desktop user, no workflows ⓘ
- ☐ ☐ ELO Desktop Client Plus user
- ☐ ☐ ELOxc Client user, e-mails only

Folder/document permissions

- ☒ ☐ Edit folders
- ☐ ☐ Edit documents
- ☒ ☐ Edit permissions ⓘ
- ☐ ☐ View all entries, ignore permissions
- ☐ ☐ Import permission
- ☐ ☐ Export permission

Folder/document options ⓘ

- ☐ ☐ Change metadata form after filing
- ☒ ☐ Edit keyword lists
- ☒ ☐ Edit retention period
- ☒ ☐ Change document status
- ☐ ☐ Change document paths ⓘ
- ☒ ☐ Author for approval documents
- ☐ ☐ Show "Additional information" tab

Delete

- ☒ ☐ Delete folders
- ☐ ☐ Delete documents
- ☒ ☐ Delete non-modifiable documents ⓘ
- ☒ ☐ Delete versions ⓘ

Workflows

- ☐ ☐ Manage workflows
- ☐ ☐ Start workflows
- ☐ ☐ Extend workflow rights
- ☒ ☐ View workflows for all users

System settings

- ☐ ☐ Edit master data
- ☐ ☐ Edit scan profiles
- ☐ ☐ Use debugger
- ☐ ☐ Edit metadata forms and fields
- ☐ ☐ Assign replication sets

The role group ELO_PowerUsers (extended rights including editing the folder structure) can have the following rights:

- Edit folders
- Delete folders
- Edit permissions
- Edit keyword lists
- Edit retention period
- Author for approval documents
- Delete versions
- View all workflows from all users (check)
- Delete non-modifiable documents
- Change document editing status

ELO area administrators

The members of this group can manage repository settings for the users they administer as well as their substitutes. They act as administrators for their own departments, are familiar with internal processes, and create the required workflow templates. They know what data has to be entered when filing documents and define the required metadata forms and keyword lists. They can create stamps and edit font colors.

ELO area administrators are not responsible for editing and working with documents, but for structure, processes, and keeping the repository in order. They also perform monitoring tasks.

<p>User manager</p> <p><input type="checkbox"/> <input type="checkbox"/> Main administrator</p> <p><input checked="" type="checkbox"/> <input type="checkbox"/> Edit user data</p> <p><input type="checkbox"/> <input type="checkbox"/> Change password</p> <p><input type="checkbox"/> <input type="checkbox"/> SAP administrator</p> <p><input type="checkbox"/> <input type="checkbox"/> DMS Desktop user, no workflows ⓘ</p> <p><input type="checkbox"/> <input type="checkbox"/> ELO Desktop Client Plus user</p> <p><input type="checkbox"/> <input type="checkbox"/> ELOxc Client user, e-mails only</p>	<p>Folder/document permissions</p> <p><input type="checkbox"/> <input type="checkbox"/> Edit folders</p> <p><input type="checkbox"/> <input type="checkbox"/> Edit documents</p> <p><input type="checkbox"/> <input type="checkbox"/> Edit permissions ⓘ</p> <p><input type="checkbox"/> <input type="checkbox"/> View all entries, ignore permissions</p> <p><input checked="" type="checkbox"/> <input type="checkbox"/> Import permission</p> <p><input checked="" type="checkbox"/> <input type="checkbox"/> Export permission</p>
<p>Folder/document options ⓘ</p> <p><input checked="" type="checkbox"/> <input type="checkbox"/> Change metadata form after filing</p> <p><input checked="" type="checkbox"/> <input type="checkbox"/> Edit keyword lists</p> <p><input type="checkbox"/> <input type="checkbox"/> Edit retention period</p> <p><input type="checkbox"/> <input type="checkbox"/> Change document status</p> <p><input type="checkbox"/> <input type="checkbox"/> Change document paths ⓘ</p> <p><input type="checkbox"/> <input type="checkbox"/> Author for approval documents</p> <p><input type="checkbox"/> <input type="checkbox"/> Show "Additional information" tab</p>	<p>Delete</p> <p><input type="checkbox"/> <input type="checkbox"/> Delete folders</p> <p><input type="checkbox"/> <input type="checkbox"/> Delete documents</p> <p><input type="checkbox"/> <input type="checkbox"/> Delete non-modifiable documents ⓘ</p> <p><input type="checkbox"/> <input type="checkbox"/> Delete versions ⓘ</p>
<p>Workflows</p> <p><input checked="" type="checkbox"/> <input type="checkbox"/> Manage workflows</p> <p><input type="checkbox"/> <input type="checkbox"/> Start workflows</p> <p><input type="checkbox"/> <input type="checkbox"/> Extend workflow rights</p> <p><input type="checkbox"/> <input type="checkbox"/> View workflows for all users</p>	<p>System settings</p> <p><input checked="" type="checkbox"/> <input type="checkbox"/> Edit master data</p> <p><input checked="" type="checkbox"/> <input type="checkbox"/> Edit scan profiles</p> <p><input type="checkbox"/> <input type="checkbox"/> Use debugger</p> <p><input checked="" type="checkbox"/> <input type="checkbox"/> Edit metadata forms and fields</p> <p><input type="checkbox"/> <input type="checkbox"/> Assign replication sets</p>

The role group ELO_AreaAdministrators (settings in the repository) can have the following rights:

- Import permission
- Export permission
- Edit metadata forms and fields
- Edit keyword lists
- Change metadata form after filing
- Edit master data
- Manage workflows
- Edit user data (only for users they administer)
-

Edit scan profiles

ELO administrators

The members of this group can manage settings in the configuration, as well as scan profiles, substitutes, and user data for all other users. They can manage organizational units, assign replication sets, remove locks, manage and move document files in the document system, back them up, or delete them permanently.

ELO administrators do not work with folders or documents in the repository, but instead generally perform administrative tasks only.

User manager

- ☒ ☐ Main administrator
- ☒ ☐ Edit user data
- ☐ ☐ Change password
- ☒ ☐ SAP administrator
- ☐ ☐ DMS Desktop user, no workflows ⓘ
- ☐ ☐ ELO Desktop Client Plus user
- ☐ ☐ ELOxc Client user, e-mails only

Folder/document permissions

- ☐ ☐ Edit folders
- ☐ ☐ Edit documents
- ☐ ☐ Edit permissions ⓘ
- ☐ ☐ View all entries, ignore permissions
- ☐ ☐ Import permission
- ☐ ☐ Export permission

Folder/document options ⓘ

- ☐ ☐ Change metadata form after filing
- ☐ ☐ Edit keyword lists
- ☐ ☐ Edit retention period
- ☐ ☐ Change document status
- ☒ ☐ Change document paths ⓘ
- ☐ ☐ Author for approval documents
- ☒ ☐ Show "Additional information" tab

Delete

- ☐ ☐ Delete folders
- ☐ ☐ Delete documents
- ☐ ☐ Delete non-modifiable documents ⓘ
- ☐ ☐ Delete versions ⓘ

Workflows

- ☐ ☐ Manage workflows
- ☐ ☐ Start workflows
- ☐ ☐ Extend workflow rights
- ☐ ☐ View workflows for all users

System settings

- ☐ ☐ Edit master data
- ☒ ☐ Edit scan profiles
- ☒ ☐ Use debugger
- ☐ ☐ Edit metadata forms and fields
- ☒ ☐ Assign replication sets

Groups and permissions concept

It makes sense to combine functions and permissions into groups.

To assign different areas in the repository different permissions, we recommend creating specific area groups. The example below illustrates how you can assign rights via groups and AND groups.

Assigning rights via groups

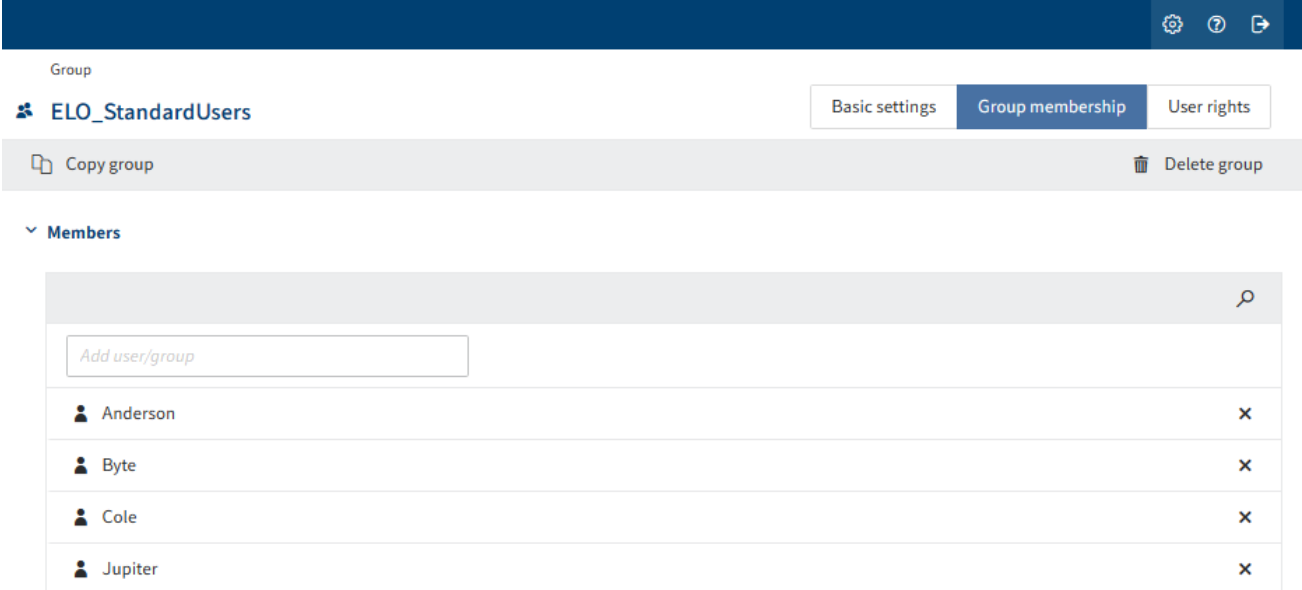
Company XYZ has HR, Production, and Logistics departments. The repository provides different permissions that can be assigned to the different departments.

Membership in the different departments also controls permissions to the documents in the repository. In our example, members of the HR department can access all documents in the HR area, while members of the production department have access to the Production area and members of the logistics department have access to the Logistics area. The groups are created according to the company departments for this reason.









The groups assigned via user rights, also referred to as role groups, are combined with the groups corresponding to department membership.

User rights should always be linked to groups and not to individual users. This allows you to track, monitor, and manage assigned rights.

The ELO_StandardUsers group in our company has the following members:



The screenshot shows the configuration page for the 'ELO_StandardUsers' group. At the top, there's a dark blue header with icons for settings, help, and sharing. Below the header, the group name 'ELO_StandardUsers' is displayed with a group icon. To the right of the name are three tabs: 'Basic settings', 'Group membership' (which is active), and 'User rights'. Below the tabs, there are two buttons: 'Copy group' and 'Delete group'. Under the 'Members' section, there is a search bar with the placeholder text 'Add user/group'. Below the search bar, there is a table listing the members of the group.

 Anderson	
 Byte	
 Cole	
 Jupiter	

The *HR Department* role group has the following members. They are granted exclusive access to documents in the *HR* area.

Group

HR Department

Basic settings

Group membership

User rights

Copy group

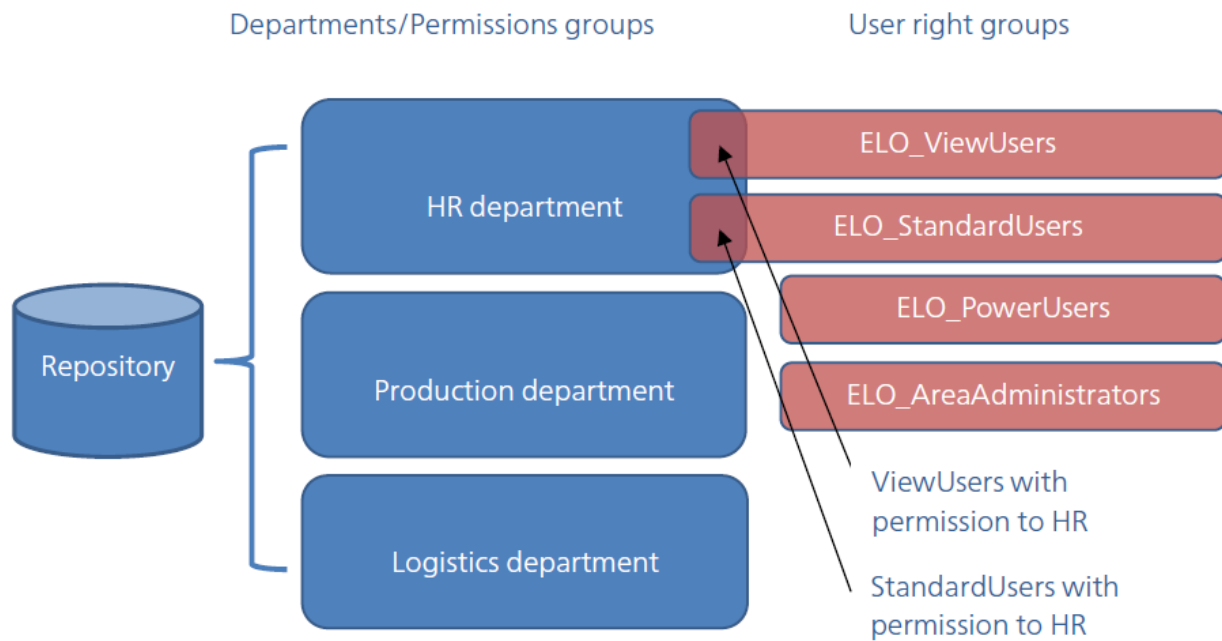
Delete group

Members

<input type="text" value="Add user/group"/>		
	Anderson	x
	Byte	x
	Farrell	x

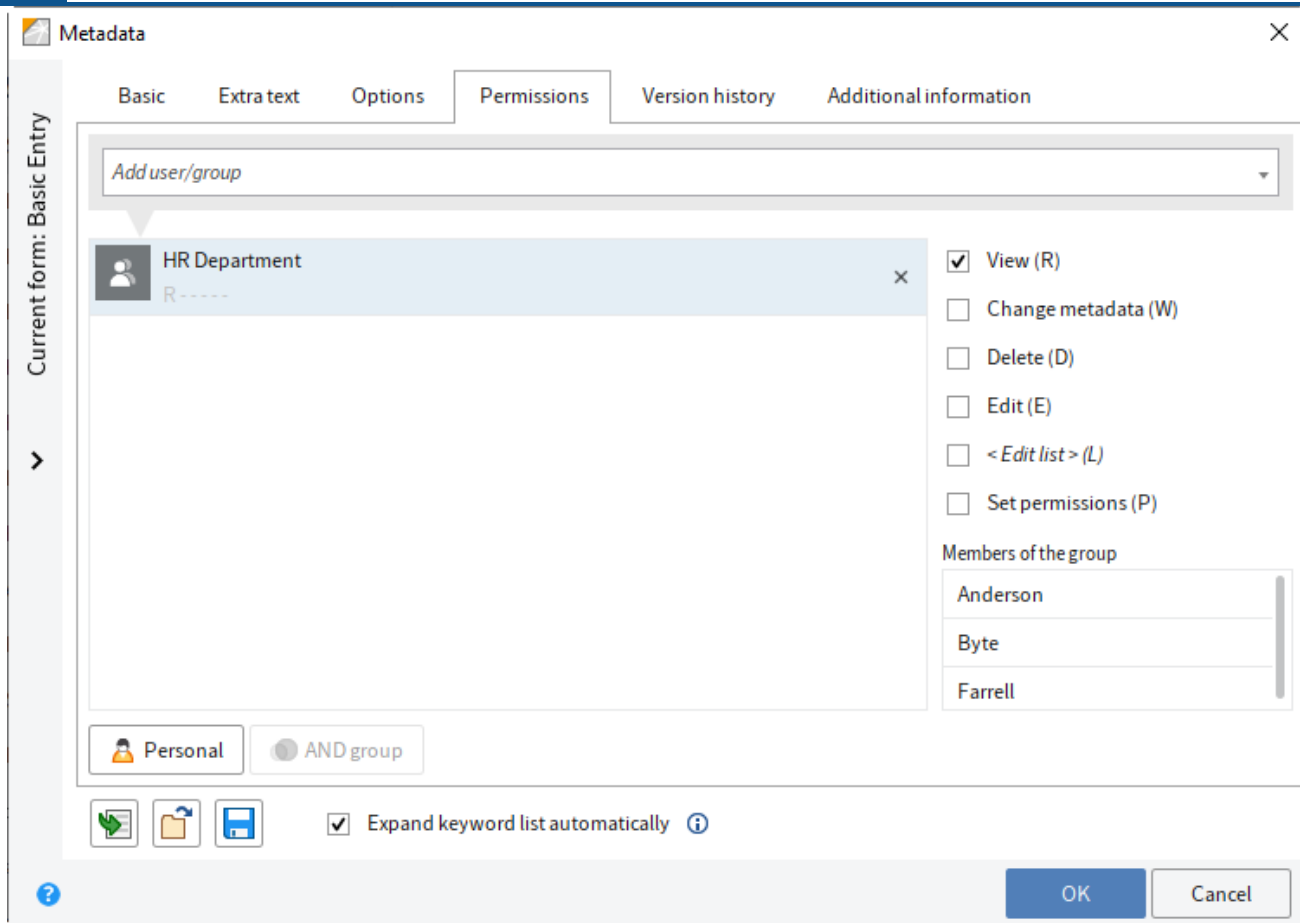
AND groups

The following figure illustrates a scenario for assigning permissions within the HR department.

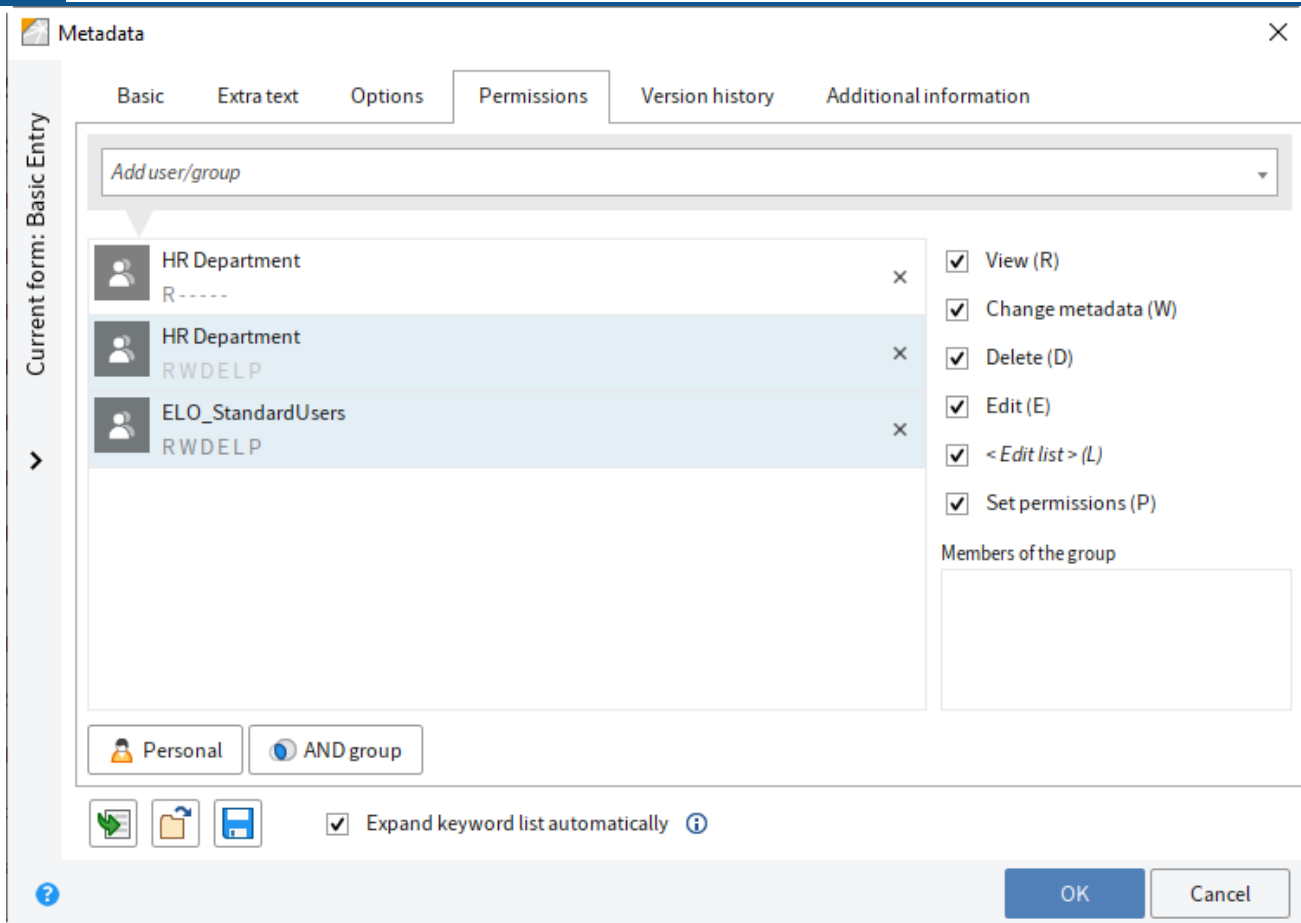


Now, we can set permissions to documents and folders in the *HR* area using an AND group: Members of both the *HR Department* and *ELO_StandardUsers* groups have permissions.

This allows you to give all members of the *HR* department view permissions to HR documents.



To ensure that only the *ELO_StandardUsers* in the *HR Department* group are given full access to these documents, we will create an AND group. An AND group contains the overlap from the selected groups.



In this example, the members of the AND group have full access to this document. ELO shows what employees are members of this group in the example.

Metadata

Basic Extra text Options **Permissions** Version history Additional information

Add user/group

Group	Permissions
HR Department R-----	<input checked="" type="checkbox"/> View (R) <input checked="" type="checkbox"/> Change metadata (W) <input checked="" type="checkbox"/> Delete (D) <input checked="" type="checkbox"/> Edit (E) <input checked="" type="checkbox"/> < Edit list > (L) <input checked="" type="checkbox"/> Set permissions (P)
HR Department & ELO_StandardUsers RWDELP	<input checked="" type="checkbox"/> View (R) <input checked="" type="checkbox"/> Change metadata (W) <input checked="" type="checkbox"/> Delete (D) <input checked="" type="checkbox"/> Edit (E) <input checked="" type="checkbox"/> < Edit list > (L) <input checked="" type="checkbox"/> Set permissions (P)

Members of the group

Anderson

Byte

Personal AND group

Expand keyword list automatically

OK Cancel

Assigning permissions via metadata forms

To ensure that the HR documents can only be edited by authorized users, we recommend defining permissions using the metadata form and not for individual entries in the repository.

HR documents

SaveCancel

Name

HR documents

ID

187

Translation variable

Translation variable

GUID

(EB3E9F97-2BA5-E022-D148-EF2A5E2393CB)

Last change

29.03.2019 08:28

Save data as a table ⓘ

> Usage

> Fields

> Form permissions

> Entry options

▼ Entry permissions

Add user or group

Search for

User or group with permissions

AND group:

1. ELO_StandardUsers

2. HR Department

HR Department

RWDELP

R-----

×

×

☒ View (R)

☒ Change metadata (W)

☒ Delete (D)

☒ Edit (E)

☒ Edit list (L)

☒ Set permissions (P)

AND group

Owner rights

Parent rights

LDAP

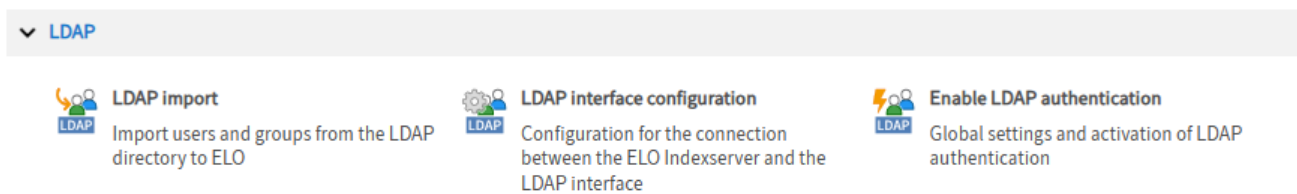
Introduction

The Lightweight Directory Access Protocol (LDAP) enables you to import users and groups from an Active Directory (AD) into the ELO system. This is done with LDAP import.

You need to set up and configure the connection between LDAP and the ELO LDAP interface for the LDAP import to work.

In addition, LDAP authentication must be enabled to allow users to log on to ELO with the data stored in the Active Directory.

You will find the menu items in the ELO Administration Console under *LDAP*.



The user administration in the LDAP directory is managed in a tree structure. In this concept, a unique name within the LDAP directory, known as the distinguished name (DN), is used as a unique key for each user. An example of a DN is `cn=John Smith,ou=people,dc=com,dc=org`. The DN in this case is composed of three parts: the common name (CN), the organizational unit (OU), and the domain component (DC). The combination of OU/DC is used to reference different branches within the LDAP tree structure. The DC addresses the top level below the LDAP directory root node. This usually represents the Internet domain of the company. The schema data is also located directly under the root node. The possible attributes are already specified in the LDAP schema, and the corresponding values for these properties are saved in the LDAP entry that is resolved through the DN.

Please note

Do not use a ; (semicolon) in group and user names in the Active Directory.

LDAP interface configuration

The *LDAP interface configuration* area in the ELO Administration Console is where you edit the connection settings, user import settings, and attribute assignment settings of the configuration file *ldap.json*. The file *ldap.json* is stored in the repository under the following path:

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

Information

Path changes are possible in the following cases:

- If you want to make a special configuration for an ELO Indexserver, copy the file to the directory of the respective ELO Indexserver and make changes to the file there.
- If you'd like to make different configurations for different ELO Indexservers, you will need a separate file for each ELO Indexserver.

The configuration only applies to a single repository. If you edit the configuration in the ELO Administration Console, you need to restart the ELO Indexserver of the repository. If there are multiple ELO Indexservers, you need to restart all of them.

Please note

You should not use LDAP to authenticate the *ELO Service* account (or the service account used). This allows the server-side ELO applications to run independently of the LDAP configuration. Disabling the LDAP connection can cause the ELO applications to no longer start. In this case, you will not be able to enable the LDAP connection in the ELO Administration Console.

Administrator accounts should not be authenticated via LDAP either.

The screenshot shows the 'LDAP interface configuration' window. On the left, a sidebar titled 'Domain selection' shows 'ELOTTEST2.LOCAL' as the selected domain with its LDAP URL 'ldap://...:389'. The main area has three tabs: 'Connection settings' (active), 'User import', and 'Attribute assignment'. The 'Connection settings' tab contains several input fields: 'Domain name' (ELOTTEST2.LOCAL), 'LDAP URL' (ldap://...:389), 'LDAP authentication account' (masked), 'LDAP password' (masked with '***'), 'Connection timeout in seconds' (10), and 'Search timeout in seconds' (9). A 'Verify connection' button is at the bottom right. A note on the right states: 'Responsible administrators use encrypted connections.'

You can make settings for multiple domains.

Under *Domain selection*, you see a list of available domains.

Add (green plus icon): Add settings for a domain

Delete (red X icon): Delete the settings of a domain

Reload data from server (yellow circle arrow icon): Reload the *Domain selection* area

Information

In case of connection problems, the ELO Indexserver log file can be set to *debug*. This makes troubleshooting easier.

Connection settings

LDAP interface configuration Save Cancel

Connection settings

User import

Attribute assignment

Domain name

elo.local

LDAP URL

ldap://:389

Responsible administrators use encrypted connections.

LDAP authentication account

?

LDAP password

...

Connection timeout in seconds

10

Search timeout in seconds

9

Verify connection

Domain name: Specify the DNS name or IP address of the domain here. The setting is used if the `userPrincipalName` is derived from the `sAMAccountName`.

LDAP URL The entries in the *LDAP URL* field determine the TCP connection to the LDAP server.

LDAP authentication account: SSO requires a technical account to search LDAP for the user name transferred by the SSO mechanism (usually `sAMAccountName`). Enter a `userPrincipalName`.

Please note

The account must have sufficient rights to read the user attributes and group memberships.

Please note

When using Kerberos: Disconnect the Kerberos account and the LDAP authentication account. The Kerberos account does not have to be created in ELO.

LDAP password: In the *LDAP password* field, you can enter the unencrypted password of the LDAP authentication account. The ELO Indexserver stores the password encrypted on restart.

Connection timeout in seconds: The LDAP interface terminates the connection to the LDAP server after this number of seconds. It then attempts to establish a connection with the next server in the list.

Search timeout in seconds: When searching for users or groups, this timeout value is passed to the LDAP server.

User import

LDAP interface configuration
Save Cancel

Connection settings

User import

Attribute assignment

DN for person search

Search filter for persons

Search filter for e-mails

Required group membership

DN for group search

Search filter for groups

Maximum nesting depth

⏪
⬅
1
➡
⏩

OU=OU/Germany,OU=ELOix Organisation
Unit for Testing,DC=elotest2,DC=local
OU=OU-Groups1,OU=ELOix Organisation
Unit for Testing,DC=elotest2,DC=local
OU=OU-Groups2,OU=ELOix Organisation
Unit for Testing,DC=elotest2,DC=local

⏪
⬅
1
➡
⏩

OU=OU/Germany,OU=ELOix Organisation
Unit for Testing,DC=elotest2,DC=local
OU=OU-Groups1,OU=ELOix Organisation
Unit for Testing,DC=elotest2,DC=local
OU=OU-Groups2,OU=ELOix Organisation
Unit for Testing,DC=elotest2,DC=local

DN for person search: Use this field to specify which branches of the LDAP directory to search for users.

Please note

The list must not be empty.

Don't enter too many branches either. The more branches, the more imprecise the search.

Search filter for persons: You can use this filter to restrict the search for users.

Search filter for e-mails: The first time the user authenticates with an e-mail address, this filter is used to search for the user in the LDAP directory.

Required group membership: With this setting, you can use the common name to restrict authentication to users who are members of a certain group in the LDAP directory. This must be entered as the common name.

DN for group search: In this field, you specify which branches of the LDAP directory the groups that are eligible for synchronization must be in. If the list is empty, all groups of the user are included in group synchronization.

Search filter for groups: You can use this filter to restrict the search for groups of a user.

Maximum nesting depth: This field can be used to specify the depth of group nesting. This refers to the collection of user groups for group synchronization.

Attribute assignment

LDAP interface configuration

Save
Cancel

Connection settings

User import

Attribute assignment

Domain prefix

Domain prefix

?

Placeholder for ELO user names

\$CN\$

?

User authentication via

sAMAccountName

?

i

Changes to the above settings may mean that existing users will be unable to log on or have to be created again under a different name.

Supervisor attribute name

?

ELO administrator of this user

Save attributes in ELO

objectguid

✗

distinguishedname

✗

mail

✗

?

+

Domain prefix: The domain prefix is required if multiple domains are configured and the sAMAccountName is saved as the Windows attribute for the ELO user. There must be a separator at the end of the domain prefix. This separates the prefix from the user name. Ideally, you should use a backslash.

Information

If you are using SSO, the domain prefix must match the NetBIOS domain name.

You will find the corresponding domain prefix for SSO in the USERDOMAIN environment variable on the client computer. For SSO with domain prefix, you need to set the option `"ntlm.domainUserFormat"` in the ELO Indexserver config.xml file. If you set the option `sAMAccountName` in the User authentication via field and specify a domain prefix, the Windows user contains the account name with the domain prefix in front.

Example:

- sAMAccountName = fritzfrei
- Domain prefix = ELO\
- Windows user = ELO\fritzfrei

Placeholder for ELO user names: The ELO user name can be made up of different LDAP user attributes. You can specify a format expression with placeholders. Enclose the placeholders in \$ signs. They must also correspond to the LDAP attribute names.

User authentication via: In the drop-down menu *User authentication via*, you can specify whether you want to set the `sAMAccountName`, the `userPrincipalName`, or the `UID` as the *Windows user* attribute (see ELO user manager).

Please note

The setting selected in the *User authentication via* field must match the settings in the *Search filter for persons* field (*User import* tab). Pay attention to capitalization.

Any umlauts should also be identical between the Active Directory and ELO user names.

The ELO Administration Console checks LDAP for the following four attributes. The ELO Administration Console uses the first attribute set for the name.

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

Information

Some environments require a custom configuration. This field enables you to enter any values.

Supervisor attribute name: In this field, you specify which attribute is used to determine the supervisor of the ELO user. This is usually the attribute `$manager$`.

Please note

The supervisor must already exist in ELO.

ELO administrator of this user: In the field *ELO administrator of this user*, you can specify which ELO user to set as administrator for users created via the LDAP interface. You can enter the ID, GUID, or ELO user name.

Save attributes in ELO: In this field, you specify which attributes are to be transferred from LDAP to ELO.

To add an attribute, enter the name of the attribute in the field. Next, click *Add* (green plus icon).

To remove an attribute, click the X icon next to it in the list of attributes.

Information

Mandatory attributes cannot be deleted. In this case, the X icon is grayed out.

LDAP import

With LDAP import, you can import users and groups from an Active Directory (AD) into the ELO system.

LDAP import

Import

i

Hits: 11

x

Select server

Server

ldap://:389

Responsible administrators use encrypted connections.

Domain user

ELOTEST2\

Password

...

Ignore certificate validation

☐

Base DN

DC=ELOTEST2,DC=LOCAL

LDAP organizational unit

ou=ou-doku,ou=eloix organisation unit for te

Filter templates

All users

Filter text

(&(objectCategory=person)(objectClass=user))

Mapping script

Reset mapping

Update existing users or groups

☐

Create groups in ELO that exist in LDAP

☐

Start search

Results list

<input type="checkbox"/> Selected		Name	ID	Groups in ELO	Missing groups
<input checked="" type="checkbox"/>	 	Andrea Andersson	14	GRP_ADMIN, GRP_GL, OPT_GRP_ADMIN, OPT_GRP_TL	
<input checked="" type="checkbox"/>	 	Bernhard Byte	15	GRP_ADMIN, OPT_GRP_ADMIN	

- Select server: The ELO Administration Console attempts to find possible LDAP servers automatically. If this field is blank, no server will be found in the domain. This may be the case with a VPN connection, for instance.
- Server: Enter the server for the LDAP connection here. You can also enter the IP address, port, or protocol here.

BNF: server ::= [ldap|ldaps]://[servername|IP address]:port

Please note

Use an encrypted connection, in this case LDAP via SSL (LDAPS).

- Domain user and password: The authentication data consists of a name and password.
- Ignore certificate validation: The certificate validation can be ignored if needed.
- Base DN and LDAP organizational unit: These entries are used to select the correct branch of the LDAP directory.
- Filter templates and filter text: Some LDAP filter expressions are already provided in the list and applied to the filter text so that they can be edited.
- Mapping script: This setting allows you to edit the data as JavaScript code.

For more information, see the next section *The mapping script*.

- Reset mapping: Deletes the text from the mapping script field.
- Update existing users or groups: If the name can be resolved to an existing entry, this entry is only processed again if this setting is enabled.

Please note

LDAP groups are only read and used when users log on.

- Create groups in ELO that exist in LDAP: Creates groups that do not yet exist in ELO.
- Start search: Performs a search and shows the results.
- Results list: Shows the list of the entries that will be imported. All valid entries are also selected. If invalid data is detected during the check, they will not be selected, and a note about the problem is shown in a tooltip.

The mapping script

Default LDAP attributes are automatically mapped to ELO attributes. To allow more flexible customization, JavaScript code can be entered in the input field. This is embedded in a code frame and is performed on every data set in the LDAP search.

The ELO Indexserver has a data structure for the users and groups: the UserInfo object. This is described in detail in the ELO Indexserver technical documentation. It can be accessed in the mapping script using the variable name `elo`.

Default mapping

- `elo.type`
 - Based on the LDAP `objectClass=person`
 - If the class exists, a user is created; otherwise a group is created.
-

- elo.name
 - Based on the LDAP attributes displayName, cn, sAMAccountName, and distinguishedName.
 - The first LDAP attribute found is used as the name.
- elo.userProps[UserInfoC.PROP_NAME_OS]
 - The value of the sAMAccountName LDAP attribute is applied.
- elo.userProps[UserInfoC.PROP_NAME_EMAIL]
 - The value of the LDAP attribute mail is applied.
- elo.superiorId
 - The LDAP attribute manager is evaluated.
 - If the manager attribute refers to an existing ELO user, the ID of this user is applied as the supervisor.
- elo.id
 - If the name refers to a valid ELO user, this ID is applied as the user ID. Otherwise -1 creates a new user.

JavaScript code frame

At the debug log level, the generated script is output to the log file.

```
// 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){
%% The text from the interface for the mapping script field is output here. %%
}
```

If the ELO Administration Console is started using Java 8, the Rhino compatibility mode is included.

```
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 );
}
```

The JavaScript frame is accessed via the `LdapImportMapping` Java interface. In the map, the ELO name in lowercase is used as the key to the `UserName` object.

Examples

- A data set can be excluded by setting `elo.id=0`.

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

- Since JavaScript code can be used, it is also possible to view outputs for testing using the error reporting mechanism.

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

or also

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

- A short example shows how to exclude items while checking the mail attribute and set the display name for the remaining users.

```
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()+')'  
    // valid e-mail -> customize the display name.  
  }  
}else{  
  elo.id=0  
  // invalid e-mail -> exclude  
}
```

Enable LDAP authentication

Enable LDAP authentication
Save
Cancel

☒ LDAP authentication is disabled

Global settings

☒ Create new users automatically

☒ Assign group ?

ELO user for internal authentication ?

Search for

Members		
	Administrator	×
	ELO Service	×

LDAP authentication is disabled/LDAP authentication is enabled: Use this toggle to enable or disable LDAP authentication.

Create new users automatically: If the option *Create new users automatically* is enabled, a new user is automatically created in ELO after logon.

Information

Initial authentication, i.e. the user does not exist in ELO yet, must take place with one of the following values:

- sAMAccountName, userPrincipalName, or mail for Active Directory
- UID or mail for OpenLDAP

Assign group: If the *Assign group* option is enabled, users are automatically assigned to the corresponding LDAP groups. For this to work, the groups must be created in ELO and the names must match the names of the groups in LDAP.

Please note

LDAP groups are only read and used when users log on.

ELO user for internal authentication: In this field, you can specify which ELO users/groups should not authenticate with LDAP. These users/groups can log on to ELO directly.