Configuration and administration

ELO Modern Authentication (Auth2)

Table of contents

ELO Modern Authentication (Auth2)

Introduction

ELO Modern Authentication (also abbreviated as Auth2) acts as a central authentication point for all clients.

Besides standard authentication with ELO user name and password, it is also possible to authenticate with identity providers, such as *Microsoft*, *Google*, or *Keycloak*.

Every identity provider (IdP) is supported, as long as it complies with the OpenID protocol.

Requirements

- Current version of the ELO clients
- For ELO user accounts, the corresponding e-mail addresses must be configured for the IdPs. The e-mail address is always used to compare the IdP account with the ELO account.

> **Information**
>
> You can configure the system to automatically create an ELO account the first time the user authenticates if the e-mail address used does not yet exist in ELO. For more information, refer to the chapter Configuration > User mapping.

> **Please note**
>
> Newer versions of ELO Modern Authentication from ELO 25 cannot be used with older ELO modules and clients.

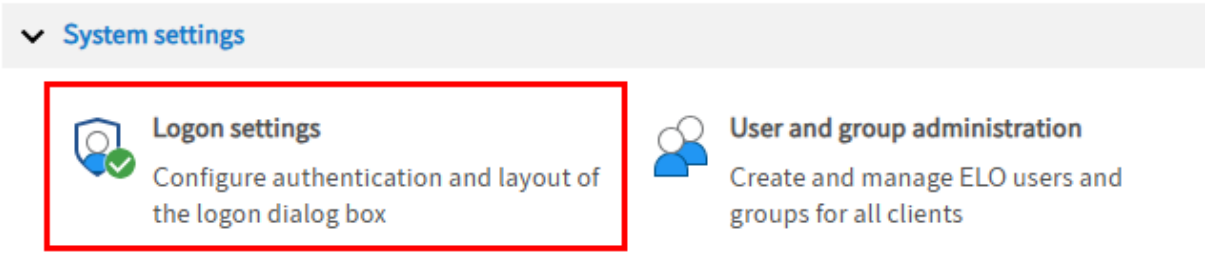
The following explains how to open the configuration area for ELO Modern Authentication.

Initial start

Only the ELO log on with the account name and password is configured initially by default.

To configure your own identity provider, proceed as follows:

1. Log on to the ELO Administration Console with a main administrator account (account with the *Main administrator* right).
2. In the *System settings* group, select the *Logon settings* menu item.



The ELO Modern Authentication configuration page opens.

3. You can select a provider you want to add a configuration for from *Add OpenID provider*.

> **Information**
>
> All OpenID-compatible identity providers are possible.

You can learn how to configure ELO Modern Authentication in the Configuration chapter.

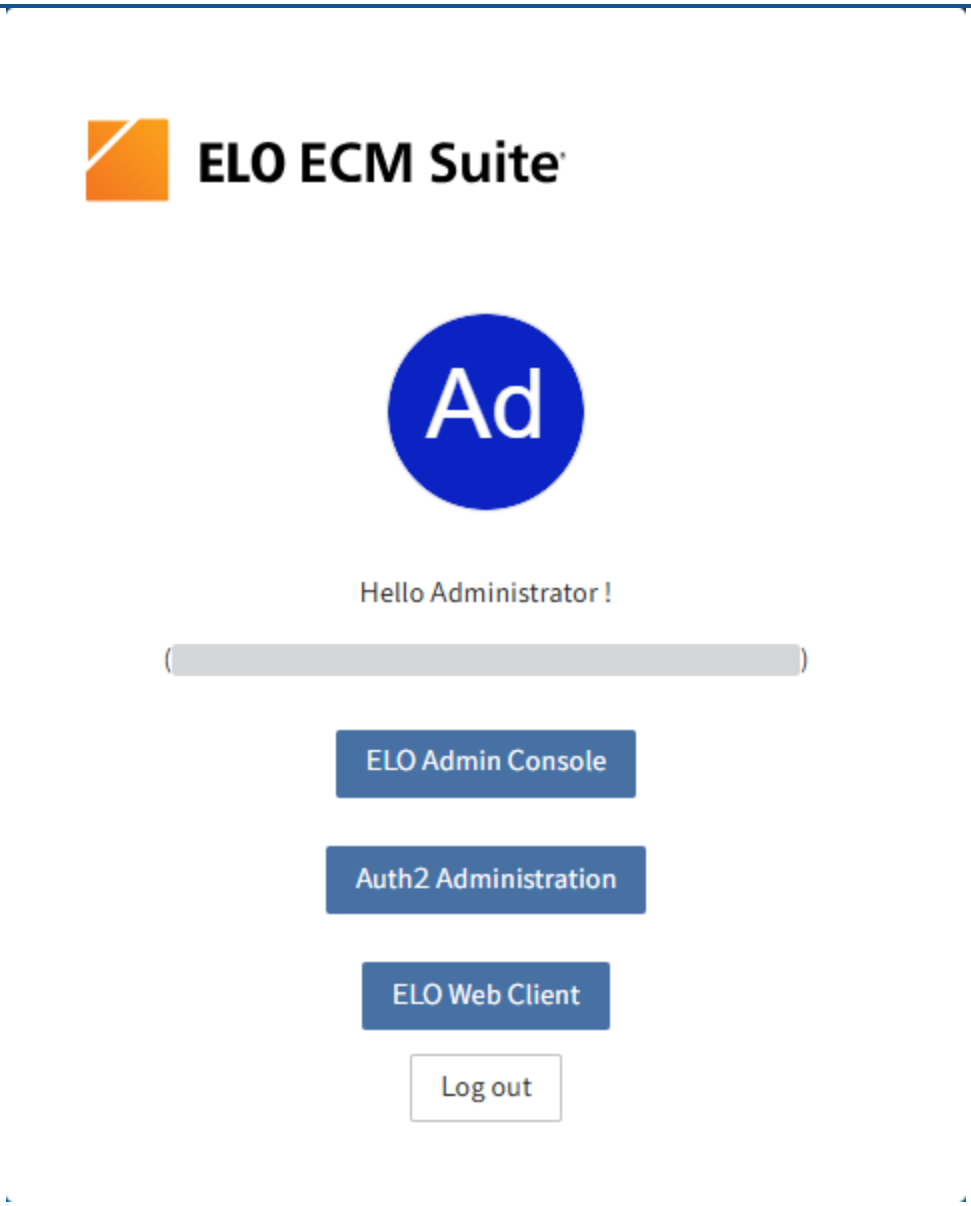
Alternatively: Open ELO Modern Authentication directly

You can also open the authentication configuration for ELO Modern Authentication directly.

1. Open the URL for ELO Modern Authentication.

   URL schema: `https:/<server>:<port>/ix-<repository>/plugin/auth2/`

2. Log on with a main administrator account.



An overview page appears with various authentication possibilities.

3. Select *Auth2Administration*.

   The ELO Modern Authentication configuration page opens.

You can now perform configuration.

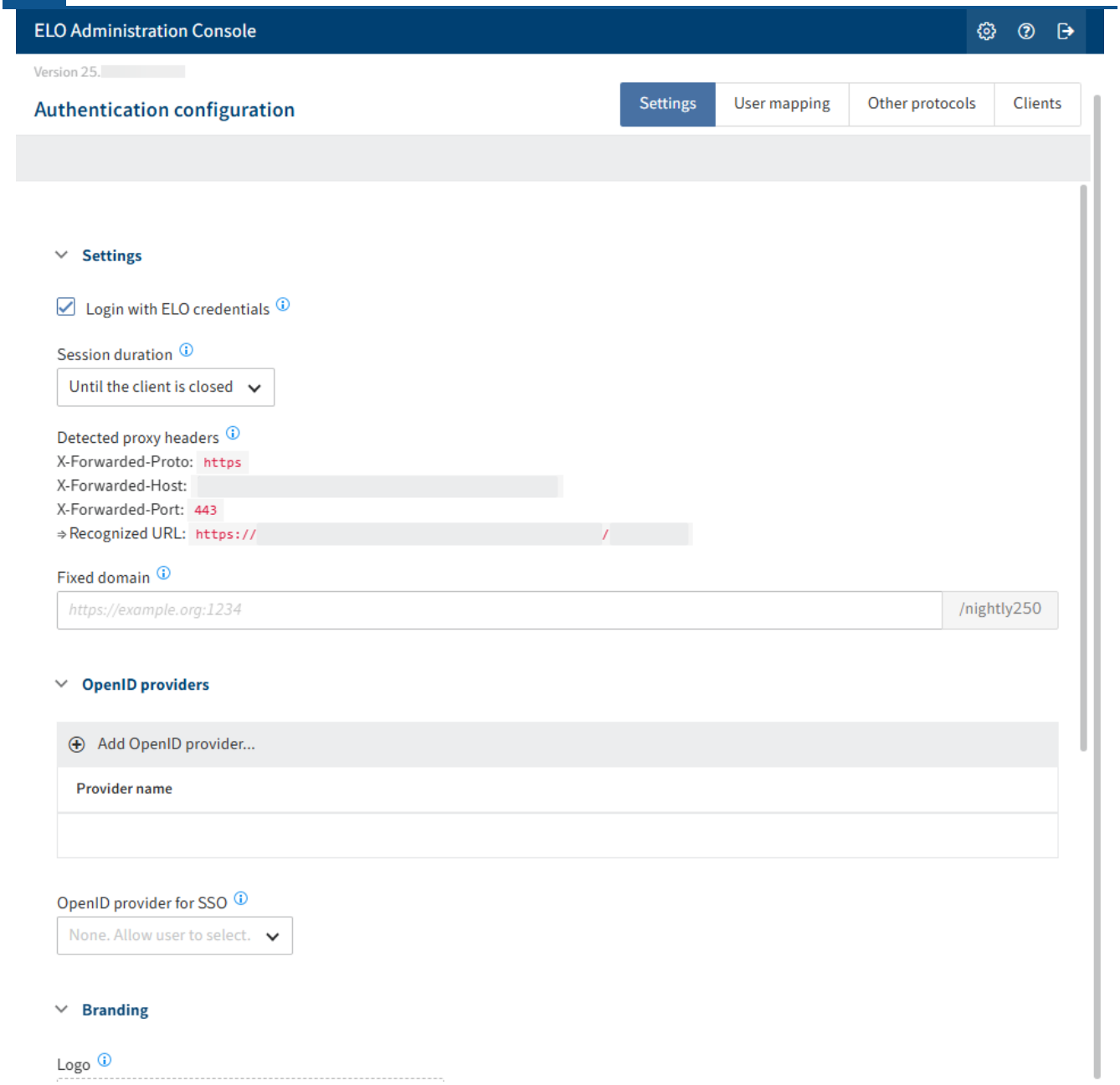
Configuration

The following describes how to configure ELO Modern Authentication.

> **Information**
>
> If there are multiple repositories in one ELO instance, they share a login configuration.

'Settings' area

You can customize the ELO Modern Authentication login page to the requirements of your company.



The following options are available in the *Login Config* area:

- Enable password-based login: If this option is enabled, users can log in using an identity provider or with an ELO account name and password, as usual.

  If this option is disabled, login is only possible via the identity provider. Service accounts and accounts with administrative rights form an exception here.

- Session duration: Select how long a session should last. After a session has ended you have to log in again.

> **Information**

Restarting the ELO Indexserver also ends the session.

- Recognized proxy headers: Shows the proxy headers to be sent by reverse proxies and load balancers.
- Fixed domain for callbacks: If you define a fixed domain for authentication, all authentication and redirects take place via this address only. This can resolve possible issues during redirects.

  If this field is left blank, the URLs are determined dynamically according to the HTTP request. This also includes information provided by *X-Forwarded* headers from reverse proxies and load balancers.

  If you want to access the repository via different domains, e.g. an intranet URL or an external URL, you will have to configure the proxies accordingly. For more information, refer to the Reverse proxies chapter.
- OpenID provider for SSO: From the drop-down menu, you can select an identity provider to trigger authentication with single sign-on. If no provider is selected here, all configured providers are shown in the logon dialog box. In this case, users can select the authentication method themselves.

Branding

You can upload logos and background images for branding purposes.

The standard, web-capable image formats can be used. The images are scaled depending on the size and resolution.

The images are added when you click *Save* and shown next time the ELO Modern Authentication login page is opened.

- Logo: You can upload a custom logo via this field, which is shown when logging in.

  If the logo is deleted, the ELO logo is displayed.
- Background image: You can upload a custom background image via this button, which is shown in the background when logging in.

  Information

  The formats PNG and JPEG are recommended. Other formats, such as SVG, WebP, or AVIF, may not be rendered correctly in the ELO Java Client.

  The recommended minimum resolution is 1920x1080. The file size should be less than 1 MB to enable fast network transfer.

  If the background image is deleted, the default background is shown.

Add OpenID provider

You must configure this first to enable authentication via one or more identity providers.

> **Please note**
>
> The OpenID provider must be able to be reached by the ELO server. This may require changes to the firewall settings.

Individual steps may vary and different ones may be required, depending on the provider.

Next, we will show you the process in the overview.

1. Select *Add OpenID provider*.

   A drop-down menu appears.

2. Select the desired provider.

   Supported providers:

   - Microsoft
   - Google
   - Keycloak
   - SAP
   - Salesforce
   - SmartWe
   - Other (option to connect another OpenID-compatible identity provider)

   The *Select an ID for the OpenID provider* dialog box appears. The name is prefilled, depending on the selection.

   Optional: Change the name for the configuration.

3. Select *OK* to confirm.

   The corresponding configuration area appears.

4. Enter the information required for the provider.

   Alternative: Select *Register with provider* if you haven't registered with the desired OpenID provider yet. Then, transfer the registration data to the configuration.

> **Information**
>
> The connection via Microsoft Azure is used as an example in the Microsoft Azure configuration chapter.
>
> Individual steps may vary, depending on the provider.
>
> And, different preparations are required, depending on the provider.

Optional: You can enable the *Hidden* option to hide the identity provider in the login dialog box. However, it can still be used by apps or integrations for authentication.

5. Save the settings.

Test

You can check the settings via *Test login*. A pop-up window opens that simulates the login page. An attempt is made to log in with the currently used account when logging in via the configured provider.

> **Please note**
>
> Comparison is done via the e-mail address. For this reason, the e-mail address the provider uses is also added in the ELO account in the *E-mail* field.

Configure single sign-on

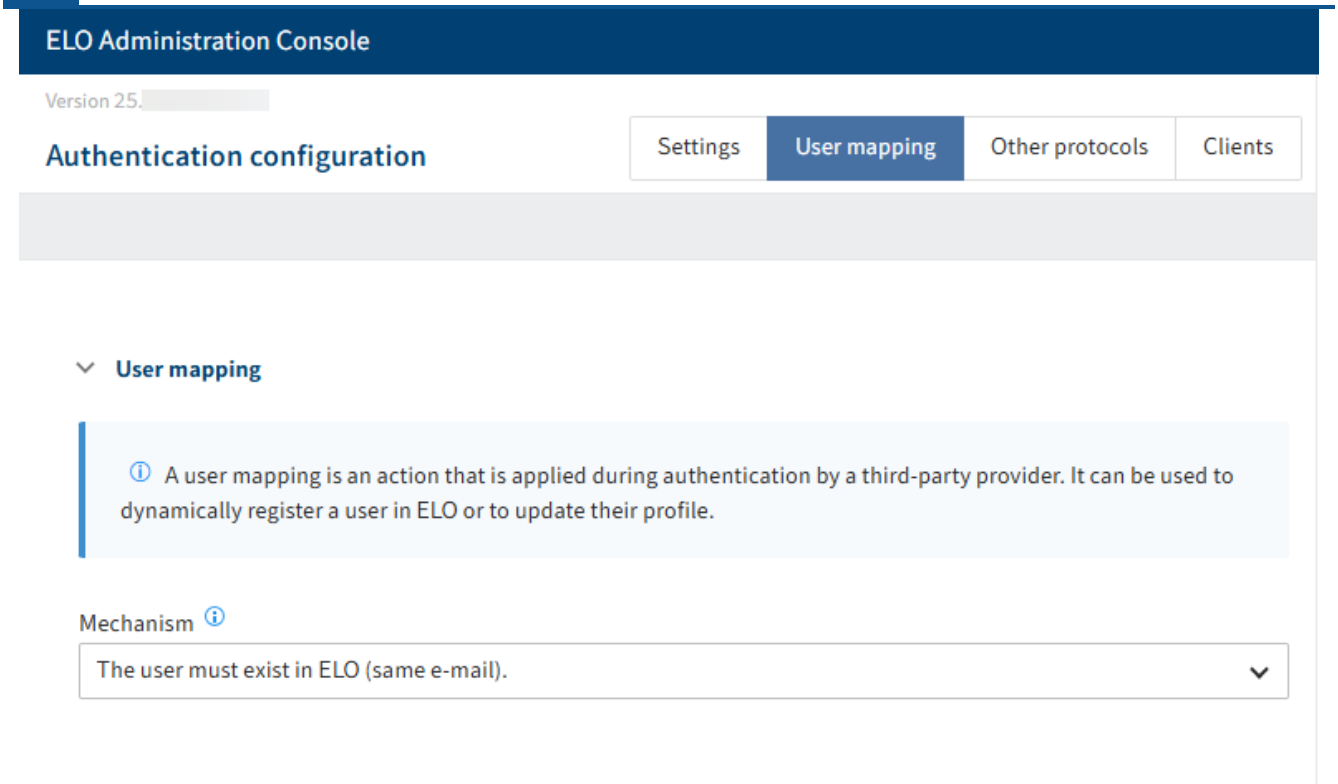
You can configure authentication using single sign-on (SSO) in the ELO clients to only work via a configured identity provider.

In the Settings area, go to the *OpenID provider for SSO* drop-down menu and select an OpenId provider to be used for authentication.

Alternatively, you can disable the option *Login with ELO credentials* if only one other identity provider is configured.

'User mapping' area

In the *User mapping* area, you can configure a method that can be used when comparing ELO accounts with the identity provider accounts.



The following mechanisms are available:

- User must exist in ELO
- Create ELO user immediately: When logging on ELO, a new account is created provided no ELO account already exists for the entered e-mail address. In the *E-mail domain restriction* field, you can define which domains are permitted for authentication.
- Call flow: Calls a flow to automatically create or update nodes during authentication in ELO. Once the flow has been executed, the user is signed on to ELO provided the account exists in ELO. To use this mechanism, you have to create a corresponding flow first.

  The flow gets the entire OpenID *UserInfo* data set from the OpenID provider. With Microsoft, this can look as follows:

  ```
  {
      "sub": "<Microsoft user ID>",
      "name": "Luise Lind",
      "family_name": "Lind",
      "given_name": "Luise",
      "picture": "https://graph.microsoft.com/v1...;value",
      "email": "l.lind@example.com"
  }
  ```

  The payloads vary depending on the OpenID provider used, but almost always contain the parameters `"sub"`, `"email"`, and `"name"`.

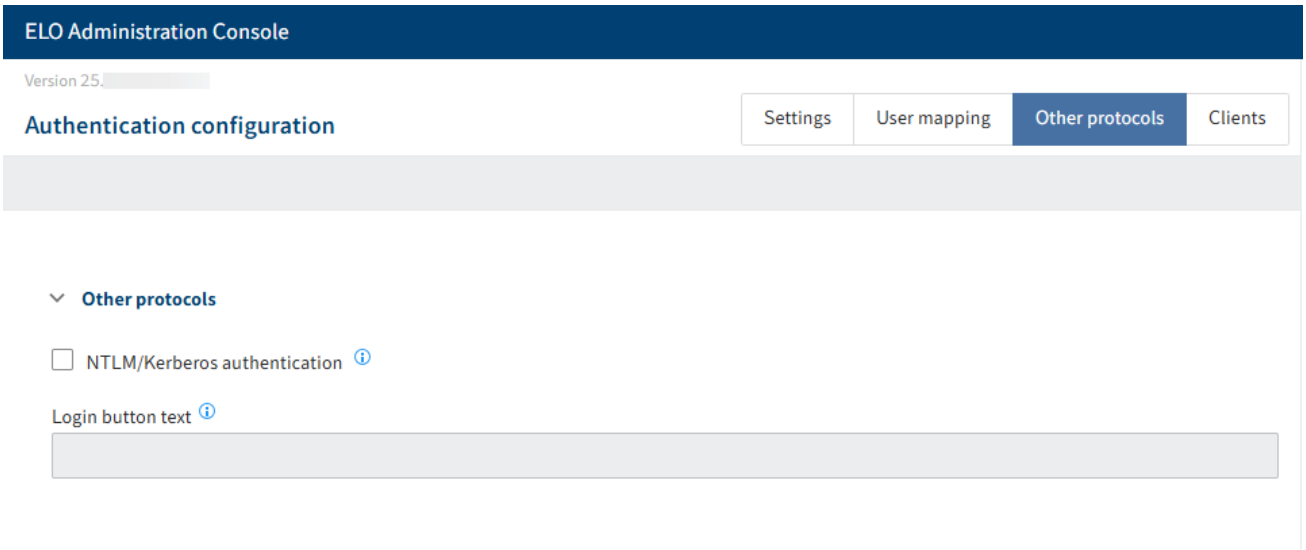
-

Call registered function (legacy): Can apply account mappings and create a new account or update an existing one during authentication with ELO.

For more information on registered functions, refer to the ELOauth plug-in documentation > Existing implementations > Registered function and Manual configuration > OAuth2.

'Other protocols' area

The *Legacy protocols* area is intended for systems that use NTLM or Kerberos.



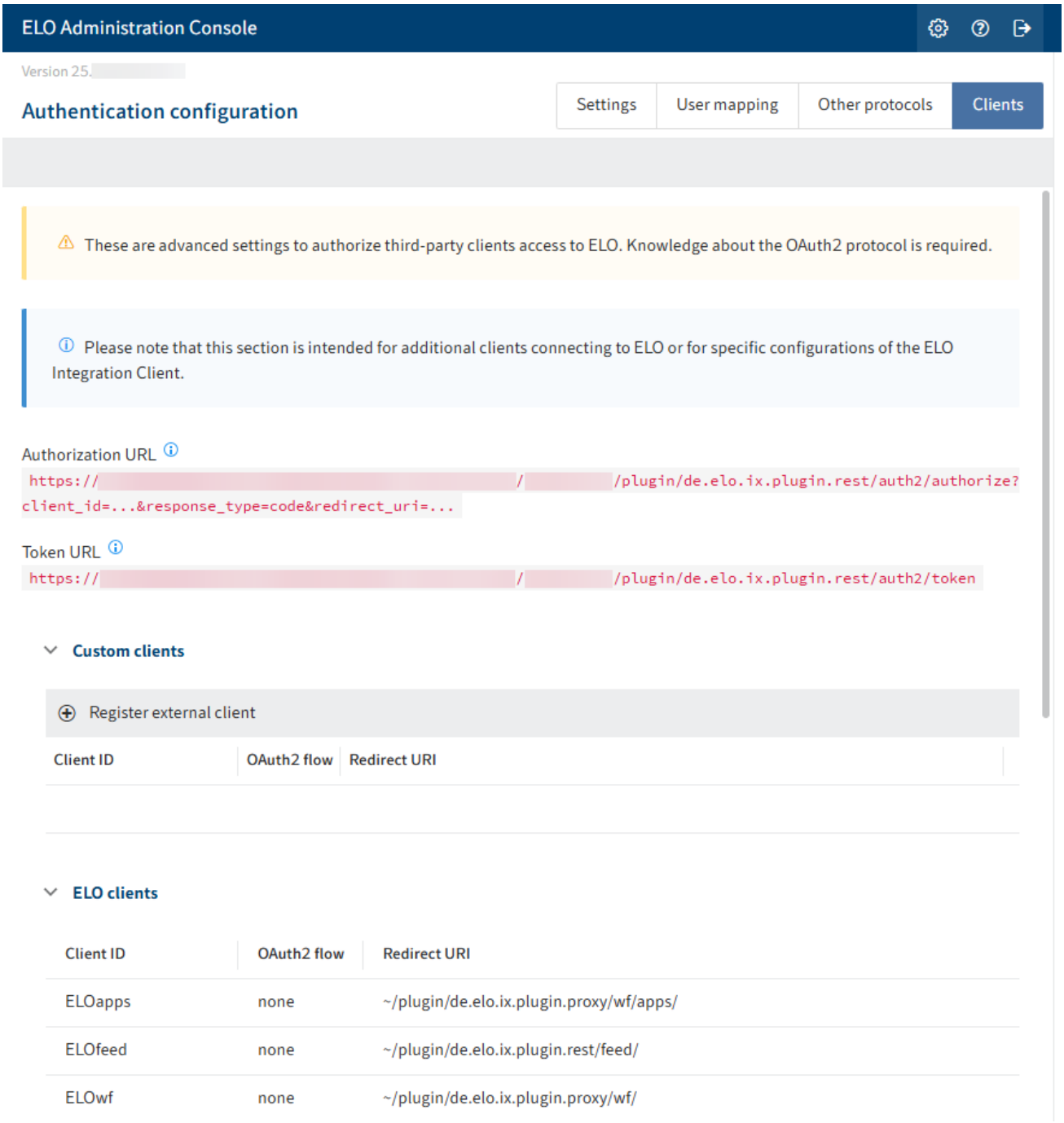
Please note

We do not recommend you use these protocols. However, this option is still offered for compatibility reasons.

Important information

- *NTLM* is no being longer developed by Microsoft as of June 2024 and is therefore considered deprecated.
- The authentication protocol *SAML* is no longer supported.
- *Kerberos* and *NTLM* do not work in the ELO Java Client with JCNN (default) if load balancer mode is enabled upstream. If the value `ASF` is set in the registry, the Business Solutions packages will not work.
- *Kerberos* and *NTLM* only work in intranet environments in which the clients are controlled by the respective company.

'Clients' area



In this area, you will find advanced settings for accessing the ELO system as well as an overview of the URLs and URIs for ELO clients and modules.

Under *External clients*, you can connect a custom external portal or a custom application with ELO.

Please note

This requires advanced knowledge of the *OAuth 2.0* protocol. You will find more information on the OAuth 2.0 Simplified and OAuth 2.0 websites.

Microsoft Azure configuration

This chapter shows how to configure authentication with Microsoft Azure.

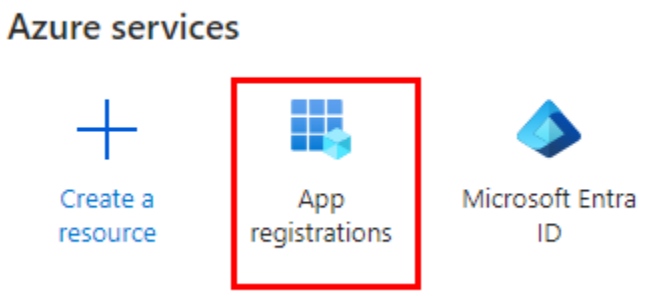
> **Information**
>
> By configuring authentication with Microsoft Azure, you can also enable the *Check out to OneDrive* function in the ELO clients.
>
> You will find more information about this function in the Connect ELO to Microsoft OneDrive documentation and in the following user documentation:
>
> - ELO Java Client
> - ELO Web Client
> - ELO Desktop Client
>
> To enable this function, follow the instructions in this chapter and note the information in the Assign permissions chapter.

Register app

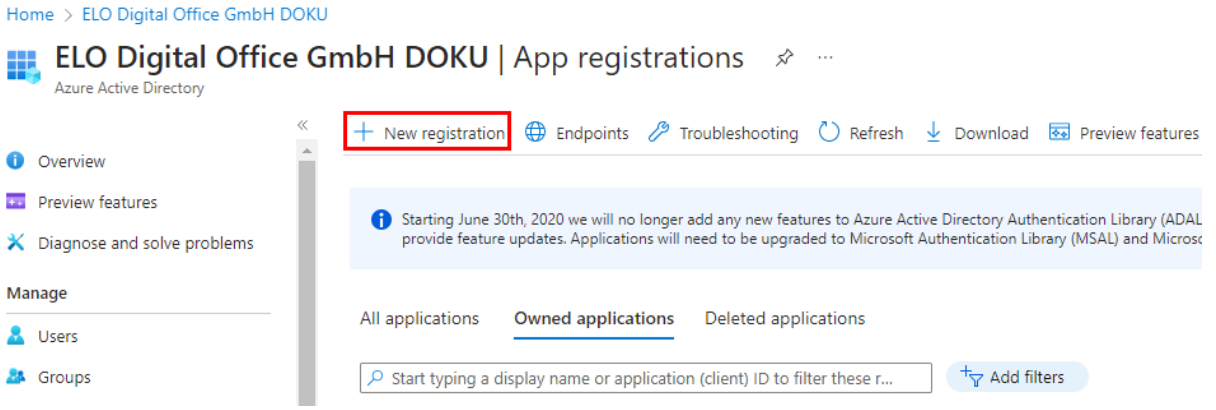
First, you need to register an app in Microsoft Azure.

> **Please note**
>
> This documentation does not cover basic configuration of a Microsoft Azure environment or subscriptions, both of which are required for this.

1. Log on to Microsoft Azure as an administrator.



2. Go to *App registrations*.



3. Select *New registration*.

   The *Register an application* page opens.

4. Enter a name for the app. You can choose any name you like.

   Example: ELOauth2

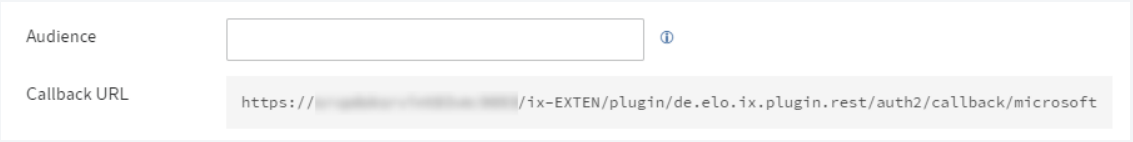
5. Under *Supported account types*, select the option *Accounts in this organizational directory only (only <name of tenant> - individual client)*.

6. Under *Redirect URI (optional)*, select the *Web* option.

7. Enter a URL that can be reached on the internet as follows:

   ```
   https://<server address>/ix-<repository>/plugin/de.elo.ix.plugin.rest/auth2/
   callback/microsoft
   ```

   Information

   This URL is also provided on the ELO Modern Authentication configuration page under *Callback URL*.

8. Select *Register*.

   The app is registered in Microsoft Azure.

Assign permissions

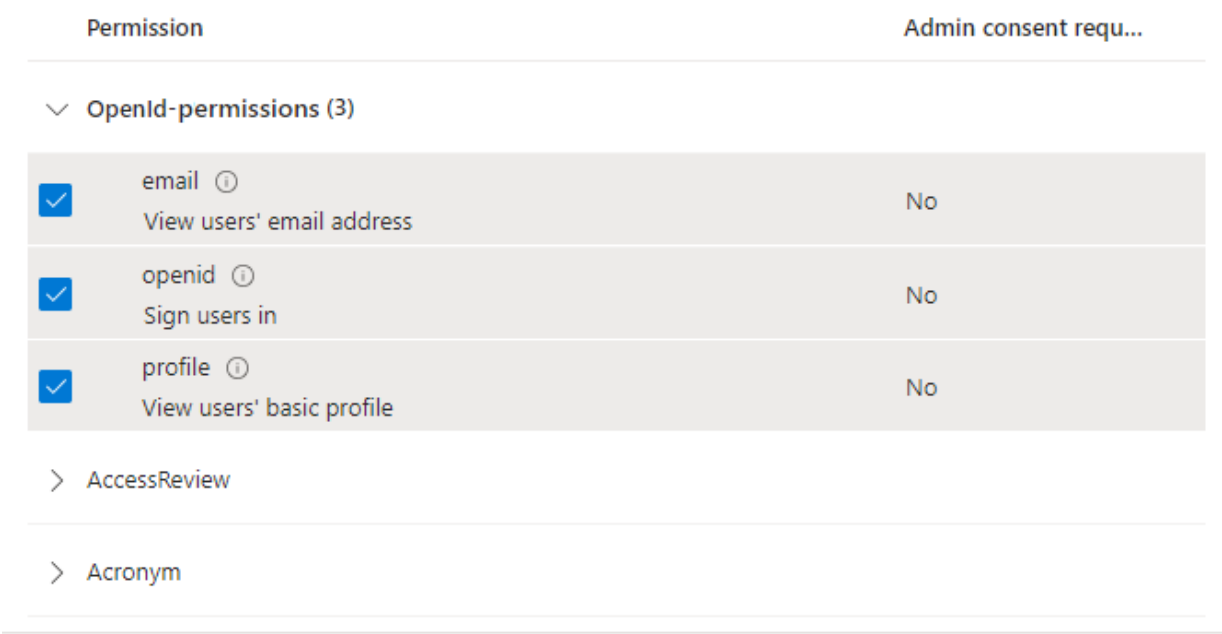
You can assign the required permissions as soon as the app is registered.

1. Open the *API permissions* area.

2.

Select *Add permissions*.

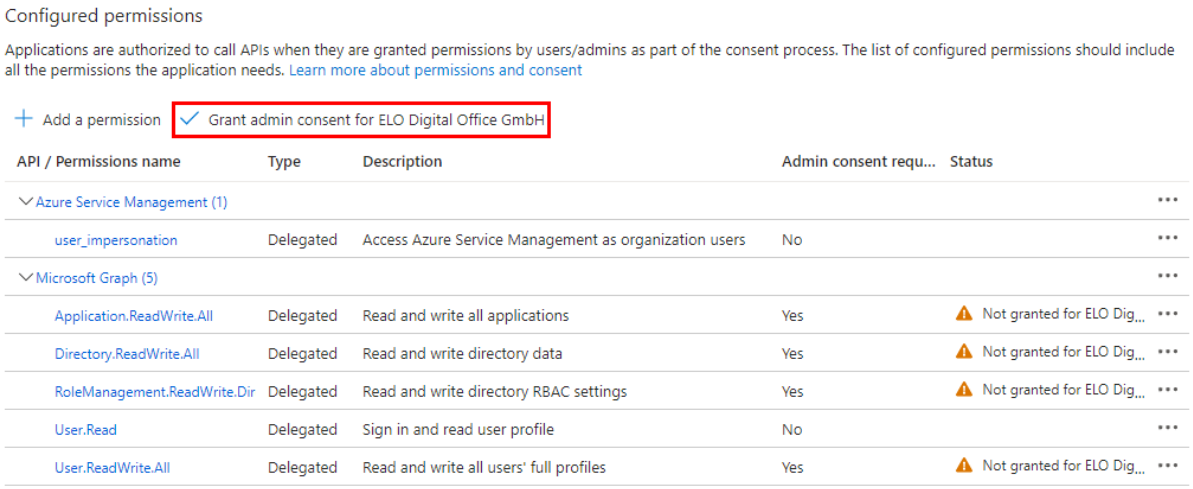
The *Request API permissions* area opens.



3. Select *Microsoft Graph*.
4. Add the following delegated permissions:
    - Microsoft Graph:
        - email
        - openid
        - profile
        - Files.ReadWrite.AppFolder
        - User.Read
        - Files.ReadWrite.All
        - offline_access

> **Information**
>
> The permissions *Files.ReadWrite.AppFolder* and *Files.ReadWrite.All* enable the *Check out to OneDrive* function in the ELO clients.

5. Confirm with *Add permissions*.



6. Select *Grant admin consent for <tenant>*.

   The *Confirm admin consent* dialog box opens.

7. Click *Yes* to confirm.

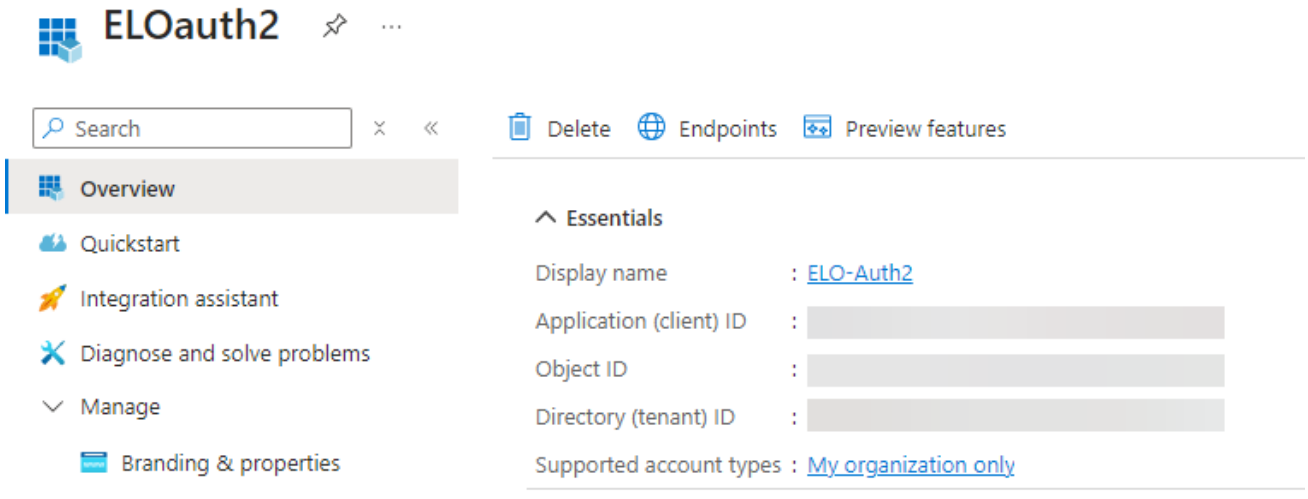
   The permissions are added.

8. On the ELO Modern Authentication configuration page, enter the following values in the *Scope* field:

   ```
   openid email profile offline_access .default
   ```

Transfer information in configuration

After the app is registered and has been assigned permissions, you can transfer the information to the ELO Modern Authentication configuration page.

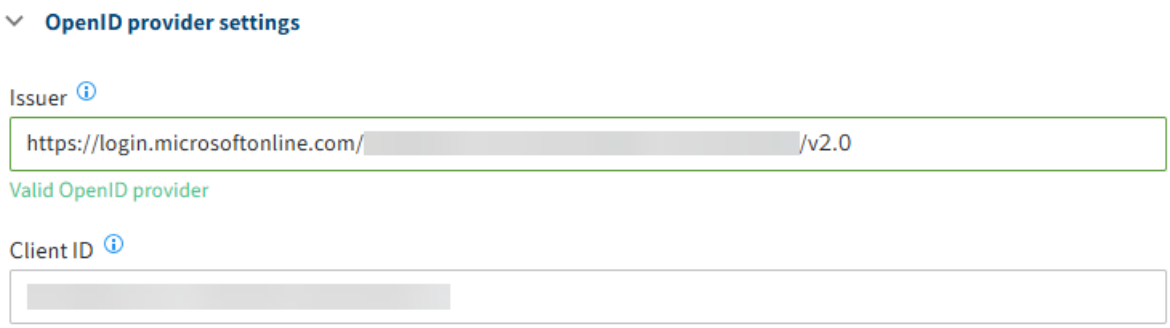


1. Open the *Overview* area in Microsoft Azure.

2.

Copy the value for *Application ID (client)*.

3. Enter the value on the ELO Modern Authentication configuration page under *Client ID*.



Optional: If you use the ELO Desktop Client and/or ELO Bot, you can also enter the copied value under *Audience*.

4. Copy the value for *Directory ID (client)* from Microsoft Azure.
5. Enter the value on the ELO Modern Authentication configuration page under *Issuer* instead of the `{tenant}` placeholder.
6. Save the settings with *Save*.

Client secret

This also requires a client secret to enable the connection to the Microsoft Azure app to work. This must be entered on the ELO Modern Authentication configuration page.

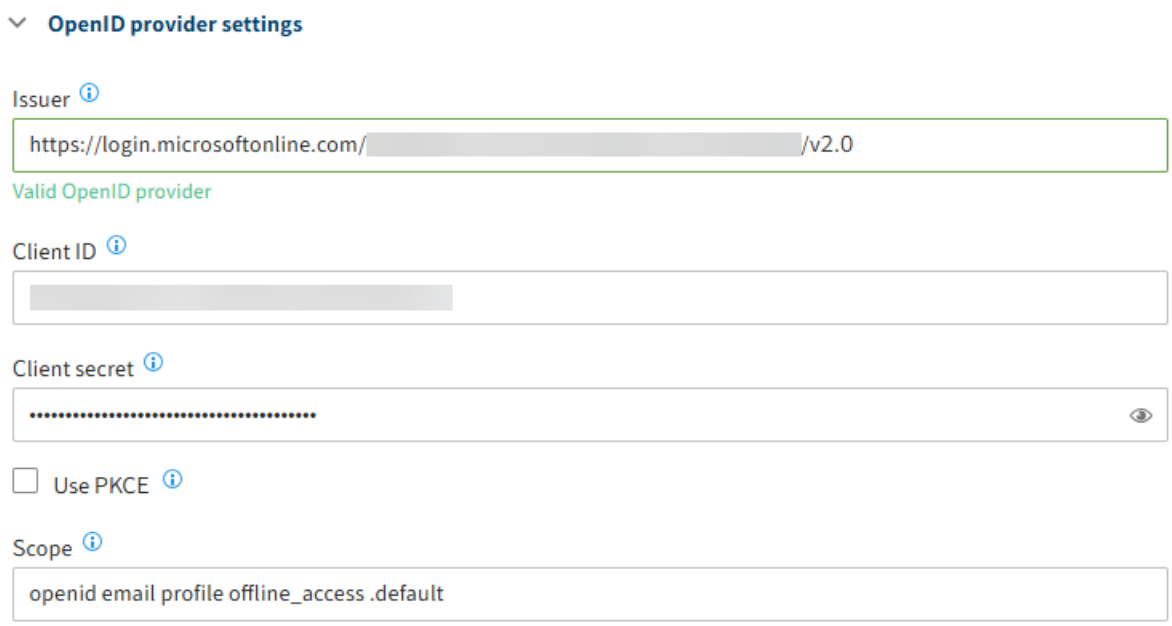
> **Important**
>
> Regularly renew the client secret before its validity expires.
>
> Once the client secret expires, it will no longer be possible to log on with ELO Modern Authentication. In this case, you have to use the Recovery URL.

1. Open the *Certificates & secrets* area in Microsoft Azure.
2. Select *New client secret*.

   The *Add a client secret* area appears.
3. Enter a short description for the client secret in the *Description* field.
4. Select a time frame for *Valid until*.
5. Confirm with *Add*.

   Microsoft Azure creates a client secret.
6.

Copy the client secret from the *Value* column.



Please note

Write down the value of the client secret immediately after you create it. This value is no longer shown in its entirety when you open the overview of secrets at a later point in time.

7. Enter the copied client secret on the ELO Modern Authentication configuration page under *Client secret*.
8. Save the settings with *Save*.

All the other fields can be left unchanged and only need to be adapted if required.

The registration in Microsoft Azure has been successfully configured.

Reverse proxies

ELO Modern Authentication is generally compatible with reverse proxies provided they send the *X-Forwarded* header.

Basics

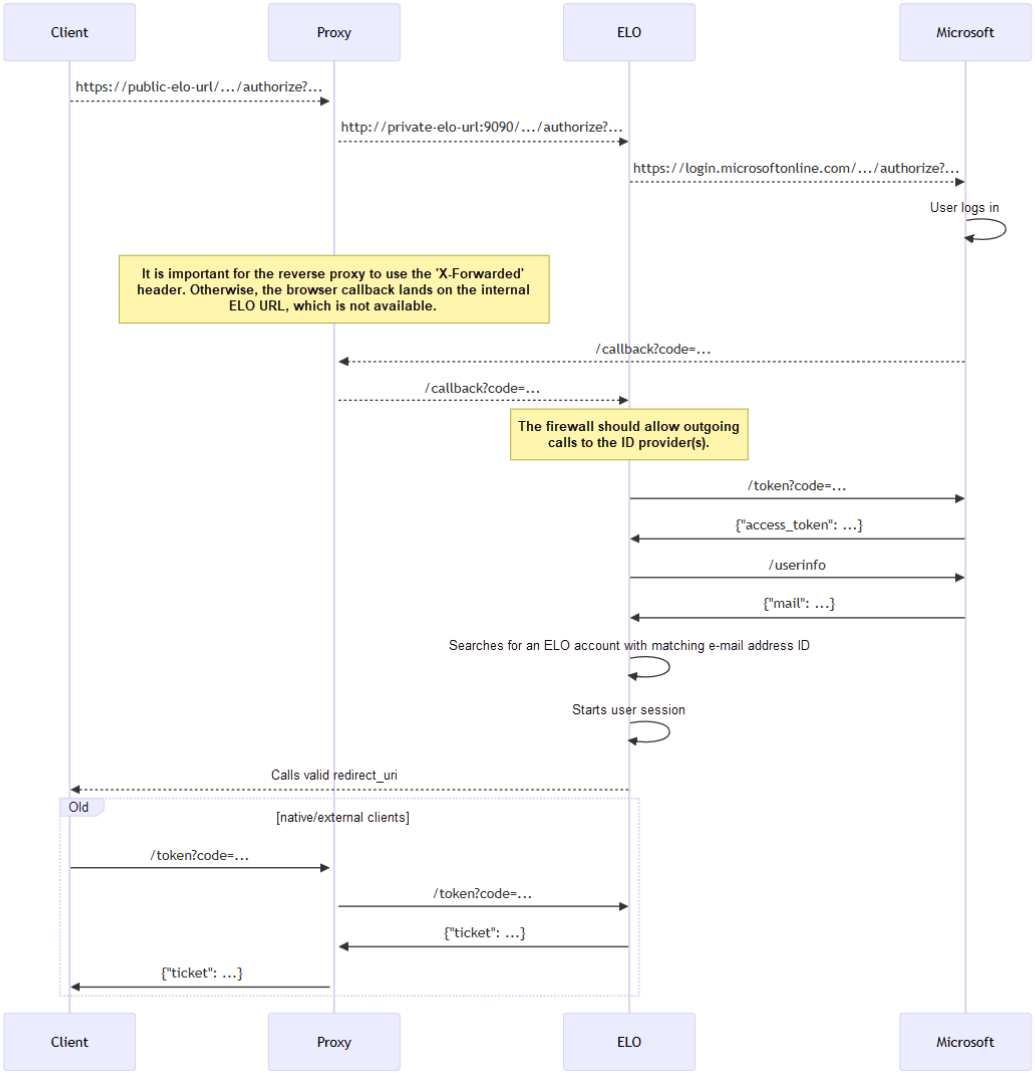
ELO Modern Authentication is operated as follows:

1. The user authenticates themselves using the identity provider or locally, depending on the use case.
2. After authentication, the browser returns to ELO.

Users are always assigned based on the configured e-mail address.

Process

The following plan shows the general process for authentication via ELO Modern Authentication and Microsoft Azure.



Example

```
https://example.org --proxy to-> http://private-network-vm:9090
```

In this example, the proxy should send the following header with every HTTP request:

```
X-Forwarded-Proto: https
X-Forwarded-Host: example.org
X-Forwarded-Port: 443
```

Otherwise, the *Auth2* plug-in is only aware of the local URL `http://private-network-vm:9090`, but not of the fact that the request has been forwarded. This results in incorrect redirects and other issues.

Check header settings

Some reverse proxies add this header automatically, and with others this is optional. For some reverse proxies, this has to be configured explicitly.

To check whether the header is configured correctly, log on the ELO Administration Console with your user name and password. If the logon process is not completed due to an incorrect redirect, you can access the Status page of ELO Modern Authentication:

```
https://<server>:<port>/ix-<repository>/plugin/de.elo.ix.plugin.rest/auth2/status
```

Under `request`, the status page indicates whether the proxy forwards the headers correctly and what the received URLs look like.


```
{
    "status": "RUNNING",
    "license": "ELO Digital Office Testversion\r\nNot for resale\r\n[2029-07-31]",
    "version": "23.05.000",
    "connection": {
        "language": "de",
        "country": "",
        "timeZone": "Europe/Berlin",
        "baseUrl": "http://          /repository/ix"
    },
    "ix": {
        "endpoint": "http://          /repository/ix",
        "instanceName": "ELO-BASE"
    },
    "user": {
        "guid": "                                                    ",
        "name": "Administrator",
        "timezone": "Europe/Berlin"
    },
    "request": {
        "url": "http://ix/repository/plugin/de.elo.ix.plugin.rest/auth2/status",
        "contextPath": "/repository",
        "dynamicBaseUrl": "http://          /repository",
        "proxyHeaders": {
            "Forwarded": null,
            "X-Forwarded-Host": "          ",
            "X-Forwarded-Proto": "http",
            "X-Forwarded-Port": "80"
        }
    }
}
```


1. Restart the ELO Indexserver.

Microsoft application proxy

If the message `Invalid redirect_uri/response_type` is output in the browser during authentication with ELO Modern Authentication (Auth2) via a Microsoft Entra application proxy, the following configuration can be changed in the Microsoft Azure Portal for successful authentication.

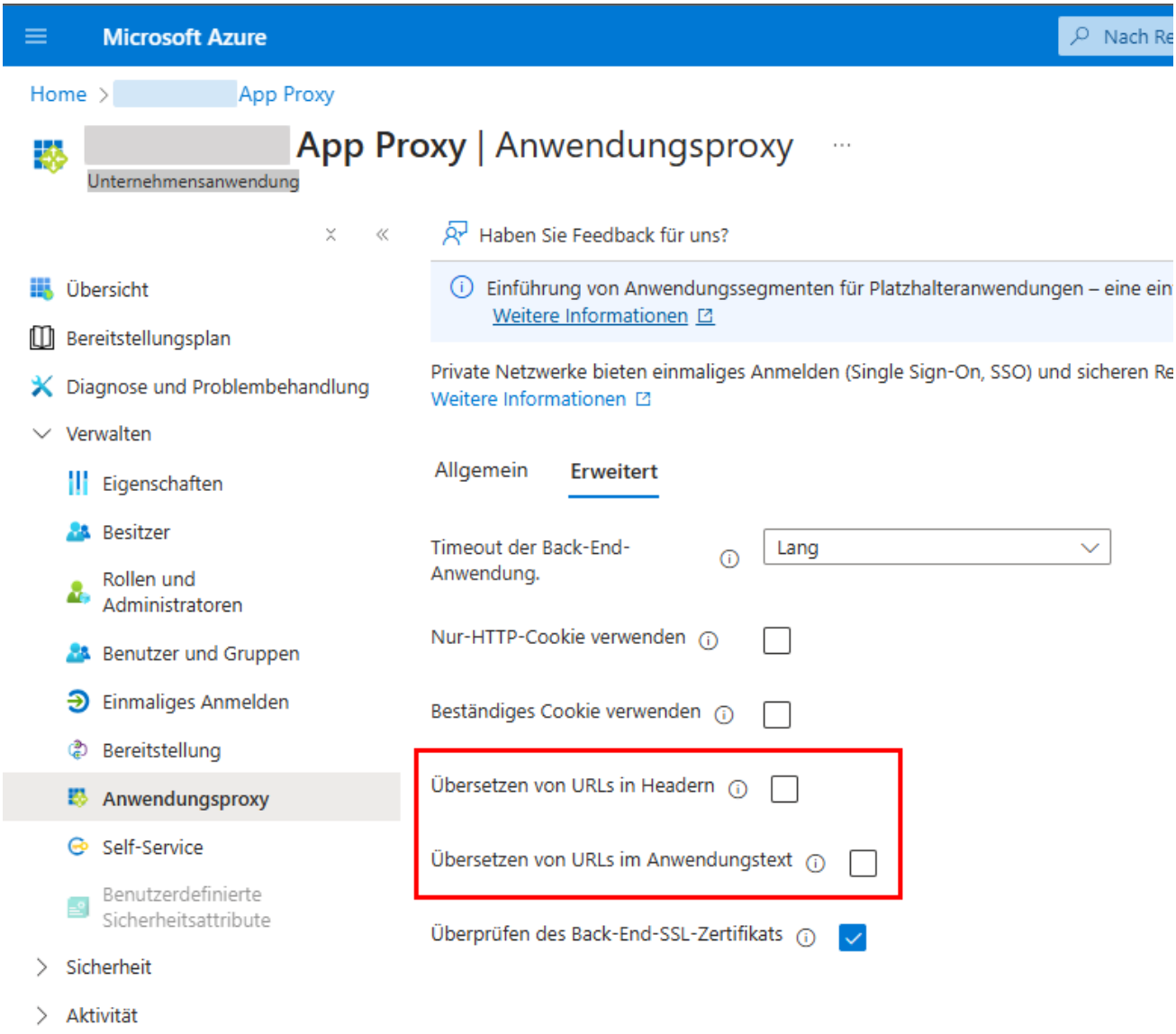
1. Sign in to the Microsoft Azure Portal: https://portal.azure.com/.
2.

Select *Microsoft Entra ID*.

3. In the sidebar, select *Organize* > *Enterprise Applications*.
4. Select the corresponding app.

   The app overview appears.

5. In the sidebar, select *Organize* > *Application Proxy*.
6. Select the *Advanced* tab.
7. Disable the options *Translate Urls in headers* and *Translate Urls in application body*.



Switch from ELOauth to ELO Modern Authentication

The previous ELOauth plug-in has been replaced with the introduction of ELO 25. ELO Modern Authentication (Auth2) is completely responsible for managing the authentication process, relying on state-of-the-art authentication standards.

New in ELO Modern Authentication:

- Central, standardized logon: Authentication is integrated fully into ELO, and is no longer an additional, separate module Thanks to the configuration of single sign-on (SSO), all clients automatically benefit from central authentication.
- Easier configuration via the ELO Administration Console Support for modern OpenID protocols ensures flexibility and compatibility.
- Individual branding: Customization options for the logon design, logo integration, and custom background images
- Compatibility with OAuth2: ELO Modern Authentication is based on OAuth2, the established standard, which is supported by providers such as Microsoft, Google, and Keycloak.
- Elimination of legacy protocols:With the introduction of ELO Modern Authentication, ELO is focusing on future-proof technologies.

  The new standard is based on *OpenID* and *OAuth2*, which platforms such as Microsoft, Google, and Keycloak also favor.

  > **Please note**
  >
  > The authentication protocol *SAML* is no longer supported.

Migration of the configuration

If the ELOauth plug-in is in use, several important steps are mandatory for migration.

Changes for the connection via other identity providers

Existing authentication settings have to be transferred to ELO Modern Authentication (Auth2).

If authentication via Microsoft Azure is configured, you will have to change the app in Microsoft Entra ID that you previously used for authentication with ELOauth. Alternatively, you can create a new app. Refer to the chapter Microsoft Azure configuration to learn how to configure the app.

Changes in the clients and web applications

With ELO Modern Authentication, no changes to the URLs are required for logging on the ELO clients and ELO apps.

Configure the URL for each logon profile or web application according to the standard format.

- For ELO Java Client and ELO Desktop Client:

```
http(s)://<server name>:<port>;/ix-<repository name>/ix
```

- For web applications (e.g. the ELO Web Client, ELO apps):

```
http(s)://<server name>:<port name>/ix-<repository name>/plugin/de.elo.ix.plugin.proxy/web
```

Troubleshooting

Check status

You can view the status of ELO Modern Authentication at the following URL:

`https://<server>:<port>/ix-<repository>/plugin/de.elo.ix.plugin.rest/auth2/status`

You have to be logged in to see the complete status information.

Recovery URL

If you can no longer log in the configuration as an administrator, there is a recovery URL. This is shown on the configuration page. Keep this URL secure.

The recovery URL schema is as follows:

`https://<Server>:<Port>/ix-<Repository>/plugin/auth2/rescue`

Re-enable access to the ELO system via ELO access data

You can re-enable access to the ELO system with ELO access data. This can be useful if you can no longer log in the configuration as an administrator or single sign-on via an OpenID provider is no longer possible.

In the ELO Indexserver configuration, set the option `loginWithEloCredentialsEnabled` to `true`.

For more information on this option, refer to the documentation ELO Indexserver > Basics > Indexserver Configure Options.

Troubleshooting via logs

If errors occur with ELO Modern Authentication, you can use logs to check them.

First, request a browser log. The browser log lists the redirects between ELO, the proxy, and the respective provider. Here, you can check whether there is an issue with redirects.

If the *Access denied* error message occurs, you can check the ELO Indexserver log to see what caused the error.

Redirect to wrong URL

If the system redirects to the wrong URL during authentication, you can configure reverse proxies. The figure in the chapter Reverse proxies > Basics shows the basic structure and changes to the URLs.

In the ELO Modern Authentication configuration, in the *Fixed domain* field you can set an address to redirect authentication to. For more information, refer to the chapter Configuration > Login Config.

OpenID provider configuration: 'Error: Connection timed out: connect' error message

This error message appears by the *Issuer* field if the ELO server is unable to reach the OpenID provider. There may be an issue with the firewall configuration.

If you use an Internet proxy (explicit web proxy), the ELO Application Server may need to be configured accordingly. You will have to configure the Internet proxy settings as *Tomcat Java Option* via the ELO Server Setup. For more information, refer to the documentation ELO Server > Custom Install > 'Application Servers' tab > ELO Server Engines.

Configuration for multiple repositories

If you use multiple repositories in one instance, they share a login configuration. This means if you configure an authentication method for one repository, this configuration applies to all other repositories in the same instances as well.

To apply changes to the authentication configuration in an Indexserver instance to all repositories, you will have to restart the other Indexserver instances.

If you want the repositories to use different login configurations, you will need separate ELO servers and ELO installations.