Konfiguration und Verwaltung

ELO Modern Authentication (Auth2)

Inhaltsverzeichnis

ELO Modern Authentication (Auth2)

Einstieg

ELO Modern Authentication (auch als Auth2 abgekürzt) ist der zentrale Authentifizierungspunkt für alle Clients.

Neben der traditionellen Anmeldung mit ELO Benutzername und Passwort ist auch die Anmeldung über Identitätsanbieter möglich, z. B. *Microsoft*, *Google* oder *Keycloak*.

Jeder Identitätsanbieter (Identity Provider; IdP) wird unterstützt, solange dieser das OpenID-Protokoll beachtet.

Voraussetzungen

- Aktuelle Versionen der ELO Clients
- Für ELO Benutzerkonten müssen die entsprechenden E-Mail-Adressen für die IdPs hinterlegt werden. Der Abgleich des IdP-Kontos mit dem ELO Konto erfolgt immer über die E-Mail-Adresse.

  > **Information**
  >
  > Sie können einstellen, dass bei der ersten Anmeldung automatisch ein ELO Konto erstellt wird, falls die verwendete E-Mail-Adresse noch nicht in ELO hinterlegt ist. Weitere Informationen dazu finden Sie im Kapitel Konfiguration > Benutzerzuordnung.

> **Beachten Sie**
>
> Neuere Versionen von ELO Modern Authentication ab ELO 25 können nicht mit älteren ELO Modulen und Clients verwendet werden.

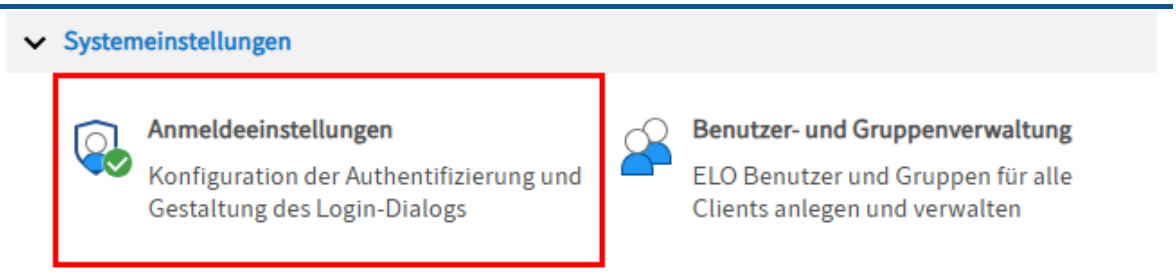
Im Folgenden erfahren Sie, wie Sie den Konfigurationsbereich für ELO Modern Authentication aufrufen.

Erster Start

Zunächst ist standardmäßig nur die ELO Anmeldung mit Kontoname und Passwort konfiguriert.

Um einen eigenen Identitätsanbieter zu konfigurieren, gehen Sie wie folgt vor:

1. Melden Sie sich mit einem Hauptadministrator-Konto (Konto mit dem Benutzerrecht *Hauptadministrator*) in der ELO Administration Console an.
2. Wählen Sie im Menüabschnitt *Systemeinstellungen* den Menüpunkt *Anmeldeeinstellungen*.



Die Konfigurationsseite für ELO Modern Authentication erscheint.

3. Über *OpenID-Anbieter hinzufügen* wählen Sie einen Anbieter aus, für den Sie eine Konfiguration vornehmen möchten.

> **Information**
>
> Möglich sind alle OpenID-kompatiblen Identitätsanbieter.

Wie Sie ELO Modern Authentication konfigurieren, erfahren Sie im Kapitel Konfiguration.

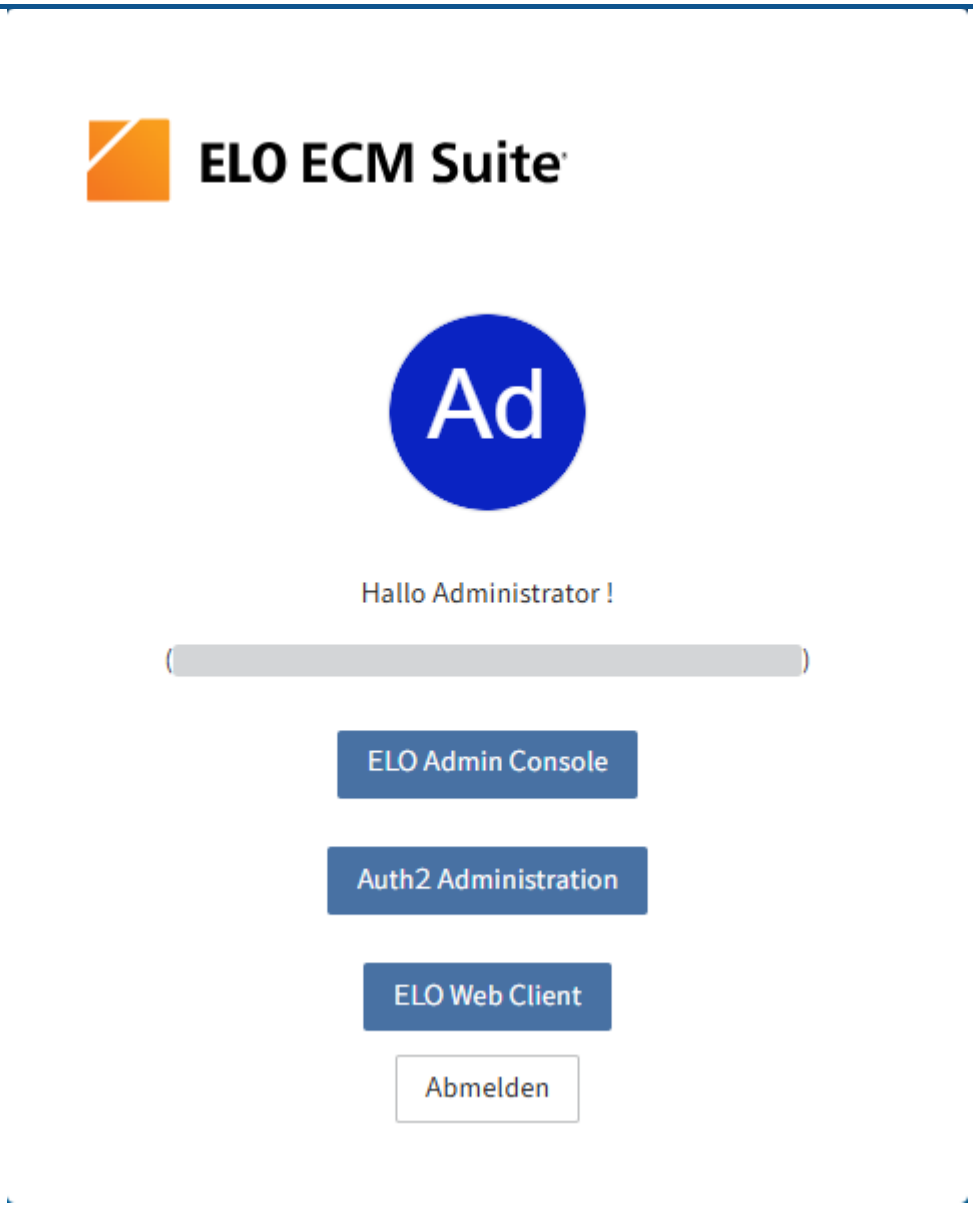
Alternativ: ELO Modern Authentication direkt aufrufen

Sie können die Anmeldekonfiguration für ELO Modern Authentication auch direkt aufrufen.

1. Rufen Sie die URL für ELO Modern Authentication auf.

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

2. Melden Sie sich mit einem Hauptadministrator-Konto an.



Eine Auswahlseite mit unterschiedlichen Anmeldemöglichkeiten erscheint.

3. Wählen Sie *Auth2 Administration*.

   Die Konfigurationsseite für ELO Modern Authentication erscheint.

Sie können nun die Konfiguration vornehmen.

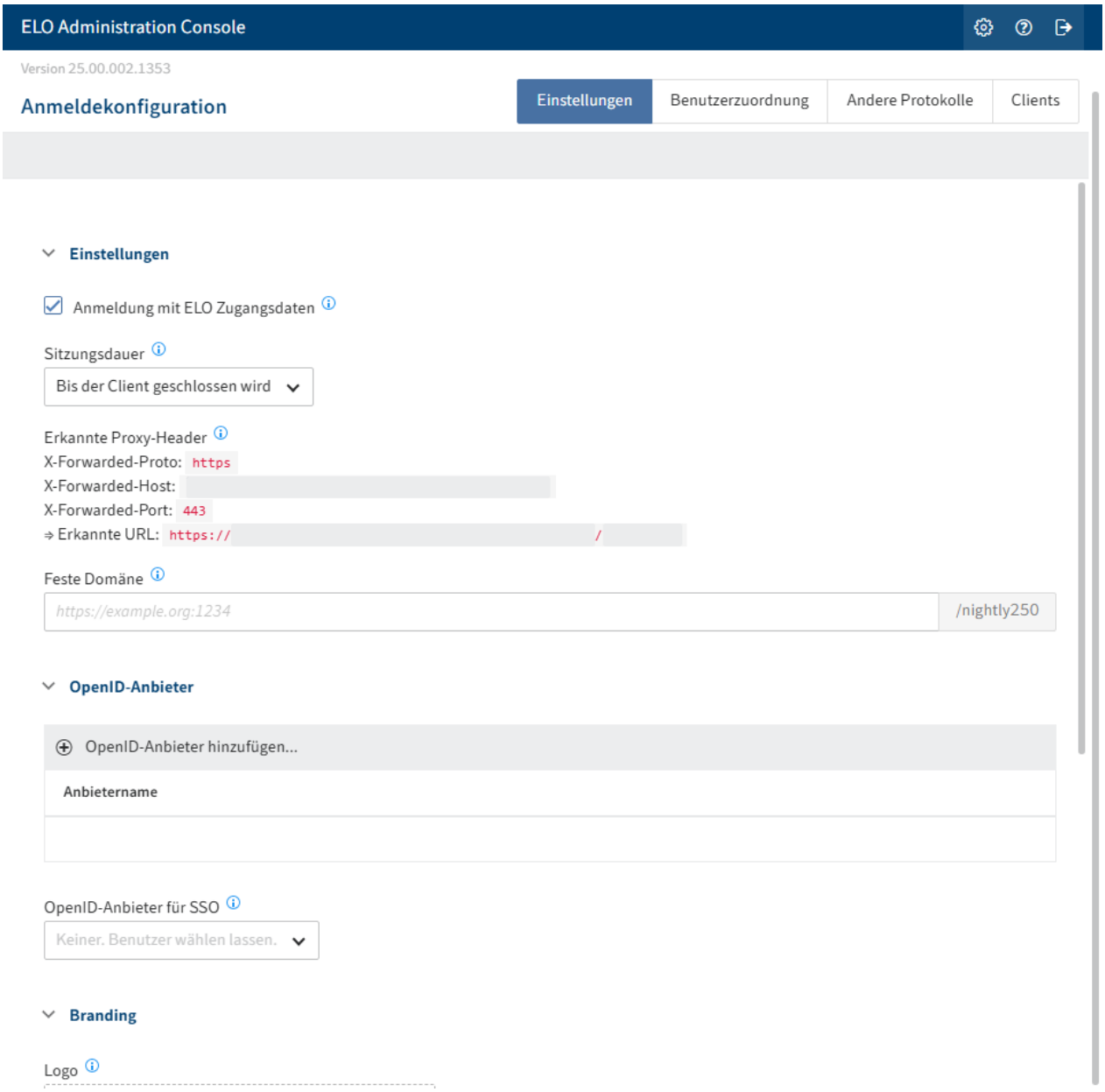
Konfiguration

Nachfolgend ist beschrieben, wie Sie ELO Modern Authentication konfigurieren.

> **Information**
>
> Wenn in einer ELO Instanz mehrere Repositorys angelegt sind, teilen sie sich eine Anmeldekonfiguration.

Bereich 'Einstellungen'

Sie können die Anmeldeseite von ELO Modern Authentication individuell an die jeweiligen Bedürfnisse des Unternehmens anpassen.



Im Bereich *Anmeldekonfiguration* haben Sie folgende Optionen:

-

Anmeldung mit ELO Zugangsdaten: Ist diese Option aktiviert, können Benutzer sich sowohl über einen Identitätsanbieter als auch "klassisch" mit ELO Kontonamen und Passwort anmelden.

Ist die Option deaktiviert, geht nur der Weg über den Identitätsanbieter. Ausgenommen davon sind Dienstkonten und Konten mit administrativen Rechten.

- Sitzungsdauer: Wählen Sie aus, wie lange eine Sitzung aufrechterhalten werden soll. Nach dem Ablauf dieser Sitzungsdauer muss man sich erneut anmelden.

  > **Information**
  >
  > Bei einem Neustart des ELO Indexservers werden die Sitzungen ebenfalls beendet.

- Erkannte Proxy-Header: Zeigt die Proxy-Header an, die von Reverse-Proxys und Load-Balancern gesendet werden sollten.

- Feste Domäne für Callbacks: Wenn Sie eine feste Domäne für die Anmeldung festlegen, laufen die Anmeldung und alle Weiterleitungen nur noch über diese Adresse ab. Dies kann mögliche Probleme bei der Weiterleitung lösen.

  Bleibt dieses Feld leer, werden die URLs dynamisch gemäß der HTTP-Anfrage bestimmt. Dies schließt auch die Informationen ein, die von *X-Forwarded*-Headern von Reverse Proxys und Load Balancern bereitgestellt werden.

  Falls Sie über verschiedene Domänen auf das Repository zugreifen möchten, z. B. über eine Intranet-URL oder eine externe URL, müssen Sie die Proxys entsprechend konfigurieren. Weitere Informationen dazu finden Sie im Kapitel Reverse Proxys.

- OpenID-Anbieter für SSO: Über das Drop-down-Menü können Sie einen Identitätsanbieter auswählen, um eine Anmeldung mit Single Sign-on zu triggern. Wenn hier kein Anbieter ausgewählt ist, werden im Anmeldedialog alle konfigurierten Anbieter angezeigt. In diesem Fall können Benutzer die Anmeldemethode selbst wählen.

Branding

Für das Branding können Sie Logos und Hintergrundbilder hochladen.

Möglich sind die gängigen webfähigen Bildformate. Die Bilder werden je nach Größe und Auflösung skaliert.

Über *Speichern* werden die Bilder übernommen und beim nächsten Aufruf der Anmeldeseite von ELO Modern Authentication angezeigt.

- Logo: Über dieses Feld können Sie ein individuelles Logo hochladen, was bei der Anmeldung auf dem Anmeldebereich angezeigt wird.

  Wird das Logo gelöscht, wird das ELO Logo angezeigt.

- Hintergrundbild: Über dieses Feld können Sie ein individuelles Hintergrundbild hochladen, was bei der Anmeldung hinter dem Anmeldebereich angezeigt wird.

  > **Information**

Empfohlen werden die Formate PNG und JPEG. Andere Formate wie SVG, WebP oder AVIF können im ELO Java Client möglicherweise nicht korrekt gerendert werden.

Die empfohlene Mindestauflösung ist 1920x1080. Die Dateigröße sollte kleiner als 1 MB sein, um eine schnelle Netzwerkübertragung zu ermöglichen.

Wird das Hintergrundbild gelöscht, wird ein Standardhintergrund angezeigt.

OpenID-Anbieter hinzufügen

Um die Anmeldung über einen oder mehrere Identitätsanbieter zu ermöglichen, müssen Sie diese zuvor konfigurieren.

Beachten Sie

Der OpenID-Anbieter muss vom ELO Server erreichbar sein. Dies erfordert ggf. Anpassungen der Firewall-Einstellungen.

Je nach Anbieter können einzelne Schritte variieren und unterschiedliche notwendig sein.

Nachfolgend zeigen wir den Ablauf in der Übersicht.

1. Wählen Sie *OpenID-Anbieter hinzufügen*.

   Ein Drop-down-Menü erscheint.

2. Wählen Sie den gewünschten Anbieter aus.

   Unterstützt werden:

   - Microsoft
   - Google
   - Keycloak
   - SAP
   - Salesforce
   - SmartWe
   - Other (Möglichkeit einen anderen OpenID-kompatiblen Identitätsanbieter anzubinden)

   Der Dialog *Bitte wählen Sie eine ID für den OpenID-Anbieter* erscheint. Der Name ist je nach Auswahl vorausgefüllt.

   Optional: Ändern Sie den Namen für die Konfiguration.

3. Bestätigen Sie mit *OK*.

   Der entsprechende Konfigurationsbereich erscheint.

4. Tragen Sie die für den Anbieter notwendigen Informationen ein.

Alternativ: Wählen Sie *Beim Anbieter registrieren*, falls Sie noch keine Registrierung beim gewünschten OpenID-Anbieter angelegt haben. Übertragen Sie anschließend die Daten der Registrierung in die Konfiguration.

> **Information**
>
> Im Kapitel Konfiguration Microsoft Azure wird als Beispiel die Einbindung über Microsoft Azure gezeigt.
>
> Je nach Anbieter können einzelne Schritte abweichen.
>
> Außerdem müssen je nach Anbieter unterschiedliche Vorarbeiten geleistet werden.

Optional: Sie können die Option *Versteckt* aktivieren, um den Identitätsanbieter im Anmeldedialog auszublenden. Er kann jedoch weiterhin von Apps oder Integrationen für die Anmeldung genutzt werden.

5. Speichern Sie die Einstellungen.

Test

Über *Anmeldung testen* können Sie die Einstellungen überprüfen. Es erscheint ein Pop-up-Fenster, welches die Anmeldeseite simuliert. Bei der Anmeldung über den konfigurierten Anbieter wird eine Anmeldung mit dem aktuell verwendeten Konto versucht.

> **Beachten Sie**
>
> Der Abgleich erfolgt über die E-Mail-Adresse. Daher muss die E-Mail-Adresse, die beim Anbieter verwendet wird, auch im ELO Konto im Feld *E-Mail* hinterlegt sein.

Konfiguration Single Sign-on

Sie können einstellen, dass die Anmeldung in den ELO Clients per Single Sign-on (SSO) ausschließlich über einen konfigurierten Identitätsanbieter abläuft.

Hierfür können Sie im Bereich Einstellungen im Drop-down-Menü *OpenID-Anbieter für SSO* einen OpenID-Anbieter auswählen, der für die Anmeldung genutzt werden soll.

Alternativ können Sie die Option *Anmeldung mit ELO Zugangsdaten* deaktivieren, falls nur ein weiterer Identitätsanbieter konfiguriert ist.

Bereich 'Benutzerzuordnung'

Im Bereich *Benutzerzuordnung* können Sie eine Methode konfigurieren, die beim Abgleich von ELO Konten mit den Konten beim Identitätsanbieter angewendet werden soll.

Folgende Mechanismen stehen zur Verfügung:

- Benutzer muss in ELO existieren
- ELO Benutzer sofort erstellen: Legt bei der Anmeldung in ELO ein neues Konto an, sofern zur eingegebenen E-Mail-Adresse noch kein ELO Konto vorhanden ist. Im Feld *E-Mail-Domäneneinschränkung* können Sie festlegen, welche Domänen für die Anmeldung zugelassen werden sollen.
- Flow aufrufen: Ruft einen Flow auf, um bei der Anmeldung in ELO automatisch Konten anzulegen oder zu aktualisieren. Nachdem der Flow ausgeführt wurde, wird der Benutzer in ELO angemeldet, sofern das Konto in ELO vorhanden ist. Um diesen Mechanismus zu nutzen, müssen Sie zuvor einen passenden Flow konfigurieren.

  Der Flow bezieht den gesamten OpenID *UserInfo*-Datensatz vom OpenID-Anbieter. Bei Microsoft kann dieser beispielsweise wie folgt aussehen:

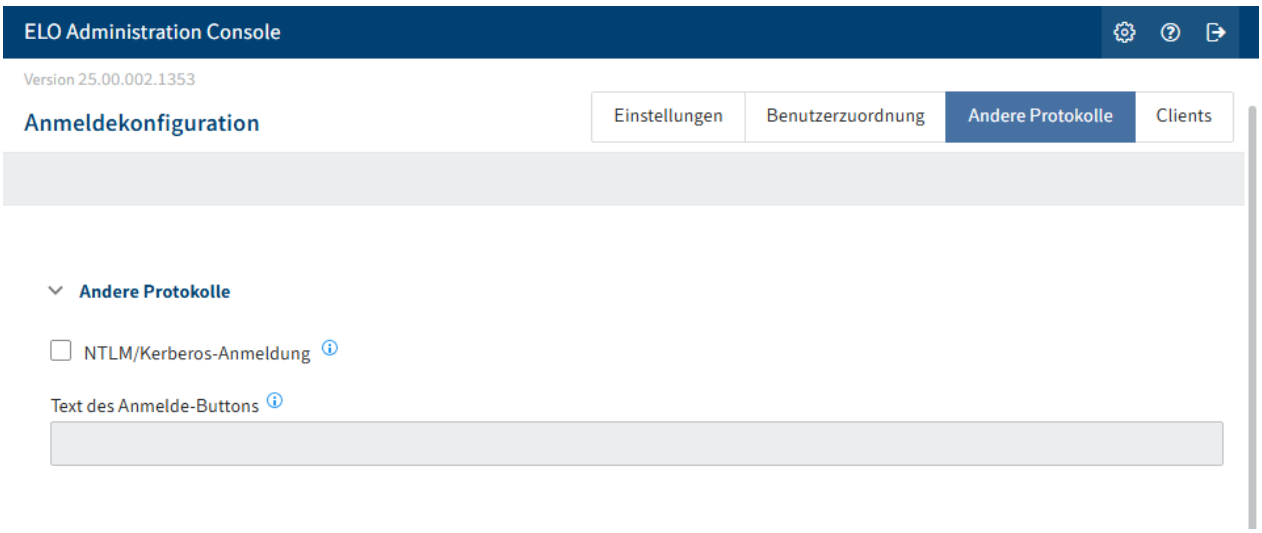
  ```
  {
      "sub": "<Microsoft Benutzer-ID>",
      "name": "Luise Lind",
      "family_name": "Lind",
      "given_name": "Luise",
      "picture": "https://graph.microsoft.com/v1...;value",
      "email": "l.lind@example.com"
  }
  ```

  Die Payloads unterscheiden sich je nach genutztem OpenID-Anbieter, beinhalten aber fast immer die Parameter `"sub"`, `"email"` und `"name"`.
- Registrierte Funktion aufrufen (Legacy): Kann Konten-Mappings übernehmen und bei der Anmeldung in ELO ein neues Konto erstellen oder ein bestehendes aktualisieren.

Weitere Informationen zu registrierten Funktionen finden Sie in der Dokumentation zum ELOauth Plug-in in den Kapiteln Bestehende Implementierungen > Registered Function und Manuelle Konfiguration > OAuth2.

Bereich 'Andere Protokolle'

Der Bereich *Andere Protokolle* ist für Systeme gedacht, die NTLM oder Kerberos einsetzen.



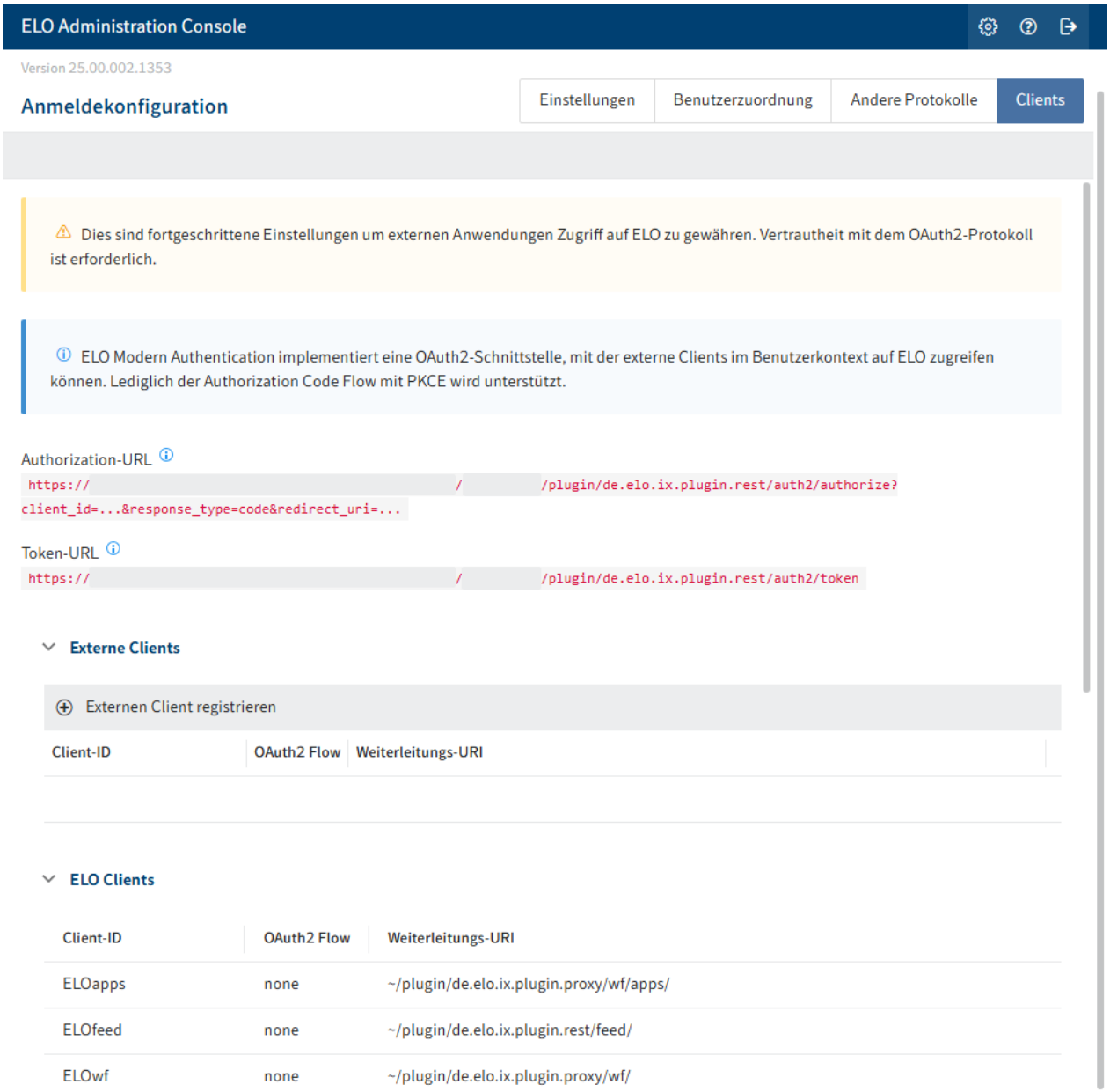
Beachten Sie

Die Nutzung dieser Protokolle wird nicht empfohlen. Aus Kompatibilitätsgründen wird diese Option dennoch angeboten.

Wichtige Hinweise

- *NTLM* wird von Microsoft seit Juni 2024 nicht mehr weiterentwickelt und gilt als überholt (deprecated).
- Das Authentifizierungsprotokoll *SAML* wird nicht mehr unterstützt.
- *Kerberos* und *NTLM* funktionieren nicht im ELO Java Client mit JCNN (Standard), wenn ein Load-Balancer-Modus vorgeschaltet ist. Ist in der Registry der Wert `ASF` eingestellt, funktionieren die Pakete der Business Solutions nicht.
- *Kerberos* und *NTLM* funktionieren nur in Intranet-Umgebungen, in denen die Clients vom jeweiligen Unternehmen kontrolliert werden.

Bereich 'Clients'



In diesem Bereich finden Sie fortgeschrittene Einstellungen zum Zugriff auf das ELO System sowie eine Übersicht der URLs und URIs für ELO Clients und Module.

Unter *Externe Clients* können Sie ein eigenes externes Portal oder eine eigene Anwendung mit ELO verbinden.

> **Beachten Sie**
>
> Hierfür sind fortgeschrittene Kenntnisse des Protokolls *OAuth 2.0* erforderlich. Weitere Informationen dazu finden Sie auf den Websites OAuth 2.0 Simplified und OAuth 2.0.

Konfiguration Microsoft Azure

Dieses Kapitel zeigt die Einrichtung der Anmeldung über Microsoft Azure.

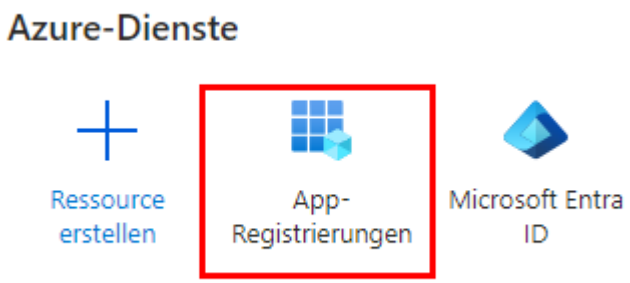
> **Information**
>
> Durch die Konfiguration der Anmeldung über Microsoft Azure können Sie auch die Funktion *Nach OneDrive auschecken* in den ELO Clients aktivieren.
>
> Weitere Informationen zu dieser Funktion finden Sie in der Dokumentation ELO mit Microsoft OneDrive verbinden sowie in den Benutzerdokumentationen:
>
> - ELO Java Client
> - ELO Web Client
> - ELO Desktop Client
>
> Um diese Funktion zu aktivieren, folgen Sie den Anweisungen in diesem Kapitel und beachten Sie die Informationen im Abschnitt Berechtigungen vergeben.

App registrieren

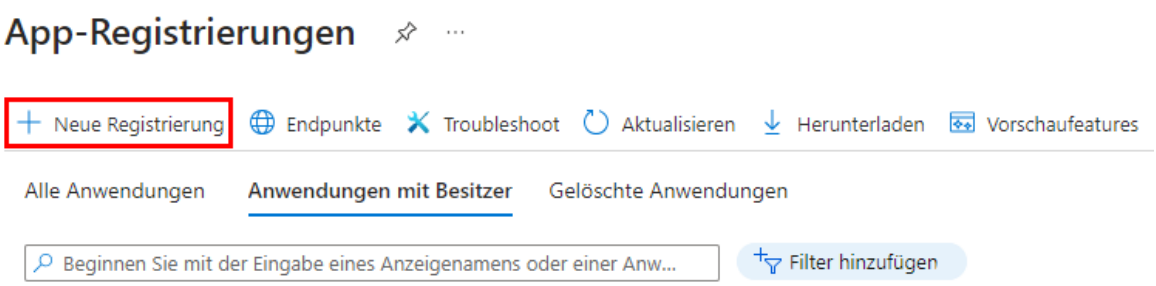
Zunächst müssen Sie eine App in Microsoft Azure registrieren.

> **Beachten Sie**
>
> Die grundlegende Einrichtung einer Microsoft-Azure-Umgebung sowie der Abschluss entsprechender Abonnements werden an dieser Stelle vorausgesetzt und sind nicht Teil dieser Dokumentation.

1. Melden Sie sich als Benutzer mit administrativen Rechten in Microsoft Azure an.



2. Öffnen Sie den Bereich *App-Registrierungen*.



3. Wählen Sie *Neue Registrierung*.

   Die Seite *Anwendung registrieren* erscheint.

4. Tragen Sie einen Namen für die App ein. Sie können diesen frei wählen.

   Beispiel: ELOauth2

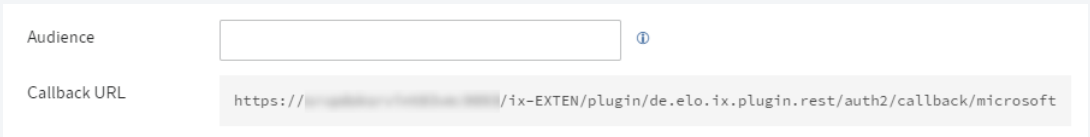
5. Wählen Sie bei *Unterstützte Kontotypen* die Option *Nur Konten in diesem Organisationsverzeichnis (nur <Name des Mandanten> – einzelner Mandant)* aus.

6. Wählen Sie bei *Umleitungs-URI (optional)* die Option *Web* aus.

7. Tragen Sie eine aus dem Internet erreichbare URL nach folgendem Schema ein:

   `https://<Server-Adresse>/ix-<Repository>/plugin/de.elo.ix.plugin.rest/auth2/callback/microsoft`

   Information

   Sie erhalten diese URL auch über die Konfigurationsseite von ELO Modern Authentication unter *Callback URL*.

8. Wählen Sie *Registrieren*.

   Die App wird in Microsoft Azure registriert.

Berechtigungen vergeben

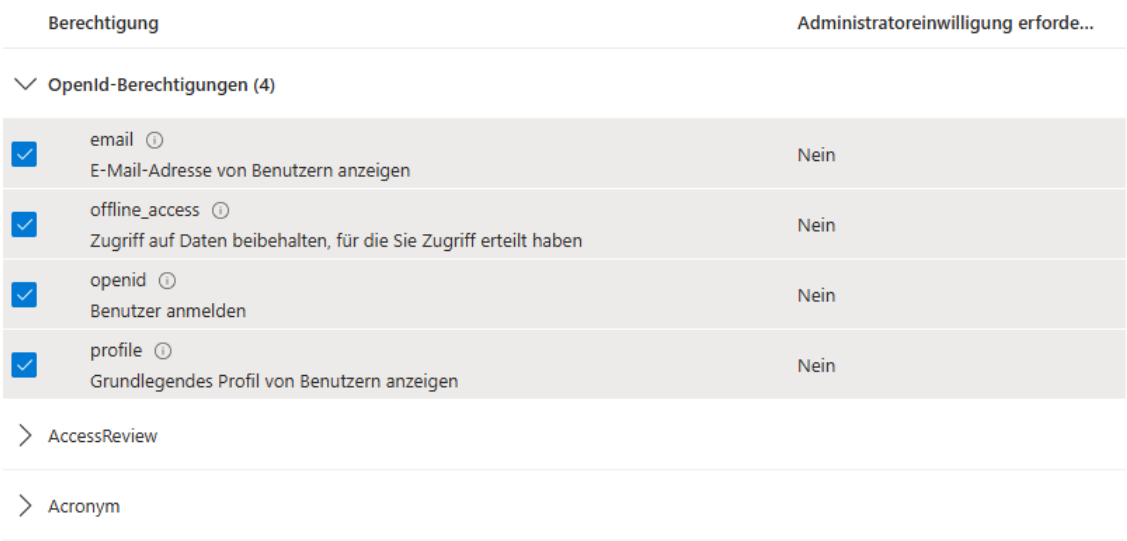
Sobald die App registriert ist, können Sie die benötigten Berechtigungen vergeben.

1. Öffnen Sie den Bereich *API-Berechtigungen*.

2. Wählen Sie *Berechtigungen hinzufügen*.

   Der Bereich *API-Berechtigungen anfordern* erscheint.

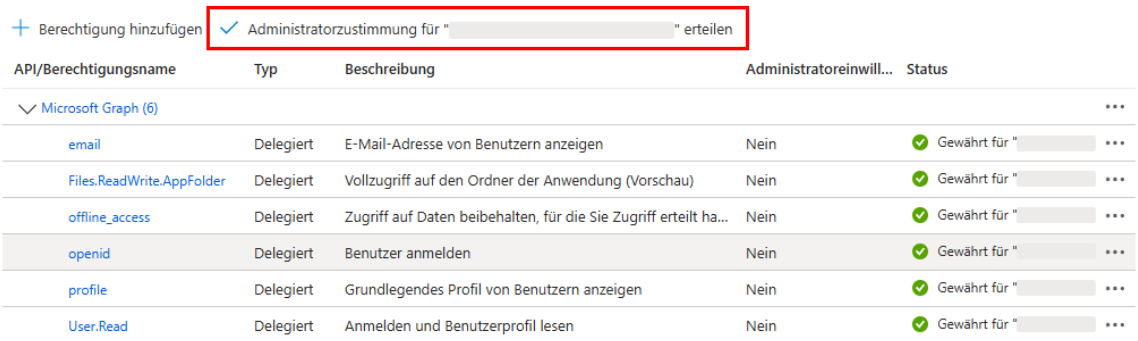
3. Wählen Sie *Microsoft Graph*.



4. Fügen Sie folgende delegierten Berechtigungen hinzu:
   - email
   - Files.ReadWrite.AppFolder
   - offline_access
   - openid
   - profile
   - User.Read

> **Information**
>
> Die Berechtigung *Files.ReadWrite.AppFolder* aktiviert die Funktion *Nach OneDrive auschecken* in den ELO Clients.

5. Bestätigen Sie mit *Berechtigungen hinzufügen*.



6. Wählen Sie *Administratorzustimmung für <Mandant> erteilen*.

   Der Abfrage-Dialog *Bestätigung der Administratoreinwilligung* erscheint.

7. Bestätigen Sie mit *Ja*.

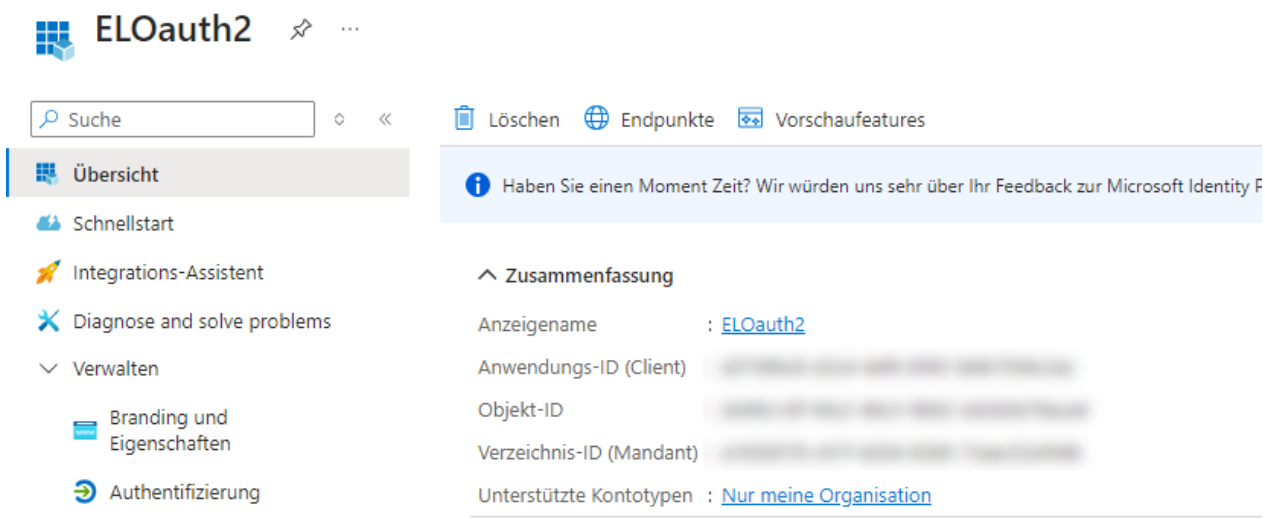
   Die Berechtigungen werden hinzugefügt.

8. Fügen Sie in der Konfigurationsseite von ELO Modern Authentication im Feld *Scope* folgende Werte ein:

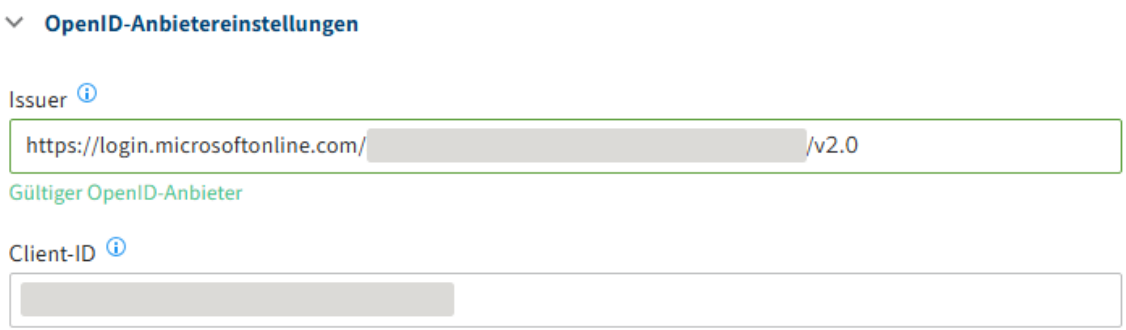
```
openid email profile offline_access .default
```

Informationen in Konfiguration übertragen

Nachdem die App registriert und mit Berechtigungen versehen ist, können Sie die Informationen in die Konfigurationsseite von ELO Modern Authentication übertragen.



1. Öffnen Sie in Microsoft Azure den Bereich *Übersicht*.
2. Kopieren Sie den Wert bei *Anwendungs-ID (Client)*.
3. Fügen Sie den Wert auf der Konfigurationsseite von ELO Modern Authentication unter *Client ID* ein.



   Optional: Falls Sie ELO Desktop Client und/oder ELO Bot einsetzen, fügen Sie den kopierten Wert zusätzlich unter *Audience* ein.

4. Kopieren Sie aus Microsoft Azure den Wert bei *Verzeichnis-ID (Mandant)*.
5. Fügen Sie den Wert auf der Konfigurationsseite von ELO Modern Authentication unter *Issuer* an Stelle des Platzhalters `{tenant}` ein.
6. Speichern Sie die Einstellungen über *Speichern*.

Geheimer Clientschlüssel (Secret)

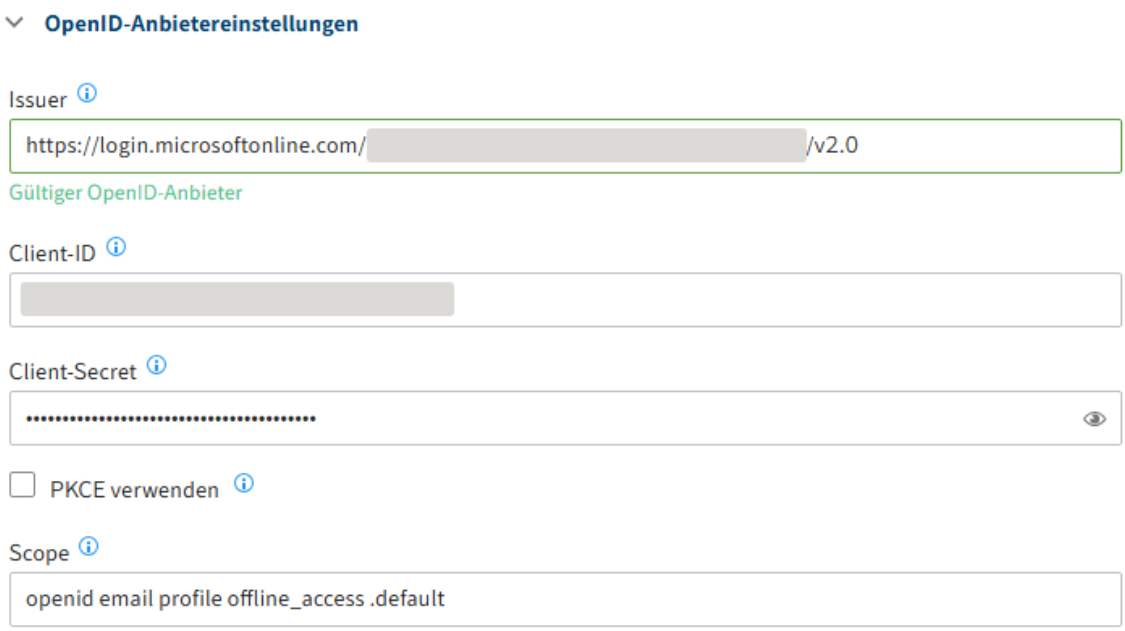
Damit die Verbindung zur Microsoft-Azure-App funktioniert, benötigt diese noch einen geheimen Clientschlüssel (Secret). Dieser muss in der Konfigurationsseite von ELO Modern Authentication eingetragen werden.

> **Achtung**
>
> Erneuern Sie regelmäßig den geheimen Clientschlüssel, bevor seine Gültigkeitsdauer abläuft.
>
> Ist der geheime Clientschlüssel abgelaufen, scheitert die Anmeldung über ELO Modern Authentication. In diesem Fall müssen Sie die Recovery-URL nutzen.

1. Öffnen Sie in Microsoft Azure den Bereich *Zertifikate & Geheimnisse*.
2. Wählen Sie *Neuer geheimer Clientschlüssel*.

   Der Bereich *Geheimen Clientschlüssel hinzufügen* erscheint.
3. Tragen Sie in das Feld *Beschreibung* eine kurze Beschreibung für den geheimen Clientschlüssel ein.
4. Wählen Sie bei *Gültig bis* einen Zeitraum aus.
5. Bestätigen Sie mit *Hinzufügen*.

   Microsoft Azure erstellt einen geheimen Clientschlüssel.
6. Kopieren Sie den Clientschlüssel aus der Spalte *Wert*.



> **Beachten Sie**

> Notieren Sie sich den Wert des geheimen Clientschlüssels unmittelbar nach dem Erstellen. Dieser Wert wird nicht mehr vollständig angezeigt, wenn Sie die Übersicht der Geheimnisse zu einem späteren Zeitpunkt erneut aufrufen.

7. Fügen Sie den kopierten Clientschlüssel in der Konfigurationsseite von ELO Modern Authentication unter *Client secret* ein.

8. Speichern Sie die Einstellungen über *Speichern*.

Alle weiteren Felder können im Standardfall unbearbeitet bleiben und müssen nur bei Bedarf angepasst werden.

Die Anmeldung über Microsoft Azure ist erfolgreich konfiguriert.

Reverse Proxys

ELO Modern Authentication ist grundsätzlich mit Reverse Proxys kompatibel, sofern diese die *X-Forwarded*-Header senden.

Grundlagen

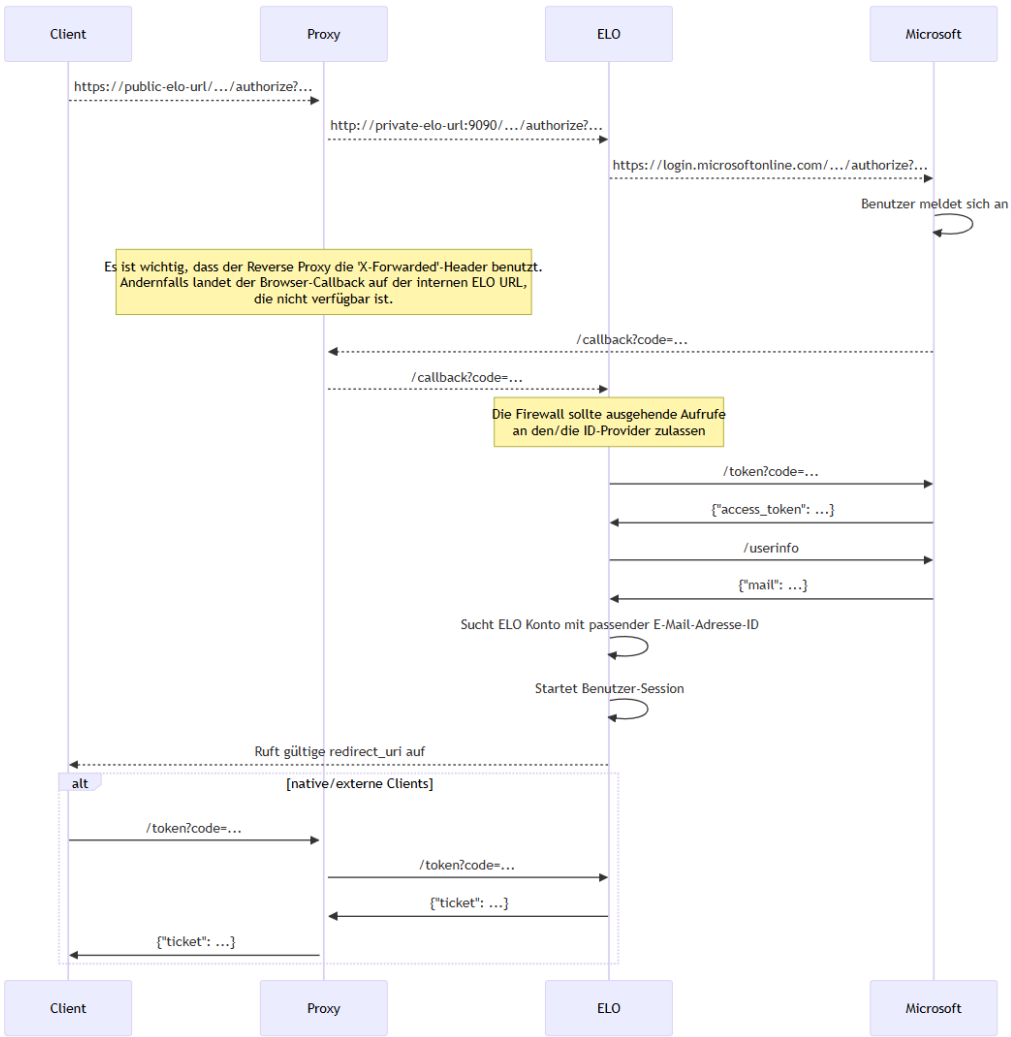
Der grundlegende Betrieb von ELO Modern Authentication verläuft wie folgt:

1. Der Benutzer authentifiziert sich über den Identitätsanbieter oder lokal, je nach Anwendungsfall.
2. Der Browser wird nach der Authentifizierung zurück zu ELO geleitet.

Die Zuordnung der Benutzer erfolgt immer anhand der hinterlegten E-Mail-Adresse.

Ablauf

Der folgende Ablaufplan zeigt den prinzipiellen Ablauf der Anmeldung über ELO Modern Authentication und Microsoft Azure.



Beispiel

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

In diesem Beispiel sollte der Proxy bei jeder HTTP-Anfrage die folgenden Header senden:

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

Andernfalls weiß das Plug-in *Auth2* nur von der lokalen URL `http://private-network-vm:9090`, aber nicht, dass die Anfrage weitergeleitet wurde. Das führt zu falschen Weiterleitungen und anderen Problemen.

Überprüfung der Header-Einstellungen

Einige Reverse Proxys fügen diese Header automatisch hinzu, bei anderen ist dies optional. Bei manchen Reverse Proxys muss dies explizit konfiguriert werden.

Um zu überprüfen, ob die Header korrekt eingestellt sind, melden Sie sich mit Ihrem Benutzernamen und Passwort in der ELO Administration Console an. Auch wenn der Anmeldevorgang aufgrund einer falschen Weiterleitung am Ende nicht abgeschlossen wird, können Sie auf die Statusseite von ELO Modern Authentication zugreifen:

```
https://<Server>:<Port>/ix-<Repository>/plugin/de.elo.ix.plugin.rest/auth2/status
```

Die Statusseite zeigt unter `request` an, ob der Proxy die Header korrekt weiterleitet und wie die empfangenen URLs aussehen.

```
{
    "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"
        }
    }
}
```

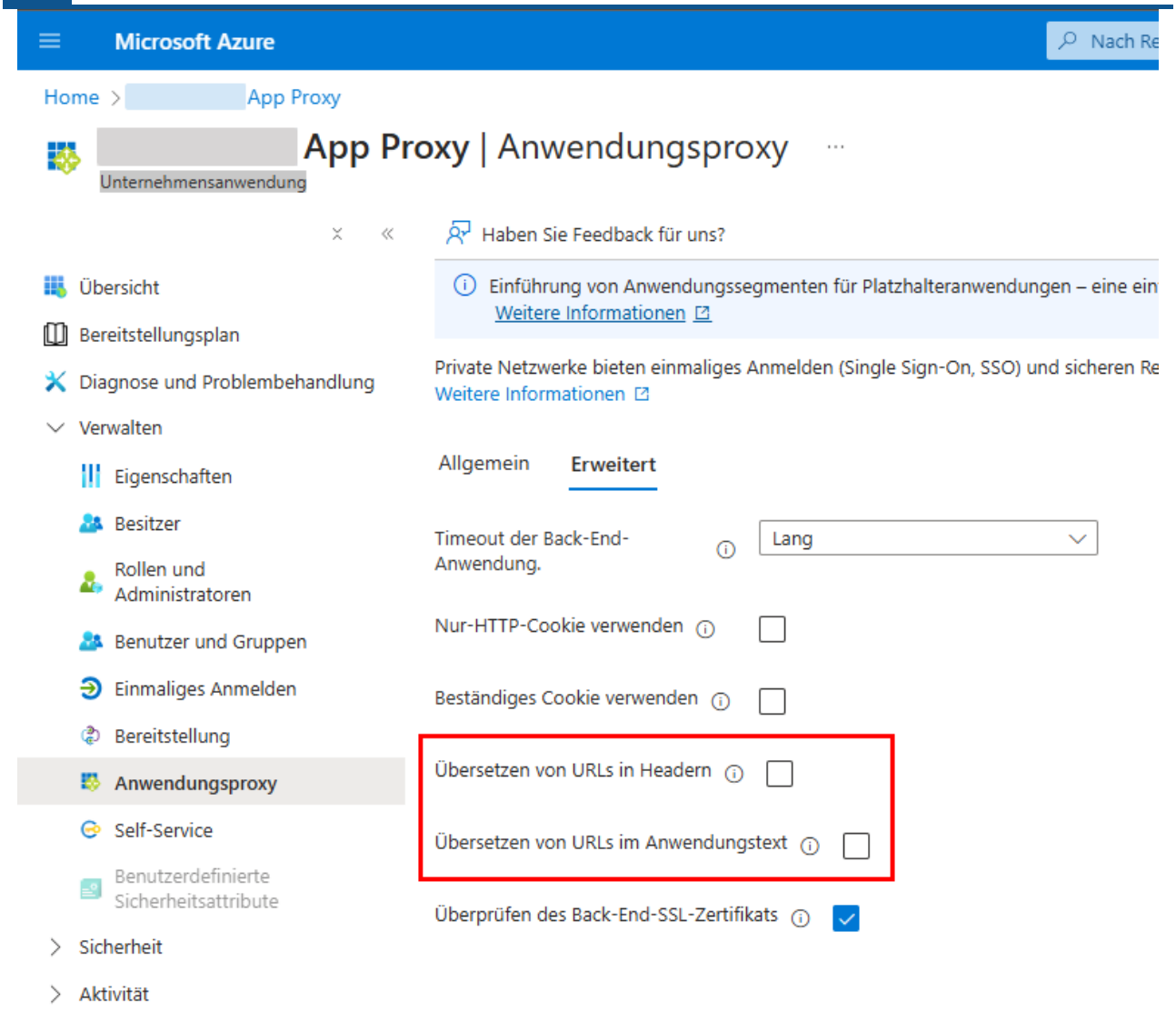

1. Starten Sie den ELO Indexserver neu.

Microsoft Anwendungsproxy

Wird bei der Anmeldung mit ELO Modern Authentication (Auth2) über ein Microsoft-Entra-Anwendungsproxy (App Proxy) die Meldung `Invalid redirect_uri / response_type` im Browser ausgegeben, kann folgende Konfiguration im Microsoft-Azure-Portal angepasst werden, damit die Anmeldung erfolgreich durchgeführt wird.

1. Melden Sie sich am Microsoft Azure Portal an: https://portal.azure.com/
2. Wählen Sie *Microsoft Entra ID*.
3. Wählen Sie in der Sidebar *Verwalten* > *Unternehmensanwendungen*.
4. Wählen Sie die entsprechende App aus.

   Die Übersicht für die App erscheint.
5. Wählen Sie in der Sidebar *Verwalten* > *Anwendungsproxy*.
6. Wählen Sie den Tab *Erweitert*.
7. Deaktivieren Sie die Optionen *Übersetzen von URLs in Headern* und *Übersetzen von URLs im Anwendungstext*.


Microsoft Azure
Nach Re
Home
App Proxy
App Proxy | Anwendungsproxy
Unternehmensanwendung
Haben Sie Feedback für uns?
Übersicht
Bereitstellungsplan
Diagnose und Problembehandlung
Verwalten
Eigenschaften
Besitzer
Rollen und Administratoren
Benutzer und Gruppen
Einmaliges Anmelden
Bereitstellung
Anwendungsproxy
Self-Service
Benutzerdefinierte Sicherheitsattribute
Sicherheit
Aktivität
Einführung von Anwendungssegmenten für Platzhalteranwendungen – eine ein
Weitere Informationen
Private Netzwerke bieten einmaliges Anmelden (Single Sign-On, SSO) und sicheren Re
Weitere Informationen
Allgemein
Erweitert
Timeout der Back-End-Anwendung.
Lang
Nur-HTTP-Cookie verwenden
Beständiges Cookie verwenden
Übersetzen von URLs in Headern
Übersetzen von URLs im Anwendungstext
Überprüfen des Back-End-SSL-Zertifikats

Wechsel von ELOauth zu ELO Modern Authentication

Mit der Einführung von ELO 25 wird das bisherige Plug-in ELOauth abgelöst. ELO Modern Authentication (Auth2) übernimmt vollständig die Verwaltung des Anmeldeprozesses und setzt dabei auf modernste Standards in der Authentifizierung.

> **Achtung**
>
> ELOauth ist ab ELO 25 nicht mehr im ELO Server Setup enthalten und wird nicht mehr unterstützt. Beim Upgrade auf ELO 25 wird das ELOauth Plug-in entfernt. Die Anmeldung über ELOauth ist danach nicht mehr möglich.
>
> Konfigurieren Sie daher bereits vor dem Upgrade die Anmeldung über ELO Modern Authentication.

Neuerungen in ELO Modern Authentication:

- Zentrales und einheitliches Login: Die Authentifizierung ist vollständig in ELO integriert und kein separates Zusatzmodul mehr. Durch die Konfiguration von Single Sign-on (SSO) profitieren alle Clients automatisch von der zentralen Anmeldung.
- Einfachere Konfiguration über die ELO Administration Console. Die Unterstützung moderner OpenID-Protokolle sorgt für Flexibilität und Kompatibilität.
- Individuelles Branding: Anpassungsmöglichkeiten für das Login-Design wie Logo-Integration und individuelle Hintergrundbilder
- Kompatibilität mit OAuth2: ELO Modern Authentication basiert auf OAuth2, dem etablierten Standard, der von Anbietern wie Microsoft, Google und Keycloak unterstützt wird.
- Vermeidung veralteter Protokolle: Mit der Einführung von Modern Authentication setzt ELO auf zukunftssichere Technologien.

  Der neue Standard setzt auf *OpenID* und *OAuth2*, die auch von Plattformen wie Microsoft, Google und Keycloak bevorzugt werden.

  > **Beachten Sie**
  >
  > Das Authentifizierungsprotokoll *SAML* wird nicht mehr unterstützt.

Migration der Konfiguration

Wenn das Plug-in ELOauth im Einsatz ist, sind einige wichtige Schritte für die Migration zu beachten.

Anpassungen für die Verbindung über andere Identitätsanbieter

Bestehende Authentifizierungseinstellungen müssen auf ELO Modern Authentication (Auth2) übertragen werden.

Falls die Anmeldung über Microsoft Azure konfiguriert ist, müssen Sie in Microsoft Entra ID die App anpassen, die Sie bisher für die Anmeldung mit ELOauth genutzt haben. Alternativ können Sie eine neue App erstellen. Wie Sie die App konfigurieren, lesen Sie im Kapitel Konfiguration Microsoft Azure.

Anpassungen in den Clients und Web-Anwendungen

Durch ELO Modern Authentication sind keine Anpassungen der URLs für die Anmeldung über die ELO Clients und ELO Apps erforderlich.

Stellen Sie für die jeweiligen Anmeldeprofile oder Web-Anwendungen die URL nach dem Standardschema ein.

- Für ELO Java Client und ELO Desktop Client:

```
http(s)://<Servername>:<Port>/ix-<Repository-Name>/ix
```

- Für Web-Anwendungen (z. B. ELO Web Client, ELO App):

```
http(s)://<Servername>:<Port>/ix-<Repository-Name>/plugin/de.elo.ix.plugin.proxy/web/
```

Troubleshooting

Status prüfen

Den Status von ELO Modern Authentication können Sie mit der folgenden URL einsehen:

`https://<Server>:<Port>/ix-<Repository>/plugin/de.elo.ix.plugin.rest/auth2/status`

Sie müssen angemeldet sein, um die vollständigen Statusinformationen anzuzeigen.

Recovery-URL

Falls Sie sich nicht mehr als Administrator in der Konfiguration anmelden können, gibt es eine Recovery-URL. Diese wird Ihnen auf der Konfigurationsseite angezeigt. Speichern Sie diese URL an einem sicheren Ort.

Die Recovery-URL folgt diesem Schema:

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

Zugang zum ELO System über ELO Zugangsdaten reaktivieren

Sie können den Zugang zum ELO System mit ELO Zugangsdaten reaktivieren. Dies kann nützlich sein, falls Sie sich nicht mehr als Administrator in der Konfiguration anmelden können oder das Single Sign-on über einen OpenID-Anbieter nicht mehr möglich ist.

Setzen Sie hierfür in der ELO Indexserver-Konfiguration die Option `loginWithEloCredentialsEnabled` auf `true`.

Weitere Informationen zu dieser Option finden Sie in der Dokumentation ELO Indexserver > Grundlagen > Indexserver Configure Options.

Problemanalyse über Logs

Falls bei ELO Modern Authentication Fehler auftreten, können Sie Logs nutzen, um diese zu überprüfen.

Fordern Sie zunächst ein Browser-Log an. Im Browser-Log werden die Weiterleitungen zwischen ELO, dem Proxy und dem jeweiligen Anbieter angezeigt. Hier können Sie untersuchen, ob ein Problem bei den Weiterleitungen vorliegt.

Falls die Fehlermeldung *Access denied* auftritt, können Sie im Log des ELO Indexservers überprüfen, was diesen Fehler verursacht hat.

Weiterleitung an falsche URL

Falls bei der Anmeldung an eine falsche URL weitergeleitet wird, können Sie Reverse Proxys konfigurieren. Den grundlegenden Ablauf und die Anpassungen der URLs sehen Sie im Schaubild im Kapitel Reverse Proxys > Grundlagen.

In der Konfiguration von ELO Modern Authentication können Sie im Feld *Feste Domäne* festlegen, an welche Adresse die Anmeldung weitergeleitet werden soll. Weitere Informationen finden Sie im Kapitel Konfiguration > Anmeldekonfiguration.

Konfiguration OpenID-Anbieter: Fehlermeldung 'Error: Connection timed out: connect'

Diese Fehlermeldung erscheint beim Feld *Issuer*, wenn der ELO Server den OpenID-Anbieter nicht erreichen kann. Womöglich liegt ein Problem mit der Firewall-Konfiguration vor.

Falls Sie einen Internet-Proxy (Explicit-Web-Proxy) nutzen, muss ggf. der ELO Application Server entsprechend konfiguriert werden. Sie müssen über das ELO Server Setup die Internet-Proxy-Einstellungen als *Tomcat Java Option* hinterlegen. Weitere Informationen finden Sie in der Dokumentation ELO Server > Custom Install > Tab 'Application Servers' > ELO Server Engines.

Konfiguration für mehrere Repositorys

Wenn Sie in einer ELO Instanz mehrere Repositorys nutzen, teilen diese sich eine Anmeldekonfiguration. D. h. wenn Sie eine Authentifizierungsmethode für ein Repository konfigurieren, gilt diese Konfiguration auch für alle anderen Repositorys in derselben Instanz.

Um Änderungen der Anmeldekonfiguration in einer Indexserver-Instanz für alle Repositorys zu übernehmen, müssen Sie die anderen Indexserver-Instanzen neu starten.

Wenn Sie möchten, dass die Repositorys unterschiedliche Anmeldekonfigurationen nutzen, benötigen Sie getrennte ELO Server und ELO Installationen.