ELO Sync

Authentifizierung und Autorisierung

Inhaltsverzeichnis

Authentifizierung und Autorisierung in ELO Sync 3
Berechtigung für Anwendungen 5

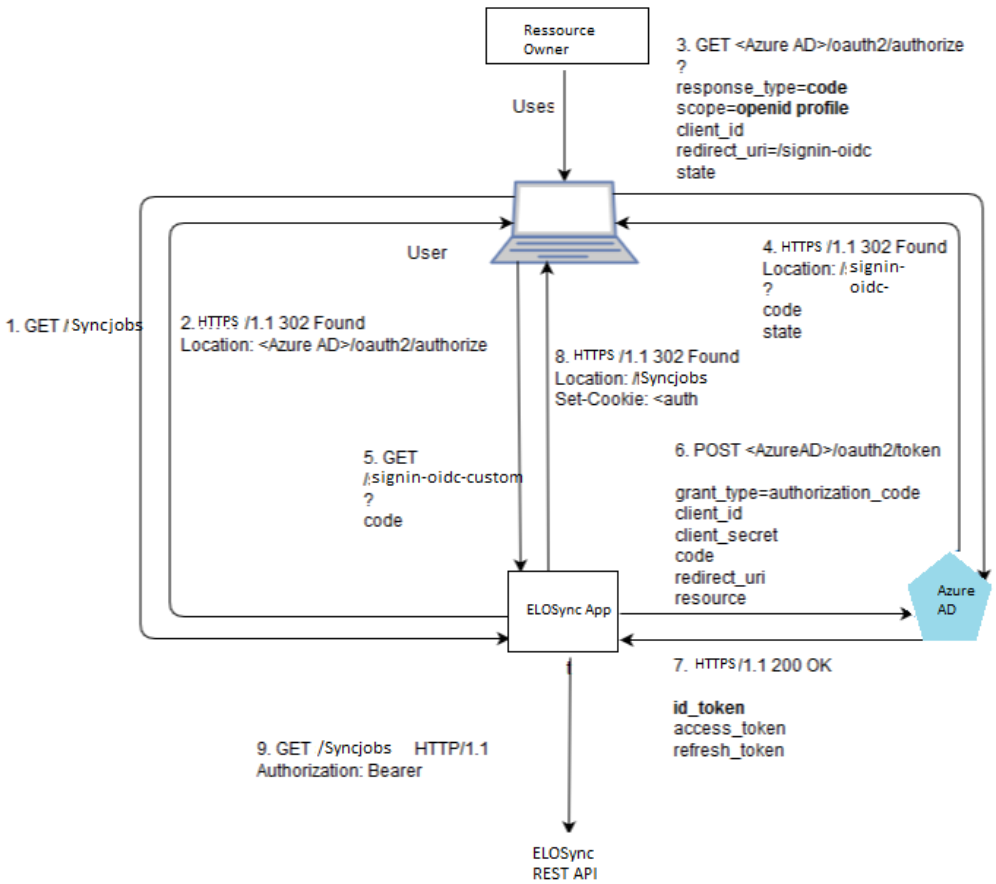
Authentifizierung und Autorisierung in ELO Sync

ELO Sync verwendet eine OpenID-Authentifizierung seiner Benutzer über die ELO Sync Web UI. Zu diesem Zweck muss eine App-Registrierung in Azure erstellt werden. Die notwendigen Schritte sind im Kapitel Azure beschrieben.

> **Information**
>
> Aus Sicht von Azure ist ELO Sync eine Confidential Client App, d.h. die Anmeldedaten müssen serverseitig verwaltet werden.
>
> Aus diesem Grund werden alle empfangenen Zugangsdaten in einem verteilten Cache in der von ELO Sync verwendeten Datenbank gespeichert.

Code Flow in ELO Sync

Die folgende Abbildung zeigt den OpenID-Authentifizierungscode Flow und den enthaltenen OAuth 2.0-Autorisierungscode Flow, der von ELO Sync verwendet wird.



Entra Benutzerzugangsdaten

Nach erfolgreicher Anmeldung in Microsoft Entra ID erhält ELO Sync die Benutzerzugangsdaten für den angemeldeten Benutzer.

Dazu gehören das Zugriffstoken und das Refresh-Token. Diese werden verwendet, um die Hintergrundsynchronisation im Kontext des Benutzers zu ermöglichen.

Die empfangenen Benutzerzugangsdaten werden zur späteren Verwendung in einem *Verteilten Cache/Datenbank* gespeichert. Die für die Speicherung verwendete Tabelle trägt den Namen *elosync_msal*.

Weitere Informationen finden Sie in der Tabellenübersicht im Kapitel über die Datenbank.

Jeder angemeldete Benutzer hat einen Eintrag in der Tabelle *elosync_msal* mit einem eindeutigen Schlüssel. Der eindeutige Schlüssel hat derzeit die folgende Struktur: `{User Object ID}.{Tenant ID}`.

Der ELO Sync Service User hat ebenfalls einen Eintrag in dieser Tabelle, da der Service User jedoch kein echter Benutzer ist, hat sein Schlüssel die Struktur: `{Client ID}_{Tenant ID}`.

Anmeldung der Benutzer in ELO

Nach Erhalt des Zugangstokens von Entra ID müssen die einzelnen Benutzer auch auf das ELO Repository zugreifen.

Aus diesem Grund wird das ELOauth Plug-in für den ELO Indexserver benötigt, dieses muss mit einem Profil konfiguriert werden, dass denselben Tenant verwendet wie ELO Sync.

Siehe das Kapitel OAuth-Abschnitt in der Konfiguration für weitere Details zur Konfiguration der ELO Sync Seite und die ELO Indexserver-Dokumentation für das ELOauth Plug-in.

Berechtigung für Anwendungen

Dieser Artikel beschreibt die Schritte, die erforderlich sind, damit eine Drittanbieter-Anwendung auf die REST-API von ELO Sync zugreifen kann.

Voraussetzung ist, dass die Anwendung des Drittanbieters in Azure mit der Berechtigung zum Zugriff auf die ELO Sync API registriert ist.

Authentifizierung mit Azure

Die Drittanbieteranwendung sollte eine Anmeldung bei Azure mit den folgenden Parametern durchführen:

```
**TODO**
```

Danach gibt die Anmeldung ein Zugriffstoken für die Anwendung zurück, das bei jeder Anfrage an ELO Sync verwendet werden muss, indem es im HTTP-Header `Authorization` gesendet wird.