Configuration et administration

ELO Modern Authentication (Auth2)

Table des matières

ELO Modern Authentication (Auth2)

Prise en main

Pour pouvoir s'authentifier via un fournisseur d'identité (Identity Provider, IDP), le compte doit exister également dans ELO avec l'e-mail correspondant.

L'équilibrage du compte IDP avec le compte ELO se fait toujours via l'e-mail.

Premier démarrage

Par défaut, seule l'authentification ELO avec nom de compte et mot de passe est configurée.

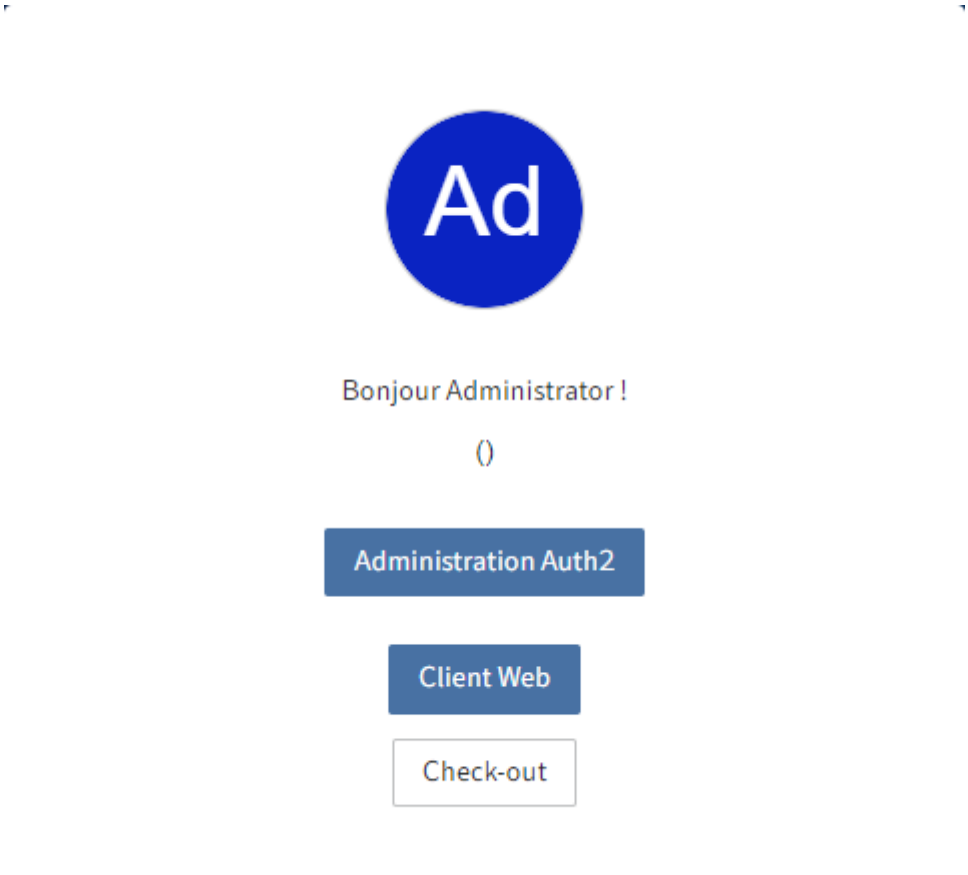
> **Information**
>
> Il est prévu d'ajouter un autre fournisseur d'identité par défaut pour ELO Cloud.

1. Lancez l'URL pour ELO Modern Authentication.

   Veuillez respecter le schéma suivant :

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

2. Pour configurer un propre fournisseur d'identité, authentifiez-vous tout d'abord avec le compte d'administrateur principal.



Une page de sélection avec différentes possibilités d'authentification s'affiche.

3. Sélectionnez *Auth2 Administration*.

   La page *Configuration d'authentification* pour ELO Modern Authentication s'affiche.

4. Via *Ajouter un fournisseur OpenID*, vous pouvez sélectionner un fournisseur pour lequel vous souhaitez effectuer la configuration.

> **Information**
>
> Tous les fournisseurs d'identité OpenID compatibles sont possibles.

Vous trouverez d'autres informations sur la configuration SAP dans le chapitre Configuration.

Configuration

Vous trouverez ci-dessous une explication au sujet de la configuration de Modern Authentication.

Lancement de la page de configuration

Vous avez plusieurs possibilités pour ouvrir la page de configuration pour ELO Modern Authentication :

- Lancement via le point de menu *Réglages d'authentification* de la console d'administration ELO.
- Authentification à ELO Modern Authentication avec compte d'administration principal et activation via le bouton *Auth2Administration*.
- Si vous êtes déjà authentifié avec un compte d'administrateur principal : lancement directement via une URL selon le schéma suivant : `https://<Server>:<Port>/ix-<Repository>/plugin/auth2/`

Recovery-URL

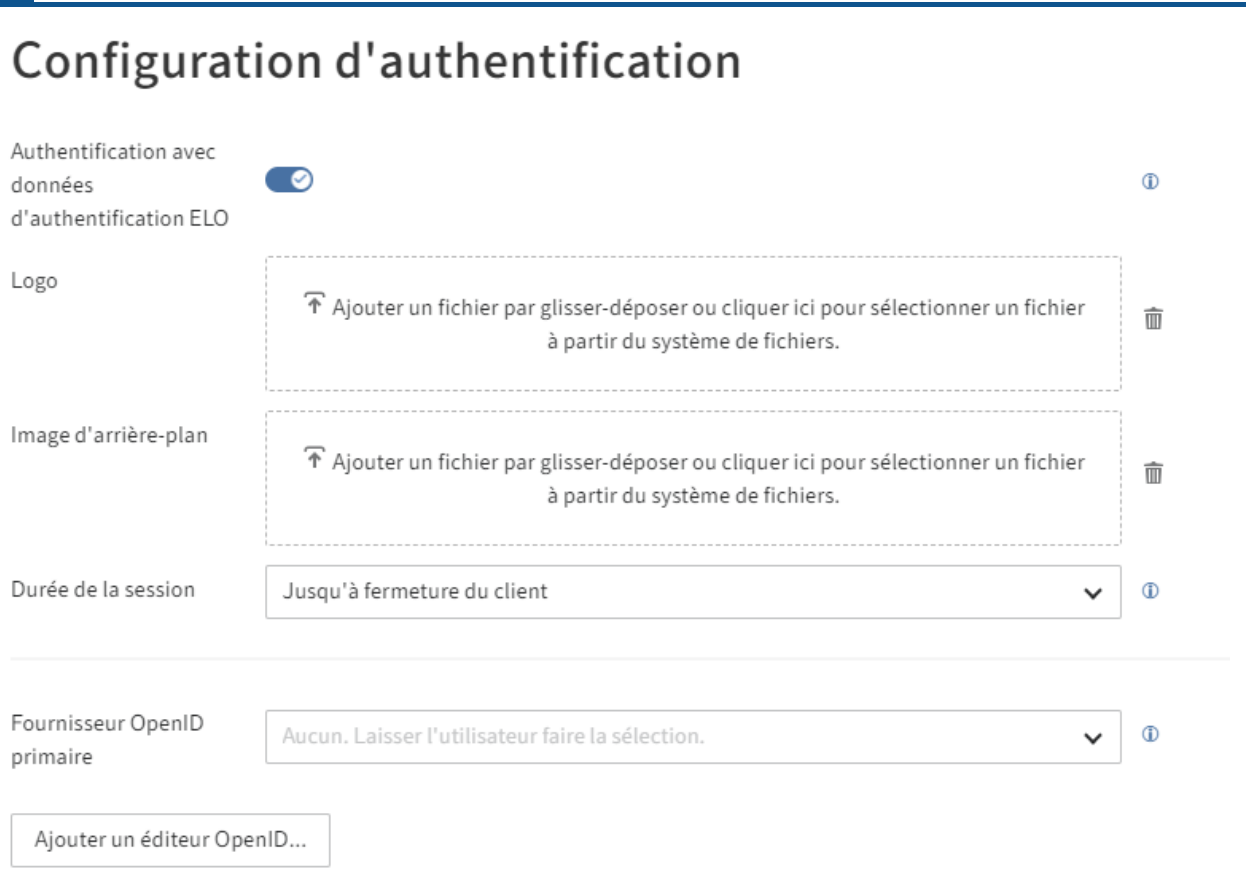
Si vous ne pouvez plus vous authentifier en tant qu'administrateur, il existe une Recovery URL. Celle-ci est affichée sur la page de configuration. Enregistrez cette URL à un emplacement sûr.

L'URL de recovery suit le schéma suivant :

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

Configuration d'authentification

Vous pouvez ajuster la page d'authentification de ELO Modern Authentication individuellement aux exigences de l'entreprise.



Vous avez les options suivantes dans la section *Login Config* :

- Enable password-based login : si cette option est activée, les utilisateurs peuvent s'authentifier via un fournisseur d'identité, ou de manière plus classique avec le nom du compte et le mot de passe. Si l'option est désactivée, il faut passer par le fournisseur d'identité. Une exception sont les comptes de service et les comptes avec des droits administratifs.
- Logo : le champ *Logo* vous permet de télécharger un logo individuel, qui sera affiché dans la section d'authentification lors de l'authentification.

  Via *Enregistrer*, l'image est copiée et elle sera affichée sur la page d'authentification de ELO Modern Authentication lors du prochain lancement de la page d'authentification.

  > **Information**
  >
  > Les formats d'image courants compatibles avec le web sont possibles. La taille peut être sélectionnée librement. Toutefois, l'image est mise à l'échelle en fonction de sa taille et de sa résolution.

  Si le logo est supprimé, c'est le logo ELO qui sera affiché.
- Image d'arrière-plan : via le champ *Image d'arrière-plan*, vous pouvez télécharger une image d'arrière-plan individuelle, qui sera affichée derrière la section d'authentification lors de l'authentification.

Via *Enregistrer*, l'image est copiée et elle sera affichée sur la page d'authentification de ELO Modern Authentication lors du prochain lancement de la page d'authentification.

> **Information**
>
> Les formats d'image courants compatibles avec le web sont possibles. La taille peut être sélectionnée librement. Toutefois, l'image est mise à l'échelle en fonction de sa taille et de sa résolution.

Si l'image d'arrière-plan est supprimée, un arrière-plan standard sera affiché.

- Durée de la session : sélectionnez combien de temps une session doit rester ouverte. Une fois la durée expirée, il faut s'authentifier à nouveau.

> **Information**
>
> Lors d'un redémarrage du serveur d'indexation ELO, les sessions seront également terminées.

- Fournisseur OpenID primaire : dans le menu déroulant, vous pouvez sélectionner quel fournisseur d'identité doit être utilisé, s'il y en a plusieurs. Si vous ne sélectionnez pas de fournisseur, tous les fournisseurs configurés sont proposés.

Ajouter un éditeur OpenID

Pour permettre l'authentification via un ou plusieurs fournisseurs d'identité, vous devez les configurer.

En fonction du fournisseur, les différentes étapes varient et plusieurs étapes pourraient s'avérer nécessaires.

Ci-dessous vous trouverez le déroulement dans l'aperçu.

1. Sélectionnez *Ajouter OpenID*.

   Un menu déroulant apparaît.

2. Sélectionnez le fournisseur souhaité.

   Sont supportés :

   - Microsoft
   - Google
   - Keycloak
   - SAP
   - Salesforce
   - SmartWe
   - Other (possibilité d'intégrer un autre fournisseur d'identité compatible avec OpenID)

   Le dialogue *Veuillez sélectionnez un ID pour le fournisseur pour OpenID*. Le nom est pré-rempli en fonction de la sélection.

En option : vous pouvez bien sûr modifier le nom für la configuration.

3. Confirmez avec *OK*.

   La section de configuration correspondante s'affiche.

4. Entrez les informations nécessaires pour le fournisseur.

   > **Information**
   >
   > Dans le chapitre Microsoft Azure, notre exemple montre l'intégration via Microsoft Azure.
   >
   > En fonction du fournisseur, les différentes étapes peuvent différer.
   >
   > Selon le fournisseur, il y a différentes étapes préliminaires.

5. Veuillez enregistrer vos réglages via *Enregistrer*.

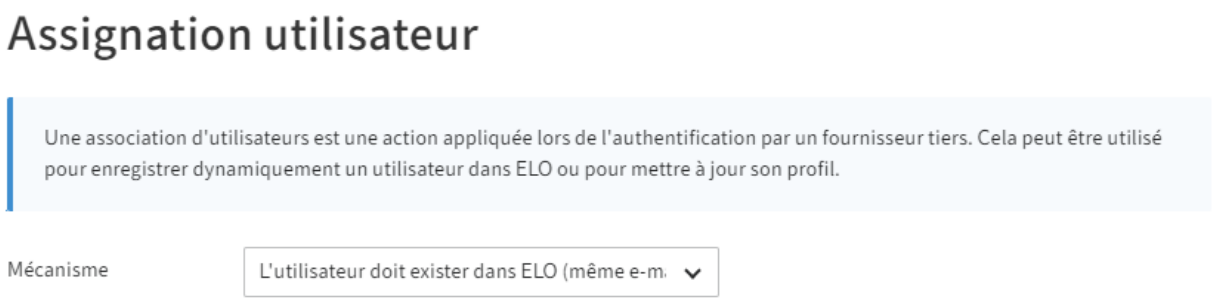
Test

Via *Tester l'authentification* vous permet de vérifier les réglages. Une fenêtre pop-up s'affiche, qui simule la page d'authentification. Lors de la connexion via le fournisseur configuré, une connexion est tentée avec le compte actuellement utilisé.

> **Remarque**
>
> Comme la comparaison se fait par l'adresse e-mail, l'adresse e-mail utilisée par le fournisseur doit également être enregistrée dans le champ *e-mail* du compte ELO.

Assignation utilisateur

Dans la section *Attribution d'utilisateurs*, vous pouvez configurer une méthode qui doit être appliquée lors de la comparaison des comptes ELO avec les comptes chez le fournisseur d'identité.



Mécanisme : via le menu déroulant, vous pouvez sélectionner de quelle manière l'assignation utilisateur doit être effectuée.

Rapports anciens

La section *Rapports anciens* est pensée pour les systèmes qui mettent en place NTLM ou Kerberos.

> **Remarque**
>
> Il n'est pas recommandé d'utiliser ces protocoles. Cette option est proposée pour des raisons de compatibilité.

Clients

La section *Clients* sert à intégrer d'autres clients, comme ELO Integration Client.

La plupart des autres clients ELO (client Web ELO, client Java ELO, client Desktop ELO, etc.) est supportée sans autre configuration.

Exploitation

Ce chapitre explique le fonctionnement de base d'ELO Modern Authentication.

Bases

1. L'utilisateur s'authentifie via le fournisseur d'identité ou localement, selon l'application.
2. Le navigateur est redirigé vers ELO après l'authentification.

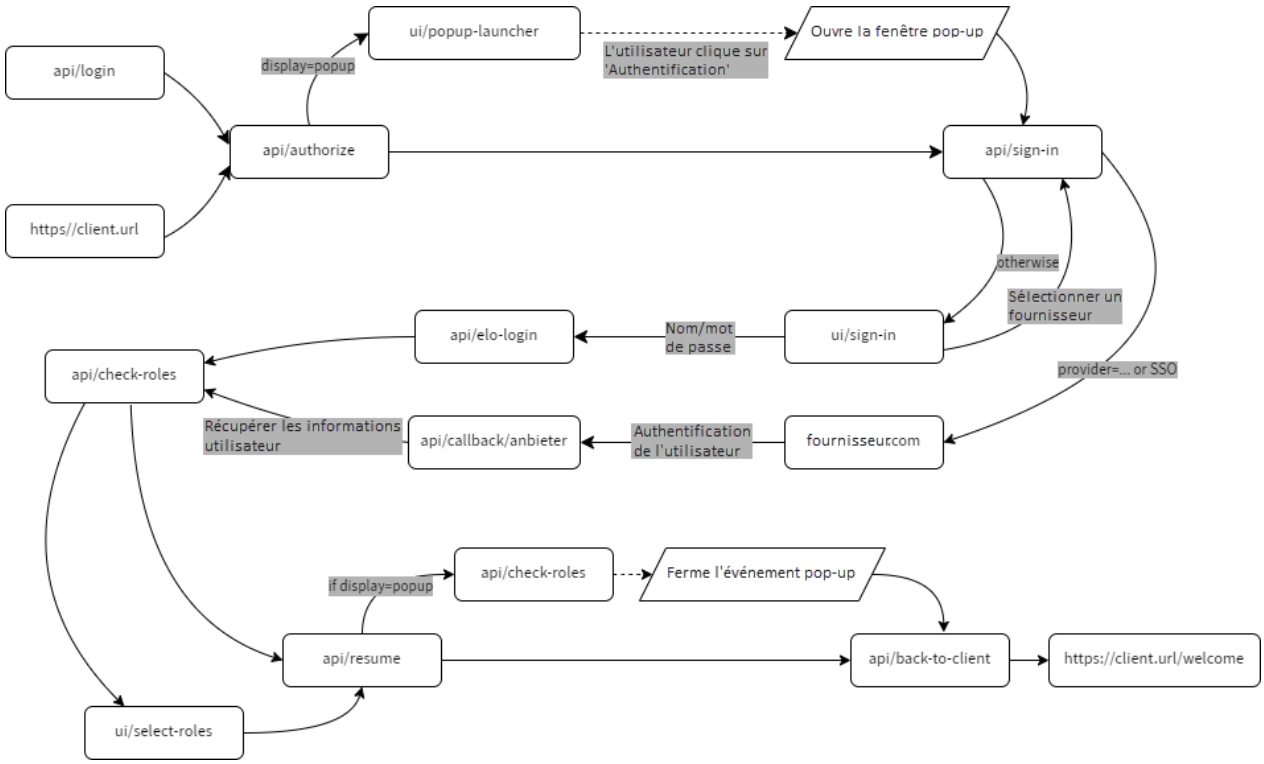
L'attribution des utilisateurs se base toujours sur l'e-mail.

La session ELOix est initiée et trois cookies sont créés :

- `ticket` : le ticket ELOix qui est disponible dans *HttpSession*
- `token` : le jeton d'accès du fournisseur d'identifiants (utile pour les intégrations Microsoft Office 365)
- `provider` : l'ID provider utilisée pour l'authentification (seulement à des fins d'information)

Déroulement

Le plan de déroulement suivant montre le principe de la connexion via ELO Modern Authentication.



Remarques sur le fonctionnement

Veuillez prendre notes des remarques suivantes.

-

Les chemins doivent terminer par un `"/"` (exemple : `.../auth2/`).

- Pour terminer la session comme il se doit, lancez `/logout`.
- Codez le paramètre URL dans `?clientUrl=some-url`.
- Pour des raisons de sécurité, la saisie des données utilisateur telles que les mots de passe ne devrait jamais se faire à l'intérieur des iFrames.
    - Pour cette raison, il existe une page spécifique `plugin/auth2/popup-launcher?...`
        - Comme les bloqueurs de publicité bloquent généralement les "pop-ups directs", l'utilisateur doit d'abord cliquer sur *Connexion* pour déclencher le processus.

Exemple : Microsoft Azure

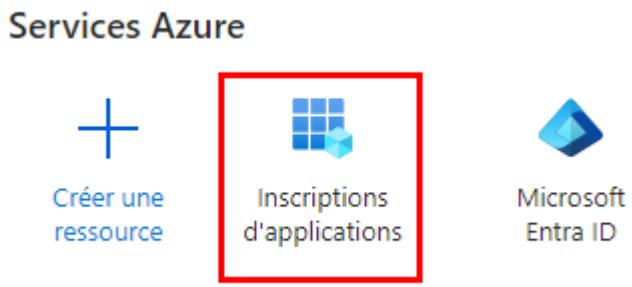
L'exemple suivant montre l'installation via Microsoft Azure.

Enregistrer une application

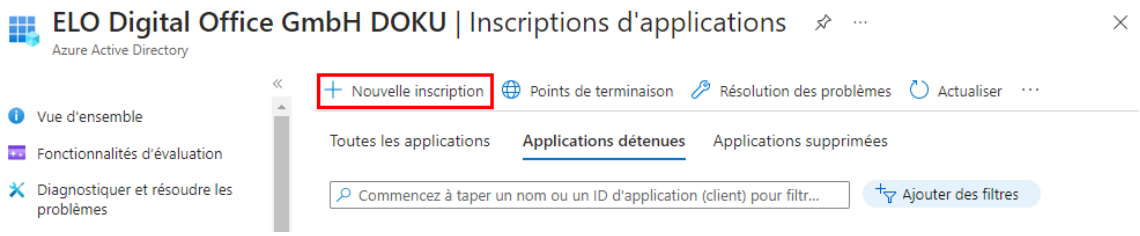
Tout d'abord, vous devez enregistrer une application dans Microsoft Azure.

> **Remarque**
>
> La configuration de base d'un environnement Microsoft Azure ainsi que la création d'abonnements correspondants est un prérequis et ne fait pas partie de cette documentation.

1. Authentifiez-vous dans Microsoft Azure avec les droits administratifs.



2. Ouvrez la section *Enregistrements d'applications*.



3. Veuillez sélectionner *Nouvel enregistrement*.

   La page *Enregistrer l'application* s'affiche.

4. Entrez un nom pour l'application. Vous pouvez sélectionner ce nom librement.

   Exemple : ELOauth2

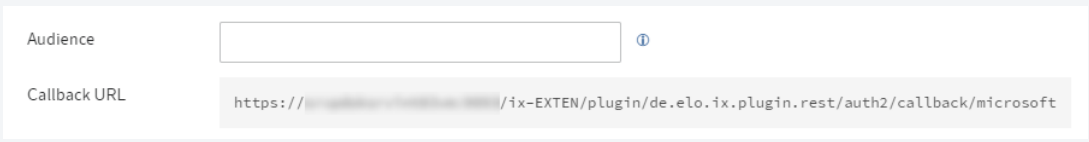
5. Sous *Types de comptes supportés*, sélectionnez l'option *Seulement les comptes dans ce répertoire d'organisation (seulement <nom du mandant> – mandant individuel)*.

6. Pour *URI de redirection (en option)*, sélectionnez l'option *Web*.

7. Veuillez entrer une adresse URL accessible depuis Internet selon le schéma suivant :

   ```
   https://<adresse serveur>/ix-<archive>/plugin/de.elo.ix.plugin.rest/auth2/callback/microsoft
   ```

Information



Vous pouvez aussi obtenir cette adresse URL via la page de configuration sous *Callback URL*.

8. Sélectionnez *Enregistrer*.

   L'application est enregistrée dans Microsoft Azure.

Attribuer des autorisations

Dès que l'application est enregistrée, vous pouvez attribuer les autorisations requises.

1. Ouvrez la section *Autorisations API*.
2. Sélectionnez *Ajouter des autorisations*

   La section *Demander les autorisations API* s'affiche.

3. Ajoutez les autorisations déléguées suivantes :
   - Microsoft Graph :
     - email
     - openid
     - profile
4. Confirmez avec *Ajouter les autorisations*.

5. Sélectionnez *Donner le consentement de l'administrateur pour <Mandant>*.

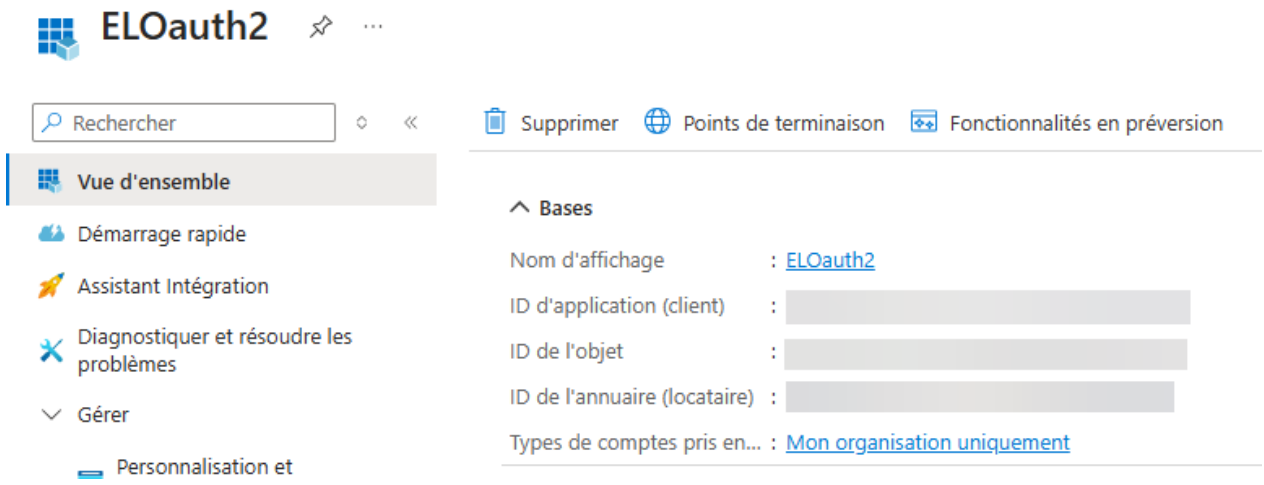
   Le dialogue de demande *Confirmation du consentement de l'administrateur* s'affiche.

6. Confirmez avec *Oui*.

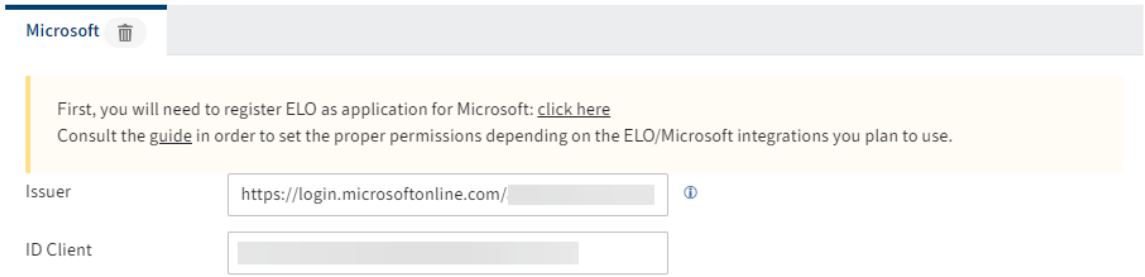
   Les autorisations sont ajoutées;

Transférer les informations dans la configuration

Une fois l'application enregistrée et les autorisations attribuées, vous pouvez transférer les informations dans la page de configuration de ELO Modern Authentication.



1. Dans Microsoft Azure, ouvrez la section *Aperçu*.
2. Copiez la valeur *ID d'application (client)*.
3. Ajoutez la valeur sur la page de configuration de ELO Modern Authentication sous *Client ID*.



Option : si vous mettez en place le client Desktop ELO, et/ou ELO Bot, ajoutez aussi la valeur copiée sous *Audience*.

4. Depuis Microsoft Azure, copiez la valeur pour *ID de répertoire (mandant)*.
5. Ajoutez la valeur sur la page de configuration de ELO Modern Authentication sous *Issuer* à la place du garde-plage`{tenant}`.
6. Veuillez enregistrer vos réglages via*Enregistrer*.

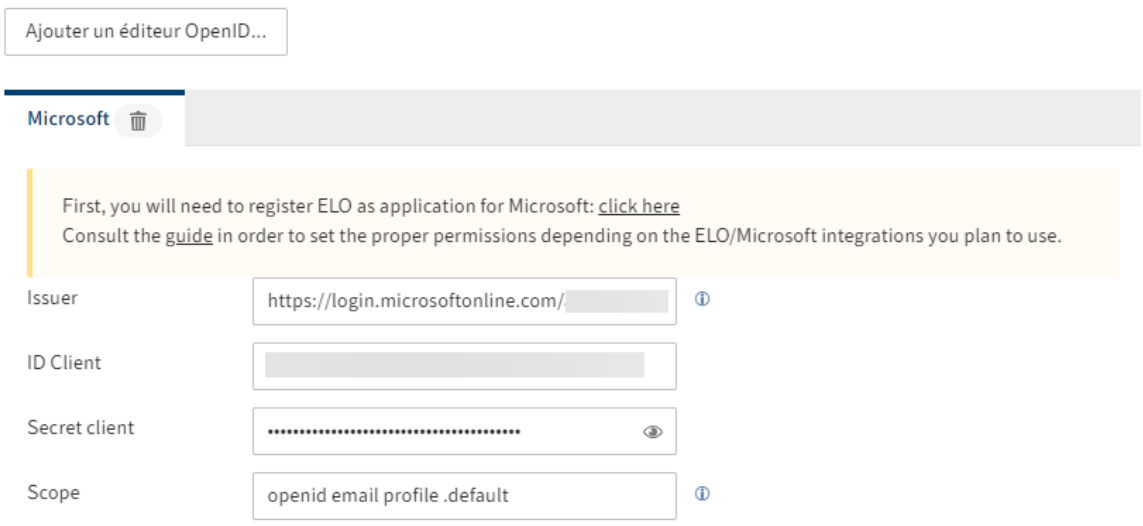
Clé client secrète

Pour que la connexion fonctionne pour l'application, celle-ci a besoin d'une clé client secrète (secret). Celle-ci doit être entrée dans la page de configuration de ELO Modern Authentication.

1. Dans Microsoft Azure, ouvrez la section *Certificats & secrets*.
2. Sélectionnez *Nouvelle clé client secrète*.

   La section *Ajouter une clé client secrète* s'affiche.
3. Dans le champ *Description*, entrez une brève description pour la clé client secrète.
4. Sélectionnez une période pour *Valide jusqu'à*.
5. Confirmez avec *Ajouter*.

   Microsoft Azure crée une clé client secrète.
6. Copiez la clé client dans la colonne *Valeur*.



7.

Ajoutez la clé client copiée sur la page de configuration de ELO Modern Authentication sous *Client secret*.

8. Veuillez enregistrer vos réglages via *Enregistrer*.

Tous les autres champs peuvent rester inchangés dans le cas standard et ne doivent être adaptés que si nécessaire.

La connexion via Microsoft Azure est configurée avec succès.