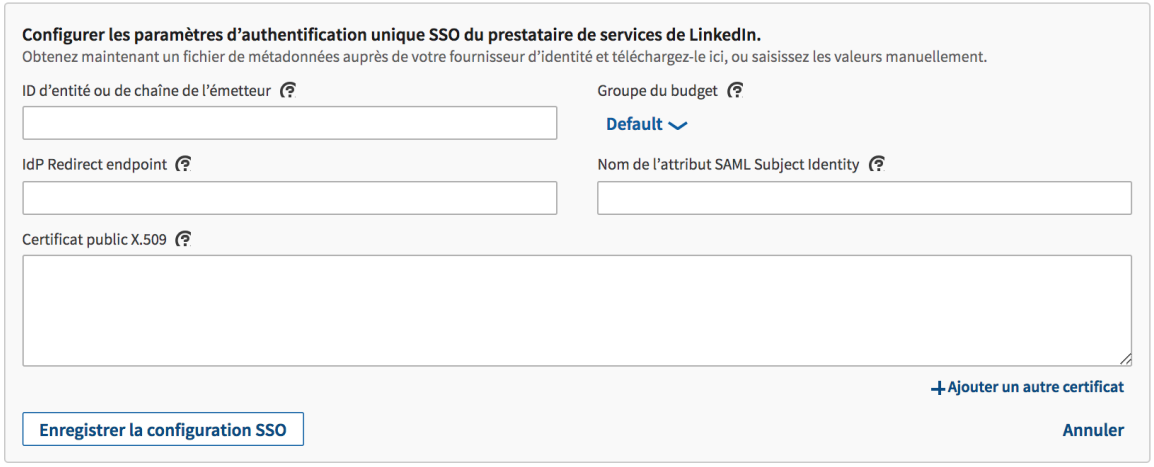
Chargement d’un fichier

1. Cliquez sur **Charger un fichier XML** pour ajouter le fichier de métadonnées à votre système de fournisseur d’identité.

2. Sélectionnez le fichier, puis cliquez sur **Ouvrir**. Si l’opération réussit, les champs sont remplis par les métadonnées.

Saisie manuelle des valeurs

1. Utilisez le lien **Cliquez ici** pour ajouter manuellement des informations.

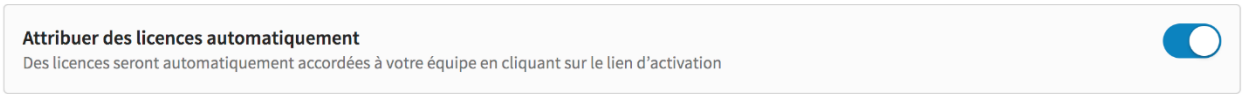


2. Entrez les informations suivantes :
    - ID d'entité ou de chaîne de l'émetteur : doit correspondre au champ md:EntityDescriptor `entityID`
    - Groupe du budget : groupe à utiliser pour attribuer des licences à l'aide de la mise en service *en temps opportun*.
    - URL de redirection : doit correspondre au champ md: SingleSignOnService `location`
        - **Remarque :** pour le moment, LinkedIn ne prend en charge que la liaison urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect.
    - Emplacement d'identité SAML : champ utilisé pour déterminer l'identité de l'employé stockée dans votre système de fournisseur d'identité par rapport à l'identité de l'employé stockée dans le processus EDI chez LinkedIn. LinkedIn utilise les règles suivantes pour identifier l'employé :
        - Si la réponse d'authentification SAML fournit une assertion SAML contenant un ensemble d'attributs, vous pouvez entrer le nom d'attribut SAML de l'attribut contenant l'identité de l'employé dans ce champ de texte. Par exemple, si un entier `employeeId` est envoyé dans un attribut SAML appelé `employeeId`, vous pouvez entrer `employeeId` dans le champ **Emplacement d'identité SAML**. LinkedIn utilisera alors l'attribut employeeId envoyé dans chaque assertion pour rechercher l'identité de l'employé. Pour permettre cela, vous devez charger l'attribut employeeId de chaque utilisateur dans le processus EDI.
        - Si rien n'est indiqué dans ce champ, LinkedIn recherche l'employé en fonction de la valeur de l'attribut `NameId` envoyé dans `<saml:Subject>`. Ce champ *doit* correspondre à l'adresse e-mail principale de l'utilisateur, telle qu'elle a été chargée pendant le processus EDI.
    - Si l'utilisateur est introuvable, soit avec l'ensemble d'attributs défini dans le champ **Emplacement d'identité SAML** soit avec l'adresse e-mail principale telle que configurée dans l'attribut NameId dans `<saml:Subject>`, LinkedIn ne doit *pas* authentifier l'utilisateur.
    - Certificat public : LinkedIn vérifie la validité de l'assertion SAML envoyée dans la réponse d'authentification SAML à l'aide du certificat x.509 utilisé pour la signature par votre fournisseur d'identité. Si nous ne sommes pas en mesure de valider la signature de la réponse d'authentification, votre utilisateur n'est pas authentifié.
3. Cliquez sur **Enregistrer la configuration SSO**.

Attribution des licences

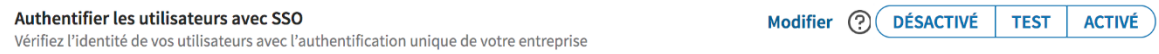
Vous pouvez attribuer automatiquement des licences à vos employés en activant l'option **Attribuer des licences automatiquement**. Lorsque cette option est activée, les utilisateurs se voient accorder automatiquement une licence s'ils n'en ont pas encore.

Remarque : lorsque vous activez l'attribution automatique de licences, les attributs d'utilisateur requis par le fournisseur d'identité s'affichent.



Remarque : l'attribution automatique de licences n'est pour le moment pas prise en charge pour Sales Navigator.

Activation de l'authentification unique



Une fois que vous avez terminé votre configuration, activez l'authentification unique. Cliquez sur le bouton **Authentifier les utilisateurs avec SSO**. Pour plus d'informations sur l'utilisation des options disponibles, reportez-vous au tableau de la section Options d'activation.

Options d'activation

Statut	Description
Désactivé	• Aucune configuration d'implémentation SSO n'est requise. • Les utilisateurs peuvent se connecter aux licences attribuées avec leur logique basée sur LinkedIn.
Test	• L'authentification unique SSO est configurée. • Le mode Test applique le SSO pour les flux initiés IdP pour les employés disposant d'un accès via le fournisseur d'identité, mais permet toujours une identification normale basée sur LinkedIn pour les flux initiés SP. Cela n'oblige pas les utilisateurs à s'authentifier via l'IdP pour se connecter. Ils peuvent accéder à l'application directement via LinkedIn. • Cette possibilité est pratique lors de la configuration initiale SSO ou si votre IdP ne prend en charge que les flux initiés IdP.
Activé	• L'authentification unique SSO est configurée et activée. • Les utilisateurs doivent se connecter via le flux initié IdP ou le flux initié SP (à moins que l'IdP prenne en charge uniquement le flux initié IdP, auquel cas les utilisateurs n'ont pas de flux initié SP). Quelle que soit la méthode choisie, l'authentification est requise. **Attention :** lorsque vous sélectionnez **Activé** après la configuration initiale, ne fermez pas la fenêtre tant que vous ne vous êtes pas assuré du bon fonctionnement du SSO. Dans le cas contraire, vous devrez contacter l'assistance clientèle pour désactiver le SSO sur votre compte. Nous vous recommandons d'utiliser l'option **Test** pour valider votre flux initié IdP avant de définir la valeur **Activé** pour le SSO.
• Flux initié IdP : lorsqu'un utilisateur passe par son fournisseur d'identité (tel qu'Okta, AAD ou Ping) pour accéder à une application. • Flux initié SP : lorsqu'un utilisateur passe directement par l'application ou par le prestataire de service pour accéder à sa licence.	

Vérification de votre configuration

Remarque : avant de vérifier votre configuration, votre liaison doit être terminée. Pour obtenir des informations et les étapes à suivre pour la liaison, consultez le Livre blanc sur la confidentialité et la sécurité de LinkedIn : Intégration de bases de données d'employés (EDI) et authentification unique (SSO) du compte administrateur.

Vérifiez que vous êtes correctement intégré à votre système de fournisseur d'identité et que les conditions suivantes sont remplies :

- L'identité de votre entreprise a été ajoutée à l'application LinkedIn (par exemple, par le biais d'un fichier CSV).
- L'authentification unique est activée.
- Vous disposez d'une application configurée dans votre fournisseur d'identité qui correspond à l'application LinkedIn, configurée selon les instructions précédentes.

Procédez au test avec :

- la connexion initiée de votre fournisseur d'identité ;
- la page de recommandation de LinkedIn, puis la connexion.

Assistance

Documentation d'aide

- Guide de l'administrateur pour l'ajout de données d'employés
- Livre blanc sur la confidentialité et la sécurité de LinkedIn : Intégration de bases de données d'employés (EDI) et authentification unique (SSO) du compte administrateur
- Didacticiel : Intégration d'Azure Active Directory à LinkedIn Learning
- Didacticiel : Intégration d'Azure Active Directory à LinkedIn Sales Navigator
- Didacticiel : Intégration d'Azure Active Directory à LinkedIn Elevate

Problèmes techniques

Si vous rencontrez un problème technique avec la configuration de l'authentification unique, contactez l'équipe responsable de votre compte ou l'équipe assistance applications via l'assistance clientèle.

Politique de confidentialité et de sécurité des données de LinkedIn

https://www.linkedin.com/legal/privacy-policy

Coordonnées de l'équipe responsable de la sécurité de LinkedIn

Si vous avez des questions relatives à la sécurité ou si vous souhaitez signaler un problème de sécurité, écrivez-nous à l'adresse security@linkedin.com.