# Guide de l’administrateur relatif à l’authentification unique

**Dernière mise à jour le 15 février 2018**
**Version 1.7**



# Exonération de responsabilité



*LinkedIn Corporation*
*1000 W. Maude Ave. Sunnyvale, CA*
*94085*

*Le présent document peut contenir des déclarations prospectives. Toute information contenue dans ce document peut être modifiée sans préavis. Le logiciel et la documentation connexe ne peuvent être utilisés ou reproduits que dans le respect des conditions du contrat de licence nous liant. Aucune partie du logiciel ou de la documentation ne peut être reproduite, transmise ou traduite sous quelque forme ou par quelque moyen que ce soit, électronique, mécanique, manuel, optique ou autre, en tout ou partie, autrement qu'en conformité avec les conditions du contrat de licence nous liant.*

*LinkedIn Corporation et le logo de LinkedIn Corporation sont des marques, des marques de service ou des marques déposées de LinkedIn Corporation aux États-Unis et dans d'autres pays. Tous les autres noms de produit, de service ou de marque sont des marques ou des marques déposées de leurs entreprises ou propriétaires respectifs.*

# Sommaire


Exonération de responsabilité

Sommaire

Présentation
- Conditions préalables
- À propos de l'authentification unique (SSO)
- Pourquoi utiliser l'authentification unique ?
- Protocoles SSO pris en charge

Configuration de l'authentification unique (SSO)
- Premiers pas avec l'authentification unique
- Connexion à votre fournisseur d'identité
  - Téléchargement d'un fichier
  - Utilisation des champs individuels
- Configuration de votre fournisseur d'identité
  - Exigences relatives à la mise en service en temps opportun
    - Adresse e-mail (requise)
    - Prénom (facultatif)
    - Nom (facultatif)
    - Attributs facultatifs supplémentaires
    - Exemple
  - Chargement d'un fichier
  - Saisie manuelle des valeurs
- Attribution des licences
- Activation de l'authentification unique
    - Options d'activation
- Vérification de votre configuration

Assistance
- Documentation d'aide
- Problèmes techniques
- Politique de confidentialité et de sécurité des données de LinkedIn
- Coordonnées de l'équipe responsable de la sécurité de LinkedIn

# Présentation

L'intégration de bases de données d'employés (EDI) permet à votre entreprise d'intégrer les données des employés de son système d'information des ressources humaines (HRIS) dans des applications LinkedIn. Cette intégration inclut une configuration facultative de l'authentification unique avec votre solution SSO. Dans ce cas, l'administrateur de votre compte peut configurer votre entreprise pour qu'elle utilise le service SSO pour s'authentifier auprès d'une application de la plateforme LinkedIn en l'intégrant à la plateforme d'entreprise.

Cette intégration est configurée dans le compte administrateur LinkedIn et est disponible uniquement pour certaines applications LinkedIn payantes.

## Conditions préalables

- Compte d'entreprise
- Privilèges administrateur complets
- Privilèges d'administration de fournisseur d'identité (IdP)

## À propos de l'authentification unique (SSO)

L'authentification unique (SSO) d'entreprise permet aux employés de votre organisation de se connecter à des applications LinkedIn prises en charge en utilisant leurs identifiants d'entreprise au lieu de leurs identifiants LinkedIn.

L'utilisation d'un système SSO et l'intégration à un fournisseur SSO ne sont pas obligatoires pour pouvoir utiliser les applications LinkedIn. Si l'authentification unique n'est pas configurée, vos employés peuvent s'authentifier avec leurs identifiants personnels LinkedIn actuels ou créer un compte.

## Pourquoi utiliser l'authentification unique ?

- Utilisation du système d'authentification existant de votre entreprise
- Sécurité accrue lorsque les employés utilisent les protocoles d'authentification par mot de passe de votre entreprise au lieu de leur compte privé
- Gestion des utilisateurs facilitée lorsque des employés quittent votre entreprise

## Protocoles SSO pris en charge

Nous prenons actuellement en charge les protocoles SAML version 2.0.

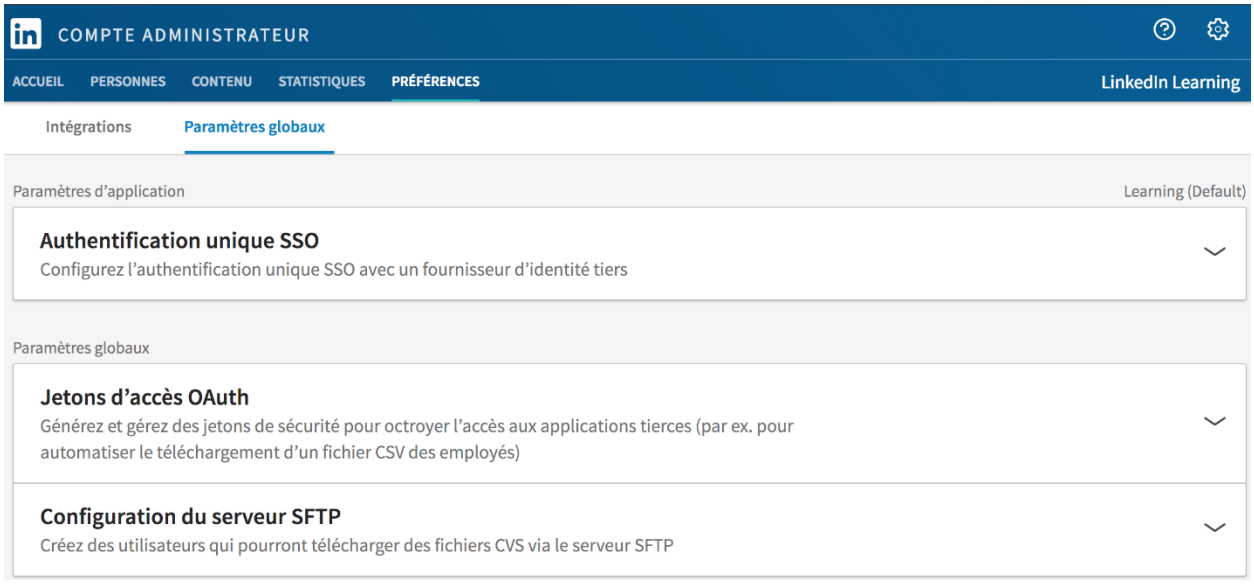
# Configuration de l’authentification unique (SSO)

## Premiers pas avec l’authentification unique

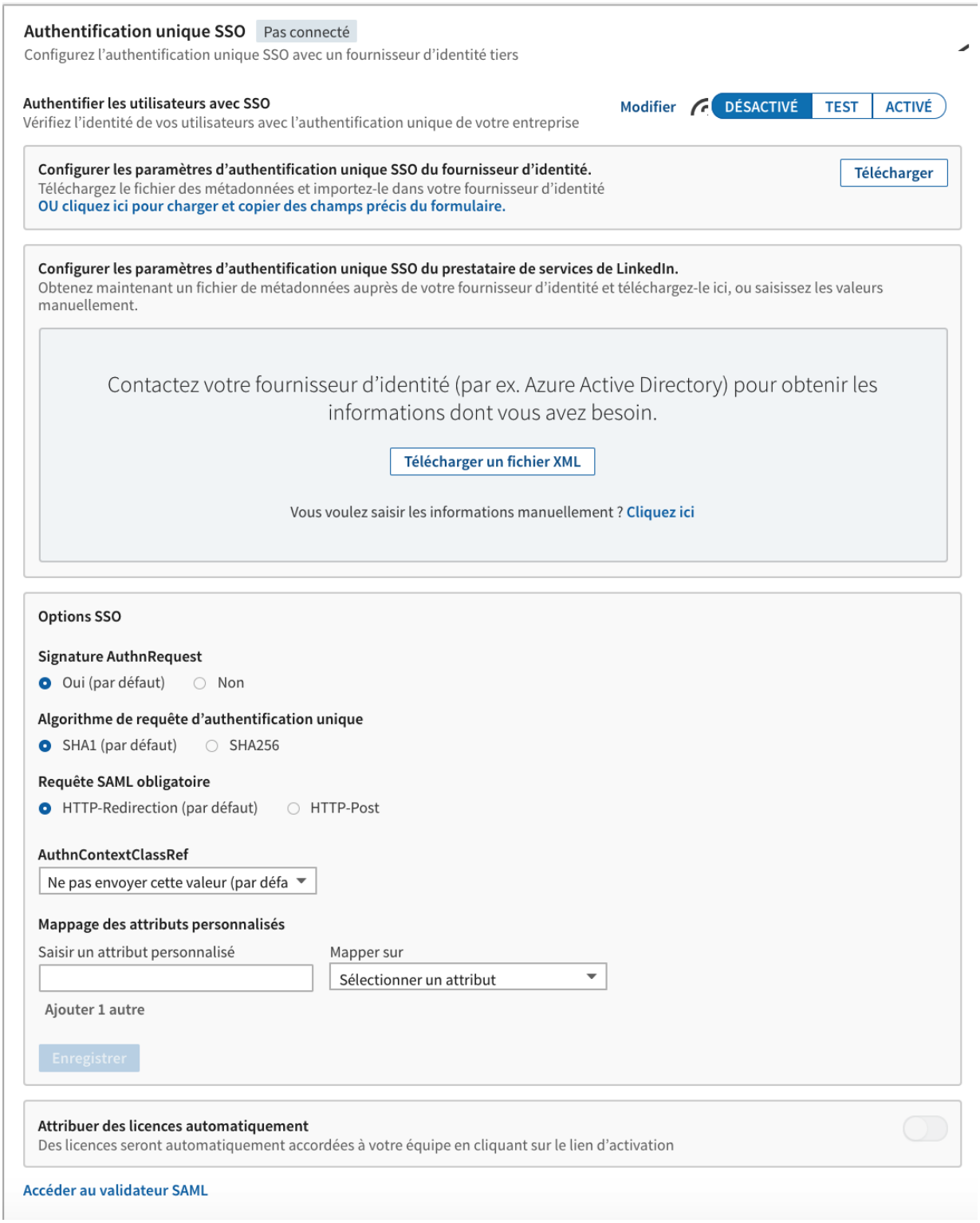
1. Accédez au compte administrateur en cliquant sur le lien suivant : http://www.linkedin.com/enterprise/accountcenter/settings

   **Remarque :** certaines applications disposent également d’un point d’accès à partir des préférences de l’application. Dans LinkedIn Learning, par exemple, vous pouvez cliquer sur **Accéder à Admin** dans la bannière et sélectionner **Préférences > Préférences générales**.

   Les préférences de l’application relatives au système SSO indiquent l’application à laquelle vous avez accédé.



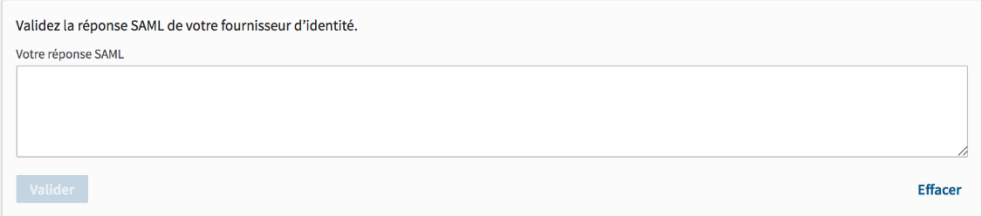
2. Ouvrez le panneau Authentification unique SSO.



3. Sélectionnez vos options SSO.
    a. Signature AuthnRequest :
        - Oui (par défaut)
        - Non
    b. Algorithme de requête d'authentification unique :
        - SHA1 (par défaut)
        - SHA256
    c. Requête SAML obligatoire :
        - HTTP-Redirection (par défaut)
        - HTTP-Post
    d. AuthnContextClassRef :
        - Ne pas envoyer cette valeur (par défaut)
        - urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport
        - urn:oasis:names:tc:SAML:2.0:ac:classes:kerberos
        - urn:federation:authentication:windows
        - TransportProtégéParMotDePasse et Windows
        - urn:oasis:names:tc:SAML:2.0:ac:classes:X509
        - urn:oasis:names:tc:SAML:2.0:ac:classes:TLSClient
    e. Mappage des attributs personnalisés. Vous pouvez indiquer des mappages de noms personnalisés pour établir une correspondance avec les préférences d'IdP (au lieu d'utiliser les mappages par défaut). Saisissez votre attribut personnalisé et sélectionnez l'attribut avec lequel le mapper. Les champs suivants peuvent être mappés avec des attributs personnalisés, fournis par les utilisateurs.
        - Prénom
        - Nom
        - Adresse e-mail principale
        - Numéro de téléphone mobile
        - Numéro de tél. prof.
        - Fonction
        - Poste
        - Manager
        - Service
        - Niveau du poste
        - Type de travail
        - Statut
        - Code de construction
        - Lieu du bureau

        Pour plus d'informations sur les attributs par défaut, reportez-vous à la section Exigences relatives à la mise en service en temps opportun.

4. (Facultatif) Cliquez sur **Accéder au validateur SAML** pour indiquer si les requêtes SAML doivent être signées. Collez la réponse SAML et cliquez sur **Valider**.




5. (Facultatif) Si vous devez configurer plusieurs instances d'application, vous pouvez sélectionner le menu **<*nom de l'application*> - <*instance*>** dans la bannière, puis l'instance que vous souhaitez configurer. Dans LinkedIn Learning, par exemple, vous sélectionneriez le menu **Learning - Default** (tel qu'illustré dans la capture d'écran de l'étape 1).

   **Remarque** : les instances d'application du menu sont classées par application. Ainsi, si vous avez accès à plusieurs instances d'une même application (par exemple, deux instances de Recruiter), vous verrez l'en-tête Recruiter, suivi des noms de chaque instance d'application.

## Connexion à votre fournisseur d'identité

Si votre système de fournisseur d'identité prend en charge les métadonnées et si vous avez configuré le protocole SAML avec la version 2.0, vous pouvez télécharger un fichier de configuration XML à lui envoyer. Le fournisseur d'identité peut ensuite le charger afin de configurer automatiquement les préférences pour la connexion à vos produits LinkedIn.

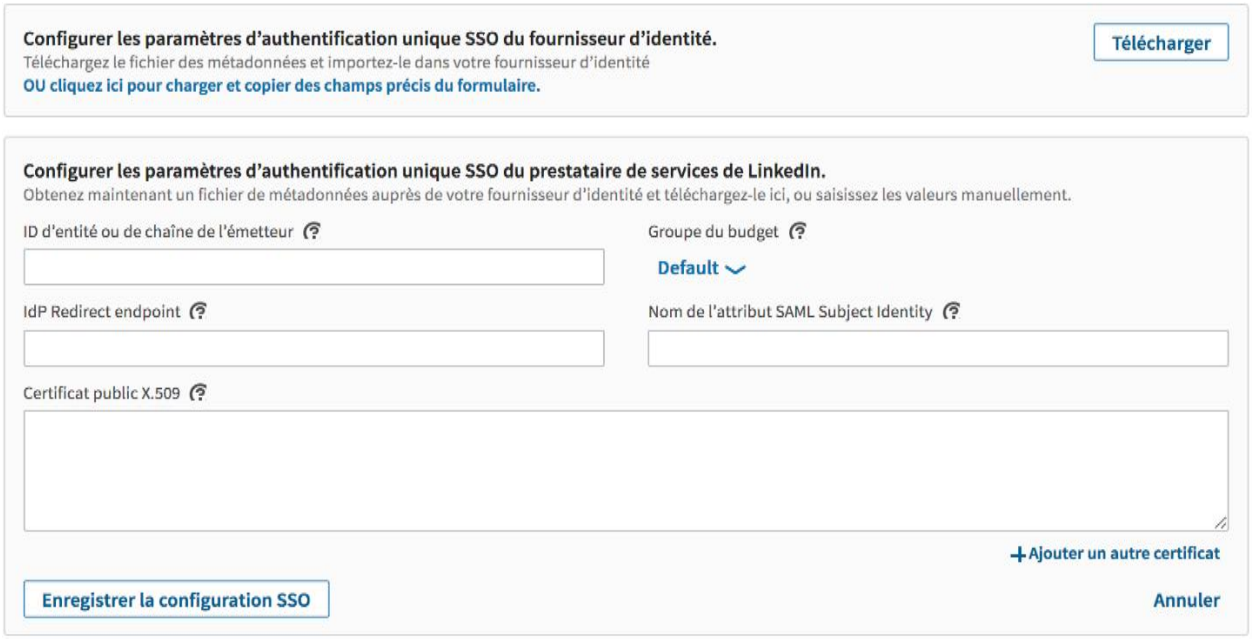
Déterminez si vous pouvez télécharger un fichier de métadonnées ou si vous devez utiliser des champs individuels. Suivez ensuite l'une des procédures indiquées dans les sections suivantes.

### Téléchargement d'un fichier

1. Cliquez sur **Télécharger** pour télécharger un fichier de métadonnées que vous pouvez utiliser avec votre système de fournisseur d'identité. Le fichier `metadata.xml` est téléchargé par votre navigateur.
2. Vérifiez qu'il contient les éléments suivants :
   `<md:AssertionConsumerService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST" Location="https://www.linkedin.com/checkpoint/enterprise/saml/[ACCOUNT ID]" index="0"/>`
3. Accédez à votre système de fournisseur d'identité.
4. Chargez le fichier des métadonnées.
   **Remarque :** il se peut que vous ne soyez pas en mesure d'importer ce fichier dans le système de votre fournisseur d'identité. Par exemple, Okta ne dispose pas de cette fonctionnalité.
5. Revenez à la configuration SSO.
6. Cliquez sur **OK** dans la boîte de dialogue de chargement, puis reportez-vous à la section Configuration de votre fournisseur d'identité.

### Utilisation de champs individuels

1. Cliquez sur le lien pour charger et copier des champs précis du formulaire dans votre système de fournisseur d'identité.




2. Copiez et collez les champs que vous souhaitez inclure.

## Configuration de votre fournisseur d'identité

Configurez votre fournisseur d'identité pour qu'il communique avec la plateforme de LinkedIn. Déterminez si vous pouvez charger un fichier de métadonnées dans votre système de fournisseur d'identité ou si vous devez saisir manuellement les valeurs. Suivez ensuite l'une des procédures indiquées dans les sections suivantes. Si vous n'utilisez pas la mise en service en temps opportun, passez à la section Chargement d'un fichier ou Saisie manuelle des valeurs.

### Exigences relatives à la mise en service en temps opportun

La flexibilité du protocole SAML 2.0 concernant l'envoi d'informations complémentaires au fournisseur de service est l'une des raisons de son utilisation répandue. Lorsqu'un fournisseur d'identité envoie une assertion, celle-ci inclut des attributs décrivant l'utilisateur. Ces attributs permettent à LinkedIn à la fois d'identifier l'utilisateur et de lui attribuer automatiquement un compte. Quelques-uns des attributs possibles sont décrits dans cette section.

### Adresse e-mail (requis)

Chaque utilisateur doit avoir une adresse e-mail valide, même lorsqu'il utilise l'authentification unique.

**Remarque :** en cas de test avec plusieurs identités d'IdP, les adresses e-mail doivent être uniques.

Dans la mesure où le fournisseur d'identité gère les informations de l'utilisateur, il doit envoyer l'adresse e-mail de celui-ci dans son assertion. Les fournisseurs d'identité utilisent différentes règles pour l'affectation de noms. LinkedIn recherche alors une adresse e-mail de façon séquentielle parmi les noms d'attribut suivants :

- EmailAddress
- email
- Email
- Mail
- emailAddress
- User.email
- http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress

### Prénom (facultatif)

À l'instar des adresses e-mail, les fournisseurs d'identité peuvent envoyer le prénom dans plusieurs champs courants. Afin d'offrir une compatibilité immédiate avec la plupart des fournisseurs d'identité, LinkedIn tente de trouver le prénom dans les noms d'attribut suivants :

- FirstName
- first_name
- firstname
- firstName
- User.FirstName
- http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname

### Nom (facultatif)

LinkedIn recherche le nom dans les noms d'attribut suivants :

- LastName
- last_name
- lastname
- lastName
- User.LastName
- http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname

### Attributs facultatifs supplémentaires

Vous pouvez fournir des informations supplémentaires, notamment les noms d'attribut suivants.

**Remarque :** bien que ces attributs soient stockés par LinkedIn, ils ne sont pas visibles depuis l'interface utilisateur pour le moment et donc indisponibles pour la gestion des utilisateurs.

| Nom d'attribut | Variations prises en charge |
|---|---|
| Service | • departmentName<br>• department<br>• User.Department |
| Manager | • Manager<br>• manager<br>• User.Manager |
| Numéro de téléphone mobile | • mobilePhoneNumber<br>• PhoneNumber<br>• phone |
| | • phoneNumber<br>• User.PhoneNumber<br>• http://schemas.xmlsoap.org/ws/2005/05/identity/claims/mobilephone |
| Numéro de tél. prof. | • WorkPhoneNumber<br>• Workphone<br>• workPhoneNumber<br>• User.WorkPhoneNumber<br>• http://schemas.xmlsoap.org/ws/2005/05/identity/claims/otherphone |
| Fonction | • workTitle<br>• Title<br>• WorkTitle<br>• User.WorkTitle |
| Poste | • jobFunction<br>• JobFunction<br>• User.JobFunction |
| Niveau du poste | • JobLevel<br>• jobLevel<br>• User.JobLevel |

| | |
|---|---|
| Type de travail | • WorkerType<br>• workerType<br>• User.WorkerType |
| Statut | • WorkerStatus<br>• workerStatus<br>• Status<br>• User.WorkerStatus |
| Code de construction | • buildingCode<br>• building |
| Lieu du bureau | • deskLocation<br>• desk |

### Exemple

E-mail : jdupont@entreprise.com
Prénom : Jeanne
Nom : Dupont
Numéro de téléphone mobile : 06 05 04 03 02
Fonction : Manager, Génie logiciel
Service : Applications logicielles
Date de début : 07/03/16
Niveau du poste : Contributeur individuel
Type de travail : employé
Statut : actif ou inactif
Manager : dsmith

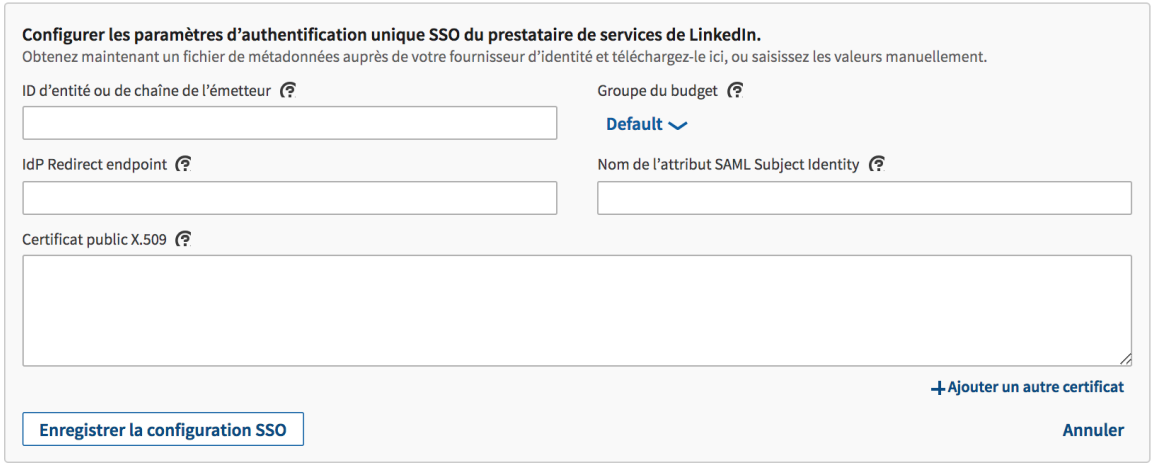
## Chargement d’un fichier

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.

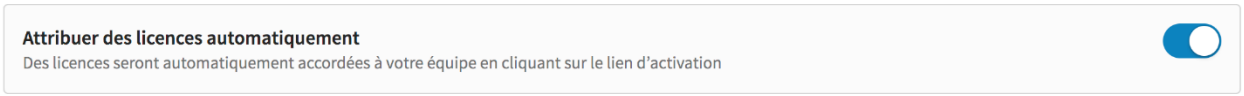


2. Entrez les informations suivantes :
    - ID d'entité ou de chaîne de l'émetteur : doit correspondre au champ md:EntityDescriptor `entityID`
    - Groupe du budget : groupe à utiliser pour attribuer des licences à l'aide de la mise en service *en temps opportun*.
    - URL de redirection : doit correspondre 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

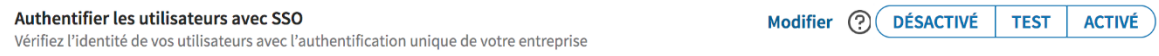
Vous pouvez attribuer automatiquement des licences à vos employés en activant l'option **Attribuer des licences automatiquement**. Lorsque cette option est activée, les utilisateurs se voient accorder automatiquement une licence s'ils n'en ont pas encore.

**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.<br>• Les utilisateurs peuvent se connecter aux licences attribuées avec leur logique basée sur LinkedIn. |
| Test | • L'authentification unique SSO est configurée.<br>• 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.<br>• 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.<br>• 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.<br><br>**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.<br>• 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 : Azure Active Directory Integration with LinkedIn Learning (en anglais)
- Didacticiel : Azure Active Directory Integration with LinkedIn Sales Navigator (en anglais)
- Didacticiel : Azure Active Directory Integration with LinkedIn Elevate (en anglais)

## 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.