# Single Sign-On

## Administratorleitfaden

**Zuletzt überarbeitet: 15. Februar 2018**
**Version 1.7**



LinkedIn

# Haftungsausschluss



*1000 W. Maude Ave.*
*Sunnyvale, CA 94085*
*USA*

*Dieses Dokument enthält möglicherweise Aussagen, die sich auf die Zukunft beziehen. Alle Informationen in diesem Dokument sind Änderungen vorbehalten. Für die Nutzung der Software oder Anfertigung einer Kopie derselben (sowie der zugehörigen Dokumentation) gelten ausschließlich die Bedingungen des mit uns geschlossenen Lizenzvertrags. Kein Teil der Software oder Dokumentation darf in irgendeiner Form reproduziert, übertragen oder übersetzt werden – weder auf elektronische, mechanische, manuelle, optische oder andere Weise, ausgenommen in dem gemäß des Lizenzvertrags zulässigen Rahmen.*

*LinkedIn Corporation und das LinkedIn Corporation Logo sind Marken, Servicemarken oder eingetragene Warenzeichen der LinkedIn Corporation in den USA und anderen Ländern. Alle anderen Marken-, Service- oder Produktnamen sind Marken oder eingetragene Warenzeichen ihrer jeweiligen Unternehmen oder Eigentümer.*

# Inhalt

# Übersicht

Über die Employee Database Integration (EDI, Mitarbeiterdatenbankintegration) kann Ihr Unternehmen eigene HRIS-Mitarbeiterdaten in LinkedIn Anwendungen integrieren. Die Integration umfasst eine optionale Konfiguration für Single Sign-On mit Ihrer SSO-Lösung. In einem solchen Fall kann der Administrator Ihres Unternehmenskontos die Authentifizierung Ihres Unternehmens für eine LinkedIn Plattformanwendung über SSO konfigurieren, und zwar über eine Integration in der Unternehmensplattform.

Die Konfiguration der Integration erfolgt über das LinkedIn Account-Center und ist nur für einige bezahlte LinkedIn Anwendungen verfügbar.

## Voraussetzungen

- Unternehmenskonto
- Vollständige Administratorrechte
- Administrationsrechte für den Identitätsanbieter (IdP)

## Informationen zu Single Sign-On (SSO)

Das Single Sign-On (SSO) für Unternehmen bietet den Mitarbeitern Ihres Unternehmens die Möglichkeit, sich mit den Anmeldeinformationen Ihres Unternehmens anstelle ihrer LinkedIn Anmeldeinformationen einzuloggen.

Die Nutzung von SSO und die Integration mit einem SSO-Anbieter ist allerdings nicht erforderlich, um LinkedIn Anwendungen nutzen zu können. Sofern SSO nicht konfiguriert ist, können Ihre Mitarbeiter sich über ihre individuellen LinkedIn Anmeldeinformationen authentifizieren oder ein neues Mitgliedskonto erstellen.

## Was spricht für die Nutzung von Single Sign-On?

- Nutzung der Authentifizierung Ihres Unternehmens
- Höhere Sicherheitsstandards, wenn Mitarbeiter die etablierten Passwortprotokolle Ihres Unternehmens anstelle ihrer eigenen Konten verwenden
- Einfachere Benutzerverwaltung, wenn Mitarbeiter Ihr Unternehmen verlassen

## Unterstützte SSO-Protokolle

Derzeit unterstützen wir SAML Version 2.0.

# Konfigurieren von Single Sign-On (SSO)

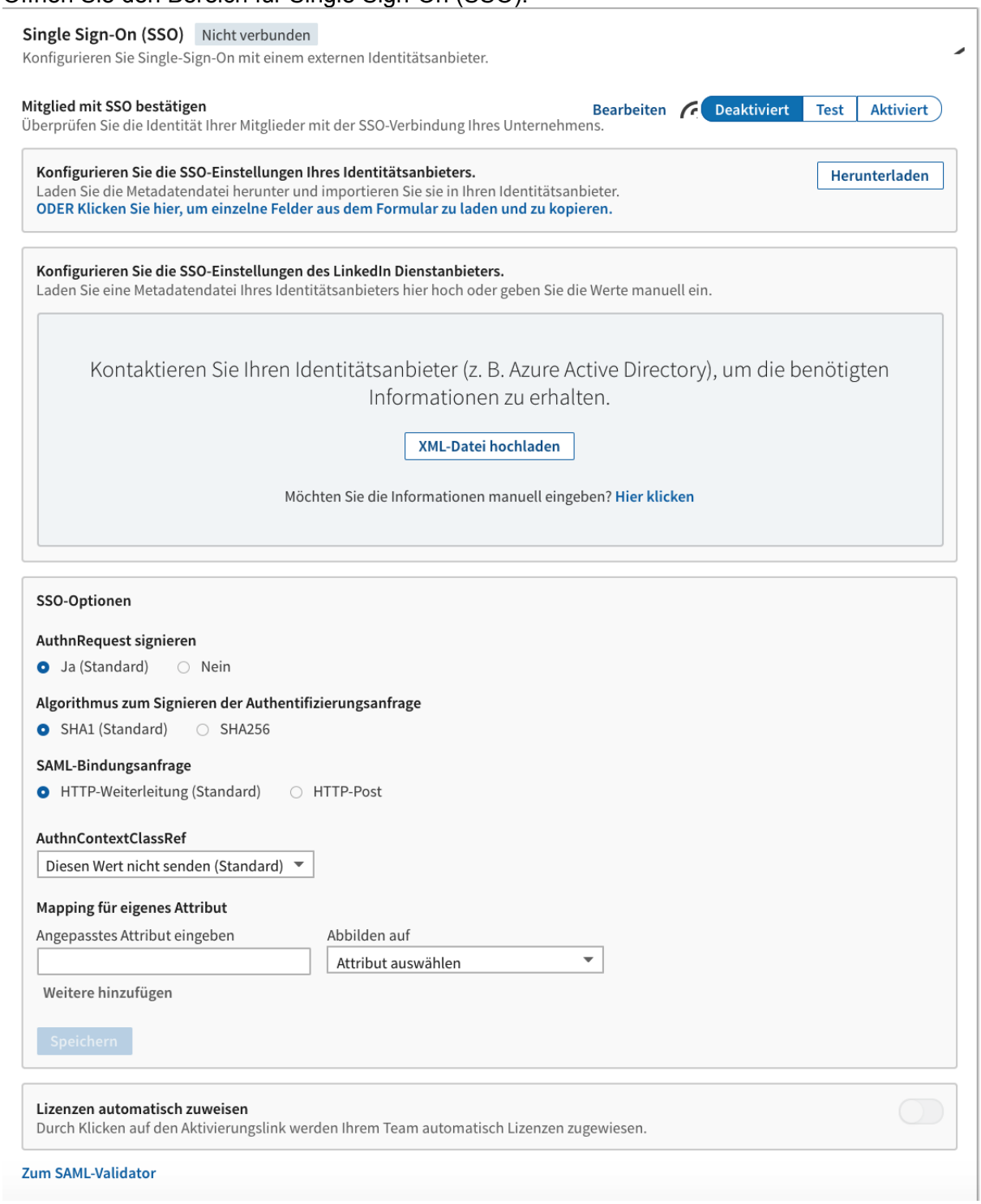
## Erste Schritte mit SSO

1. Rufen Sie das Account-Center über den folgenden Link auf:
   http://www.linkedin.com/enterprise/accountcenter/settings

   **Hinweis:** Manche Anwendungen bieten einen Zugriffspunkt in ihren Anwendungseinstellungen. In Learning können Sie beispielsweise im Banner auf **Zur Administratorseite** klicken und dann **Einstellungen > Globale Einstellungen** wählen.

   In den Anwendungseinstellungen für SSO wird die Anwendung aufgeführt, auf die Sie zugegriffen haben.

2. Öffnen Sie den Bereich für Single Sign-On (SSO).



3. Wählen Sie Ihre SSO-Optionen aus.
    a. AuthnRequest signieren:
        - Ja (Standard)
        - Nein
    b. Algorithmus zum Signieren der Authentifizierungsanfrage:
        - SHA1 (Standard)
        - SHA256
    c. SAML-Bindungsanfrage:
        - HTTP-Weiterleitung (Standard)
        - HTTP-Post
    d. AuthnContextClassRef:
        - Diesen Wert nicht senden (Standard)
        - urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport
        - urn:oasis:names:tc:SAML:2.0:ac:classes:kerberos
        - urn:federation:authentication:windows
        - PasswordProtectedTransport und Fenster
        - urn:oasis:names:tc:SAML:2.0:ac:classes:X509
        - urn:oasis:names:tc:SAML:2.0:ac:classes:TLSClient
    e. Mapping für eigenes Attribut: Sie können eine Zuordnung für benutzerdefinierte Namen festlegen, um diese an die IdP-Einstellungen anzupassen (wenn Sie nicht die Standard-Mappings nutzen möchten). Geben Sie Ihr benutzerdefiniertes Attribut ein und wählen Sie das Attribut aus, dem Sie das benutzerdefinierte Attribut zuordnen möchten. Die folgenden Felder lassen sich benutzerdefinierten, vom Mitglied bereitgestellten Attributen zuordnen.
        - Vorname
        - Nachname
        - Primäre E-Mail-Adresse
        - Mobiltelefonnummer
        - Geschäftl. Telefon
        - Jobbezeichnung
        - Tätigkeitsbereich
        - Manager
        - Abteilung
        - Job-Level
        - Arbeitertyp
        - Status des Arbeitnehmers
        - Building-Code
        - Standort des Schreibtischs

        Weitere Informationen zu Standardattributen finden Sie unter Anforderungen für „Just-in-Time-Provisioning“ (JIT).

### Vorname (optional)

Unter Umständen senden Identitätsanbieter nicht nur E-Mail-Adressen, sondern auch Vornamen in unterschiedlichen allgemeinen Feldern. Damit eine unmittelbare Kompatibilität mit einem Großteil der Identitätsanbieter gewährleistet ist, sucht LinkedIn in den folgenden Attributnamen nach dem Vornamen:

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

### Nachname (optional)

LinkedIn sucht in den folgenden Attributnamen nach dem Nachnamen:

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

### Zusätzliche optionale Attribute

Sie haben die Möglichkeit, zusätzliche Informationen anzugeben, einschließlich der folgenden Attributnamen.

**Hinweis:** Diese Attribute werden zwar von LinkedIn gespeichert, werden derzeit aber nicht auf der Benutzeroberfläche angezeigt und sind daher nicht für die Benutzerverwaltung nutzbar.

| Attributname | Unterstützte Variationen |
|---|---|
| Abteilung | • departmentName<br>• department<br>• User.Department |
| Manager | • Manager<br>• manager<br>• User.Manager |
| Mobiltelefon-nummer | • mobilePhoneNumber<br>• PhoneNumber<br>• phone |

| | |
|---|---|
| | • phoneNumber<br>• User.PhoneNumber<br>• http://schemas.xmlsoap.org/ws/2005/05/identity/claims/mobilephone |
| Geschäftliche Telefonnummer | • WorkPhoneNumber<br>• Workphone<br>• workPhoneNumber<br>• User.WorkPhoneNumber<br>• http://schemas.xmlsoap.org/ws/2005/05/identity/claims/otherphone |
| Jobbezeichung | • workTitle<br>• Title<br>• WorkTitle<br>• User.WorkTitle |
| Tätigkeitsbereich | • jobFunction<br>• JobFunction<br>• User.JobFunction |
| Job-Level | • JobLevel<br>• jobLevel<br>• User.JobLevel |
| Arbeitnehmertyp | • WorkerType<br>• workerType<br>• User.WorkerType |
| Status des Arbeitnehmers | • WorkerStatus<br>• workerStatus<br>• Status<br>• User.WorkerStatus |
| Building-Code | • buildingCode<br>• building |
| Standort des Schreibtischs | • deskLocation<br>• desk |

Beispiel

E-Mail-Adresse: mmustermann@unternehmen.com
Vorname: Max
Nachname: Mustermann
Mobiltelefonnummer: 5551234567
Titel: Manager, Abteilung für Softwareentwicklung
Abteilung: Softwareanwendungen
Startdatum: 07.03.16
Job-Level: Einzelner Mitarbeiter
Arbeitnehmertyp: Mitarbeiter
Status des Arbeitnehmers: aktiv oder inaktiv
Manager: dmüller

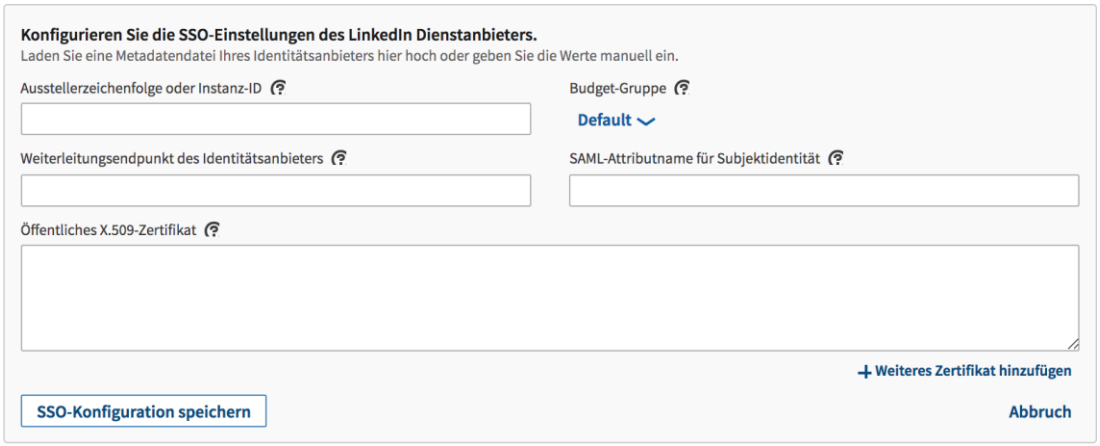
## Hochladen einer Datei

1. Klicken Sie auf **XML-Datei hochladen**, um die Metadatendatei von Ihrem Identitätsanbieter hochzuladen.


2. Wählen Sie die Datei und klicken Sie auf **Öffnen**. Sofern der Vorgang erfolgreich war, werden die angezeigten Felder mit Metadaten ausgefüllt.

## Manuelles Eingeben von Werten

1. Nutzen Sie den Link **Hier klicken**, um Informationen manuell hinzuzufügen.



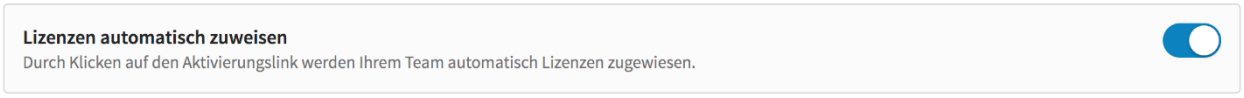
Geben Sie die folgenden Informationen ein:

- Ausstellerzeichenfolge oder Instanz-ID: muss mit dem Feld „md:EntityDescriptor `entityID`“ übereinstimmen.
- Budgetgruppe: eine Gruppe, die Sie nutzen können, um Lizenzen über *Just-in-Time* bereitzustellen.
- Weiterleitungs-URL: muss mit dem Feld „md:SingleSignOnService `location`“ übereinstimmen.
  - **Hinweis:** LinkedIn bietet derzeit nur Unterstützung für die „urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect“-Bindung.
- Ort für SAML-Identität: Dieses Feld dient dazu, die in Ihrem Identitätsanbieter gespeicherte Mitarbeiteridentität mit der Mitarbeiteridentität abzugleichen, die über den EDI-Prozess bei LinkedIn gespeichert ist. LinkedIn nutzt die folgenden Regeln für die Ermittlung des Mitarbeiters:
  - Wenn die SAML-Authentifizierungsantwort eine SAML-Assertation bereitstellt, in der ein Attributsatz enthalten ist, können Sie den SAML-Attributnamen des Attributs angeben, der die Identität des Mitarbeiters in diesem Textfeld enthält. Wenn beispielsweise ein Integer `employeeId` in einem SAML-Attribut mit dem Namen `employeeId` gesendet wird, besteht die Möglichkeit, `employeeId` in das Feld **Ort für SAML-Identität** einzufügen. LinkedIn nutzt dann die in jeder Assertation gesendete „employeeId“, um die Mitarbeiteridentität zu ermitteln. Wenn Sie diesen Prozess nutzen möchten, müssen Sie die „employeeId“ jedes Mitglieds in den EDI-Prozess hochladen.
  - Wenn in diesem Feld nichts angegeben ist, sucht LinkedIn den Mitarbeiter anhand des Werts von `NameId`, übermittelt in `<saml:Subject>`. In diesem Feld *muss* die primäre E-Mail-Adresse des Mitglieds angegeben sein, gemäß des Uploads im Rahmen des EDI-Prozesses.
- Wenn wir das Mitglied nicht anhand des im Feld **Ort für SAML-Identität** festgelegten Attributs und auch nicht anhand der primären E-Mail-Adresse, gemäß der Festlegung in „NameId“ in `<saml:Subject>`, finden können, authentifiziert LinkedIn das Mitglied *nicht*.
- Öffentliches Zertifikat: LinkedIn prüft die Gültigkeit der SAML-Assertation, die während der SAML-Authentifizierungsantwort gesendet wird, mithilfe des x.509-Zertifikats, das von Ihrem Identitätsanbieter für die Signatur genutzt wird. Wenn wir die Signatur der Authentifizierungsantwort nicht prüfen können, wird Ihr Mitglied nicht authentifiziert.

3. Klicken Sie auf **SSO-Konfiguration speichern**.

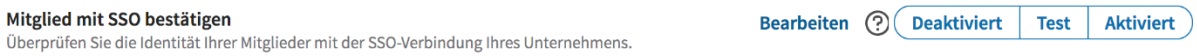
## Zuweisen von Lizenzen

Sie haben die Möglichkeit, Ihren Mitarbeitern Lizenzen automatisch zuzuweisen, indem Sie die Option **Lizenzen automatisch zuweisen** aktivieren. Sobald die Option aktiviert ist, erhalten Mitglieder automatisch eine Lizenz, sofern sie nicht bereits über eine verfügen.
**Hinweis:** Die Benutzerattribute, die auf Seiten des Identitätsanbieters erforderlich sind, werden angezeigt, wenn Sie die automatische Zuweisung von Lizenzen aktivieren.




**Hinweis:** Für Sales Navigator wird die automatische Zuweisung von Lizenzen derzeit nicht unterstützt.

# Aktivieren von Single Sign-On




Nachdem Sie Ihre Konfiguration abgeschlossen haben, aktivieren Sie SSO. Klicken Sie auf die Umschaltoption **Mitglied mit SSO bestätigen**. In der Tabelle Aktivieren von Optionen werden Informationen dazu aufgeführt, wann die verfügbaren Optionen genutzt werden.

## Aktivieren von Optionen

| Status | Beschreibung |
|---|---|
| Aus | • Keine Einrichtung für SSO-Implementierung erforderlich.<br>• Mitglieder können sich über ihre Logik auf Basis von LinkedIn für zugewiesene Lizenzen einloggen. |
| Test | • SSO wird eingerichtet und konfiguriert.<br>• Der Testmodus erzwingt SSO für Abläufe, die über IdP initiiert werden, für Mitarbeiter, denen Zugriff über den IdP gewährt wird. Normale Anmeldungen auf Basis von LinkedIn sind allerdings weiterhin für die Abläufe möglich, die über SP initiiert werden. Dabei ist es nicht erforderlich, dass Mitglieder sich für die Anmeldung über den IdP authentifizieren. Sie können direkt über LinkedIn auf die Anwendung zugreifen.<br>• Dies ist bei der Erstkonfiguration von SSO nützlich oder wenn Ihr Identitätsanbieter nur Abläufe unterstützt, die über den IdP initiiert werden. |
| Ein | • SSO wird eingerichtet und aktiviert.<br>• Benutzer müssen sich über den IdP- oder SP-initiierten Ablauf einloggen (es sei denn, der IdP unterstützt nur Abläufe, die über den IdP-Ablauf initiiert werden, in welchem Fall kein SP initiiert wird). Unabhängig von der Methode ist eine Authentifizierung erforderlich.<br><br>**Achtung:** Wenn Sie nach der Ersteinrichtung die Option **Ein** auswählen, schließen Sie das Fenster nicht, bis SSO wie gewünscht funktioniert. Andernfalls müssen Sie den Kundenservice einbeziehen, um SSO für Ihr Konto zu deaktivieren. Wir empfehlen, dass Sie die Option **Test** für die Prüfung des über IdP initiierten Ablaufs nutzen, bevor Sie für SSO die Option **Ein** auswählen. |

- Über den IdP initiierter Ablauf: Wenn ein Mitglied über den Identitätsanbieter (wie z. B. Okta, AAD oder Ping) auf eine Anwendung zugreifen möchte.
- Über den SP eingeleiteter Ablauf: Wenn ein Mitglied direkt über die Anwendung oder den Dienstanbieter auf seine Lizenz zugreifen möchte.

## Prüfen der Einrichtung

**Hinweis:** Bevor Sie Ihre Einrichtung prüfen können, muss die Bindung abgeschlossen sein. Informationen sowie eine schrittweise Beschreibung der Bindung finden Sie im Whitepaper von LinkedIn zu Datenschutz und Sicherheit: Account Center Employee Database Integration (EDI) and Single Sign-On (SSO).

Stellen Sie sicher, dass die Integration mit Ihrem Identitätsanbieter ordnungsgemäß erfolgt ist und folgende Voraussetzungen erfüllt sind:

- Sie benötigen eine LinkedIn Anwendung, der Ihre Unternehmensidentität bereits hinzugefügt wurde (beispielsweise über einen CSV-Upload).
- SSO ist aktiviert.
- Sie verfügen über eine Anwendung, die gemäß der vorstehenden Beschreibung und zur jeweiligen LinkedIn Anwendung passend in Ihrem Identitätsanbieter konfiguriert wurde.

Testen Sie Folgendes:

- Eine über Ihren Identitätsanbieter initiierte Anmeldung
- Anmeldung über die LinkedIn Empfehlungsseite

# Support

## Support-Dokumentation

- Administratorleitfaden zum Hinzufügen von Mitarbeiterdaten
- Whitepaper zu Datenschutz und Sicherheit: Account Center Employee Database Integration (EDI) and Single Sign-On (SSO)
- Tutorial: Azure Active Directory-Integration mit LinkedIn Learning
- Tutorial: Azure Active Directory-Integration mit LinkedIn Sales Navigator
- Tutorial: Azure Active Directory-Integration mit LinkedIn Elevate

## Technische Probleme

Wenn Sie bei der Einrichtung von SSO auf technische Probleme stoßen, wenden Sie sich über den Hilfebereich an Ihr Account-Team oder das Team für den Anwendungssupport.

## LinkedIn Datenschutz- und Datensicherheitsrichtlinie

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

## LinkedIn Ansprechpartner zum Thema Sicherheit

Wenn Sie Fragen zum Thema Sicherheit haben oder ein Sicherheitsproblem melden möchten, schreiben Sie uns unter security@linkedin.com.