



Single Sign-On Administrator Guide

**Last Revised October 26, 2016
Version 1.1**

Disclaimer

© 2016 LinkedIn Corporation, All Rights Reserved

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

This document may contain forward looking statements. Any information in this document is subject to change without notice. The software (and related documentation) may be used or copied only in accordance with the terms of your license agreement with us. No part of the software or documentation may be reproduced, transmitted, or translated in any form or by any means, electronic, mechanical, manual, optical, or otherwise, in part or in whole, except in accordance with the terms of your license agreement with us.

LinkedIn Corporation and the LinkedIn Corporation logo are trademarks, servicemarks, or registered trademarks of LinkedIn Corporation in the United States and other countries. All other brand, service or product names are trademarks or registered trademarks of their respective companies or owners.

Contents

[Disclaimer](#)

[Contents](#)

[Overview](#)

[Prerequisites](#)

[About Single Sign-On \(SSO\)](#)

[Why Should you use Single Sign-On?](#)

[Supported SSO Protocols](#)

[Configuring Single Sign-On \(SSO\)](#)

[Getting Started with SSO](#)

[Connecting to your Identity Provider](#)

[Downloading a File](#)

[Working with Individual Fields](#)

[Configuring your Identity Provider](#)

[Requirements for Just-in-Time \(JIT\) Provisioning](#)

[Email Address \(Required\)](#)

[First Name \(Optional\)](#)

[Last Name \(Optional\)](#)

[Additional Optional Attributes](#)

[Example](#)

[Uploading a File](#)

[Entering Values Manually](#)

[Assigning Licenses](#)

[Enabling Single Sign-On](#)

[Verifying your Setup](#)

[Support](#)

[Supporting Documentation](#)

[LinkedIn's Privacy and Data Security Policy](#)

[LinkedIn Security Contacts](#)

Overview

User Database Integration (UDI) allows your company to integrate its HRIS employee data into LinkedIn applications. The integration includes an optional configuration for Single Sign-On with your SSO solution. In this case, the administrator for your company account can configure your company to authenticate to a LinkedIn platform application using SSO through integration with the enterprise platform.

The integration is configured through the LinkedIn Account Center and is only available for some paid LinkedIn applications (for example, LinkedIn Learning or Elevate).

Prerequisites

- Company account
- Super administrator privileges
- Identity Provider (IdP) administrative privileges

About Single Sign-On (SSO)

Enterprise Single Sign-On (SSO) allows your company's employees to sign into supported LinkedIn applications using their corporate credentials instead of their LinkedIn credentials.

Using SSO and integrating with an SSO provider is not required to use LinkedIn applications. If SSO is not configured, your employees can authenticate themselves using their current personal LinkedIn credentials or create a new member account.

Why Should you use Single Sign-On?

- Leverage your existing company's authentication
- Better security when employees use your company's established password protocols rather than their individual accounts
- Easier user management when employees leave your company

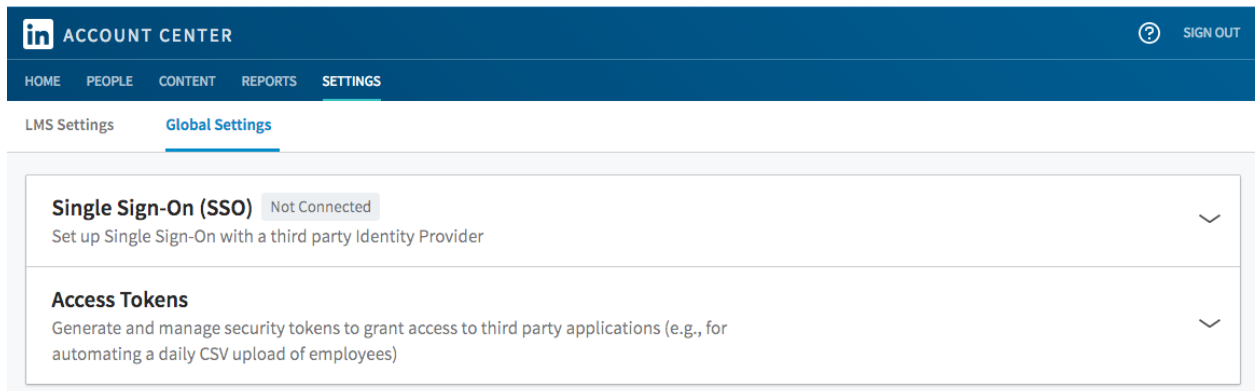
Supported SSO Protocols

We currently support SAML version 2.0.

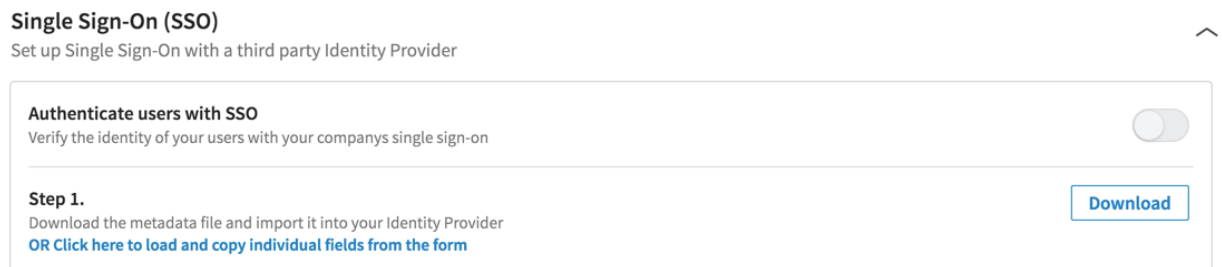
Configuring Single Sign-On (SSO)

Getting Started with SSO

1. Log in to the Account Center using your Enterprise Administrator role.
2. Select the **Settings** tab.
3. Select the **Global Settings** tab.



4. Open the Single Sign-On (SSO) panel.



Connecting to your Identity Provider

If your identity provider supports metadata, and if you've configured SAML using version 2.0, you can download an XML configuration file to send them, which they can then upload to automatically configure their settings for connecting to your LinkedIn products.

Determine if you can download a metadata file or if you need to work with individual fields, then follow one of the procedures in the next sections.

Downloading a File

1. Click **Download** to download a metadata file you can use with your Identity Provider system. The `metadata.xml` file downloads through your browser.
2. Verify that the metadata file contains the following:

```
<md:AssertionConsumerService
Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
Location="https://www.linkedin.com/checkpoint/enterprise/saml/[AC
COUNT ID]" index="0"/>
```

3. Access your Identity Provider system.
4. Upload the metadata file.
Note: You might not be able to import this file into your Identity Provider. For example, Okta does not have this functionality.
5. Return to the SSO setup.
6. Click **OK** on the upload dialog, then see [Connecting to your Identity Provider](#).

Working with Individual Fields

1. Click the link to load and copy individual fields from the form in your Identity Provider.

Step 1.

Download the metadata file and import it into your Identity Provider

OR [Click here to load and copy individual fields from the form](#)

Download

Entity ID

linkedin.com

Assertion Consumer Service (ACS) URL

https://www.linkedin.com/checkpoint/enterprise/saml/1005904

SP X.509 Certificate (signing)

```
MIIDozCCAougAwIBAgJAKLIyNzF3mW7MA0GCSqGSIb3DQEBBQUAMGxwCzAJBgNVBAYTA1VTMzsw
CQYDVQQLDAJDQTEWMBQGA1UEBwwNTW91bnRhaW4gVmlldzEdMBsGA1UECgwUTGlua2Vka29y
cG9yYXRpb24xFTATBgNVBAMMDGxpbnRhaW4gVmlldzEdMBsGA1UECgwUTGlua2Vka29y
MjAzNDRaMGxwCzAJBgNVBAYTA1VTMzswCQYDVQQLDAJDQTEWMBQGA1UEBwwNTW91bnRhaW4gVmlldzEdMBsGA1UECgwUTGlua2Vka29y
```

2. Copy and paste the fields you want to include.

Configuring your Identity Provider

Configure your Identity Provider to talk with LinkedIn's platform. Determine if you can upload a metadata file from your Identity Provider or if you need to enter values manually, then follow one of the procedures in the next sections.

Requirements for Just-in-Time (JIT) Provisioning

One reason SAML 2.0 has become so popular is its flexibility when sending extra information to the service provider. When an identity provider sends an assertion, it includes attributes describing the user. These attributes allow LinkedIn to both identify the user and automatically provision users. A few of the possible attributes are described in this section.

Email Address (Required)

Every user is required to have a valid email address, even when using SSO. Since the identity provider is responsible for managing user information, it must send the user's email address in its assertion. Identity providers use different naming conventions, so LinkedIn Learning looks for an email address in the following attribute names sequentially:

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

First Name (Optional)

Just like email addresses, identity providers might send the first name in several common fields. To provide out-of-the-box compatibility with most identity providers, LinkedIn tries to find the first name in the following attribute names:

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

Last Name (Optional)

LinkedIn looks for the last name in the following attribute names:

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

Additional Optional Attributes

Optionally, you can provide additional information, including the following attribute names.

Attribute Name	Supported Variations
Department	<ul style="list-style-type: none">• departmentName• department• User.Department
Manager	<ul style="list-style-type: none">• Manager• manager• User.Manager
Mobile Phone Number	<ul style="list-style-type: none">• mobilePhoneNumber• PhoneNumber• phone• phoneNumber• User.PhoneNumber• http://schemas.xmlsoap.org/ws/2005/05/identity/claims/mobilephone
Work Phone Number	<ul style="list-style-type: none">• WorkPhoneNumber• Workphone• workPhoneNumber• User.WorkPhoneNumber• http://schemas.xmlsoap.org/ws/2005/05/identity/claims/otherphone
Work Title	<ul style="list-style-type: none">• workTitle• Title• WorkTitle• User.WorkTitle
Job Function	<ul style="list-style-type: none">• jobFunction• JobFunction• User.JobFunction
Job Level	<ul style="list-style-type: none">• JobLevel• jobLevel• User.JobLevel
Worker Type	<ul style="list-style-type: none">• WorkerType• workerType

	<ul style="list-style-type: none"> • User.WorkerType
Worker Status	<ul style="list-style-type: none"> • WorkerStatus • workerStatus • Status • User.WorkerStatus
Building Code	<ul style="list-style-type: none"> • buildingCode • building
Desk Location	<ul style="list-style-type: none"> • deskLocation • desk

Example

Email: jdoe@company.com

First name: Jane

Last Name: Doe

Mobile Phone Number: 5551234567

Title: Manager, Software Engineering

Department: Software Applications

Start Date: 03/07/16

Job Level: Individual Contributor

Worker Type: employee

Worker Status: active or inactive

Manager: dsmith

Uploading a File

1. Click **Upload XML file** to add the metadata file from your Identity Provider.

Step 2.

Now, get a metadata file from your Identity Provider and upload it here, or manually enter values

Go to your Identity Provider (e.g. Okta) to get the information you need.

[Upload XML file](#)

Want to input the information manually? [Click here](#)

2. Select the file and click **Open**. If successful, the fields display filled with the metadata.

Entering Values Manually

1. Use the **Click here** link to add information manually.

Step 2.

Now, get a metadata file from your Identity Provider and upload it here, or manually enter values

Issuer String or Entity ID

Redirect URL

SAML Identity location

Public Certificate

[Save SSO Configuration](#)

[Cancel](#)

2. Enter the following information:
 - Issuer String or Entity ID: must match the `md:EntityDescriptor entityID` field
 - Redirect URL: must match the `md:SingleSignOnService location` field
 - **Note:** LinkedIn currently only supports the `urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect` binding.
 - SAML identity location: This is the field used to identify the employee identity stored in your Identity Provider with the employee identity stored through the UDI process at LinkedIn. LinkedIn uses the following rules to identify the employee:
 - If the SAML Authentication response provides a SAML assertion containing a set of attributes, you can provide the SAML attribute name of the attribute containing the employee's identity in this text field. For example, if an integer `employeeId` is sent in a SAML attribute called `employeeId`, you could insert `employeeId` into the **SAML identity location** field, and LinkedIn uses the `employeeId` sent in each assertion to look up the employee identity. To enable this, you must upload the `employeeId` of each user in the UDI process.
 - If nothing is specified in this field, LinkedIn looks up the employee by the value of the `NameId` sent in the `<saml:Subject>`. This field *must* be the primary email address of the user, as uploaded during the UDI process.
 - If we cannot find the user by either the attribute set in the **SAML identity location** field or by the primary email address, as set in the `NameId` in the `<saml:Subject>`, LinkedIn does *not* authenticate the user.

- Public Certificate: LinkedIn verifies the validity of the SAML assertion sent in the SAML authentication response using the x.509 certificate used for signing by your Identity Provider. If we cannot validate the signature of the authentication response, your user is not authenticated.
3. Click **Save SSO Configuration**.

Assigning Licenses

You can automatically assign licenses to your employees by toggling **Automatically assign Learning licenses**. When enabled, users are automatically granted a license if they don't already have one.

Note: User attributes required on the Identity Provider side display when you enable automatic licenses.

Single Sign-On (SSO) Not Connected

Set up Single Sign-On with a third party Identity Provider

Authenticate users with SSO
Verify the identity of your users with your companys single sign-on Edit

Step 1.
Download the metadata file and import it into your Identity Provider
[OR Click here to load and copy individual fields from the form](#) Download

Automatically assign Learning licenses
Your team will be automatically granted licenses by clicking on activation link

Enabling Single Sign-On

After you have completed your configuration, enable SSO. Click the **Authenticate users with SSO** toggle.

Warning: Do not close the window until you are sure SSO is working properly; otherwise, you will need to contact customer support to disable SSO on your account.

Verifying your Setup

Verify that you're correctly integrated with your Identity Provider and have the following in place:

- Have a LinkedIn application with your enterprise identity added (for example, through a CSV upload)
- SSO is enabled
- An application configured in your Identity Provider, corresponding to the LinkedIn application, configured as previously instructed

Test using:

- Your Identity Provider initiated login
- LinkedIn's referral page, then log in

Support

Supporting Documentation

- Adding Employee Data Administrator Guide
- Privacy and Security Whitepaper: Account Center User Database Integration (UDI)

LinkedIn's Privacy and Data Security Policy

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

LinkedIn Security Contacts

If you have any security questions or you would like to report a security issue, write to us at security@linkedin.com.