



# Single Sign-On Administrator Guide

**Last Revised May 26, 2017**  
**Version 1.5**

# Disclaimer

© 2017 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](#)

[Enable Options](#)

[Verifying your Setup](#)

[Support](#)

[Supporting Documentation](#)

[Technical Issues](#)

[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.

## 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, with the exception of Lookup Enterprise. 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
- SSO is a requirement for Lookup Enterprise

## Supported SSO Protocols

We currently support SAML version 2.0.

# Configuring Single Sign-On (SSO)

## Getting Started with SSO

1. Access the Account Center using the following link:  
<http://www.linkedin.com/enterprise/accountcenter/settings>

**Note:** Some applications also have an access point from their application settings. For example, in Learning you can click **Go to Admin** in the banner and select **Settings > Global Settings**.

The application settings for SSO reflect the application you have accessed.

The screenshot displays the LinkedIn Account Center interface. At the top, there is a navigation bar with the LinkedIn logo, 'ACCOUNT CENTER', and a 'Learning - Default' indicator. Below this, a menu includes 'HOME', 'PEOPLE', 'CONTENT', 'REPORTS', and 'SETTINGS'. The 'Global Settings' tab is selected. The main content area is divided into two sections: 'Application Settings' and 'Global Settings'. Under 'Application Settings', there is a 'Single Sign-On (SSO)' option with a description: 'Set up Single Sign-On with a third party Identity Provider'. Under 'Global Settings', there are three options: 'SCIM Setup' (Add configurations to integrate your user database using a SCIM Server), 'OAuth Access Tokens' (Generate and manage security tokens to grant access to third party applications (e.g., for automating a daily CSV upload of employees)), and 'SFTP Setup' (Create Users that will be able to upload CSV files via SFTP). Each option has a downward arrow icon on the right side.

## 2. Open the Single Sign-On (SSO) panel.

The screenshot shows the 'Single Sign-On (SSO)' configuration panel. At the top, it says 'Set up Single Sign-On with a third party Identity Provider'. Below this, there's a section 'Authenticate users with SSO' with a status indicator showing 'OFF', 'TEST', and 'ON' buttons. The main content area has two sections: 'Configure your Identity provider SSO settings.' with a 'Download' button and a link to load and copy individual fields, and 'Configure the LinkedIn service provider SSO settings.' with instructions to get a metadata file and an 'Upload XML file' button. A note at the bottom of the second section says 'Want to input the information manually? Click here'.

3. (Optional) If you need to configure multiple application instances, you can select the **<application name> - <instance>** menu in the banner, then select the instance you want to configure. For example, in Learning you might be selecting the **Learning - Default** menu (as shown in the screenshot in Step 1).

**Note:** Application instances in the menu are organized by application, so if you have access to multiple instances of the same application (for example, two Recruiter instances), then you see a header for Recruiter followed by the names of the individual application instances.

## 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`



Because 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 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

You can provide additional information, including the following attribute names.

**Note:** While these attributes are stored by LinkedIn, they are currently not visible from the UI to use for user management.



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

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

### 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](#)

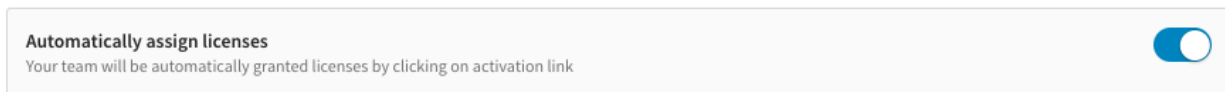
2. Enter the following information:
  - Issuer String or Entity ID: must match the `md:EntityDescriptor entityID` field
  - Redirect URL: must match the `md:SingleSignOnService location` field
    - **Note:** LinkedIn currently only supports the `urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect` binding.
  - 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 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.



**Note:** Automatically assigning licenses is not currently supported for Lookup or Sales Navigator.

## Enabling Single Sign-On

Authenticate users with SSO

Verify the identity of your users with your company's single sign-on



After you have completed your configuration, enable SSO. Click the **Authenticate users with SSO** toggle. See the [Enable Options](#) table for information about when to use the available options.

### Enable Options

Status	Description
Off	<ul style="list-style-type: none"> <li>• No SSO implementation setup required.</li> <li>• Users can sign in to assigned licenses with their LinkedIn-based logic.</li> </ul>
Test	<ul style="list-style-type: none"> <li>• SSO is set up and configured.</li> <li>• Test mode enforces SSO for IdP-initiated flows for employees given access through the IdP, but still allows normal LinkedIn-based sign in for SP-initiated flows. It does not require users to authenticate through the IdP to sign in. They can access the application directly through LinkedIn.</li> <li>• This is useful when configuring SSO for the first time, or if your IdP only supports IdP-initiated flows.</li> </ul>
On	<ul style="list-style-type: none"> <li>• SSO is set up and enabled.</li> <li>• Users must sign in through the IdP-initiated flow or SP-initiated flow (unless IdP only supports IdP-initiated flow, in which case they do not</li> </ul>

	<p>have SP-initiated). Regardless of which method is used, authentication is required.</p> <p><b>Warning:</b> When selecting <b>On</b> after initial setup, 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. It's recommended that you use the <b>Test</b> option to validate your IdP-initiated flow before setting SSO to <b>On</b>.</p>
<ul style="list-style-type: none"><li>• IdP-Initiated Flow: When a user starts in their Identity Provider (such as Okta, AAD, or Ping) to access an application.</li><li>• SP-Initiated Flow: When a user goes directly to the application or service provider to access their license.</li></ul>	

## Verifying your Setup

**Note:** Before verifying your setup, you must have your binding completed. For information and steps on binding, see LinkedIn's Privacy and Security Whitepaper: Account Center Employee Database Integration (EDI) and Single Sign-On (SSO).

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 sign in
- LinkedIn's referral page, then sign in

# Support

## Supporting Documentation

- Adding Employee Data Administrator Guide
- Privacy and Security Whitepaper: Account Center Employee Database Integration (EDI) and Single Sign-On (SSO)
- [Tutorial: Azure Active Directory integration with LinkedIn Lookup](#)

## Technical Issues

If you have technical issues with the SSO setup, contact your account team or application support team through the help center.

## 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](mailto:security@linkedin.com).