Single Sign-On Administrator Guide

Last Revised May 26, 2017
Version 1.5

Disclaimer

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

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.

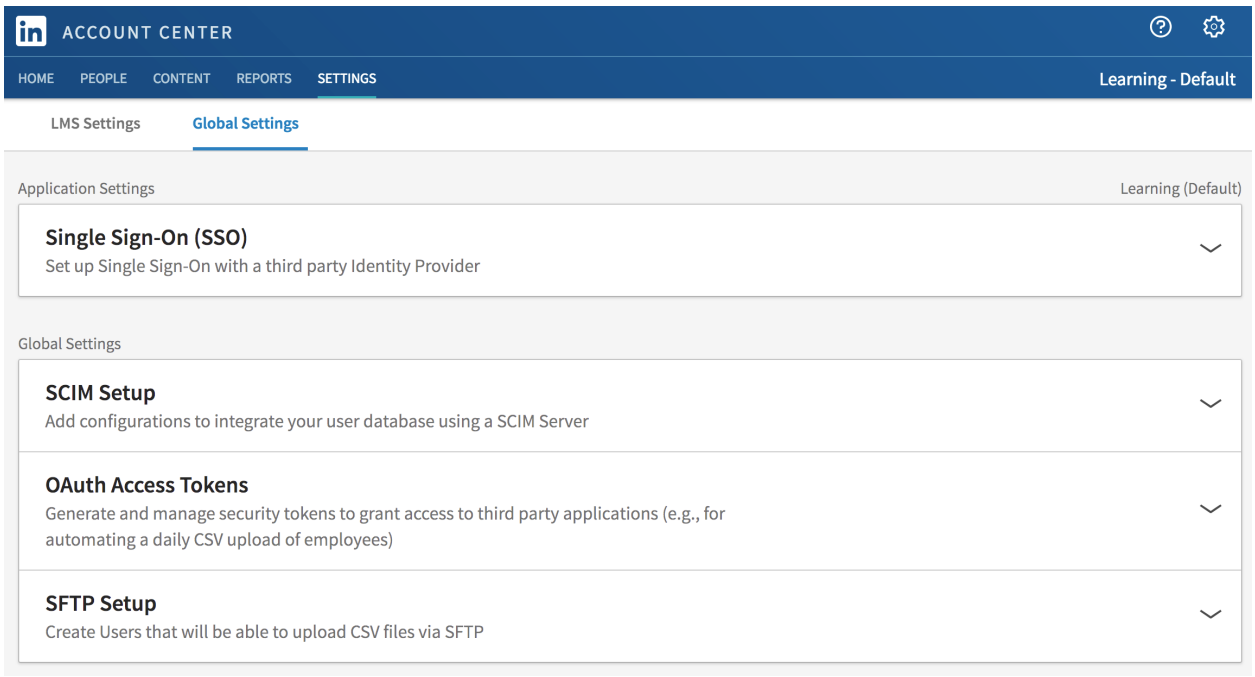
Configuring Single Sign-On (SSO)

Getting Started with SSO

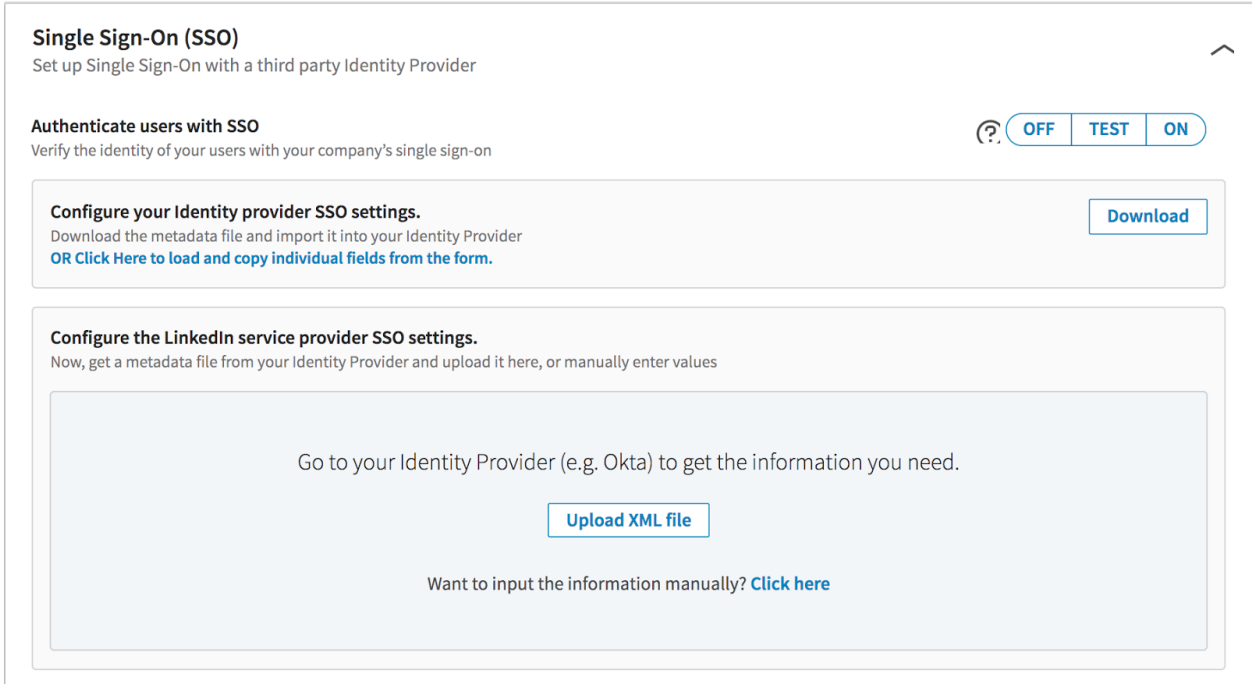
1. Access the Account Center using the following link:
   http://www.linkedin.com/enterprise/accountcenter/settings

   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.



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



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

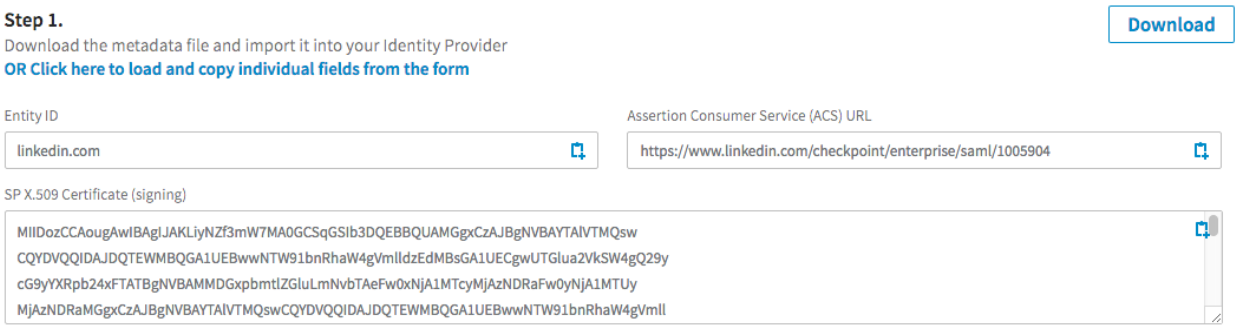
1. Click **Download** to download a metadata file you can use with your Identity Provider system. The `metadata.xml` file downloads through your browser.
2. Verify that the metadata file contains the following:
   `<md:AssertionConsumerService`

```
Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
Location="https://www.linkedin.com/checkpoint/enterprise/saml/[ACCOUNT 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 Configuring your Identity Provider.

Working with Individual Fields

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



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. If you aren't using JIT, proceed to Uploading a File or Entering Values Manually.

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.

Note: When testing with multiple IdP identities, email addresses must be unique.

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	• departmentName • department • User.Department
Manager	• Manager • manager • User.Manager
Mobile Phone Number	• mobilePhoneNumber • PhoneNumber • phone • phoneNumber • User.PhoneNumber • http://schemas.xmlsoap.org/ws/2005/05/identity/claims/mobilephone
Work Phone Number	• WorkPhoneNumber • Workphone • workPhoneNumber • User.WorkPhoneNumber • http://schemas.xmlsoap.org/ws/2005/05/identity/claims/otherphone
Work Title	• workTitle • Title • WorkTitle • User.WorkTitle
Job Function	• jobFunction • JobFunction • User.JobFunction
Job Level	• JobLevel • jobLevel • User.JobLevel
Worker Type	• WorkerType • workerType • User.WorkerType
Worker Status	• WorkerStatus

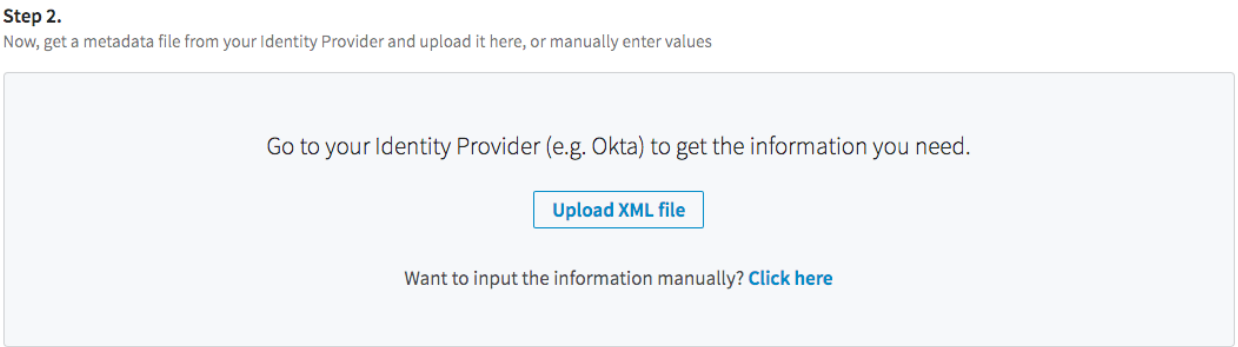
	• workerStatus • Status • User.WorkerStatus
Building Code	• buildingCode • building
Desk Location	• deskLocation • desk

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

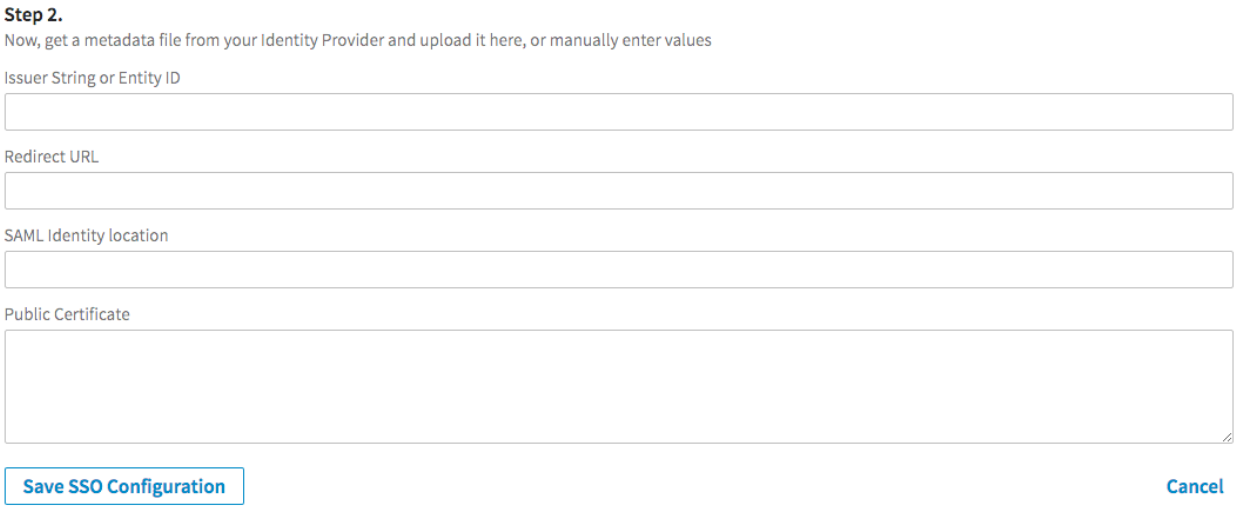
1. Click **Upload XML file** to add the metadata file from your Identity Provider.



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.



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.

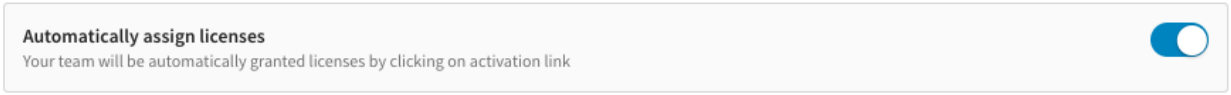
- Public Certificate: LinkedIn verifies the validity of the SAML assertion sent in the SAML authentication response using the x.509 certificate used for signing by your Identity Provider. If we cannot validate the signature of the authentication response, your user is not authenticated.

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

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	• No SSO implementation setup required. • Users can sign in to assigned licenses with their LinkedIn-based logic.
Test	• SSO is set up and configured. • 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. • This is useful when configuring SSO for the first time, or if your IdP only supports IdP-initiated flows.
On	• SSO is set up and enabled. • 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

	have SP-initiated). Regardless of which method is used, authentication is required. **Warning:** When selecting **On** 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 **Test** option to validate your IdP-initiated flow before setting SSO to **On**.
• IdP-Initiated Flow: When a user starts in their Identity Provider (such as Okta, AAD, or Ping) to access an application. • SP-Initiated Flow: When a user goes directly to the application or service provider to access their license.	

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.