



Recruiter Single Sign-On (SSO)

Introduction to SSO and implementation guide for:

okta



Who this guide is for



**Account Center
Administrators**



**IT / House Security
Professionals**



Table of contents

- 1 Introduction to Single Sign-On (SSO)
- 2 Activating SSO with Okta
- 3 Appendix

Introduction to Single Sign-On (SSO)



What is SSO?

SSO is a way of sharing security credentials and login information between different systems. It trusts one system (e.g. Okta) to authenticate a user's identity for another system (e.g. Recruiter).

SSO does not transfer user data to or from LinkedIn.

SSO Identity Providers (IdPs) include:



Azure
Active Directory

okta

onelogin

... and many more

Note: LinkedIn is SAML 2.0 certified and also supports Sign-In with Google. We currently don't support OAuth2.0 or OpenID.



Why use SSO for Recruiter?

Increased security

SSO offers the most secure way to log in to Recruiter by requiring employees to use your company's established authentication protocols.

Centralized access control

SSO simplifies the process of blocking access to an employee's corporate Recruiter License if they leave your company ([learn more](#)).

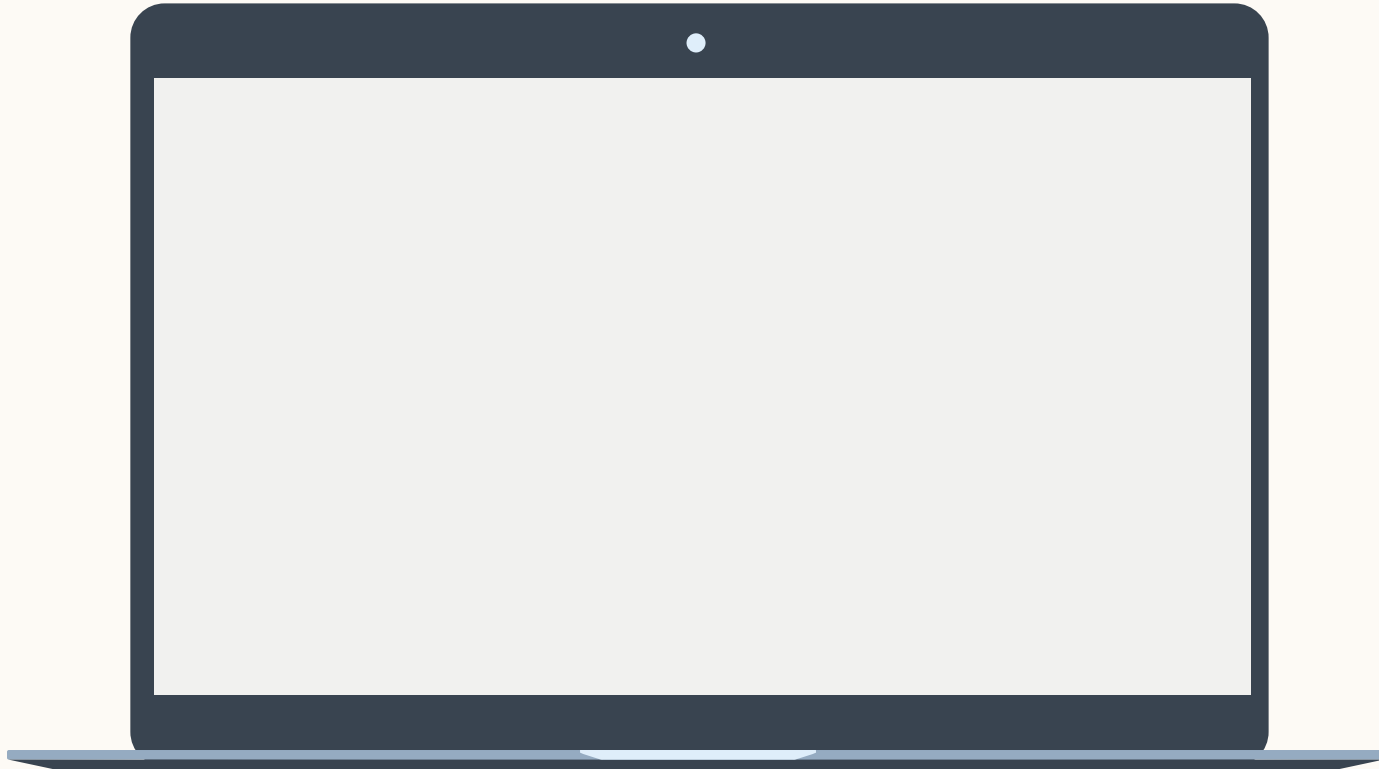
No need for 2FA

SSO eliminates LinkedIn's requirement for two factor authentication.



What does log-in look like?

With SSO set up, this is the user journey when logging in to Recruiter.



Why do users still need to enter LinkedIn login credentials?

Users must log in to their LinkedIn Member Identity once a day for security purposes.

Many Recruiter product features depend upon a user's personal LinkedIn account, using shared connections, degree of connection, and candidate feedback.

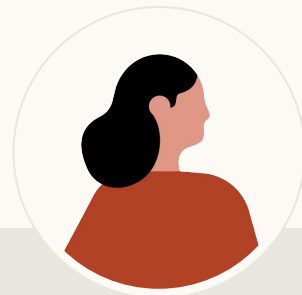
To enable this, recruiters and hiring managers must 'bind' (connect) their personal LinkedIn account with Recruiter. Once a day, you must log in to both your Corporate Identity using SSO and your LinkedIn Member Identity using standard login.



Corporate Identity

**Controlled centrally by
your employer**

**Information about you
and your position**



Member Identity

Controlled by you

**Information about your
entire career**

SSO does not solve for everything

It doesn't speed up log-in

Users still need to log in to their LinkedIn Profile once a day for security purposes.

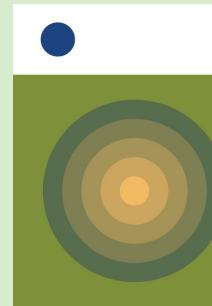
SSO adds slightly more friction, as users also need to periodically re-enter their SSO/IdP credentials (depending on the IdP session length set by the company).

It doesn't automate user management

Admins will still need to log in to Account Center to make changes such as:

- Granting Project Creator or Hiring Collaborator licenses to users
- Updating a user's permissions, roles, or access to Account Center
- Reassigning licenses/projects from one user to another
- Revoking a user's license/permissions
- Updating a user's email, name, license/permissions settings

[Learn more about managing licenses](#)



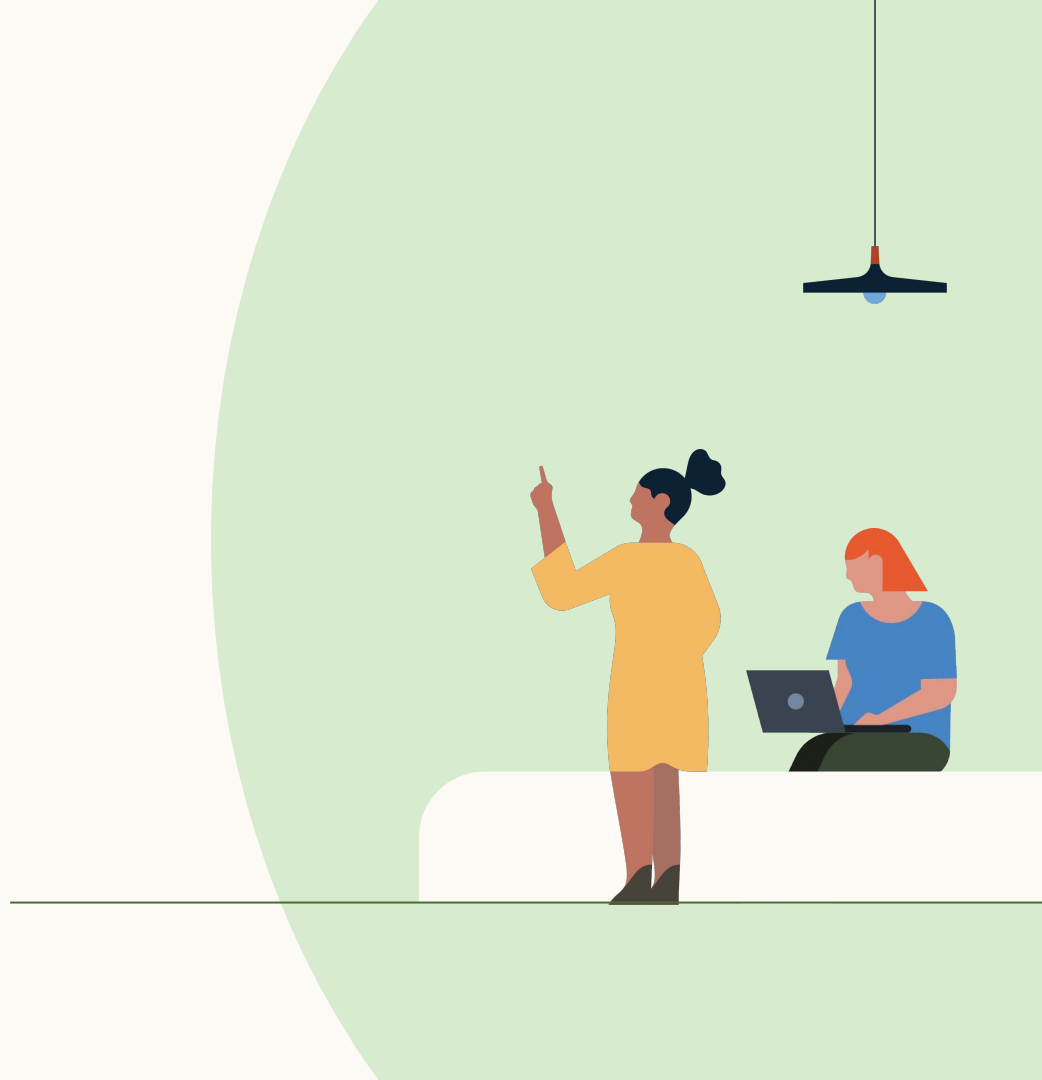
Changing the SSO session length

SSO session length (or timeout) refers to how long LinkedIn waits before re-pinging a user's IdP/SSO provider to re-authenticate the user. The default session length (or timeout) for LinkedIn Talent Solutions SSO is 8 hours.

To change the session length, please [file a support ticket](#).

Things to note:

- Every time LinkedIn re-authenticates a user through SSO, the user does not necessarily need to re-enter their IdP/SSO credentials. This depends on what the company sets up for their IdP session length.
- LinkedIn SSO session timeout does not impact a user's IdP or Recruiter session timeouts.
- Neither you nor LinkedIn can check your current SSO session length. For certainty, you can request an adjustment to the session length, based on your preference.



Changing session lengths



Is a short or long SSO session length best?

Short session timeout

A short session timeout **optimizes for security.**

If an employee leaves the company, you can block access to their Recruiter license by removing or deactivating them in your IdP platform.

However, users will be asked to re-enter their SSO credentials more frequently.

Long session timeout

A long session timeout **optimizes for usability.**

Users won't have to re-enter their SSO credentials as often.

However, if you want to stop a terminated employee from using Recruiter by removing or deactivating them in your IdP platform, a long session timeout is less effective. For example, if the session timeout is 30 days, and the user is removed from the IdP on day 1, they will still have access to Recruiter for another 29 days.



Deactivating users



What happens when a user leaves my organization?

If an employee leaves, the first thing your IT team should do is remove or deactivate the employee in your IdP platform.

Then, if the employee tries to access Recruiter and their SSO session has expired, login will fail as the IdP will no longer authenticate them. Note: If SSO session length is one week, the employee retains access for the full week, even if they are deactivated at the start of the week.

The Recruiter license will remain assigned to the employee until your Account Center admin parks, reassigns, or revokes it. This part is not done automatically.



Activating SSO with Okta

For help with other IdPs,
[see this guide](#)



Pre-work checklist for a successful SSO implementation

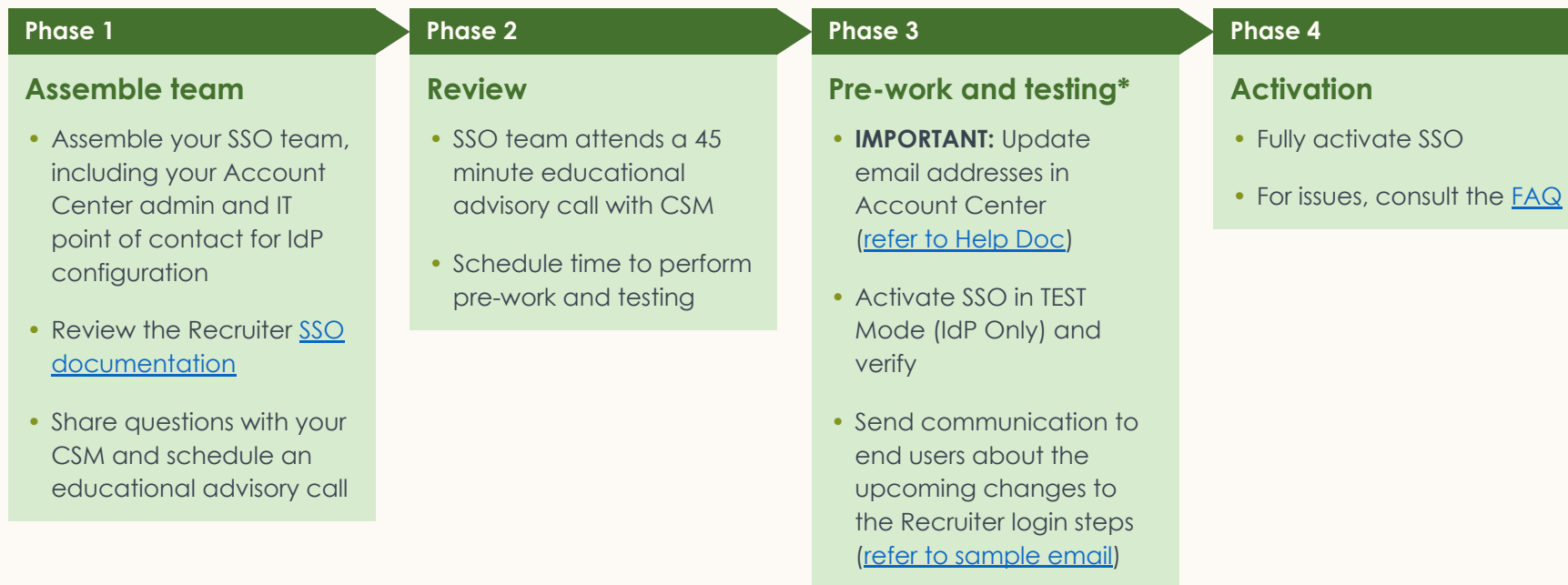
IMPORTANT: Admin(s) to confirm that all users have work emails in Account Center. If users don't have a work email, they will be locked out after SSO is activated. Work emails need to match the users' IdP-specific emails. Refer to the [Admin guide on updating user emails in Account Center](#).

- Confirm that your organization uses a SAML 2.0 compliant IdP (e.g. Okta, Azure Active Directory) or Sign-In with Google.
- Confirm which Recruiter dashboards will have SSO activated. Some organizations have more than one.
- Identify Account Center admin for each dashboard and any relevant internal IT point of contact. If you're not sure who your admins are, submit a ticket to LinkedIn customer support via the [Recruiter Help Center](#). To configure SSO, admins will need both IdP and Recruiter dashboard access:
 - IdP access: To arrange this, contact your IT or Security department (whoever has IdP admin/manager access), or your IdP service provider. Note that this may add extra time to your implementation.
 - Recruiter dashboard admin access: The admin will need a "Product Settings and Account Center Admin" license for each dashboard you want to enable SSO on. This can be done by either:
 - Giving your IdP Admin or Manager the license on your dashboard(s), OR
 - Transferring the relevant information from your IdP admin to a Dashboard admin to enter in Account Center
- Admin to make teams aware of upcoming changes to their Recruiter log-in. [Refer to sample email](#).

Please note: Your organization will need to activate SSO directly—enablement requires access to settings / permissions within your IdP that LinkedIn's support team cannot access.



Planning your SSO implementation



**The time required to complete pre-work and testing will depend on the number of users and the number of dashboards. You need to set up SSO for each individual dashboard.*



5 steps to enabling SSO

Complete these steps for each Recruiter dashboard requiring SSO

Connecting your Identity Provider

Setting up SSO

Activate SSO

Step 1

- Log in to Account Center, download LinkedIn's metadata, and upload it into your IdP

Step 2

- Log in to your IdP, download its metadata and upload it into Account Center

Step 3

- In Account Center, complete the settings to set up SSO

Step 4

- Grant access to LTS products for your users in your IdP

Step 5

- Activate SSO in Account Center
- Use Test Mode to limit usage of SSO to ensure it's working correctly

For a step-by-step guide to setting up SSO, refer to the slides below.
For more information, see our [SSO FAQ](#).

You may also want to refer to our [Privacy](#) and [Security](#) policies.



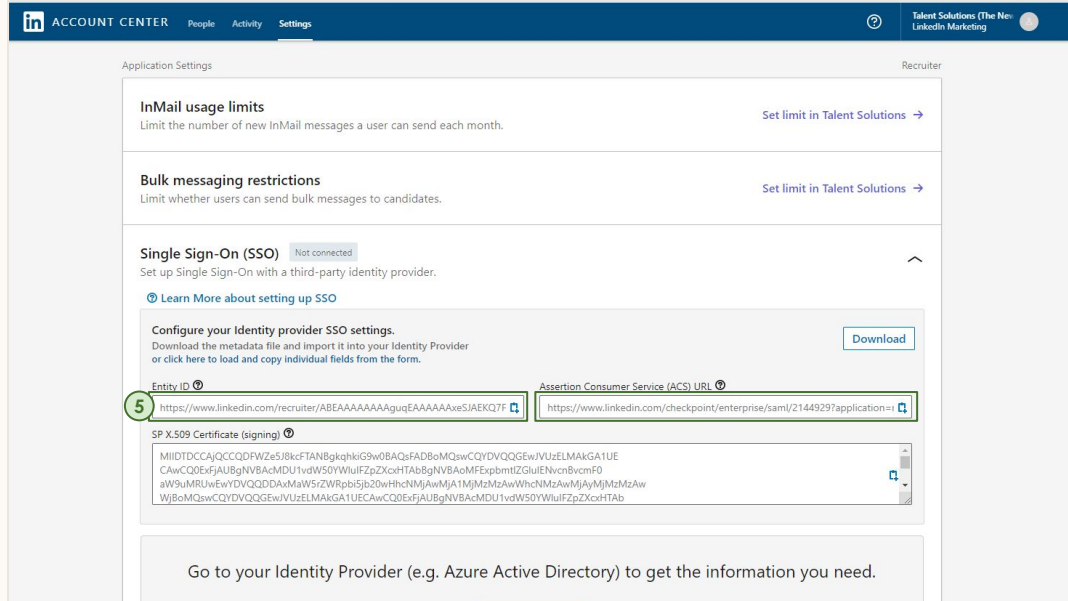
Step 1

Upload LinkedIn metadata from Account Center into your IdP

Part 1 of 4 – Access Account Center metadata

We recommend having two browser windows / tabs open.

- 1 Log in to LinkedIn Account Center
- 2 Go to [Settings](#)
- 3 Expand the Single Sign-On (SSO) panel
- 4 Click **Download**
- 5 Copy and save the values from the **Entity ID** and **Assertion Consumer Service (ACS) URL** fields (you will need these in Okta)



Step 1

Upload LinkedIn's Metadata from Account Center into your IdP

Part 2 of 4 – Create a new Okta Application

We recommend having two browser windows / tabs open.

- 6 Log in to Okta
- 7 Go to your Applications page
- 8 Click on **Add Application** and search for *LinkedIn Talent Solutions*
- 9 Select the **LinkedIn Talent Solutions** tile
- 10 Select **Add** on the following screen

NOTE: Each Talent Solutions dashboard has a separate **Assertion Consumer Service (ACS) URL**. You will need to create **a separate Application** for each Recruiter dashboard that requires SSO activation.

The screenshot shows the Okta Applications page. The top navigation bar includes 'Classic UI', 'Search people, apps', user 'V. Lim', 'Linkedin-dev-106637', 'Help and Support', and 'Sign out'. The main navigation bar has 'Get Started', 'Dashboard', 'Directory', 'Applications', 'Security', 'Workflow', 'Reports', 'Settings', 'Upgrade', and 'My Apps'. The page content shows 'Back to Applications' and 'Add Application' with a 'Create New App' button. A search bar contains 'LinkedIn Talent Solutions'. Below the search bar, search results for 'LinkedIn Talent Solutions' are displayed. The first result, 'LinkedIn Talent Solutions SAML', is highlighted with a green box and a circled '9'. Other results include 'LinkedIn Sales Navigator SWA', 'Dploy Solutions Portal SWA', 'Acuity Management Sr SAML', 'Essendant Solutions C SWA', and 'AmericanFunds Retirement SWA'. A 'CATEGORIES' sidebar on the left lists various application categories with counts.

CATEGORIES	Count
Featured	
API Management	6
Apps	6268
Apps for Good	13
CASB	2
Directories and HR Systems	13
Security Applications	702
Okta Applications	16
VPN	22

Step 1

Upload LinkedIn's Metadata from Account Center into your IdP

Part 3 of 4 – Name the Okta Application

You will now see the General Settings for your new Okta Application.

- 11 Give the Application a name users will recognize e.g. *LinkedIn Talent Solutions*
- 12 Click **Done** to continue to the new Application's settings
- 13 Select **Sign On**, then **Edit**

The screenshot shows the Okta Admin Console interface. At the top, there is a navigation bar with the Okta logo, a search bar, and user information (V. Lim, LinkedIn-dev-106637). Below the navigation bar, the main content area is titled 'Add LinkedIn Talent Solutions'. A tab labeled '1 General Settings' is active. The 'General Settings - Required' section contains the following fields:

- Application label:** A text input field containing 'LinkedIn Talent Solutions'. A green box highlights this field, and a circled '11' is next to the label. Below the field, it says 'This label displays under the app on your home page'.
- Application Visibility:** Two checkboxes:
 - Do not display application icon to users
 - Do not display application icon in the Okta Mobile App

At the bottom of the settings panel, there are 'Cancel' and 'Done' buttons. The 'Done' button is highlighted with a green box. To the right of the settings panel, there is a 'General settings' section with the text: 'All fields are required to add this application unless marked optional.'

At the bottom of the page, there is a footer with copyright information: '© 2021 Okta, Inc. Privacy Version 2020.12.2 OPI Preview Cell (US) Status site'. On the right side of the footer, there are links for 'Download Okta Plugin' and 'Feedback'.



Step 1

Upload LinkedIn's Metadata from Account Center into your IdP

Part 4 of 4 – Enter SAML Details in Okta

We recommend having two browser windows / tabs open.

- 14 Add the **Entity ID** and **Assertion Consumer Service (ACS) URL** you saved from Account Center into Okta
- 15 Ensure the **Application username format** is set to Email, as LinkedIn will expect to match this against email addresses in Account Center
- 16 If you want to share additional information (for example, 'Department' or 'Manager'), set it up in the **Configure profile mapping**

SAML 2.0

Default Relay State
All IDP-initiated requests will include this RelayState.

Disable Force Authentication
Never prompt user to re-authenticate.

SAML 2.0 is not configured until you complete the setup instructions.
[View Setup Instructions](#)
Identity Provider metadata is available if this application supports dynamic configuration.

ADVANCED SIGN-ON SETTINGS
These fields may be required for a LinkedIn Talent Solutions proprietary sign-on option or general setting.

14 Entity ID
Enter your Entity ID. Refer to the Setup Instructions above to obtain this value.

Assertion Consumer Service (ACS) URL
Enter your Assertion Consumer Service (ACS) URL. Refer to the Setup Instructions above to obtain this value.

CREDENTIALS DETAILS

15 Application username format

Update application username on

Password reveal Allow users to securely see their password (Recommended)

i Password reveal is disabled, since this app is using SAML with no password.

NOTE:

Fields to map Attribute Statements to in Account Center include:

- Building Code
- Department
- Desk Location
- Job Function
- Job Level
- Manager
- Mobile Phone Number
- Primary Email Address
- First Name
- Last Name
- Worker Status
- Worker Type
- Work Title
- Work Phone Number



Step 2

Upload your IdP metadata into LinkedIn Account Center

We recommend the use of dynamic SSO configuration, which allows you to import/export the SSO metadata as an XML file.

- 1 Log in to your IdP
- 2 Under the settings for your new Application there will be a link to download **Identity Provider metadata**
- 3 Save this XML
- 4 Log in to LinkedIn Account Center
- 5 Go to Settings
- 6 Expand the Single Sign-On (SSO) panel
- 7 Click **Upload XML File**
- 8 Upload your saved XML and click **Save SSO Configuration**

[See appendix if dynamic configuration doesn't work.](#)

The screenshot shows the 'Sign On' settings page in LinkedIn Account Center. The 'SAML 2.0' section is expanded, showing a 'Default Relay State' field. A yellow callout box with a '2' highlights a message: 'Identity Provider metadata is available if this application supports dynamic configuration.' Below this, the 'CREDENTIALS DETAILS' section is visible, with options for 'Application username format' (Okta username) and 'Password reveal' (Allow users to securely see their password).

The screenshot shows the 'Single Sign-On (SSO) Not connected' configuration page. It prompts the user to 'Configure your Identity provider SSO settings.' There are fields for 'Entity ID' (https://www.linkedin.com/recruiter) and 'Assertion Consumer Service (ACS) URL' (https://www.linkedin.com/checkpoint/enterprise/saml/2046480/application-...). A 'Download' button is present. Below, a 'SP X.509 Certificate (signing)' field contains a long alphanumeric string. A yellow callout box with a '7' highlights an 'Upload XML File' button. At the bottom, there is a link to 'Click here' for manual input.



Step 3

Complete SSO settings in Account Center

Once configuration of your Okta Application and Account Center is complete, you can adjust settings within Account Center.

Defaults are set for the most common scenarios. Consult with your in-house IT Security team about making any changes.

① If you configured profile mappings in your Okta Application (see Step 1, Part 4) you can configure them in Account Center.

SSO Options

Sign AuthnRequest
 No(default) Yes

Authentication Request Signing Algorithm
 SHA1 (default) SHA256

SAML Request Binding
 HTTP-Redirect (default) HTTP-Post

Encrypt SAML assertion
 No(default) Yes

AuthnContextClassRef
No items ▼

Custom Attribute Mapping

① Enter custom attribute Map to

Add another

NOTE:

Fields to map Attribute Statements to in Account Center include:

- Building Code
- Department
- Desk Location
- Job Function
- Job Level
- Manager
- Mobile Phone Number
- Primary Email Address
- First Name
- Last Name
- Worker Status
- Worker Type
- Work Title
- Work Phone Number

Step 4

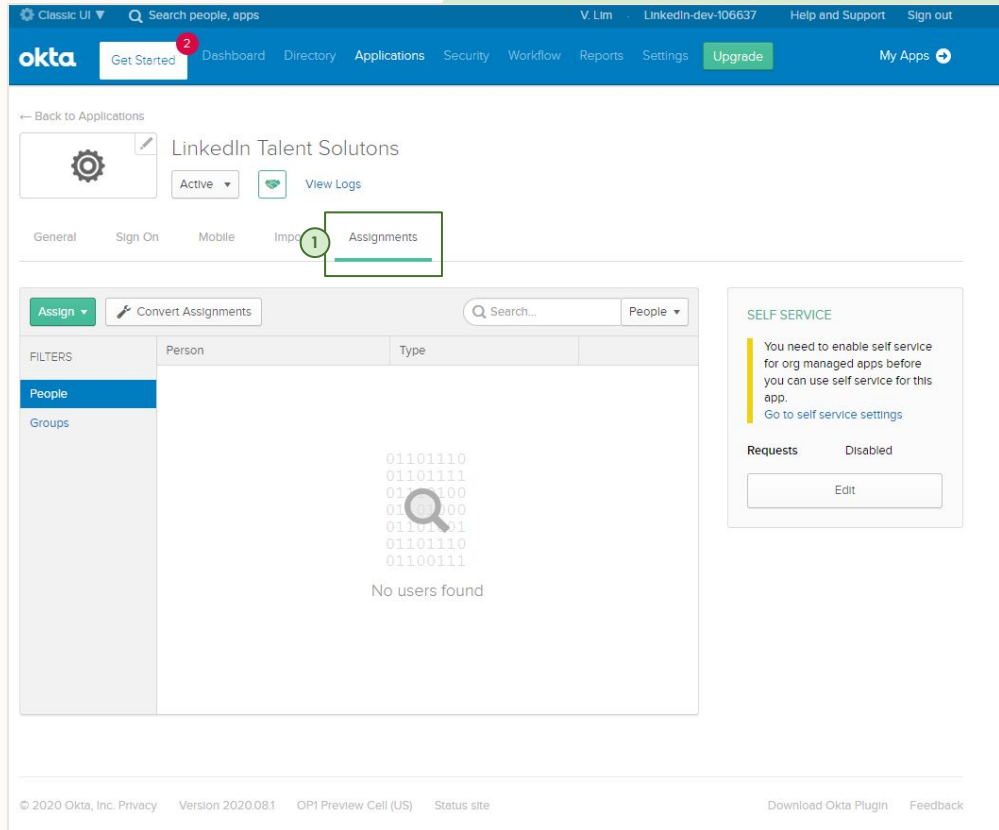
Manage employee access within your IdP

- 1 Follow the instructions of your IT Security team to ensure the right People or Groups have access to your Okta Application. This can be done in your application under **Assignments**.

Note: SSO uses work email addresses

The user's email address in Account Center must match the employee email address in Okta. If the emails don't match, the user will be locked out of Recruiter once SSO is switched ON.

Learn more about [updating user emails in Account Center](#).



The screenshot displays the Okta Admin Console interface for the 'LinkedIn Talent Solutions' application. The top navigation bar includes the Okta logo, a search bar, and user information (V. Lim, LinkedIn-dev-106637). The main content area shows the application settings for 'LinkedIn Talent Solutions', which is currently 'Active'. The 'Assignments' tab is selected and highlighted with a red circle and the number '1'. Below the tabs, there is an 'Assign' button and a search bar. The main content area shows a table with columns for 'Person' and 'Type', but it is empty, displaying 'No users found'. A magnifying glass icon is overlaid on the table. On the right side, there is a 'SELF SERVICE' section with a message: 'You need to enable self service for org managed apps before you can use self service for this app. Go to self service settings'. Below this message, there is a 'Requests' section with a 'Disabled' status and an 'Edit' button. The footer contains copyright information (© 2020 Okta, Inc.), version information (Version 2020.08.1), and links for 'Download Okta Plugin' and 'Feedback'.



Step 5

Activate SSO in LinkedIn Account Center

The final step is to switch on SSO within LinkedIn Account Center:

- 1 Go to Settings
- 2 Expand the Single Sign-On (SSO) panel
- 3 Select either:

TEST Mode (IDP ONLY) to enable SSO for IdP-initiated login flows only, and still allow normal login to Recruiter via LinkedIn.com ([learn more](#))

OR:

ON to enable and require SSO for all users and login flows accessing LinkedIn Recruiter

Single Sign-On (SSO) Not connected

Set up Single Sign-On with a third-party identity provider.

[Learn More about setting up SSO](#)

3 Edit **OFF** TEST Mode (IDP ONLY) ON

Configure your Identity provider SSO settings.
Download the metadata file and import it into your Identity Provider or [click here to load and copy individual fields from the form.](#) Download

Go to your Identity Provider (e.g. Azure Active Directory) to get the information you need.

Upload XML file

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

SSO Options

Sign AuthnRequest
 No(default) Yes

Authentication Request Signing Algorithm
 SHA1 (default) SHA256

SAML Request Binding
 HTTP-Redirect (default) HTTP-Post

Encrypt SAML assertion
 No(default) Yes

AuthContextClassRef
No items

Custom Attribute Mapping

Enter custom attribute Map to

Add another Save

Thank you





Appendix

Step 1 (alt):

Configuring LinkedIn metadata in your IdP (manually)

If you can't upload XML into your IdP, you can configure LinkedIn Account Center manually.

- 1 Log in to LinkedIn Account Center
- 2 Go to Settings
- 3 Expand the Single Sign-On (SSO) panel
- 4 In the **Configure your Identity Provider SSO settings**, select **Click here to load and copy individual fields from the form**
- 5 Log in to your IdP
- 6 Configure a new Application
- 7 On the Application Configuration, copy the values loaded in Account Center to the appropriate field in your IdP

Single Sign-On (SSO) Not connected

Set up Single Sign-On with a third-party identity provider.

[Learn More about setting up SSO](#)

4 **Configure your Identity provider SSO settings.** Download
Download the metadata file and import it into your Identity Provider or click here to load and copy individual fields from the form.

Go to your Identity Provider (e.g. Azure Active Directory) to get the information you need.

Upload XML file

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

[Go to SAML validator](#)

Change to Google OAuth

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

Entity ID	Assertion Consumer Service (ACS) URL
linkedin.com	https://www.linkedin.com/checkpoint/enterprise/saml/1005904
SP X-509 Certificate (signing)	
<code>MIIDozCCAcouGAwIFBAGIJAkUJkZ3EmWVtMAAGCiqGSlb3DQEBAQAAIGxhCzAIBghVBAYTAjAVTMCqsw CQYDVQIQDAJDUQTEWMBQGA1UEBwwNTW91bnRhaW4gVmVudDZEdDMSBzGALUECgwUTGUaazVhS2w4gQZ3y cG9yYXRpb24xFTAtBgNVBAMMDGxpbnRlbnRlbnVlAeFw0d0ljl1MToyMjA0MjRlRmF0eWlyljl1MTUy MjA0NDRaMjGpCzAIBghVBAYTAjAVTMCqswCQYDVQIQDAJDUQTEWMBQGA1UEBwwNTW91bnRhaW4gVmVudl</code>	

6

Step 2 (alt):

Configuring IdP metadata in Account Center (manually)

If you can't download a metadata XML file from your IdP, you can configure the required fields in Account Center manually.

- 1 Log in to LinkedIn Account Center
- 2 Go to Settings
- 3 Expand the Single Sign-On (SSO) panel
- 4 Underneath the **Upload XML file** button, click on "Click here"
- 5 Copy the values for each field from your IdP
- 6 Click **Save SSO Configuration**

Single Sign-On (SSO) Not connected

Set up Single Sign-On with a third-party identity provider.

[Learn More about setting up SSO](#)

Configure your Identity provider SSO settings.

Download the metadata file and import it into your Identity Provider or click here to load and copy individual fields from the form.

[Download](#)

Go to your Identity Provider (e.g. Azure Active Directory) to get the information you need.

4 [Upload XML file](#)

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

[Go to SAML validator](#)

[Change to Google OAuth](#)

Configure the LinkedIn service provider SSO settings.

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

Issuer String or Entity ID [?]	Budget Group [?]
<input type="text"/>	<input type="text" value="No items"/>
IdP redirect endpoint [?]	SAML Subject Identity attribute name [?]
<input type="text"/>	<input type="text"/>
X.509 Public certificate [?]	
<input type="text"/>	

[+ Add certificate](#)

6 [Save SSO configuration](#) Cancel

How often do users need to log in?

Product	Current session length	Definition	Can customers configure?	Notes
LinkedIn.com	365 days (fixed)	How often users must re-enter their email and password to access LinkedIn.com (flagship)	No	
Talent Solutions Recruiter	30 days (fixed)	How often Recruiter requires a user to re-enter their flagship credentials	No	<p>If you've logged in to LinkedIn.com in the last 15 minutes, we won't ask you to re-enter your credentials to access Recruiter.</p> <p>If it's been more than 15 minutes, you will need to re-enter your LinkedIn credentials to access Recruiter.</p>
Single Sign-On	8 hours (changeable)	<p>How often Recruiter will re-ping a user's identity provider to re-authenticate</p> <p><i>(Note: how often you have to re-enter your IdP email/password depends on the IdP session length, see below)</i></p>	Yes	<p>The default SSO session length is 8 hours.</p> <p>To adjust the SSO session timeout, please raise a support ticket with LinkedIn.</p> <p>For accounts with multiple LOBs using SSO (e.g. different departments use Recruiter, Learning, or SalesNav), a user's SSO session length will depend on the last application the user accessed.</p>
Identity Provider (e.g., OneLogin, Okta, etc...)	Differs per provider	How often the IdP requires a user to re-enter their credentials	Yes	You should be able to configure this through your IdP. LinkedIn cannot adjust this session length.

Note: If your users experience different session lengths, ask them to check their browser cookie settings—if cookies are disabled, they will be prompted to log in every time. Also check if they are seat sharing and/or using a different browser, as these can also affect session lengths. If the issue is still not resolved, please [raise a support ticket](#).



Sample email to send to your employees

Comms before launching SSO - set expectations for user experience when logging in.

Hi [NAME],

I hope this email finds you well. [COMPANY NAME] will be ramping a new security feature for LinkedIn Recruiter called Single Sign-On (SSO). SSO will help us boost security by acting as an extra layer of protection against unauthorized Recruiter users.

What does this mean for you?

As a Recruiter user, you'll be asked to enter in your [IdP name] credentials before logging in to Recruiter. This extra step helps us ensure the security of our data. After you log in, you can use Recruiter as normal.

If you experience any issues logging in to Recruiter, please contact your Recruiter admin or log a ticket with LinkedIn support.

Thanks for your support,

<<YOUR NAME>>

Additional Resources

[Set up Single Sign-on for Recruiter \(Help Center article\)](#)

[SSO FAQ \(English\)](#)

[LinkedIn privacy policy](#)

LinkedIn security email
security@linkedin.com

User email updates

To update the email address of a small number of users

[Updating a user to work email in Account Center \(admin guide\)](#)

To update the email address of multiple users in bulk

1. [Assign unique user IDs to bulk manage users in Account Center](#)
2. [Edit user attributes in bulk via CSV in Recruiter](#)

