Privacy and Security Whitepaper: Account Center Employee Database Integration (EDI) and Single Sign-On (SSO)

Last Revised April 2017

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.

General Information

Account Center Employee Database Integration - What is it and how does it work?

Employee Database Integration (EDI) allows your company to integrate its HRIS employee data into LinkedIn applications. This data can then be used to authenticate and manage your employees' access to certain paid LinkedIn applications by your system administrators. The integration includes:

- **Employee Data**: Uploading employee data from your HRIS systems.
- **SSO**: Optionally configuring Single Sign-On with your SSO solution.

If you configure and enable SSO, your employees can log into supported LinkedIn applications using your corporate identity provider. This provides an extra layer of security by requiring authentication against your identity provider before granting access.

Note, however, that authentication requires the employee to bind their EDI identity with their personal LinkedIn account. Once you have configured EDI, actions taken by the individual within the LinkedIn application are performed as the employee rather than the employee's personal LinkedIn account. This distinction allows your employees and your company to have more precise control over their respective data.

The integration is configured through the LinkedIn *Account Center* and is only available for some paid LinkedIn applications.

Which LinkedIn applications support EDI?

Currently, LinkedIn Learning, Elevate, Sales Navigator and Lookup support EDI, with support for more applications planned.

Note: Lookup specifically supports System for Cross-domain Identity Management (SCIM) through Azure Active Directory (AAD), and SSO through supported Identity Providers. SCIM is an open standard for automating the exchange of user identity information between identity domains, or IT systems.

Can LinkedIn applications leveraging EDI access data from an employee's personal LinkedIn member account?

Yes, but only if the LinkedIn application supports EDI and the member has expressly permitted it.

Binding (or *linking*) a personal LinkedIn account to your employee's EDI identity allows the Linkedin application and the employee to leverage his or her own personal data (such as their connections) in LinkedIn applications that support EDI. Binding is currently required to access the company's LinkedIn Application.

How do I get access to Account Center?

Account Center has features for Enterprise customers in addition to support for EDI. Please contact your sales representative for more information.

Employee Data

What is the employee data in EDI used for?

The employee data is used to create an identity for the employee and to build an employee profile. The identity is used for a few purposes including:

- **Authentication**: Determines access for the LinkedIn products that you have purchased. When using SSO, it is used in conjunction with your SSO provider to authenticate users.
- **Usage Tracking**: This allows us to provide metrics on how your employees are using each Linkedin application.

The employee profile is used for the following purposes.

- **Search**: Employee search provides a way to find employees. For example, this allows your company administrators to find employees to grant access rights.
- **Application Configuration**: LinkedIn applications can use profile data for configuration. For example, licenses to access application features can be assigned based on profile data.

What protocols do you support to upload employee data?

The employee data can be uploaded via the LinkedIn Account Center through a web-based user interface (collectively, with the below methods, the EDI interface). Additionally, the following protocols are supported for uploading EDI employee data.

- **SFTP**: Data is uploaded via SFTP to Linkedin SFTP servers secured by public key infrastructure.
- **HTTPS**: Data is POSTed to Linkedin datacenters via HTTPS using a generated access token.

Data is represented in a CSV format, and the file is encrypted in-transit and at-rest on the server during processing.

What employee data needs to be uploaded?

EDI supports uploading a variety of data about a company's employees. The minimal set of recommended fields are listed below:

Field	Description
Unique ID	A unique identifier (usually immutable) for the employee.

Primary Email Address	The primary email address to which communications will be sent.
First Name	The employee's preferred first name.
Last Name	The employee's preferred last name.

Do I need to upload data for all of the company employees?

No. You may upload data for a the part of your organization that uses LinkedIn applications. If you choose to upload data on all of your employees, however, you can then take advantage of full employee searches and license automation across your entire organization.

Single Sign-On (SSO)

Single Sign-On (SSO) - What is it and how does it work?

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.

Which LinkedIn applications support SSO?

Currently, LinkedIn Learning, Elevate, Sales Navigator, and Lookup support SSO, with support for more applications planned.

What protocols do you support for SSO?

We currently support SAML v2.

Is SSO required? What if I do not have an SSO solution for my company or do not want to use SSO?

Using SSO and integrating with an SSO provider is not required to use most LinkedIn applications. If SSO is not configured, your employees may authenticate themselves using their current personal LinkedIn credentials or create a new member account for all LinkedIn applications with the exception of Lookup. SSO is a requirement for Lookup, as it integrates directly with Azure Active Directory.

Account Binding

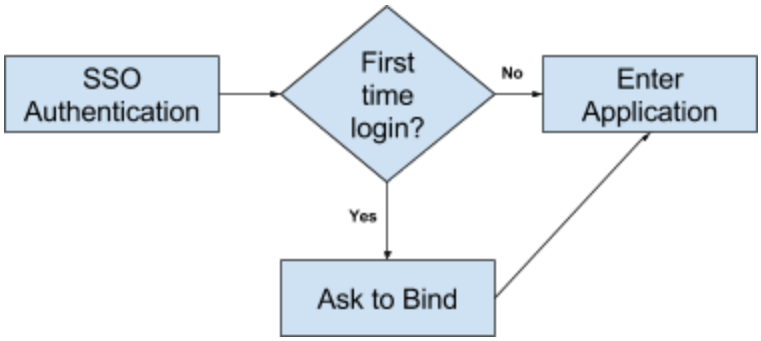
What is Account Binding, and how is it used?

Account binding allows your employee to “bind” their personal LinkedIn account to their EDI employee account. Binding provides the following features.

- Access to personal member account data (such as public profile data or connections) from your employee’s EDI identity when using purchased LinkedIn applications.
- Employee retains the right and control to the binding based on their privacy concerns.
- A clear separation between personally owned data associated with the member account and company owned data associated with the EDI identity.
- Authentication to Linkedin applications when not using SSO

How do I setup my account bindings?

Binding is setup when an employee first logs into a purchased LinkedIn application that supports EDI.



As part of the application onboarding flow, your employee may bind their personal LinkedIn account to their EDI identity.

Is binding required to use my purchased LinkedIn applications?

For the purchased LinkedIn applications that use EDI, binding is currently required. This requirement is determined by the individual LinkedIn applications and may change based on the application’s feature set.

When bound, what data is the company allowed to see on behalf of the employee?

During the binding process, the employee is presented with a list of permissions that enables the company to use the employee's personal LinkedIn account in certain ways. The employee is free to accept the binding or create a new account to bind. The goal of this process is to make it very clear to the employee how his or her personal data is used by the EDI identity and LinkedIn application. The exact list of permissions varies by application. Some examples of permissions include:

- **View Profile**: LinkedIn member profile data of the bound personal account is made available to the company via the Linkedin application. As always, the data would follow the member's privacy settings.
- **View Connections**: The member's personal connections are accessible to the company via the Linkedin application.

Only a few read permissions to a personal LinkedIn account are currently grantable. Write permissions to the personal LinkedIn account are not currently grantable and would require further authentication and authorization by the employee at the time of the write. All permissions are granted per application, and grants are not shared across applications.

What can an employee do if they have privacy concerns over the binding?

Employees can unbind their personal LinkedIn accounts at any time by contacting customer service. When doing so, the data for that Linkedin personal account from that point onwards is no longer available to the company and the LinkedIn applications the company has purchased. Additionally, customer service personnel can assist members in finding what EDI identity to which their Linkedin personal account is currently bound.

What happens when an employee leaves the company?

If an employee leaves the company, it is up to the company to inform LinkedIn by uploading new employee data and removing old entries through the EDI interface. This can be done, for example, by uploading a CSV with the employee who has left marked as "inactive." If an employee is removed from all applications to which he or she has access, the employee's personal LinkedIn account is automatically unbound from their EDI identity and the company loses access to that employee's personal LinkedIn data.

In addition, at any time, the employee may choose to manually unbind their personal LinkedIn account from their EDI identity by contacting customer service.

Data Security, Privacy, and Confidentiality

Will other companies be able to access my company's data?

No. Other companies will not have access to your data that you uploaded.

Will my company have full access to my employees' personal LinkedIn accounts?

No. When logging in as an employee with a EDI identity, the user is logged in as that EDI identity, **not** as their personal LinkedIn account. As a result, your company has only restricted access to the employee's bound LinkedIn account, described in part below:

- No access to the employee's personal LinkedIn account data not explicitly granted by the employee (whether directly to the company or via the LinkedIn application).
- No access to unpaid sites, such as other content or functionality on www.linkedin.com, as the employee's bound LinkedIn account.
- No access to usage data when a member logs into a non-work related LinkedIn application with their personal LinkedIn account rather than their EDI identity.

For my employees with privacy concerns, what personal data is made available to my company when employees bind their LinkedIn accounts?

The employee is providing the company access to data only for the permissions they have explicitly granted during the binding step for the paid LinkedIn application. They may unbind at any time if any concerns arise. Any other data read or written to the employee's personal LinkedIn account, whether bound or not, must be explicitly approved and authenticated by the employee in-application. Once the unbinding takes place, the company may no longer use the granted permissions and access the granted data associated with that personal LinkedIn account.

What data uploaded through EDI can each of my employees access?

All employee data uploaded through EDI are visible to all EDI identities. Please do not add data to EDI that you do not want each user to see.

Can I control who can administer my EDI and paid LinkedIn application data?

Yes. EDI is configured only by the designated LinkedIn application administrators in your company. In addition, each application can manage its own set of administrators and roles based on their specific feature sets.

What can I do to make sure my data is purged from LinkedIn?

You can contact your customer support representative to ask for your company data to be purged.

Does LinkedIn have a SOC2 or SOC3 report available?

No. LinkedIn does not have a SOC2 or SOC3 report available at this time.

What is LinkedIn's privacy and data security policy?

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

What security protocols/measures does LinkedIn use to protect customer data?

Our collection and use of member data and customer related data is governed by LinkedIn's privacy policy: https://www.linkedin.com/legal/privacy-policy.

Security Assessments

Did LinkedIn perform any penetration tests?

We performed a penetration test of the SSO integration, the admin portal, and all EDI interfaces (including UI-based CSV upload, SFTP, HTTPS, and SCIM) as well as targeted source code review during development. All issues identified prior to release that would impact the security posture of the user's LinkedIn account were remediated or the integrity and confidentiality of the enterprise data were confirmed.

Can you share more about your penetration testing methodology?

Our application testing methodology includes testing for:

- OWASP Top Ten vulnerabilities
- mobile and web application vulnerabilities including XSS, CSRF
- injection issues including LDAP, XML, SQL
- data communications
- authentication and authorization frameworks
- information disclosure messages in logs

We also perform regular network vulnerability scanning of our internal and external networks.

What does LinkedIn do to protect its accounts?

Our systems proactively evaluate member login attempts for suspicious activity and to detect for potential intrusions. Many of these takeover attempts use automated tools to guess passwords, which our systems work to detect and then deploy roadblocks against. We also monitor key site metrics 24×7 looking for and mitigating attacks against our login system. We've also moved the majority of our member traffic to HTTPS, which provides authentication of our site and protects against man-in-the-middle attacks.

We also compare username and password combinations we find on the Internet to our member's credentials, and in the event we find matches, we promptly invalidate the password for the account and then notify the member to update their password.

How do I contact LinkedIn Security?

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