



Guía del inicio de sesión único para administradores

Última revisión: 15 de febrero de 2018
Versión 1.7

Exención de responsabilidad

© 2018 LinkedIn Corporation. Todos los derechos reservados.

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

Este documento puede contener predicciones. La información de este documento puede modificarse sin previo aviso. El software (y la documentación relacionada) solo pueden usarse o copiarse de conformidad con las condiciones del acuerdo de licencia. Queda prohibido reproducir, transmitir o traducir el software y la documentación de ninguna forma y por ningún medio, ya sea electrónico, mecánico, manual, digital o de otro tipo, ni en su totalidad ni en parte, salvo de conformidad con las condiciones del acuerdo de licencia.

LinkedIn Corporation y su logotipo son marcas comerciales, de servicio o registradas de LinkedIn Corporation en Estados Unidos y otros países. Los demás nombres de marcas, productos y servicios son marcas comerciales o registradas de sus respectivos propietarios o empresas.

Índice

[Exención de responsabilidad](#)

[Índice](#)

[Resumen](#)

[Requisitos previos](#)

[Acerca del inicio de sesión único \(SSO\)](#)

[¿Por qué usar el inicio de sesión único?](#)

[Protocolos SSO compatibles](#)

[Configuración del inicio de sesión único \(SSO\)](#)

[Primeros pasos con el SSO](#)

[Conexión con tu proveedor de identificación](#)

[Descarga del archivo](#)

[Uso de campos individuales](#)

[Configuración de tu proveedor de identificación](#)

[Requisitos para la asignación justo a tiempo \(JIT\)](#)

[Dirección de correo electrónico \(obligatorio\)](#)

[Nombre \(opcional\)](#)

[Apellidos \(opcional\)](#)

[Otros atributos opcionales](#)

[Ejemplo](#)

[Carga del archivo](#)

[Introducción de valores a mano](#)

[Asignación de licencias](#)

[Activación del inicio de sesión único](#)

[Opciones de activación](#)

[Verificación de la configuración](#)

[Asistencia](#)

[Documentación de ayuda](#)

[Problemas técnicos](#)

[Política de privacidad y seguridad de datos de LinkedIn](#)

[Contactos de seguridad de LinkedIn](#)

Resumen

La integración de bases de datos de empleados (EDI) te permite usar el sistema de información de recursos humanos (HRIS) de tu empresa en las aplicaciones de LinkedIn. La integración incluye una configuración opcional para el inicio de sesión único con tu solución SSO. En este caso, el administrador de tu cuenta puede configurar la empresa de manera que use el SSO para autenticarse en una aplicación de la plataforma de LinkedIn a través de la integración con la plataforma empresarial.

La integración se configura desde el Centro de cuentas de LinkedIn y solo está disponible para algunas aplicaciones de pago de LinkedIn.

Requisitos previos

- Cuenta de empresa
- Privilegios de administrador completos
- Privilegios de administración del proveedor de identificación (IdP)

Acerca del inicio de sesión único (SSO)

El SSO para empresas permite que los empleados accedan a las aplicaciones compatibles de LinkedIn usando sus credenciales corporativas en lugar de las credenciales de LinkedIn.

No es necesario usar un método de SSO ni integrar un proveedor de SSO para utilizar las aplicaciones de LinkedIn. Si no se configura el SSO, los empleados podrán identificarse con sus credenciales personales de LinkedIn o crearse una cuenta.

¿Por qué usar el inicio de sesión único?

- Se aprovechan las credenciales corporativas actuales
- Mayor seguridad cuando los empleados usan los protocolos para contraseñas de tu empresa en lugar de su cuenta privada
- Gestión de usuarios más sencilla cuando los empleados dejan la empresa

Protocolos SSO compatibles

Actualmente admitimos el protocolo SAML versión 2.0.


Configuración del inicio de sesión único (SSO)

Primeros pasos con el SSO

1. Accede al Centro de cuentas desde este enlace:
<http://www.linkedin.com/enterprise/accountcenter/settings>

Nota: Algunas aplicaciones también cuentan con un punto de acceso en sus ajustes. Por ejemplo, en Learning puedes ir a **Acceso administradores** en el banner y elegir **Configuración > Configuración global**.

Los ajustes de la aplicación para el SSO muestran la aplicación a la que has accedido.



The screenshot shows the LinkedIn Account Center interface for the 'Learning' application. The top navigation bar includes 'INICIO', 'PERSONAS', 'CONTENIDO', 'INFORMES', and 'CONFIGURACIÓN'. The 'CONFIGURACIÓN' section is active, with sub-tabs for 'Integraciones' and 'Configuración global'. The 'Configuración global' sub-tab is selected, showing three main configuration sections: 'Inicio de sesión único (SSO)', 'Credenciales de acceso OAuth', and 'Establecimiento de SFTP'. Each section has a brief description and a dropdown arrow on the right.

Configuración de la aplicación	Learning (Default)
Inicio de sesión único (SSO) Establece un inicio de sesión único con un proveedor externo de gestión de identificación de usuarios.	▼
Configuración global	
Credenciales de acceso OAuth Genera y gestiona credenciales de seguridad para otorgar acceso a aplicaciones de terceros (p. ej. para automatizar una carga diaria de un archivo CSV de empleados).	▼
Establecimiento de SFTP Crea usuarios que puedan cargar archivos CSV a través de SFTP.	▼

2. Abre el panel Inicio de sesión único (SSO).

Inicio de sesión único (SSO) No conectado

Establece un inicio de sesión único con un proveedor externo de gestión de identificación de usuarios.

Autenticar usuarios con SSO Editar DESACTIVADO TEST ACTIVADO

Verifica la identidad de tus usuarios con el inicio de sesión único (SSO) de tu empresa.

Configurar los ajustes de SSO de tu proveedor de identificación. Descargar

Descarga el archivo de metadatos e impórtalo a tu proveedor de identificación de usuarios.
[O haz clic aquí para cargar y copiar campos individuales del formulario.](#)

Configurar los ajustes de SSO del proveedor de servicio de LinkedIn

Ahora, obtén un archivo de metadatos de tu proveedor de identificación de usuarios y cárgalo aquí, o introduce los valores manualmente.

Dirígete a tu proveedor de identificación de usuarios (como Azure Active Directory) para conseguir la información que necesitas.

Cargar archivo XML

¿Quieres introducir la información manualmente? [Haz clic aquí](#)

Opciones del SSO

Solicitud de autorización para acceder

Sí (por omisión) No

Algoritmo para la solicitud de autenticación para acceder

SHA1 (por omisión) SHA256

Solicitud vinculante SAML

HTTP-Redirect (por omisión) HTTP-Post

AuthnContextClassRef

No enviar este valor (por omisión) ▾

Atributo Mapping personalizado

Introducir atributo personalizado Mapear hacia ▾

Añadir otro

Guardar

Asignar licencias automáticamente 🔴

A tu equipo se le otorgarán licencias de forma automática al hacer clic en el enlace de activación.

[Ir al validador del SAML](#)

3. Selecciona tus opciones para el SSO.
 - a. Solicitud de autorización para acceder:
 - Sí (por omisión)
 - No
 - b. Algoritmo para la solicitud de autenticación para acceder
 - SHA1 (por omisión)
 - SHA256
 - c. Solicitud vinculante SAML
 - HTTP-Redirect (por omisión)
 - HTTP-Post
 - d. AuthnContextClassRef:
 - No enviar este valor (por omisión)
 - urn:oasis:names:tc:SAML:2.0:ac:classes>PasswordProtectedTransport
 - urn:oasis:names:tc:SAML:2.0:ac:classes:kerberos
 - urn:federation:authentication:windows
 - PasswordProtectedTransport y windows
 - urn:oasis:names:tc:SAML:2.0:ac:classes:X509
 - urn:oasis:names:tc:SAML:2.0:ac:classes:TLSClient
 - e. Atributo Mapping personalizado. Puedes especificar asignaciones con un nombre personalizado que se correspondan con ajustes del IdP (en lugar de usar las asignaciones por omisión). Indica tu atributo personalizado y cómo asignarlo. Los siguientes campos se pueden asignar a atributos personalizados y proporcionados por el usuario.
 - Nombre
 - Apellidos
 - Correo electrónico principal
 - Teléfono móvil
 - Teléfono del trabajo
 - Cargo laboral
 - Función laboral
 - Responsable
 - Departamento
 - Nivel laboral
 - Tipo de trabajador
 - Estado del trabajador
 - Código del edificio
 - Ubicación del escritorio

Encontrarás más información sobre los atributos predeterminados en el apartado [Requisitos para la asignación justo a tiempo \(JIT\)](#).

- (Opcional) Haz clic en **Ir al validador del SAML** para indicar si las solicitudes de SAML deben firmarse. Copia la respuesta al SAML y haz clic en **Validar**.



- (Opcional) Si necesitas configurar varias instancias de aplicaciones, puedes seleccionar el menú **<nombre de la aplicación> - <instancia>** en el banner y elegir la instancia que quieres configurar. Por ejemplo, en Learning podrías seleccionar el menú **Learning – Default** (como se muestra en la imagen del Paso 1)

Nota: Las instancias que aparecen en el menú se clasifican por aplicación. En caso de que tengas acceso a varias instancias de la misma aplicación (por ejemplo, dos instancias de Recruiter), verás el encabezado Recruiter seguido de los nombres de cada instancia.

Conexión con tu proveedor de identificación

Si tu proveedor de identificación admite metadatos y has configurado SAML con la versión 2.0, puedes descargar un archivo de configuración XML para enviárselo. El proveedor podrá cargarlo para configurar automáticamente los ajustes y conectarse a tus productos de LinkedIn.

Determina si puedes descargar un archivo con metadatos o si debes usar los campos individuales. A continuación, sigue uno de los procesos de los siguientes apartados.

Descarga del archivo

- Haz clic en **Descargar** para descargar un archivo con metadatos que puedes usar en el sistema de tu proveedor de identificación. El archivo `metadata.xml` se descarga desde el navegador.
- Comprueba que contenga lo siguiente:

```
<md:AssertionConsumerService
Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
Location="https://www.linkedin.com/checkpoint/enterprise/saml/[A
CCOUNT ID]" index="0"/>
```
- Accede al sistema de tu proveedor de identificación.
- Carga el archivo de metadatos.

Nota: Es posible que este archivo no se pueda importar en el sistema de tu proveedor de identificación. Por ejemplo, Okta no ofrece esta funcionalidad.
- Vuelve a la configuración del SSO.
- Haz clic en **Aceptar** en el diálogo de carga. A continuación, consulta el apartado [Configuración de tu proveedor de identificación](#).

Uso de campos individuales

1. Haz clic en el enlace para cargar y copiar campos individuales del formulario en el sistema de tu proveedor de identificación.

Configurar los ajustes de SSO de tu proveedor de identificación.
Descarga el archivo de metadatos e impórtalo a tu proveedor de identificación de usuarios.
O haz clic aquí para cargar y copiar campos individuales del formulario.

Descargar

Configurar los ajustes de SSO del proveedor de servicio de LinkedIn
Ahora, obtén un archivo de metadatos de tu proveedor de identificación de usuarios y cárgalo aquí, o introduce los valores manualmente.

Cadena del emisor o ID de la entidad

Grupo de presupuesto
Default

Punto final de redirección de IdP

Nombre de atributo de identidad de asunto SAML

Certificado público X.509

+ Añadir otro certificado

Guardar configuración de SSO

Cancelar

2. Copia y pega los campos que quieras incluir.

Configuración de tu proveedor de identificación

Configura el sistema de tu proveedor de identificación para que se comuniquen con la plataforma de LinkedIn. Determina si puedes cargar un archivo con metadatos de tu proveedor de identificación o si debes introducir los valores manualmente. A continuación, sigue uno de los procesos de los siguientes apartados. Si no utilizas la asignación justo a tiempo, ve a [Carga del archivo](#) o [Introducción de valores a mano](#).

Requisitos para la asignación justo a tiempo (JIT)

Uno de los motivos por los que se ha generalizado el uso del protocolo SAML 2.0 es su flexibilidad para enviar información adicional al proveedor del servicio. Cuando un proveedor de identificación envía una aserción, esta incluye atributos que describen al usuario. Estos atributos permiten a LinkedIn identificar al usuario y atribuirlo automáticamente a una cuenta. En este apartado se describen algunos de los posibles atributos.

Dirección de correo electrónico (obligatorio)

Todos los usuarios deben tener una dirección válida de correo electrónico aunque utilicen el SSO.

Nota: Al probar con varias identificaciones del IdP, las direcciones de correo electrónico deben ser únicas.

Como el proveedor de identificación gestiona la información del usuario, debe enviar la dirección de correo electrónico del usuario en su aserción. Los proveedores de identificación usan distintas convenciones para asignar nombres, y LinkedIn busca una dirección de correo electrónico entre los siguientes nombres de atributos de forma secuencial:

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

Nombre (opcional)

Al igual que con las direcciones de correo electrónico, los proveedores de identificación pueden enviar el nombre en varios campos comunes. Para ofrecer compatibilidad de serie con la mayoría de los proveedores de identificación, LinkedIn intenta encontrar el nombre en los siguientes nombres de atributos:

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

Apellidos (opcional)

LinkedIn busca los apellidos en los siguientes nombres de atributos:

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

Otros atributos opcionales

Puedes proporcionar información adicional, incluidos los siguientes nombres de atributos.

Nota: Aunque estos atributos se almacenan en LinkedIn, no se ven en la interfaz y, por tanto, no están disponibles para la gestión de los usuarios.

Nombre del atributo	Variaciones compatibles
Departamento	<ul style="list-style-type: none">• departmentName• department• User.Department
Responsable	<ul style="list-style-type: none">• Manager• manager• User.Manager
Teléfono móvil	<ul style="list-style-type: none">• mobilePhoneNumber• PhoneNumber• phone

	<ul style="list-style-type: none"> • phoneNumber • User.PhoneNumber • http://schemas.xmlsoap.org/ws/2005/05/identity/claims/mobilephone
Teléfono del trabajo	<ul style="list-style-type: none"> • WorkPhoneNumber • Workphone • workPhoneNumber • User.WorkPhoneNumber • http://schemas.xmlsoap.org/ws/2005/05/identity/claims/otherphone
Cargo laboral	<ul style="list-style-type: none"> • workTitle • Cargo • WorkTitle • User.WorkTitle
Función laboral	<ul style="list-style-type: none"> • jobFunction • JobFunction • User.JobFunction
Nivel laboral	<ul style="list-style-type: none"> • JobLevel • jobLevel • User.JobLevel
Tipo de trabajador	<ul style="list-style-type: none"> • WorkerType • workerType • User.WorkerType
Estado del trabajador	<ul style="list-style-type: none"> • WorkerStatus • workerStatus • Estado • User.WorkerStatus
Código del edificio	<ul style="list-style-type: none"> • buildingCode • building
Ubicación del escritorio	<ul style="list-style-type: none"> • deskLocation • desk

Ejemplo

Correo electrónico: mlopez@empresa.com

Nombre: María

Apellidos: López Pérez

Teléfono móvil: 655-123-456

Cargo: Responsable de ingeniería de software

Departamento: Aplicaciones de software

Fecha de inicio: 07/03/16

Nivel laboral: Contribuidor individual

Tipo de trabajador: empleado

Estado del trabajador: activo o inactivo

Responsable: dsmith

Carga del archivo

1. Haz clic en **Cargar archivo XML** para añadir los metadatos de tu proveedor de identificación.

Configurar los ajustes de SSO del proveedor de servicio de LinkedIn
Ahora, obtén un archivo de metadatos de tu proveedor de identificación de usuarios y cárgalo aquí, o introduce los valores manualmente.

Dirígete a tu proveedor de identificación de usuarios (como Azure Active Directory) para conseguir la información que necesitas.

[Cargar archivo XML](#)

¿Quieres introducir la información manualmente? [Haz clic aquí](#)

2. Selecciona el archivo y haz clic en **Abrir**. Si todo va bien, los campos aparecerán cumplimentados con los metadatos.

Introducción de valores a mano

1. Utiliza el enlace **Haz clic aquí** para añadir la información manualmente.

Configurar los ajustes de SSO del proveedor de servicio de LinkedIn
Ahora, obtén un archivo de metadatos de tu proveedor de identificación de usuarios y cárgalo aquí, o introduce los valores manualmente.

Cadena del emisor o ID de la entidad ?	Grupo de presupuesto ?
<input type="text"/>	Default v
Punto final de redirección de IdP ?	Nombre de atributo de identidad de asunto SAML ?
<input type="text"/>	<input type="text"/>
Certificado público X.509 ?	
<input type="text"/>	

[+ Añadir otro certificado](#)

[Guardar configuración de SSO](#) [Cancelar](#)

2. Introduce los siguientes datos:

- Cadena del emisor o ID de la identidad: debe coincidir con el campo `md:EntityDescriptor entityID`.
- Grupo de presupuesto: grupo que se usará para la asignación de licencias *justo a tiempo*.
- URL de redireccionamiento: debe coincidir con el campo `md:SingleSignOnService location`.
 - **Nota:** Actualmente, LinkedIn solo admite la vinculación de `urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect`.
- Ubicación de identidad de SAML: este campo se utiliza para contrastar la identidad del empleado almacenado en el sistema de tu proveedor de identificación con la almacenada en el proceso EDI de LinkedIn. LinkedIn utiliza las siguientes reglas para identificar al empleado:
 - Si la respuesta de la autenticación SAML proporciona una aserción SAML que contiene un conjunto de atributos, puedes indicar el nombre del atributo SAML que contiene la identidad del empleado en este campo de texto. Por ejemplo, si se envía un valor `employeeId` a un atributo SAML llamado `employeeId`, puedes escribir `employeeId` en el campo **Ubicación de identidad de SAML**. LinkedIn utilizará el atributo `employeeId` enviado en cada aserción para buscar la identidad del empleado. Para permitir esta acción, debes cargar el atributo `employeeId` de cada usuario durante el proceso EDI.
 - Si este campo se deja vacío, LinkedIn busca al empleado en función del valor del atributo `NameId` que se ha enviado en `<saml:Subject>`. Este campo *debe* ser la dirección de correo electrónico principal del usuario, cargada durante el proceso EDI.
- Si no se puede encontrar al usuario ni con el atributo indicado en el campo **Ubicación de identidad de SAML** ni con la dirección de correo electrónico principal (indicada en `<saml:Subject>`), LinkedIn *no* podrá autenticar al usuario.
- Certificado público: LinkedIn comprueba la validez de la aserción SAML enviada en la respuesta de autenticación SAML mediante el certificado x.509 que el proveedor de identificación ha usado para firmar. Si no se puede validar la firma de la respuesta de autenticación, no se autentica al usuario.

3. Haz clic en **Guardar configuración de SSO**.

Asignación de licencias

Puedes otorgar licencias automáticamente a tus empleados activando **Asignar licencias automáticamente**. Cuando esta opción está habilitada, los usuarios reciben una licencia si aún no tienen una.

Nota: Cuando activas las licencias automáticas, se muestran los atributos de usuario necesarios en el proveedor de identificación.

Asignar licencias automáticamente

A tu equipo se le otorgarán licencias de forma automática al hacer clic en el enlace de activación.



Nota: La asignación automática de licencias no está disponible ahora mismo para Sales Navigator.

Activación del inicio de sesión único

Autenticar usuarios con SSO

Verifica la identidad de tus usuarios con el inicio de sesión único (SSO) de tu empresa.

Editar ⓘ DESACTIVADO TEST ACTIVADO

Cuando hayas completado la configuración, habilita el SSO. Activa la opción **Autenticar usuarios con SSO**. Consulta más información sobre cuándo usar las opciones disponibles en la tabla [Opciones de activación](#).

Opciones de activación

Estado	Descripción
Desactivado	<ul style="list-style-type: none">No se requiere ninguna configuración de implantación del SSO.Los usuarios pueden acceder a las licencias asignadas con su lógica basada en LinkedIn.
Test	<ul style="list-style-type: none">El SSO está configurado.El modo test aplica el inicio de sesión único a procesos iniciados por el IdP para empleados con acceso a través del proveedor de identificación, pero sigue permitiendo la identificación estándar de LinkedIn en procesos iniciados por un proveedor de servicios (SP). Este método no obliga a los usuarios a autenticarse a través del IdP, ya que pueden acceder a la aplicación directamente a través de LinkedIn.Resulta práctico cuando se configura el SSO por primera vez o si el proveedor de identificación solo es compatible con procesos iniciados por el IdP.
Activado	<ul style="list-style-type: none">El SSO está configurado.Los usuarios deben iniciar sesión a través del proceso iniciado por el IdP o SP (a menos que el proveedor de identificación solo sea compatible con procesos iniciados por el IdP, en cuyo caso no disponen de la opción del SP). Con independencia del método que se use, la autenticación es obligatoria. <p>Advertencia: cuando selecciones Activado después de la configuración inicial, no cierres la ventana hasta comprobar que el SSO funciona correctamente. De lo contrario, deberás contactar con el servicio de atención al cliente para deshabilitar el SSO de tu cuenta. Te recomendamos usar la opción Test para verificar el proceso iniciado por tu IdP antes de configurar el SSO como Activado.</p>
	<ul style="list-style-type: none">Proceso iniciado por el IdP: cuando un usuario intenta acceder a una aplicación a través de su proveedor de identificación (como Okta, AAD o Ping).Proceso iniciado por el SP: cuando un usuario intenta acceder a su licencia directamente desde la aplicación o el proveedor de servicios (SP).

Verificación de la configuración

Nota: Antes de verificar la configuración, debes haber finalizado la vinculación de cuentas. Encontrarás más información y las instrucciones en el documento sobre privacidad y seguridad de LinkedIn: integración de bases de datos de empleados (EDI) e inicio de sesión único (SSO) del Centro de cuentas.

Comprueba que la integración con el proveedor de identificación funciona correctamente y que se dan las siguientes condiciones:

- La identidad de tu empresa se ha añadido a la aplicación de LinkedIn (por ejemplo, cargando un archivo CSV).
- El SSO está habilitado.
- Se ha configurado una aplicación de LinkedIn en tu proveedor de identificación de acuerdo con las instrucciones anteriores.

Lleva a cabo la prueba con:

- La sesión iniciada en el sistema de tu proveedor de identificación
- La página de recomendación de LinkedIn y después inicia sesión

Asistencia

Documentación de ayuda

- Guía para administradores sobre cómo añadir datos de empleados (en inglés)
- Documento privacidad y seguridad: integración de bases de datos de empleados (EDI) e inicio de sesión único (SSO) (en inglés)
- [Tutorial: Integración de Azure Active Directory con LinkedIn Learning \(en inglés\)](#)
- [Tutorial: Integración de Azure Active Directory con LinkedIn Sales Navigator \(en inglés\)](#)
- [Tutorial: Integración de Azure Active Directory con LinkedIn Elevate \(en inglés\)](#)

Problemas técnicos

Si tienes problemas técnicos con la configuración del SSO, contacta con tu equipo de cuentas o asistencia para aplicaciones a través del Centro de ayuda.

Política de privacidad y seguridad de datos de LinkedIn

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

Contactos de seguridad de LinkedIn

Si tienes dudas sobre cuestiones de seguridad o si quieres informarnos sobre un problema de seguridad, escribe a security@linkedin.com.