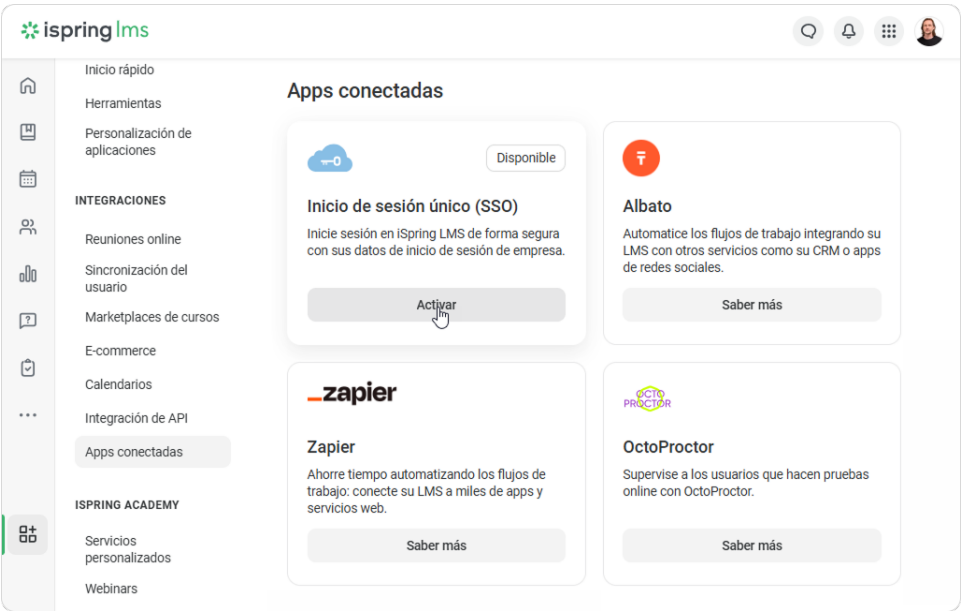


Autorización SAML 2.0

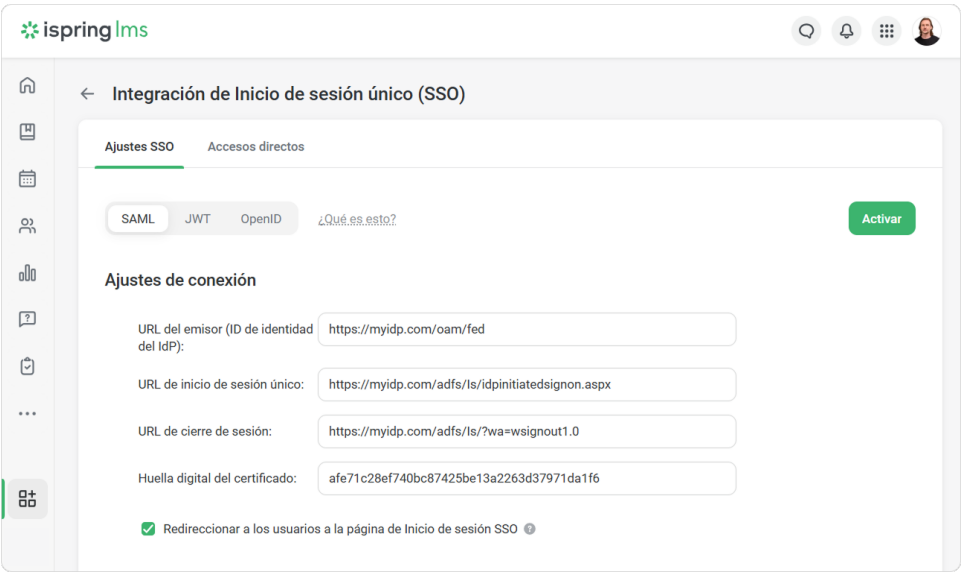
La autorización con SAML 2.0 también funciona en la aplicación móvil.

Para configurar la autenticación SAML 2.0 en su cuenta:

- 1. Vaya a **Servicios > Apps conectadas**.
- 2. Luego, en la sección de **Inicio de sesión único (SSO)**, haga clic en **Activar**.



- 3. Complete los campos del formulario, añadiendo la URL y otros detalles de su proveedor de identidad. El último es el recurso que se supone que sus usuarios deben usar para la autorización inicial en su portal corporativo.



URL del emisor (ID de identidad del IdP)	La URL que identifica de manera única el servicio del proveedor de identidad. Este valor es igual al Emisor elemento en la solicitud SAML 2.0 enviada por el proveedor de identidad.
URL de inicio de sesión único	Ruta al script del servidor que genera solicitudes de confirmación de identificador SAML 2.0 para gestionar la autorización.
URL de cierre de sesión	Ruta al script del servidor que genera solicitudes de confirmación de identificador SAML 2.0 para gestionar el cierre de sesión.

Huella digital del certificado	Una versión breve del certificado de clave pública para verificar una firma digital. Se utiliza para confirmar las solicitudes de firma emitidas por un proveedor de identidad. Saber más sobre las huellas digitales del certificado aquí .
Redireccionar a los usuarios a la página de Inicio de sesión SSO	Si esta opción está habilitada, la página de usuario de iSpring tendrá la siguiente URL: https://yourcompany.ispringlearn.com/sso/login .

4. Si es necesario, [correlacione los campos](#) en iSpring LMS y su servicio SSO.

Asociar campos de iSpring LMS y atributos de SSO

Los atributos asociados se sincronizan automáticamente cuando un usuario inicia sesión.

Usuario

▼

sub

Correo electrónico

▼

email

Fecha de contratación

▼

Escribir atributo

Las fechas deben enviarse en formato Unix Timestamp

Nombre

▼

given_name

🗑

Apellido

▼

family_name

🗑

+ Añadir un campo

5. Después, haga clic en **Activar**.
6. Luego, [añada un enlace](#) al sitio corporativo en la sección **Accesos directos**.

← Integración de Inicio de sesión único (SSO)

Ajustes SSO

Accesos directos

Los accesos directos están ahora en la sección Ajustes

Puede añadir nuevos enlaces a sitios y servicios usados frecuentemente en Ajustes > Opciones adicionales > Accesos directos.

Ir a accesos directos

Si recibe un error 400 y un mensaje sobre que la solicitud está compuesta incorrectamente ("No se puede recuperar metadatos para el IdP '<https://myidp.com/oam/fed>' porque no es un IdP válido para este SP") después de haber habilitado SAML 2.0 en su cuenta de iSpring LMS, significa que el valor establecido para el **URL del Emisor (IdP Entity ID)** es incorrecto.



Wrong Request

Cannot retrieve metadata for IdP 'https://myidp.com/oam/fed' because it isn't a valid IdP for this SP.

[← Go Back](#)

Para hacer que la autorización SAML 2.0 funcione correctamente en su cuenta, copie la URL del texto de error y péguela en el **campo URL del Emisor (ID de Entidad IdP)**.

← Integración de Inicio de sesión único (SSO)

Ajustes SSO

Accesos directos

SAML

JWT

OpenID

[¿Qué es esto?](#)

Activar

Ajustes de conexión

URL del emisor (ID de identidad del IdP):

URL de inicio de sesión único:

URL de cierre de sesión:

Huella digital del certificado:

☒ Redireccionar a los usuarios a la página de Inicio de sesión SSO ?