

Autorización OpenID

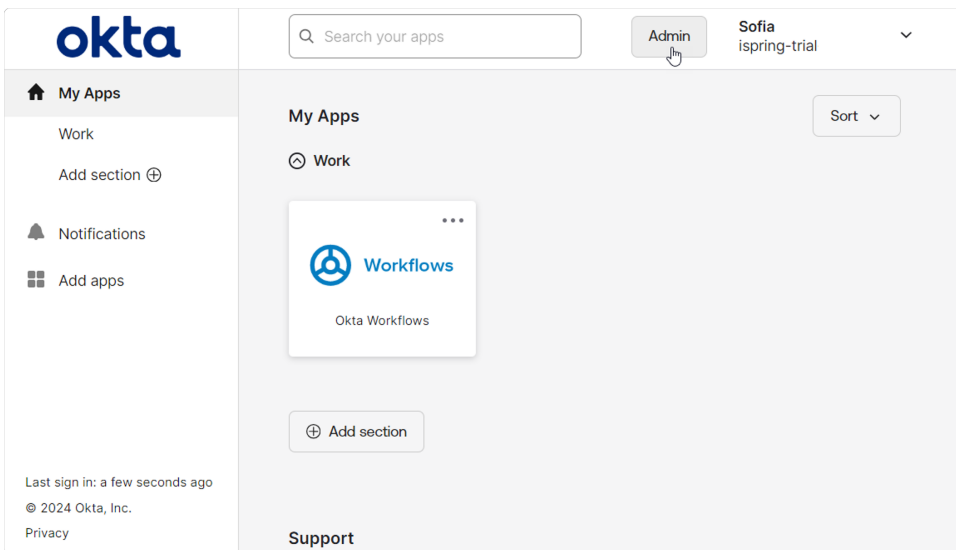
OpenID es una tecnología popular de inicio de sesión único (SSO) que permite el acceso a todos los recursos web de la empresa con las mismas credenciales. En iSpring LMS, el protocolo OpenID Connect funciona con el proveedor de identidad Okta, que es un servidor de autorización que autentica a los usuarios y transmite información sobre una autorización exitosa a LMS.

La autorización con OpenID y Okta funciona en la aplicación móvil.

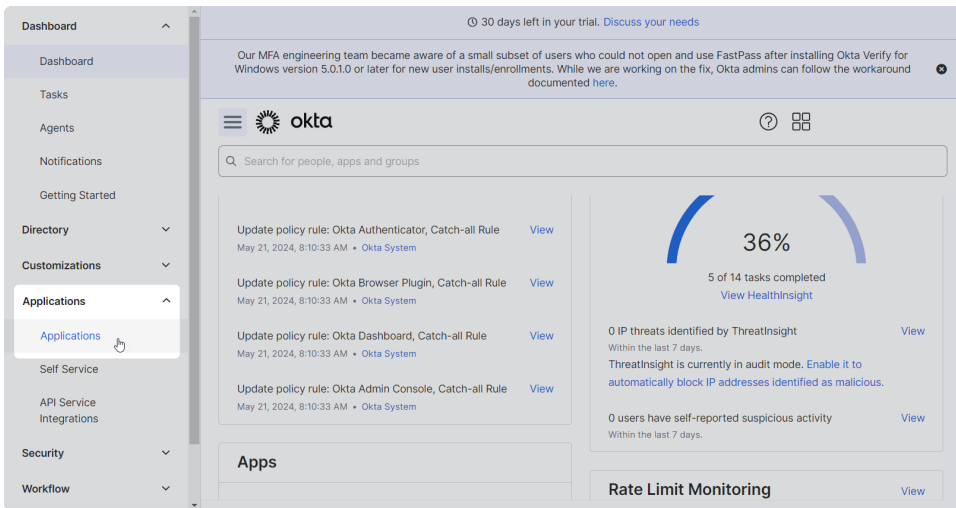
- [Configuración del servidor de autorización de Okta](#)
- [Configurando iSpring LMS](#)
- [Añadiendo usuarios a iSpring LMS](#)
- [Autorización sin OpenID](#)

Configuración del servidor de autorización de Okta

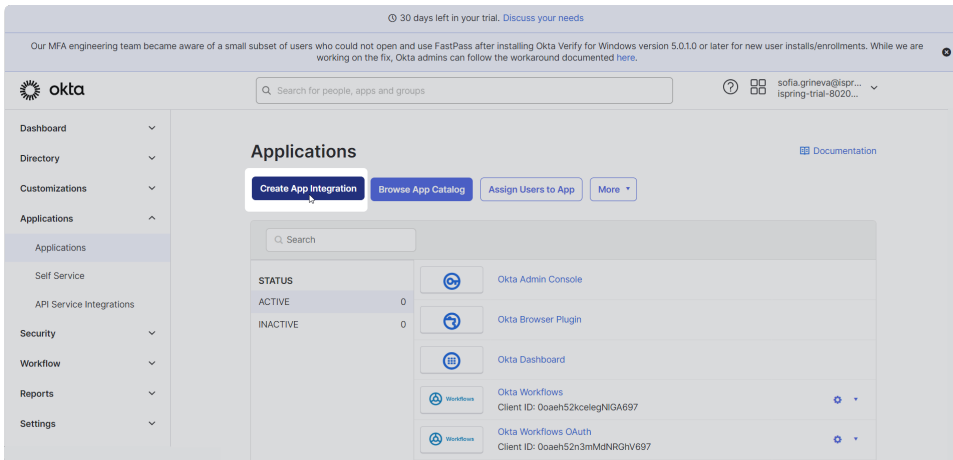
1. Inicie sesión en su cuenta de Okta y haga clic en **Admin**.



2. Después, abra la sección de **Applications** (Aplicaciones) en el menú de la barra lateral.



3. En la sección **Applications** (Aplicaciones), haga clic en **Create App Integration** (Crear integración de app).



4. At el segundo paso, seleccione **OIDC - OpenID Connect** y **Web Application** (Aplicación web), y haga clic en Next (Siguiente).

Create a new app integration

Sign-in method
[Learn More](#)

- ☒ **OIDC - OpenID Connect**
Token-based OAuth 2.0 authentication for Single Sign-On (SSO) through API endpoints. Recommended if you intend to build a custom app integration with the Okta Sign-In Widget.
- ☐ **SAML 2.0**
XML-based open standard for SSO. Use if the Identity Provider for your application only supports SAML.
- ☐ **SWA - Secure Web Authentication**
Okta-specific SSO method. Use if your application doesn't support OIDC or SAML.
- ☐ **API Services**
Interact with Okta APIs using the scoped OAuth 2.0 access tokens for machine-to-machine authentication.

Application type
What kind of application are you trying to integrate with Okta?
Specifying an application type customizes your experience and provides the best configuration,

- ☒ **Web Application**
Server-side applications where authentication and tokens are handled on the server (for example, Go, Java, ASP.Net, Node.js, PHP)
- ☐ **Single-Page Application**
Single-page web applications that run in the browser where the

5. Después de eso, comience a configurar la aplicación.

En la **Sección de URLs de redireccionamiento de inicio de sesión**, añada tres enlaces más bajo el predeterminado:

`https://companyname.ispringlearn.com/sso/login/oidc`
`http://companyname.ispringlearn.com/sso/login/oidc`
`islearn://companyname.ispringlearn.com/sso/login/oidc`

Para que la autorización en la aplicación móvil funcione, añada una URL de retorno modificada al servidor de autorización. Intercambia el esquema **https** por **islearn**: por ejemplo, cambia `https://auth.dev.mycompany.com/sso/login/oidc` a `islearn://auth.dev.mycompany.com/sso/login/oidc`

En la sección de **Sign-out redirect URLs** (URLs de redirección de cierre de sesión), añada un enlace más debajo del predeterminado:

<https://companyname.ispringlearn.com/login/?logout=1>

The screenshot shows the Okta Admin Console interface. On the left is a navigation menu with options: Dashboard, Directory, Customizations, Applications, Security, Workflow, Reports, and Settings. The main content area is titled 'Sign-in redirect URIs' and includes a checkbox for 'Allow wildcard * in sign-in URI redirect.' Below this, there are four input fields for redirect URIs: 'http://localhost:8080/authorization-code/callback', 'https://my1.ispringlearn.com/sso/login/oidc', 'http://my1.ispringlearn.com/sso/login/oidc', and 'islearn://my1.ispringlearn.com/sso/login/oidc'. Each field has a delete button (X). There is also an '+ Add URI' button. Below this section is another section titled 'Sign-out redirect URIs (Optional)' with two input fields: 'http://localhost:8080' and 'https://my1.ispringlearn.com/login/?logout=1', each with a delete button (X) and an '+ Add URI' button. A 'Learn More' link is present in both sections.

6. Luego, añada **Base URLs** (URLs base) — básicamente es el enlace a su cuenta de iSpring LMS.

The screenshot shows the 'Trusted Origins' section in the Okta Admin Console. It includes a 'Learn More' link at the top. Below it, the 'Base URIs (Optional)' section is highlighted. It contains a text input field with the value 'https://my1.ispringlearn.com/' and a delete button (X). Below the input field is a '+ Add URI' button. A mouse cursor is pointing at the input field. Below this section is the 'Assignments' section, which has a 'Controlled access' heading and three radio button options: 'Allow everyone in your organization to access', 'Limit access to selected groups', and 'Skip group assignment for now'. A 'Learn More' link is also present in this section.

Además, en la sección **Grant type allowed** (Tipos de concesión permitidos) anterior, seleccione **Refresh Token** (Actualizar Token) y **Implicit (Hybrid)** (Implícito (Híbrido)).

Search for people, apps and groups

Grant type
[Learn More](#)

Client acting on behalf of itself
☐ Client Credentials

Core grants
☒ Authorization Code
☒ Refresh Token

Advanced [^](#)

These grants are more sensitive and should be enabled only if necessary.
 Okta direct auth API grants
☐ OTP
☐ OOB
☐ MFA OTP
☐ MFA OOB

Other grants
☒ Implicit (hybrid)

Sign-in redirect URIs
☐ Allow wildcard * in sign-in URI redirect.

7. En la sección **Assignments** (Tareas), marque **Allow everyone in your organization to access** (Permitir que todos en su organización accedan). Finalmente, haga clic en **Save** (Guardar).

okta

Search for people, apps and groups

Assignments

Controlled access
 Select whether to assign the app integration to everyone in your org, only selected group(s), or skip assignment until after app creation.

☒ Allow everyone in your organization to access
☐ Limit access to selected groups
☐ Skip group assignment for now

Enable immediate access (Recommended)
 Recommended if you want to grant access to everyone without pre-assigning your app to users and use Okta only for authentication.

☒ Enable immediate access with **Federation Broker Mode**

To ensure optimal app performance at scale, Okta End User Dashboard and provisioning features are disabled. [Learn more about Federation Broker Mode](#).

Save [Cancel](#)

Para iniciar sesión sin un código de verificación enviado a la aplicación Okta Verify, vaya a **Sign On** (Iniciar sesión) > **User authentication** (Autenticación de usuario) y seleccione **Okta Dashboard** (Panel de control).

okta

Search for people, apps and groups

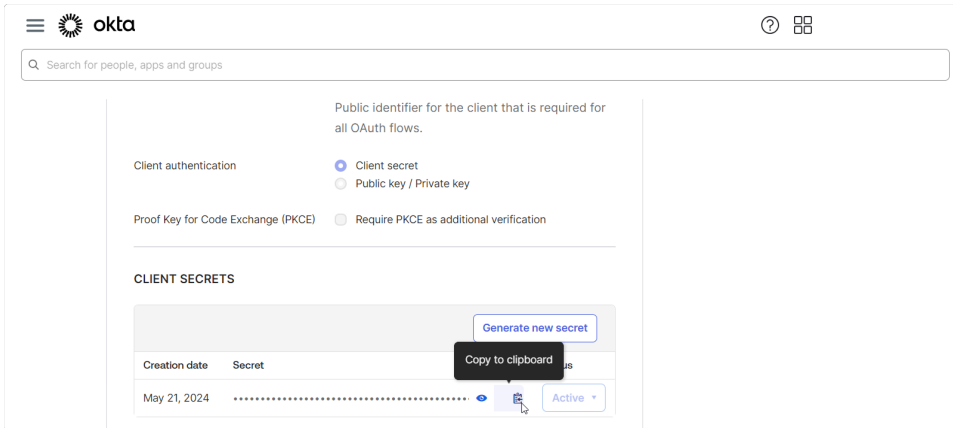
Applications

User authentication [Cancel](#)

Authentication policy
 Any two factors
 Okta Browser Plugin
 Okta Dashboard

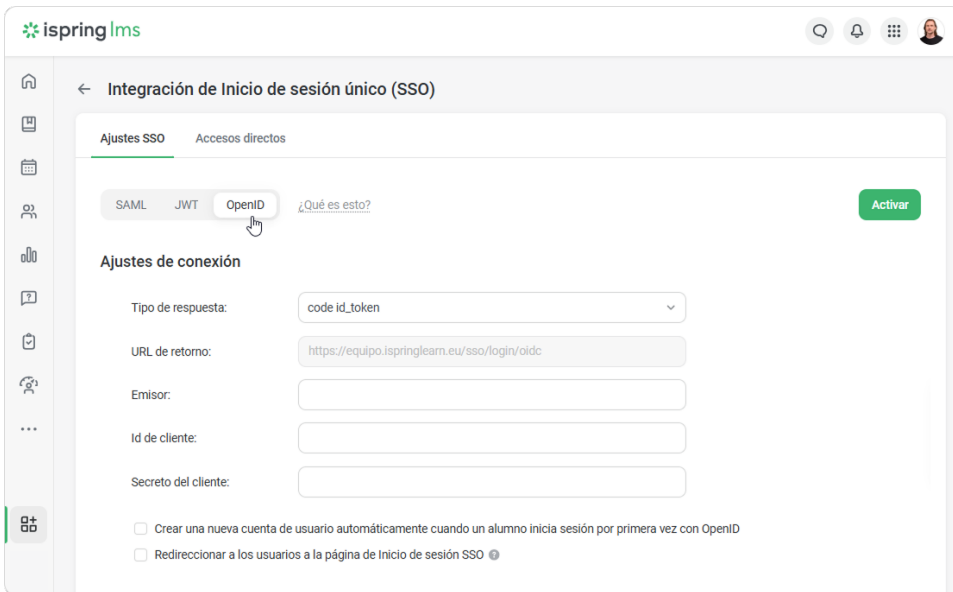
© 2024 Okta, Inc. [Privacy](#) [Status site](#) [OK14 US Cell](#) [Version 2024.05.1 E](#) [Download Okta Plugin](#) [Feedback](#)

8. Abra la pestaña **General** y copie su **Client Id** (Id de cliente) y **Client Secret** (Secreto de cliente).



Configurando iSpring LMS

1. Inicie sesión en su cuenta de iSpring LMS. Luego, vaya a los **Ajustes SSO** y haga clic en **OpenID**.

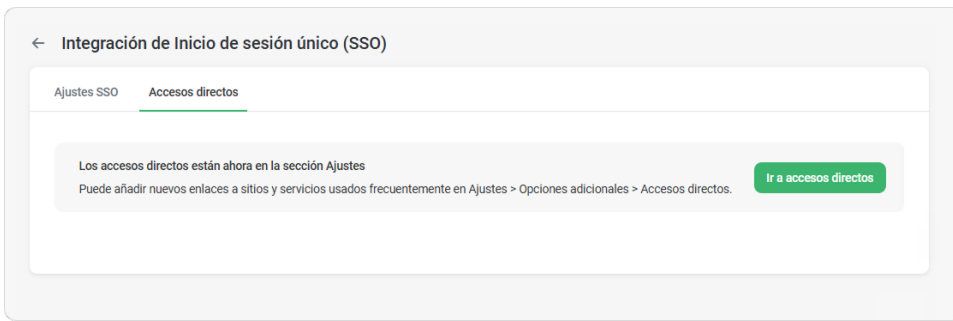


2. Rellene los campos del formulario y marque **Crear una nueva cuenta de usuario automáticamente cuando un alumno inicia sesión por primera vez con OpenID**.

Crear una nueva cuenta de usuario automáticamente cuando un alumno inicia sesión por primera vez con OpenID	Marque esta opción para habilitar a los usuarios no registrados para que sean añadidos a iSpring LMS cuando intenten iniciar sesión.
Tipo de respuesta	El tipo de respuesta que emite el servidor de autorización.
URL de retorno	La dirección web de la página a la que se redirige a los usuarios no autenticados.
Emisor	El emisor del token de seguridad. Este valor se puede recuperar en el servidor de autorización: solo copia la URL de su cuenta de Okta sin "-admin".
Id de cliente	El identificador del cliente que se puede copiar en el servidor de autorización.
Secreto del cliente	Este parámetro se usa para autenticar la aplicación cuando solicita acceso a la cuenta de un usuario. Se genera en el servidor de autorización.

3. Si es necesario, [correlacione los campos](#) en iSpring LMS y su servicio SSO. Es mejor asegurarse de que no falten campos obligatorios en los Ajustes del perfil de usuario. De lo contrario, un campo obligatorio adicional, como Cumpleaños, puede interrumpir el proceso de integración.

4. Haga clic en **Activar**.
5. A continuación, [añada un enlace](#) al sitio corporativo en la sección **Accesos directos**.



Añadiendo usuarios a iSpring LMS

Incluso si los usuarios aún no están presentes en la base de datos del iSpring LMS, se añadirán automáticamente a la lista de usuarios. Lo único que puede impedir que se añada un nuevo usuario puede ser la limitación de su plan de suscripción.

Para crear usuarios al iniciar sesión con OpenID, usamos los siguientes parámetros recibidos del servidor de autorización:

Reclamar	Campo de perfil en iSpring LMS
preferred_username	Usuario
email	Correo electrónico
family_name	Apellido
given_name	Nombre

Autorización sin OpenID

Si ha habilitado OpenID en su cuenta de iSpring LMS y por alguna razón no puede iniciar sesión utilizando el inicio de sesión único, escriba la siguiente dirección web: https://yourcompany.ispringlearn.com/login?no_sso.

Ahora iniciará sesión en la cuenta como de costumbre, utilizando tu usuario y contraseña.