# Autorización JWT

Una de las formas de realizar el inicio de sesión único en iSpring LMS es utilizar JSON Web Token (JWT). Es un estándar abierto para el paso de "claims" entre partes en un entorno de aplicación web. Se utiliza para cifrar y pasar la identidad de los usuarios autenticados entre su sitio web corporativo y iSpring LMS. En otras palabras, proporciona una transferencia fluida y segura de los datos de usuario desde su sitio web a iSpring LMS.

JWT funciona con la aplicación móvil.

## Requisitos

- Acceso a su hosting con el rol *Administrador*
- Una cuenta de iSpring LMS
- Un usuario de LMS con el rol *Administrador de la cuenta*

Para autenticar a un usuario en el lado de iSpring LMS, un mensaje JWT debe contener el correo electrónico del usuario. La contraseña y otra información del usuario no son obligatorias para el SSO.


Un enlace completo con un token JSON se ve así:
https://yourcompany.ispringlearn.com/sso/login/jwt?jwt=XXXXXX.YYYYYY.ZZZ

## Partes de JWT

El token JWT está codificado y consta de 3 partes, separadas por puntos:

1. **XXXXXX es una cabecera codificada**

   Codificado en BASE64, conserva información sobre el tipo de token (“JWT”) y el algoritmo de cifrado (“HS256”). En la notación de objetos JS se ve así:

   ```
   {
   "Type": "JWT",
   "ALG":
   "HS256"}
   ```

2. **YYYYYY es una carga útil codificada**

   Este es el cuerpo del mensaje del token que aprueba el ID del usuario (correo electrónico). También se representa en el formato BASE64. La notación JS limpia se ve así:

   ```
   {
   "IAT": 123456789,
   "JTI": f4as6d5f4as6d54fasd6df4,
   "exp": 123456849,
   "email":
   "username@yourcompany.com"}
   ```

| | |
|---|---|
| **IAT (Issued At)** | Guarda el momento en que se creó este token. |
| **JTI (JWT ID)** | El identificador del token, emitido automáticamente y codificado. |

| | |
|---|---|
| **exp** | Hora de expiración de este token. |
| **email** | Dirección de correo electrónico de un usuario (o un ID de usuario) que desea autenticar. La dirección de correo electrónico de un usuario debe ser la misma en ambos recursos, su sitio web e iSpring LMS. |

3. **ZZZ es una firma**

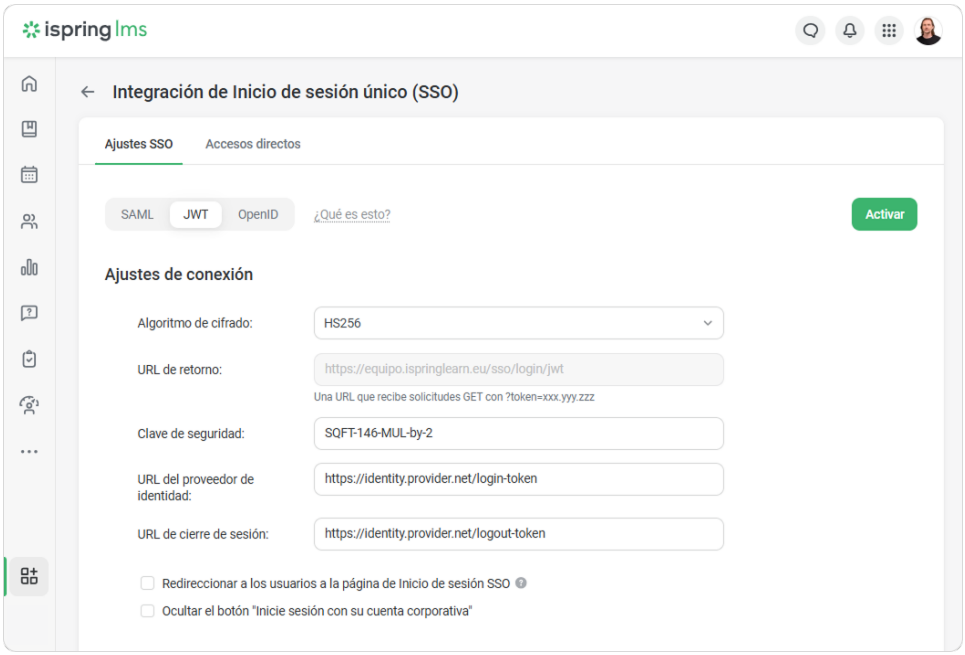
   Esta parte contiene una clave para cifrar todo el mensaje (las 3 partes). Tiene este aspecto:

```
HMACSHA256(base64UrlEncode(XXXXXX) + "." + base64UrlEncode(YYYYYY), secret)
```

| | |
|---|---|
| **secret** | Esta es una clave criptográfica que utilizan ambas partes de este proceso para codificar el mensaje. |

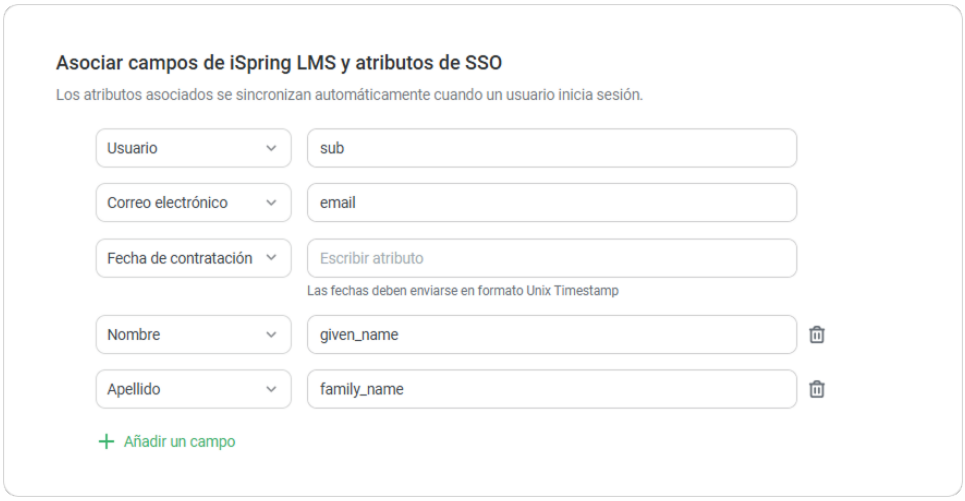
# Configuración de parámetros SSO

1. Inicie sesión en su cuenta de iSpring LMS. Luego vaya a los **Ajustes SSO** y haga clic en **JWT**.
2. Rellene los campos del formulario.




| | |
|---|---|
| **Algoritmo de cifrado** | El algoritmo utilizado para firmar/cifrar. |
| **URL de retorno** | La dirección web de una página a la que se dirigen los usuarios que han pasado por la autenticación de identidad. |
| **Clave de seguridad** | La clave criptográfica y la parte secreta del token JWT. |
| **URL del proveedor de identidad** | La dirección web de una página donde se conserva el script que genera tokens JWT. |
| **URL de cierre de sesión** | La dirección web de una página donde se conserva el script que genera tokens JWT para el cierre de sesión de los usuarios. |

3. Luego, correlacione los campos en iSpring LMS y su servicio SSO.



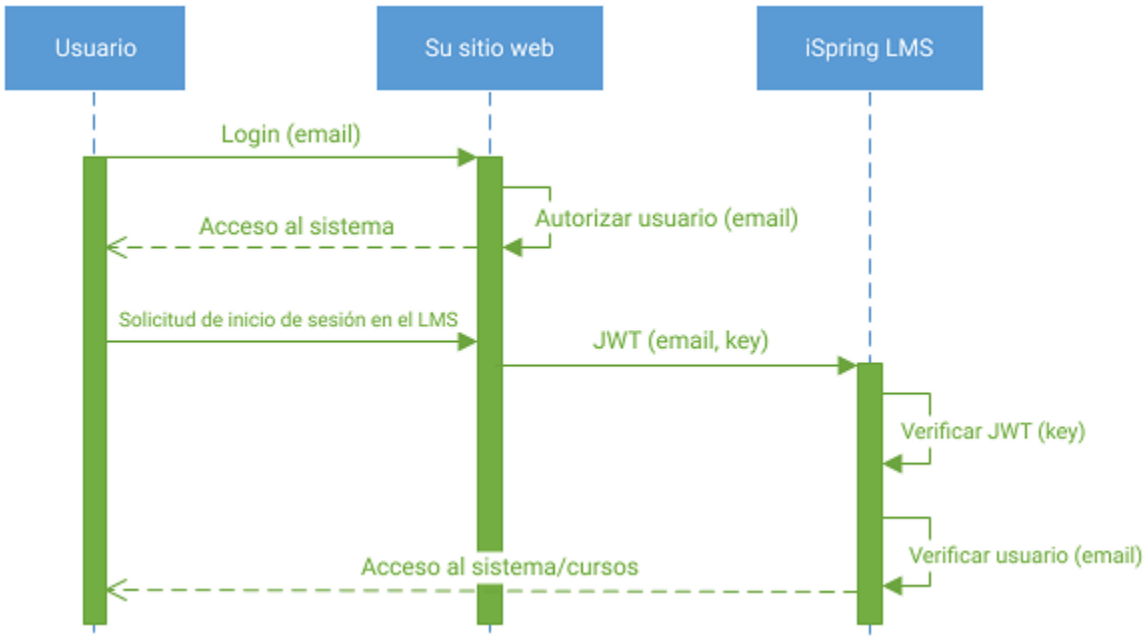

4. Por último, haga clic en **Activar**.

Recomendamos utilizar el protocolo HTTPS en lugar de HTTP para un mayor nivel de seguridad.

Si ha habilitado JWT 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, usando su usuario y contraseña.

## Lógica de procesamiento

Todo el proceso se muestra en el diagrama de secuencia temporal UML a continuación:




## Ejemplo de autorización

Si los usuarios aún no están incluidos en la base de datos de iSpring LMS, al autorizarse con JWT, se añaden automáticamente y quedan autorizados en el sistema. El único obstáculo para añadir automáticamente un nuevo usuario puede ser el límite de su suscripción.

Otro ejemplo de autorización automática es el caso en que los usuarios inician sesión con iSpring LMS sin una autorización previa en su sitio web corporativo. Si la tecnología JWT está habilitada en su cuenta de iSpring LMS, los usuarios serán redirigidos automáticamente a una página correspondiente del sitio web del proveedor de identidad: https://www.yourwebsite.com/login-token/.

Después de que se ingresen el inicio de sesión y la contraseña en el lado del proveedor de identidad, los usuarios se autorizan en iSpring LMS.

# Ejemplos de código PHP

## Realización del servicio de autenticación (inicio de sesión)

Este servicio debe colocarse en su sitio web. Autentica a un usuario e inicia sesión de forma remota en el lado de iSpring LMS. En este ejemplo, iSpring LMS interactúa con el servicio de autenticación. Posibles casos y resultados:

1. Si el usuario está autorizado, el sistema redirige a este usuario a iSpring LMS.
2. Si no está autorizado, el sistema procesa el formulario de entrada del usuario. Si tiene éxito, el sistema redirige a este usuario a iSpring LMS.

Un ejemplo en GitHub: authentication.php

## Procesamiento de solicitudes de cierre de sesión del usuario

iSpring LMS LMS también proporciona la posibilidad de cerrar sesión a un usuario del sistema. Este servicio debe colocarse en su sitio web. En este ejemplo, el script comprueba un correo electrónico, realiza el cierre de sesión del usuario y muestra el mensaje correspondiente.

Un ejemplo en GitHub: logout.php

# Autorización sin JWT

Si ha habilitado JWT en su cuenta de iSpring LMS pero no puede iniciar sesión utilizando el inicio de sesión único por alguna razón, escriba la siguiente dirección web: https://yourcompany.ispringlearn.com/login?no_sso=1.

Ahora iniciará sesión en la cuenta como de costumbre, usando su usuario y contraseña.