

# Cómo configurar SSO con Microsoft AD FS

- [Requisitos del sistema](#)
- [Paso 1. Verificar ajustes de AD FS](#)
- [Paso 2. iSpring Cloud Ajustes](#)
- [Paso 3. Configuración de la parte confiable de AD FS](#)
- [Paso 4. Creando reglas de reclamaciones](#)
- [Paso 5. Ajustando los Ajustes de Confianza](#)
- [Paso 6. Punto final Ajustes](#)
- [Paso 7. Verificar inicio de sesión único \(SSO\)](#)
- [Correlación de campos de iSpring Cloud y SSO](#)
- [Autorización sin SAML](#)

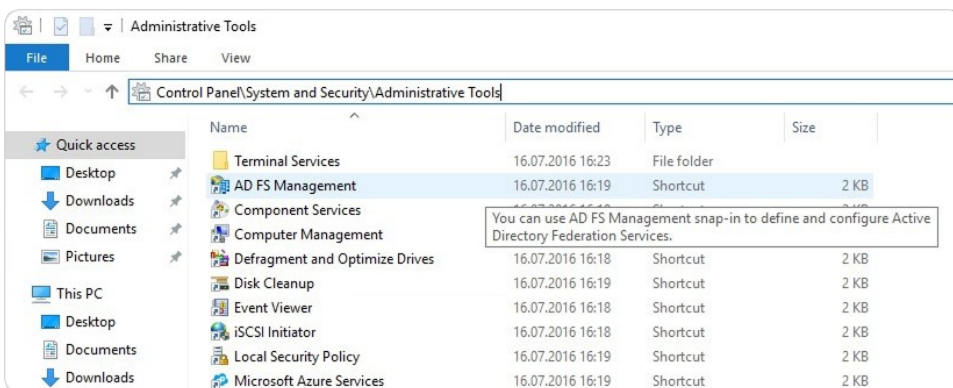
## Requisitos del sistema

- Un servidor con Microsoft Server 2019/ 2016/ 2012 R2 en ejecución
- AD FS 5.0/4.0/3.0 instalado en su servidor
- Un certificado SSL para firmar su página de usuario de AD FS y la huella digital de ese certificado
- Una cuenta de iSpring Cloud
- Un usuario con el rol *Titular de la cuenta*

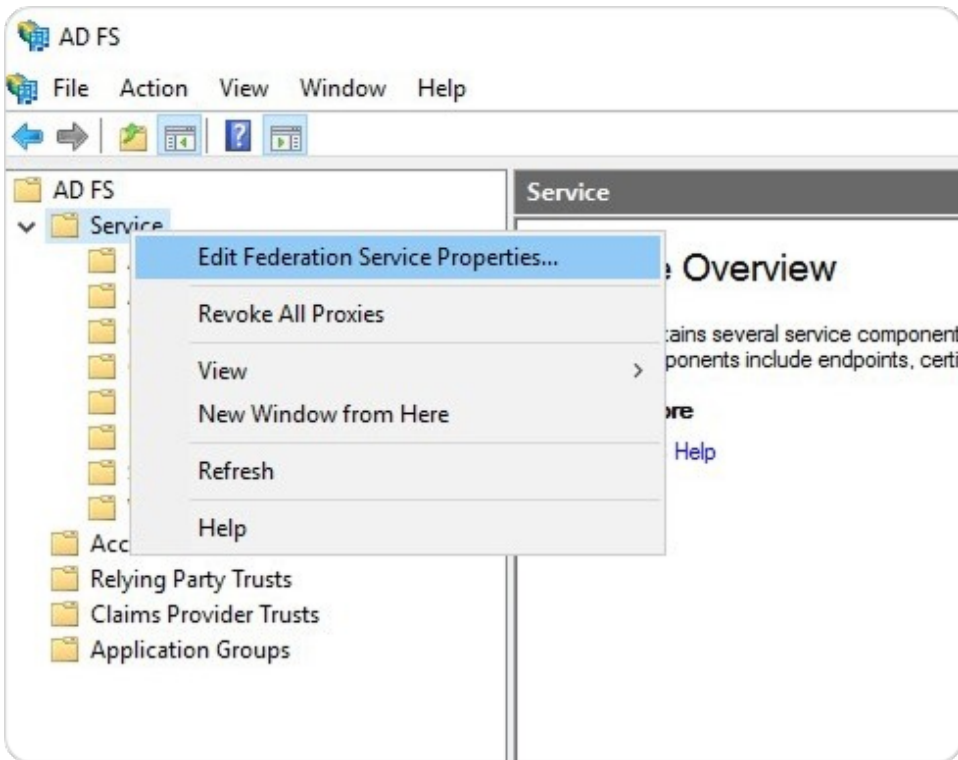
Esta guía cubre la configuración de SSO SAML mediante AD FS 4.0 en Windows Server.

## Paso 1. Verificar ajustes de AD FS

1. Inicie sesión en su servidor AD FS y abra la consola de administración de ADFS mediante el acceso directo en **Control Panel** (Panel de control) > **System and Security** (Sistema y seguridad) > **Administrative Tools** (Herramientas administrativas).

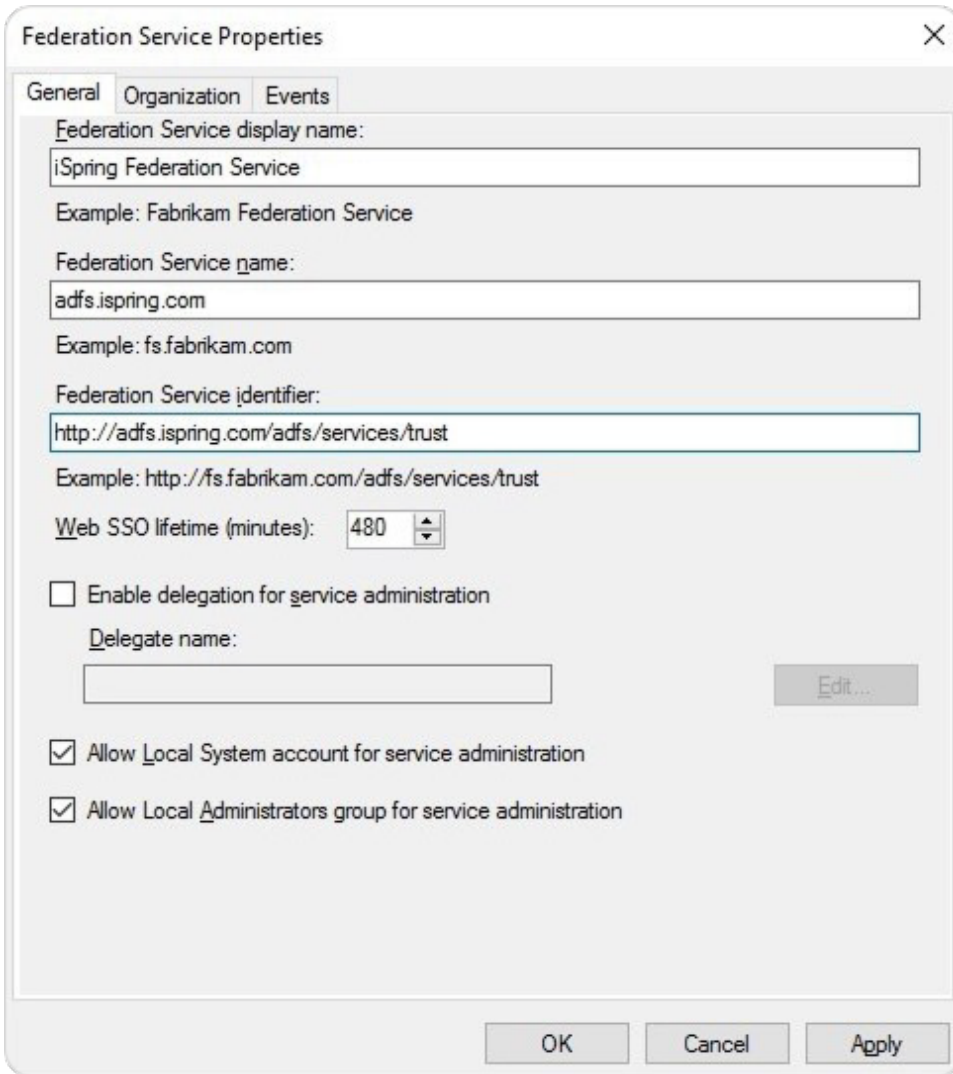


2. Haga clic derecho en **Service** (Servicio) y seleccione **Edit Federation Service Properties** (Editar propiedades del servicio de federación).



3. Verifique que los ajustes **General** (Generales) coincidan con sus entradas DNS y nombres de certificado. Tome nota del **Federation Service Identifier** (Identificador del servicio de federación), ya que se usa en los ajustes de configuración SAML 2.0 de iSpring Cloud.

4. En el campo de nombre **Federation Service** (Servicio de federación), utilice un dominio de tercer nivel, por ejemplo, [adfs.ispring.com](https://adfs.ispring.com).



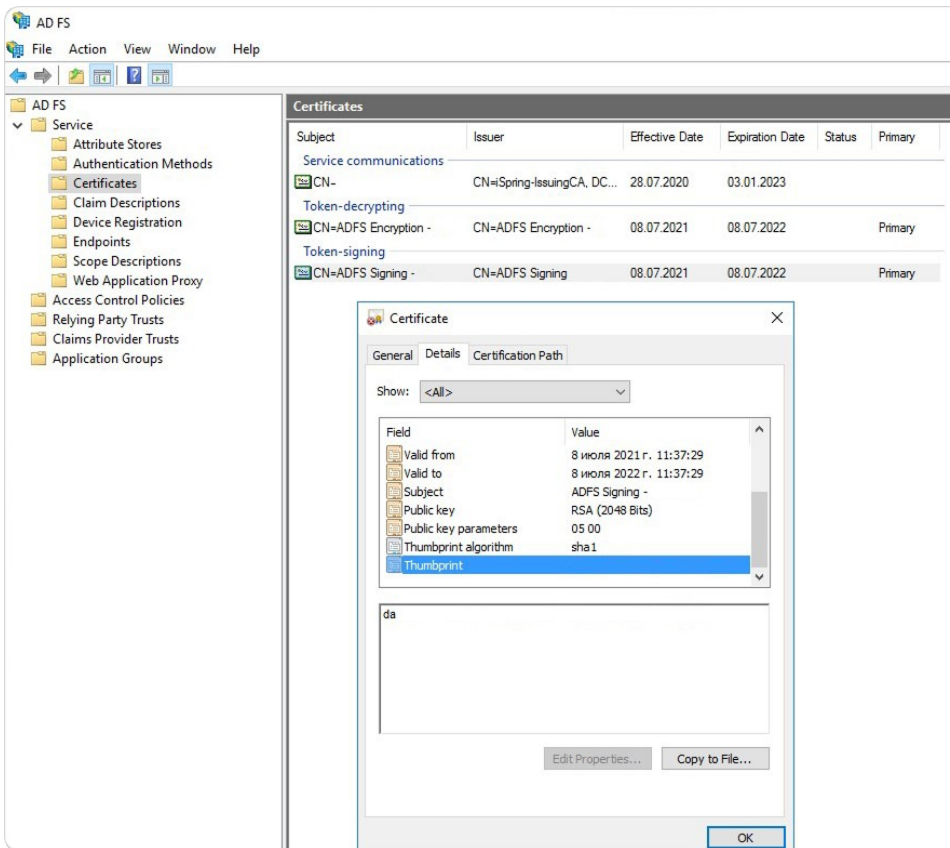
The screenshot shows the 'Federation Service Properties' dialog box with the 'General' tab selected. The fields are filled with the following values:

- Federation Service display name:** iSpring Federation Service
- Example:** Fabrikam Federation Service
- Federation Service name:** adfs.ispring.com
- Example:** fs.fabrikam.com
- Federation Service identifier:** http://adfs.ispring.com/adfs/services/trust
- Example:** http://fs.fabrikam.com/adfs/services/trust
- Web SSO lifetime (minutes):** 480
- ☐ Enable delegation for service administration
- Delegate name:** (empty field)
- ☒ Allow Local System account for service administration
- ☒ Allow Local Administrators group for service administration

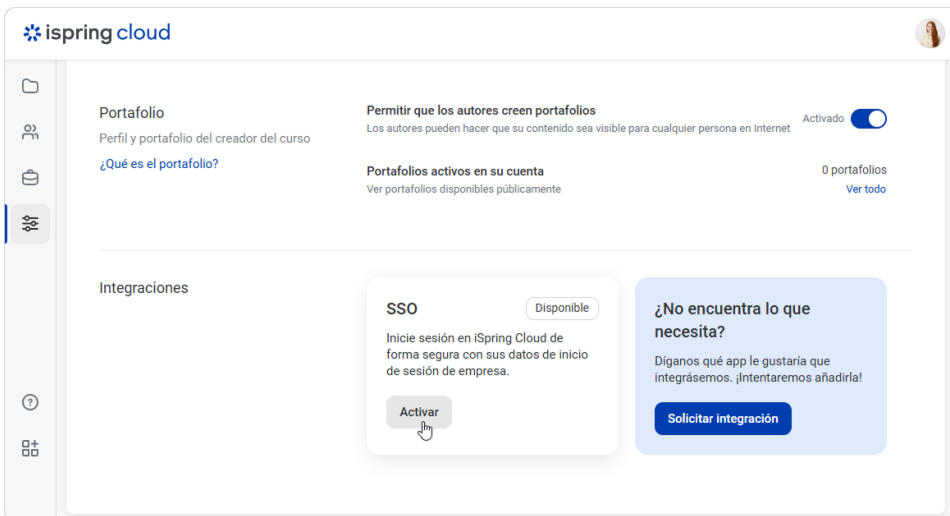
Buttons at the bottom: OK, Cancel, Apply.

## Paso 2. iSpring Cloud Ajustes

1. Examine los certificados.
2. Haga clic con el botón derecho en el certificado y seleccione **View Certificate** (Ver certificado).
3. Ir a la pestaña **Details** (Detalles).
4. Encuentra el campo **Thumbprint** (Huella Digital) y copia el contenido.



5. Inicie sesión en su cuenta de iSpring Cloud. A continuación, vaya a **Ajustes > Integraciones**. Haga clic en **Activar** en la tarjeta de SSO.



6. Inserte su **Thumbprint** (huella digital) en el campo **Huella digital del certificado** y elimine todos los espacios entre los caracteres.
7. En iSpring Cloud, en la página de **ajustes de integración SSO**, rellene estos campos:

| Nombre del campo                       | Ejemplo                                                                                                                                 |
|----------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------|
| URL del emisor (ID de entidad del IdP) | <a href="http://YOUR_ADFS_SERVERNAME/adfs/services/trust">http://YOUR_ADFS_SERVERNAME/adfs/services/trust</a>                           |
| URL de inicio de sesión único          | <a href="https://YOUR_ADFS_SERVERNAME/adfs/ls/idpinitiatedsignon.aspx">https://YOUR_ADFS_SERVERNAME/adfs/ls/idpinitiatedsignon.aspx</a> |
| URL de cierre de sesión                | <a href="https://YOUR_ADFS_SERVERNAME/adfs/ls/?wa=wsignout1.0">https://YOUR_ADFS_SERVERNAME/adfs/ls/?wa=wsignout1.0</a>                 |

Los parámetros de la URL de inicio de sesión único y la URL de cierre de sesión pueden diferir, según el AD FS.

**ispring cloud**

← Integración SAML SSO 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 ⓘ

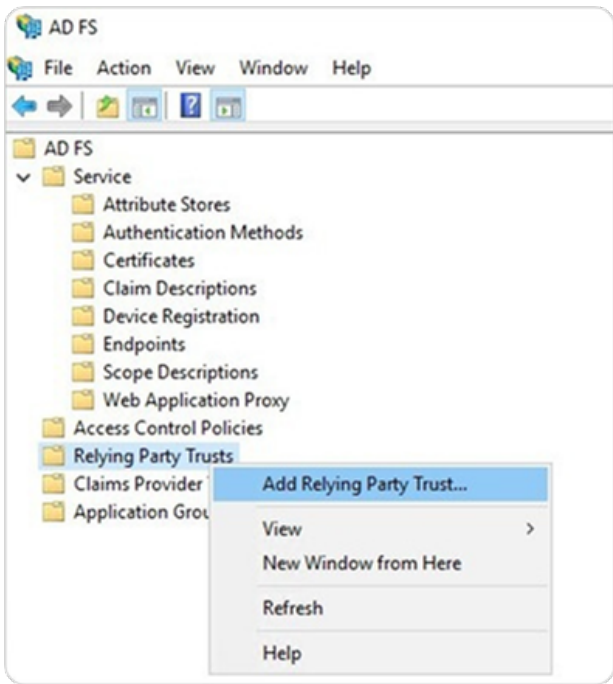
☐ Enlace a su portal corporativo

|                                                                     |                                                                                                                                                                                                                                                                                      |
|---------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>URL del emisor (ID de identidad del IdP)</b>                     | La URL que identifica de forma única el servicio del proveedor de identidad. Este valor es igual al elemento <b>E misor</b> de la solicitud SAML enviada por el proveedor de identidad.                                                                                              |
| <b>URL de inicio de sesión único</b>                                | Es la ruta al script del servidor que genera solicitudes de confirmación de identificador SAML para gestionar la autorización.                                                                                                                                                       |
| <b>URL de cierre de sesión</b>                                      | Es la ruta al script del servidor que genera solicitudes de confirmación de identificador SAML para gestionar el cierre de sesión.                                                                                                                                                   |
| <b>Huella digital del certificado</b>                               | Esta es una versión abreviada <a href="#">del certificado de clave pública</a> para verificar una firma digital. Se utiliza para confirmar solicitudes de firma emitidas por un proveedor de identidad. Saber más sobre las huellas digitales de certificados <a href="#">aquí</a> . |
| <b>Redirigir a los usuarios a la página de inicio de sesión SSO</b> | Si esta opción está habilitada, la página de usuario de iSpring tendrá la siguiente URL: <a href="https://yourcompany.ispring.com/sso/login">https://yourcompany.ispring.com/sso/login</a> .                                                                                         |

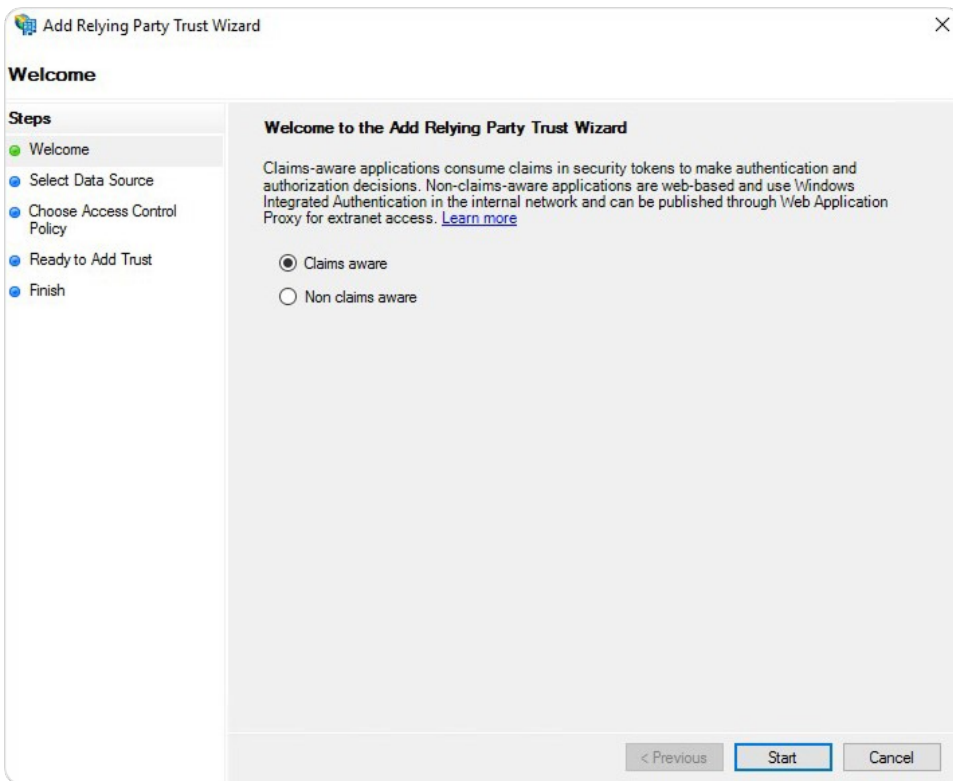
8. Haga clic en **Activar**.

### Paso 3. Configuración de la parte confiable de AD FS

1. Vaya a la consola de administración de AD FS y seleccione **Relying Party Trusts** (Confianzas de partes confiables), haga clic con el botón derecho sobre ella y seleccione **Add Relying Party Trust** (Añadir confianza de parte confiable).



2. Seleccione **Claims aware** (Consciente de las reclamaciones) y haga clic en **Start** (Iniciar).



3. En la **Select Data Source** (Seleccionar origen de datos) fase, seleccione la última opción: **Enter data about the relying party manually** (Introducir datos sobre la parte confiable manualmente).

**Add Relying Party Trust Wizard**

### Select Data Source

**Steps**

- Welcome
- Select Data Source
- Specify Display Name
- Configure Certificate
- Configure URL
- Configure Identifiers
- Choose Access Control Policy
- Ready to Add Trust
- Finish

Select an option that this wizard will use to obtain data about this relying party:

☐ Import data about the relying party published online or on a local network

Use this option to import the necessary data and certificates from a relying party organization that publishes its federation metadata online or on a local network.

Federation metadata address (host name or URL):

Example: fs.contoso.com or https://www.contoso.com/app

☐ Import data about the relying party from a file

Use this option to import the necessary data and certificates from a relying party organization that has exported its federation metadata to a file. Ensure that this file is from a trusted source. This wizard will not validate the source of the file.

Federation metadata file location:

☒ Enter data about the relying party manually

Use this option to manually input the necessary data about this relying party organization.

< Previous   **Next >**   Cancel

4. En la siguiente pantalla, introduzca un **Display name** (Nombre para mostrar) que pueda reconocer en el futuro. Haga clic en **Next** (Siguiente).

**Add Relying Party Trust Wizard**

### Specify Display Name

**Steps**

- Welcome
- Select Data Source
- Specify Display Name
- Configure Certificate
- Configure URL
- Configure Identifiers
- Choose Access Control Policy
- Ready to Add Trust
- Finish

Enter the display name and any optional notes for this relying party.

Display name:

Notes:

< Previous   **Next >**   Cancel

5. En la etapa **Configure Certificate** (Configurar certificado), deje los valores Predeterminadas. Haga clic en **Next** (Siguiente).

Add Relying Party Trust Wizard

### Configure Certificate

**Steps**

- Welcome
- Select Data Source
- Specify Display Name
- Configure Certificate
- Configure URL
- Configure Identifiers
- Choose Access Control Policy
- Ready to Add Trust
- Finish

Specify an optional token encryption certificate. The token encryption certificate is used to encrypt the claims that are sent to this relying party. The relying party will use the private key of this certificate to decrypt the claims that are sent to it. To specify the certificate, click Browse.

Issuer:  
Subject:  
Effective date:  
Expiration date:

View... Browse... Remove

< Previous Next > Cancel

6. En la siguiente pantalla, marque la casilla **Enable support for the SAML 2.0 WebSSO protocol** (Habilitar soporte para el protocolo WebSSO SAML 2.0). La URL del servicio será: <https://youraccount.ispring.com/module.php/saml/sp/saml2-acps.php/default-sp>.

Add Relying Party Trust Wizard

### Configure URL

**Steps**

- Welcome
- Select Data Source
- Specify Display Name
- Configure Certificate
- Configure URL
- Configure Identifiers
- Choose Access Control Policy
- Ready to Add Trust
- Finish

AD FS supports the WS-Trust, WS-Federation and SAML 2.0 WebSSO protocols for relying parties. If WS-Federation, SAML, or both are used by the relying party, select the check boxes for them and specify the URLs to use. Support for the WS-Trust protocol is always enabled for a relying party.

☐ Enable support for the WS-Federation Passive protocol

The WS-Federation Passive protocol URL supports Web-browser-based claims providers using the WS-Federation Passive protocol.

Relying party WS-Federation Passive protocol URL:

Example: <https://fs.contoso.com/adfs/ls/>

☒ Enable support for the SAML 2.0 WebSSO protocol

The SAML 2.0 single-sign-on (SSO) service URL supports Web-browser-based claims providers using the SAML 2.0 WebSSO protocol.

Relying party SAML 2.0 SSO service URL:

<https://youraccount.ispring.com/module.php/saml/sp/saml2-acps.php/default-sp>

Example: <https://www.contoso.com/adfs/ls/>

< Previous Next > Cancel

7. En la etapa **Configure Identifiers** (Configurar identificadores), añada el **Relying party trust identifier** (Identificador de confianza de parte confiable) como <https://youraccount.ispring.com/module.php/saml/sp/metadata.php/default-sp>. Haga clic en **Add** (Añadir).



Add Relying Party Trust Wizard

### Configure Identifiers

**Steps**

- Welcome
- Select Data Source
- Specify Display Name
- Configure Certificate
- Configure URL
- Configure Identifiers**
- Choose Access Control Policy
- Ready to Add Trust
- Finish

Relying parties may be identified by one or more unique identifier strings. Specify the identifiers for this relying party trust.

Relying party trust identifier:  
  
Add

Example: https://fs.contoso.com/adfs/services/trust

Relying party trust identifiers:  
  
Remove

< Previous   Next >   Cancel

8. Luego, haga clic en **Next** (Siguiente).

Add Relying Party Trust Wizard

### Configure Identifiers

**Steps**

- Welcome
- Select Data Source
- Specify Display Name
- Configure Certificate
- Configure URL
- Configure Identifiers**
- Choose Access Control Policy
- Ready to Add Trust
- Finish

Relying parties may be identified by one or more unique identifier strings. Specify the identifiers for this relying party trust.

Relying party trust identifier:  
  
Add

Example: https://fs.contoso.com/adfs/services/trust

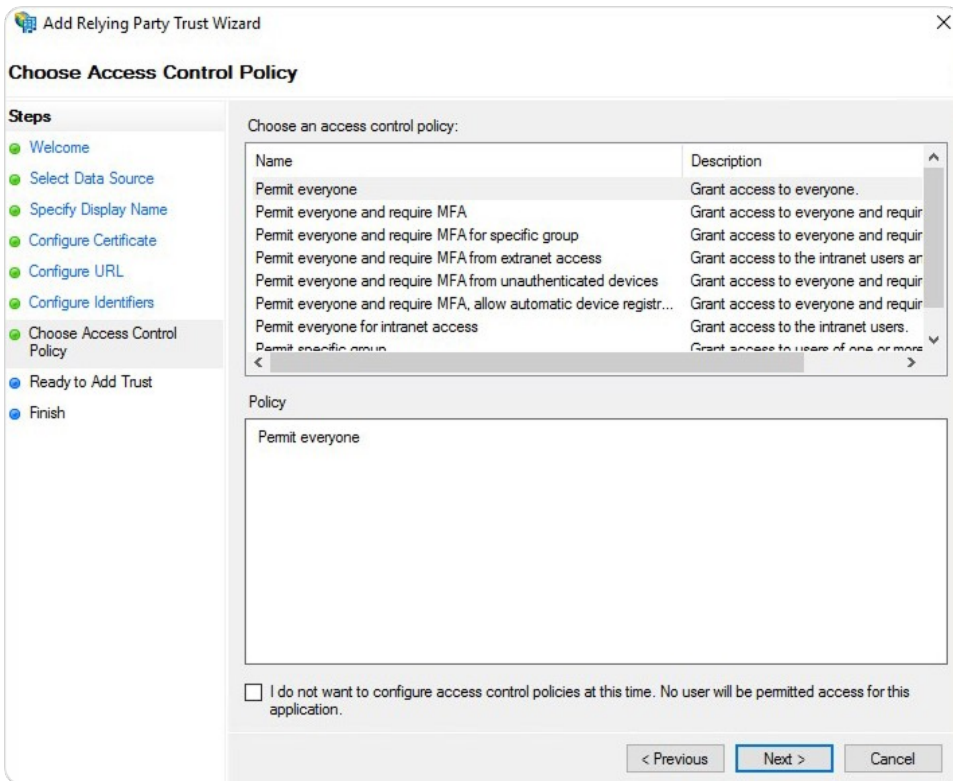
Relying party trust identifiers:  

https://youraccount.ispringlearn.com/module.php/saml/sp/metadata.php/default-sp

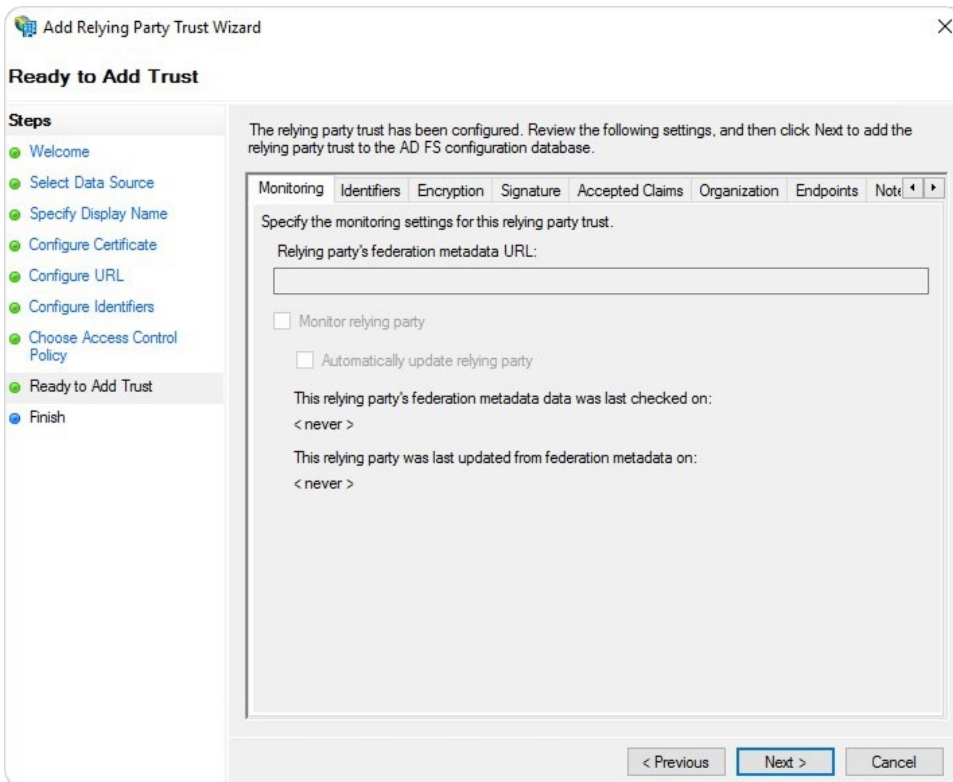
  
Remove

< Previous   **Next >**   Cancel

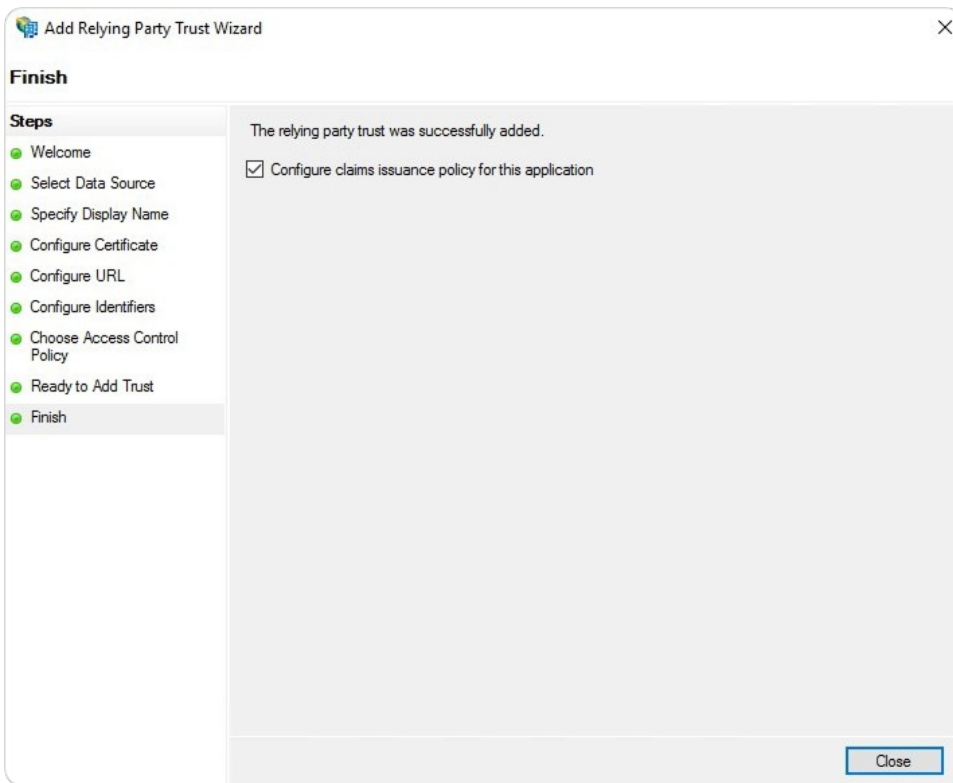
9. En el siguiente paso, elija **Permit everyone** (Permitir a todos). Haga clic en **Next** (Siguiente).



10. En la etapa **Ready to Add Trust** (Listo para Añadir Confianza), deje los valores Predeterminadas. Haga clic en **Next** (Siguiente).

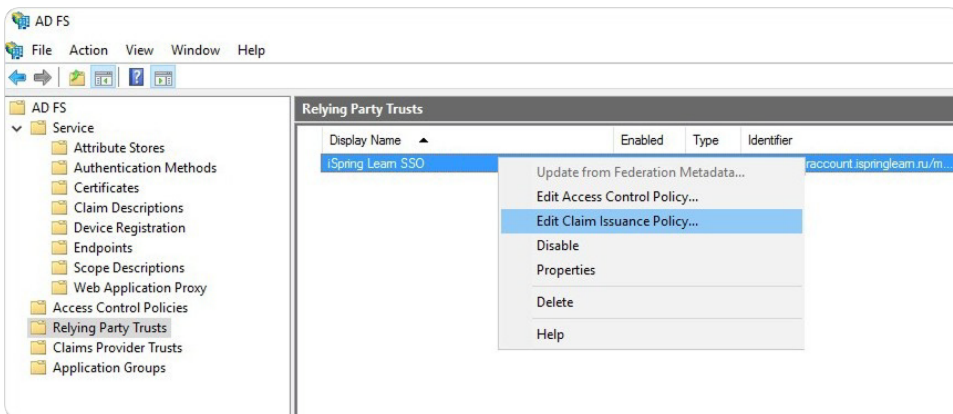


11. En el último paso, marque la casilla **Configure claims issuance policy for this application** (Configurar la directiva de emisión de reclamaciones para esta aplicación). Luego, haga clic en **Close** (Cerrar).



## Paso 4. Creando reglas de reclamaciones

1. Abra el panel de control de AD FS. En la sección de **Relying Party Trusts** (Confianzas de la Parte Dependiente), haga clic derecho en el nombre y haga clic en **Edit Claim Issuance Policy** (Editar Política de Emisión de Reclamaciones).



2. Añada la primera regla. Para hacer esto, haga clic en **Add Rule...** (Añadir regla...).

Edit Claim Issuance Policy for iSpring Learn SSO

Issuance Transform Rules

The following transform rules specify the claims that will be sent to the relying party.

| Order | Rule Name | Issued Claims |
|-------|-----------|---------------|
|-------|-----------|---------------|

↑

↓

Add Rule... Edit Rule... Remove Rule...

OK Cancel Apply

3. Seleccione **Send LDAP Attributes as Claims** (Enviar atributos LDAP como reclamaciones). Haga clic en **Next** (Siguiendo).

Add Transform Claim Rule Wizard

### Select Rule Template

**Steps**

- Choose Rule Type
- Configure Claim Rule

Select the template for the claim rule that you want to create from the following list. The description provides details about each claim rule template.

Claim rule template:

Send LDAP Attributes as Claims

Send LDAP Attributes as Claims

Send Group Membership as a Claim

Transform an Incoming Claim

Pass Through or Filter an Incoming Claim

Send Claims Using a Custom Rule

multiple claims from a single rule using this rule type. For example, you can use this rule template to create a rule that will extract attribute values for authenticated users from the displayName and telephoneNumber Active Directory attributes and then send those values as two different outgoing claims. This rule may also be used to send all of the user's group memberships. If you want to only send individual group memberships, use the Send Group Membership as a Claim rule template.

< Previous   Next >   Cancel

4. En el paso **Configure Claim Rule** (Configurar regla de reclamación), en el campo Nombre de la regla de reclamación, introduzca un nombre para la regla, por ejemplo, **Attributes of iSpring Cloud** (Atributos de iSpring Cloud).

Add Transform Claim Rule Wizard

### Configure Rule

**Steps**

- Choose Rule Type
- Configure Claim Rule

You can configure this rule to send the values of LDAP attributes as claims. Select an attribute store from which to extract LDAP attributes. Specify how the attributes will map to the outgoing claim types that will be issued from the rule.

Claim rule name:

Attributes to iSpring Learn

Rule template: Send LDAP Attributes as Claims

Attribute store:

Active Directory

Mapping of LDAP attributes to outgoing claim types:

|   | LDAP Attribute (Select or type to add more) | Outgoing Claim Type (Select or type to add more) |
|---|---------------------------------------------|--------------------------------------------------|
| ▶ | E-Mail-Addresses                            | email                                            |
| * |                                             |                                                  |

< Previous   Finish   Cancel

5. Elija **Active Directory** como su almacén de atributos.

**Add Transform Claim Rule Wizard**

### Configure Rule

**Steps**

- Choose Rule Type
- Configure Claim Rule

You can configure this rule to send the values of LDAP attributes as claims. Select an attribute store from which to extract LDAP attributes. Specify how the attributes will map to the outgoing claim types that will be issued from the rule.

Claim rule name:

Rule template: Send LDAP Attributes as Claims

Attribute store:

Mapping of LDAP attributes to outgoing claim types:

|   | LDAP Attribute (Select or type to add more) | Outgoing Claim Type (Select or type to add more) |
|---|---------------------------------------------|--------------------------------------------------|
| ▶ | E-Mail-Addresses                            | email                                            |
| * |                                             |                                                  |

< Previous   **Finish**   Cancel

6. A continuación, seleccione estos valores:

- En la columna **LDAP Attribute** (Atributo LDAP), establezca E-Mail-Addresses.
- En la columna **Outgoing Claim Type** (Tipo de reclamación saliente), establezca el valor de correo electrónico, como en iSpring Cloud <https://youraccount.ispring.com/settings/sso>.

**Add Transform Claim Rule Wizard**

### Configure Rule

**Steps**

- Choose Rule Type
- Configure Claim Rule

You can configure this rule to send the values of LDAP attributes as claims. Select an attribute store from which to extract LDAP attributes. Specify how the attributes will map to the outgoing claim types that will be issued from the rule.

Claim rule name:

Rule template: Send LDAP Attributes as Claims

Attribute store:

Mapping of LDAP attributes to outgoing claim types:

|   | LDAP Attribute (Select or type to add more) | Outgoing Claim Type (Select or type to add more) |
|---|---------------------------------------------|--------------------------------------------------|
| ▶ | E-Mail-Addresses                            | email                                            |
| * |                                             |                                                  |

< Previous   **Finish**   Cancel

7. Haga clic en **Finish** (Finalizar) para guardar la nueva regla.

**Add Transform Claim Rule Wizard**

### Configure Rule

**Steps**

- Choose Rule Type
- Configure Claim Rule

You can configure this rule to send the values of LDAP attributes as claims. Select an attribute store from which to extract LDAP attributes. Specify how the attributes will map to the outgoing claim types that will be issued from the rule.

Claim rule name:

Rule template: Send LDAP Attributes as Claims

Attribute store:

Mapping of LDAP attributes to outgoing claim types:

|   | LDAP Attribute (Select or type to add more) | Outgoing Claim Type (Select or type to add more) |
|---|---------------------------------------------|--------------------------------------------------|
| ▶ | E-Mail-Addresses                            | email                                            |
| • |                                             |                                                  |

< Previous   **Finish**   Cancel

8. Luego, añada la segunda regla y seleccione **Transform an Incoming Claim** (Transformar una reclamación entrante) como plantilla.

**Add Transform Claim Rule Wizard**

### Select Rule Template

**Steps**

- Choose Rule Type
- Configure Claim Rule

Select the template for the claim rule that you want to create from the following list. The description provides details about each claim rule template.

Claim rule template:

Claim rule template description:

Using the Transform an Incoming Claim rule template you can select an incoming claim, change its claim type, and optionally change its claim value. For example, you can use this rule template to create a rule that will send a role claim with the same claim value of an incoming group claim. You can also use this rule to send a group claim with a claim value of "Purchasers" when there is an incoming group claim with a value of "Admins". Multiple claims with the same claim type may be emitted from this rule. Sources of incoming claims vary based on the rules being edited.

< Previous   **Next >**   Cancel

9. Ingrese el **Transform Account Name** (Nombre de la cuenta de transformación) y haga clic en **OK**.



# Edit Rule - Transform Account Name



You can configure this rule to map an incoming claim type to an outgoing claim type. As an option, you can also map an incoming claim value to an outgoing claim value. Specify the incoming claim type to map to the outgoing claim type and whether the claim value should be mapped to a new claim value.

Claim rule name:

Transform Account Name

Rule template: Transform an Incoming Claim

Incoming claim type:

Windows account name

Incoming name ID format:

Unspecified

Outgoing claim type:

Name ID

Outgoing name ID format:

Transient Identifier

- ☒ Pass through all claim values
- ☐ Replace an incoming claim value with a different outgoing claim value

Incoming claim value:

Outgoing claim value:

Browse...

- ☐ Replace incoming e-mail suffix claims with a new e-mail suffix

New e-mail suffix:

Example: fabrikam.com

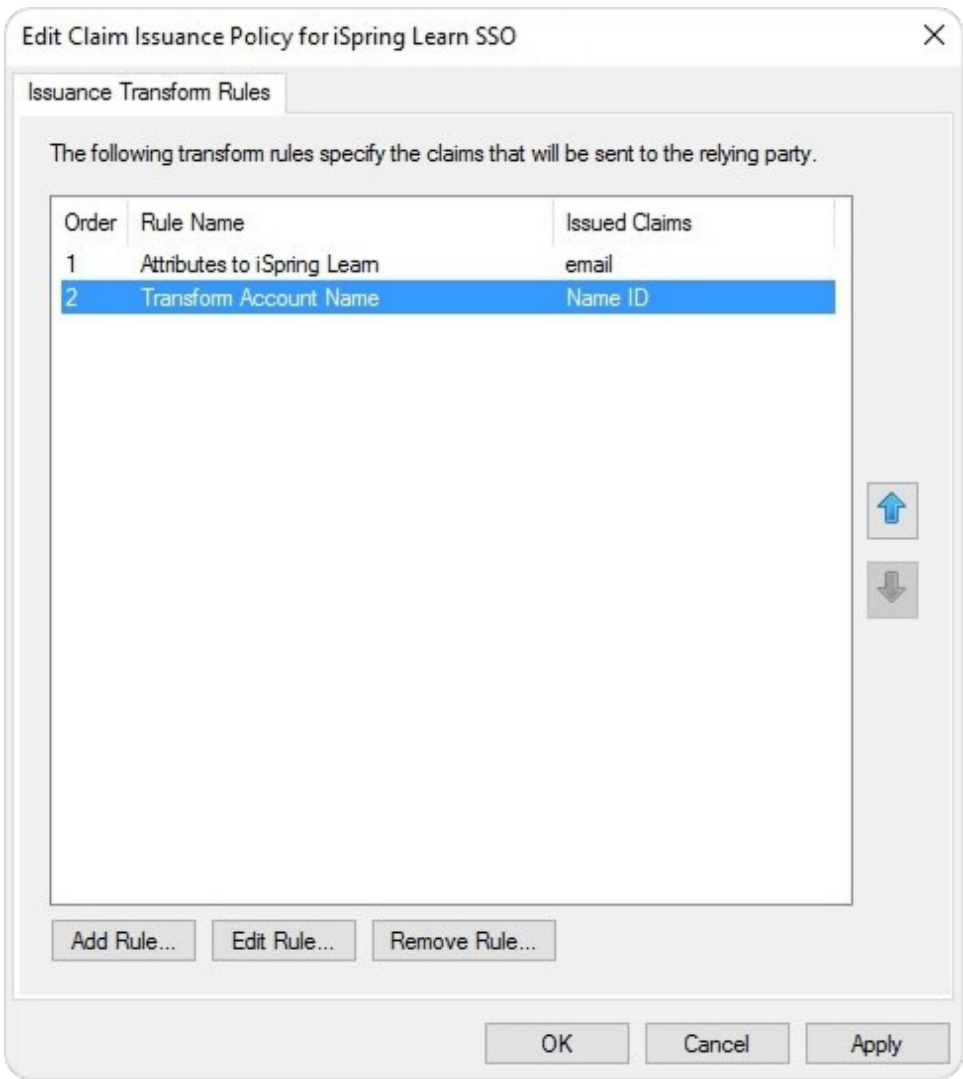
View Rule Language...

OK

Cancel



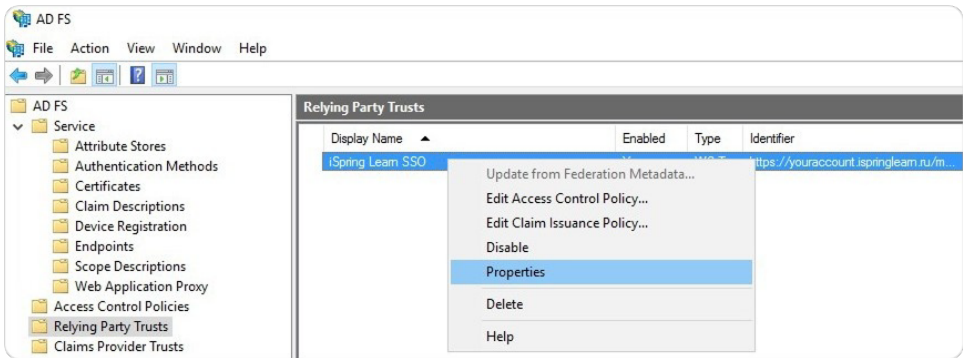
10. Haga clic en **Apply** (Aplicar) y luego en **OK** para confirmar.



## Paso 5. Ajustando los Ajustes de Confianza

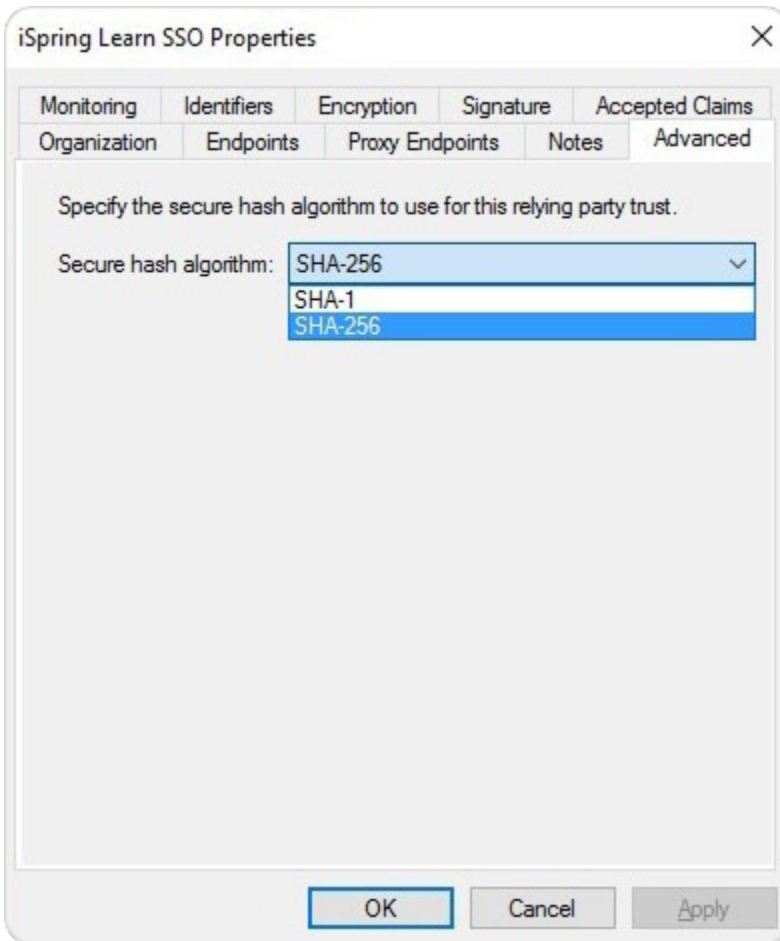
Asegúrese de que el **Secure hash algorithm** (Algoritmo de hash seguro) esté configurado en **SHA-256** en los ajustes de seguridad. Para hacer esto:

1. Abra el panel de control de AD FS. En la sección **Relying Party Trusts** (Partes confiables), haga clic con el botón derecho en el nombre y luego en **Properties** (Propiedades).



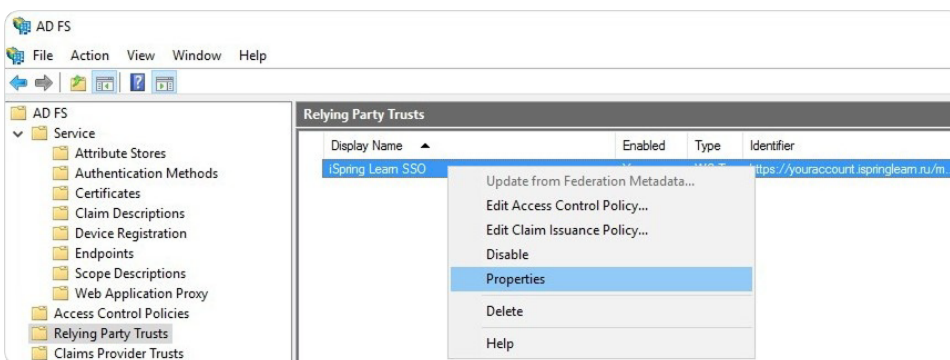
2. Vaya a la pestaña **Advanced** (Avanzado) y seleccione **SHA-256** en el campo **Secure hash algorithm** (Algoritmo de hash seguro).

3. Haga clic en .

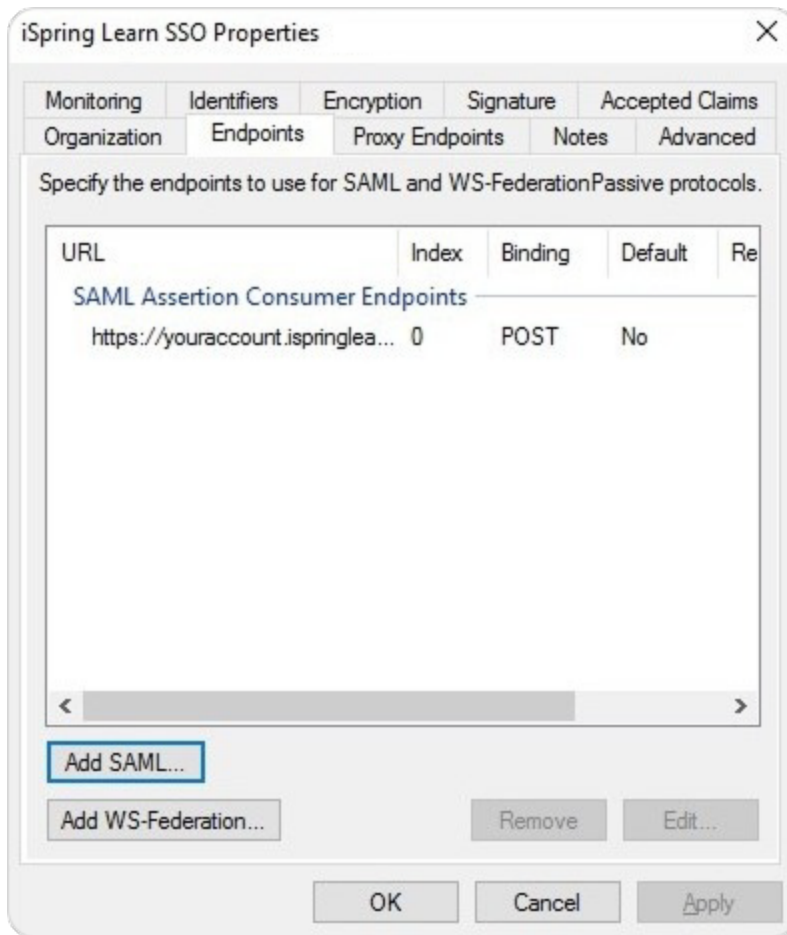


## Paso 6. Punto final Ajustes

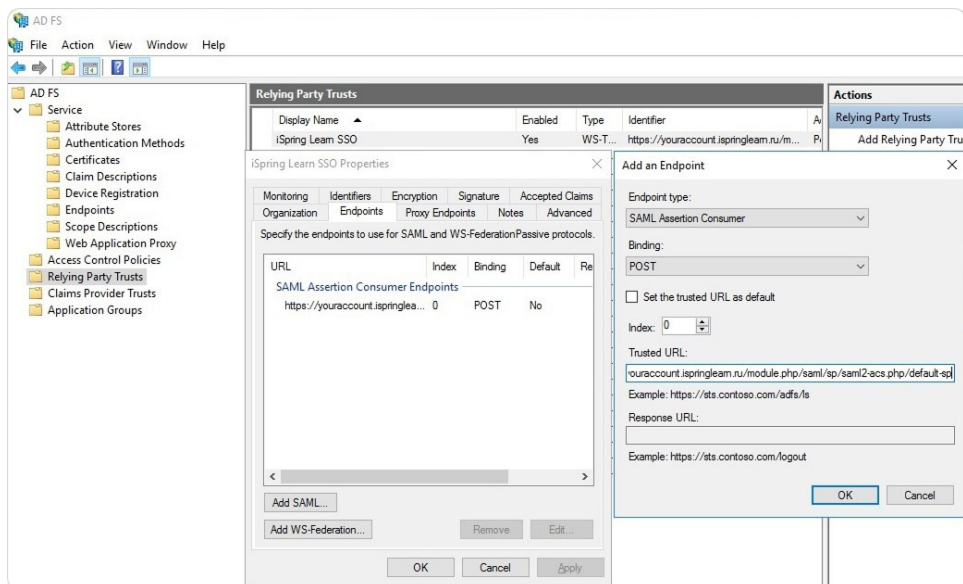
1. Abra el panel de control de AD FS. En la sección **Relying Party Trusts** (Partes confiables), haga clic con el botón derecho en el nombre y luego en **Properties** (Propiedades).



2. En la pestaña **Endpoints** (Extremo), verifica el punto predeterminado:
  - Para el tipo de **Extremo** (Endpoints), seleccione **SAML Assertion Consumer**.
  - Para el tipo **Index** (Índice), seleccione **0**.
  - Para el tipo **Binding** (Enlace), seleccione **POST**.



- En el campo **Trusted URL** (URL confiable), introduzca una dirección como <https://youraccount.ispring.com/module.php/saml/sp/saml2-acs.php/default-sp>. Deje en blanco el campo **Response URL** (URL de respuesta) y haga clic en **OK**.

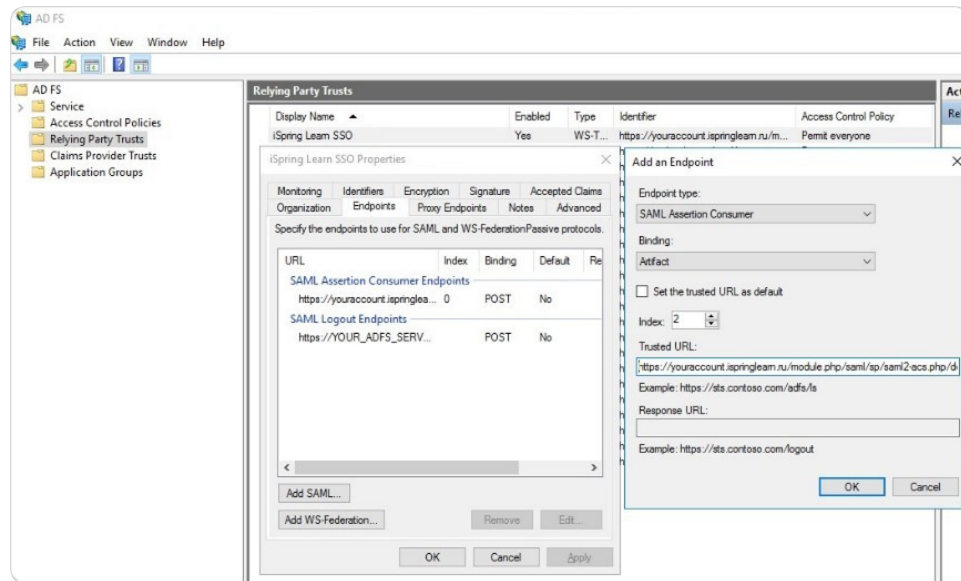


3. Luego añade 2 puntos de cierre de sesión.

a. Para añadir un punto:

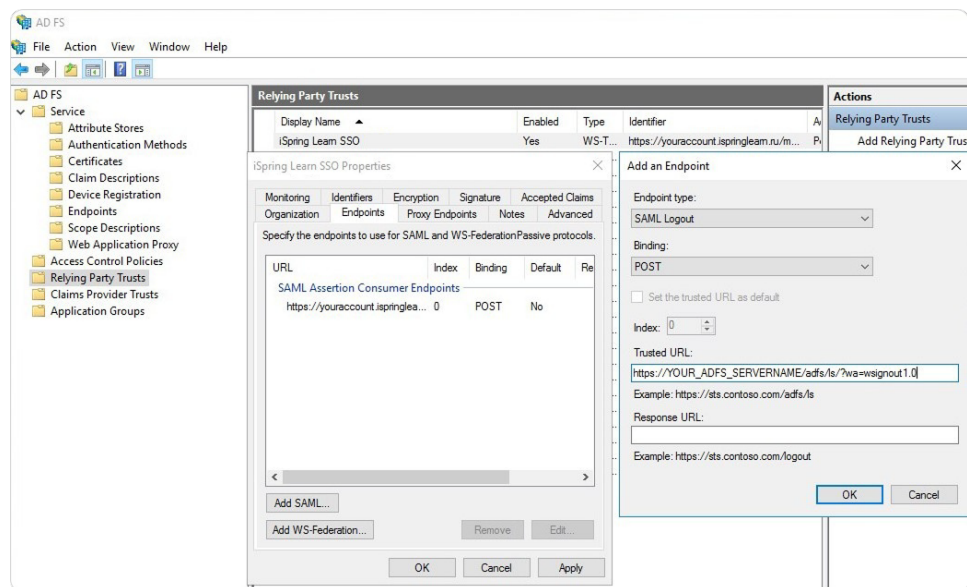
- Haga clic en **Add SAML** (Añadir SAML).
- Para el parámetro de tipo de **Endpoint** (Extremo), seleccione **SAML Assertion Consumer**.
- Para **Binding** (Enlace), seleccione **Artifact**.
- Para **Index** (Índice), seleccione 2.

- v. En el campo **Trusted URL** (URL confiable), introduzca una dirección como <https://youraccount.ispring.com/module.php/saml/sp/saml2-acss.php/default-sp>.
- vi. Deje en blanco el campo **Response URL** (URL de respuesta) y haga clic en **OK**.



b. Añada un nuevo punto. Para hacer esto:

- i. Haga clic en **Add SAML** (Añadir SAML).
- ii. Para tipo de **Endpoint (Extremo)**, seleccione **SAML Logout**.
- iii. Para **Binding (Enlace)**, seleccione **POST**.
- iv. En el campo **Trusted URL** (URL confiable), introduzca una dirección como [https://YOUR\\_ADFS\\_SERVERNAME/adfs/ls/?wa=wsignout1.0](https://YOUR_ADFS_SERVERNAME/adfs/ls/?wa=wsignout1.0).
- v. Deje en blanco el **Response URL** (URL de respuesta) y haga clic en **OK**.



4. Asegúrese de que se hayan añadido los tres puntos finales. Haga clic en **Apply** (Aplicar) y luego en **OK** para confirmar.

The screenshot shows the 'iSpring Learn SSO Properties' dialog box with the 'Endpoints' tab selected. The dialog has a title bar with a close button. Below the title bar are two rows of tabs: 'Monitoring', 'Identifiers', 'Encryption', 'Signature', 'Accepted Claims' in the first row, and 'Organization', 'Endpoints', 'Proxy Endpoints', 'Notes', 'Advanced' in the second row. The 'Endpoints' tab is active, displaying the text 'Specify the endpoints to use for SAML and WS-FederationPassive protocols.' Below this is a table with columns: 'URL', 'Index', 'Binding', 'Default', and 'Re'. The table is divided into two sections: 'SAML Assertion Consumer Endpoints' and 'SAML Logout Endpoints'. The 'Add SAML...' button is highlighted with a blue border. At the bottom of the dialog are 'OK', 'Cancel', and 'Apply' buttons.

| URL                                      | Index | Binding  | Default | Re |
|------------------------------------------|-------|----------|---------|----|
| <b>SAML Assertion Consumer Endpoints</b> |       |          |         |    |
| https://youraccount.ispringlea...        | 0     | POST     | No      |    |
| https://youraccount.ispringlea...        | 2     | Artifact | No      |    |
| <b>SAML Logout Endpoints</b>             |       |          |         |    |
| https://YOUR_ADFS_SERV...                |       | POST     | No      |    |

## Paso 7. Verificar inicio de sesión único (SSO)

1. Vaya a su cuenta de iSpring Cloud <https://youraccount.ispring.com/>.
2. Haga clic en **Iniciar sesión con su cuenta corporativa**.

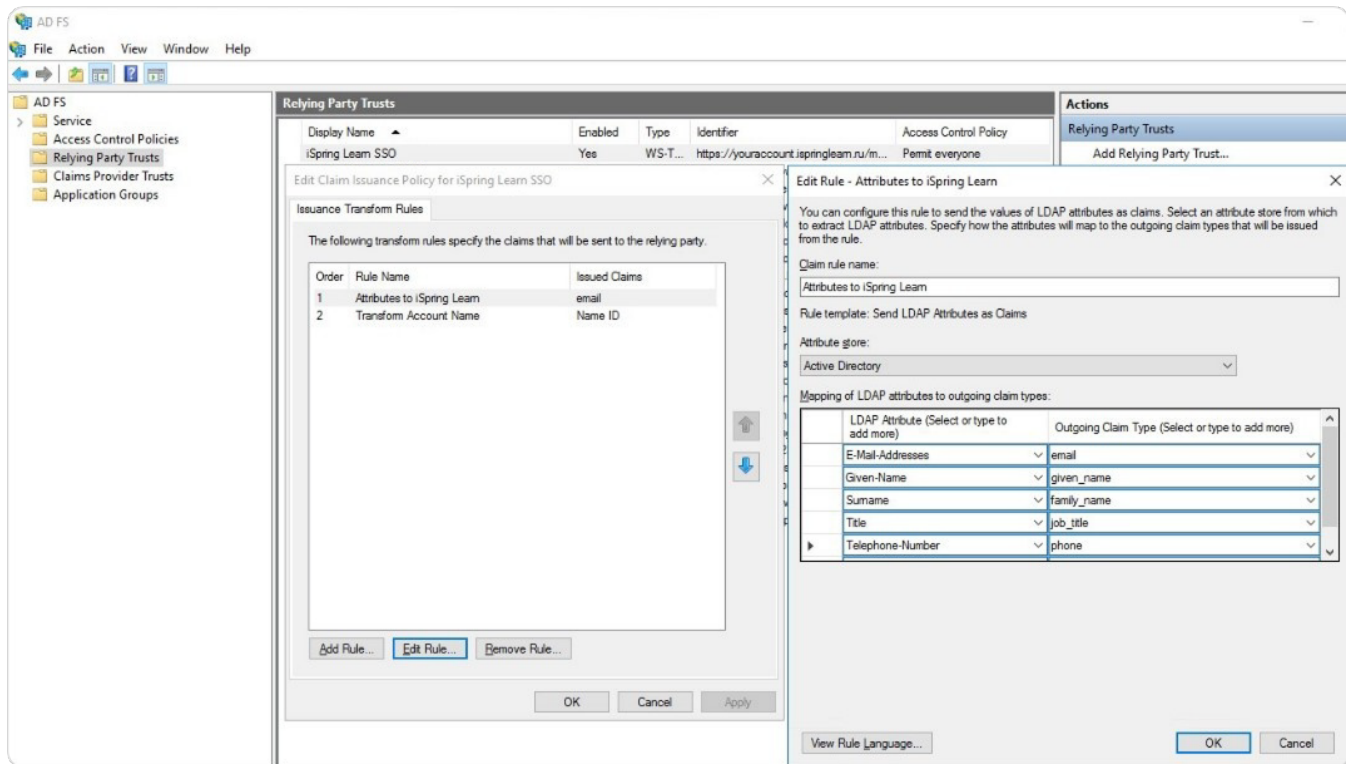
Se abrirá la cuenta personal del usuario.

Si se produce un error durante la configuración, envíe una captura de pantalla del error a [support@ispring.es](mailto:support@ispring.es).

## Correlación de campos de iSpring Cloud y SSO

Además de las reglas, también puede especificar campos de **correlación** de iSpring Cloud y atributos SSO: Nombre, Apellido, Puesto, Teléfono, etc. Saber más sobre la [correlación de campos de iSpring Cloud y SSO](#).

En el lado de AD FS:



En el lado de iSpring Cloud:

### 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                                   |                   |

## Autorización sin SAML

Si ha habilitado OpenID en su cuenta de iSpring Cloud pero por alguna razón no puede iniciar sesión mediante inicio de sesión único, escriba la siguiente dirección web: [https://yourcompany.ispring.com/login?no\\_sso](https://yourcompany.ispring.com/login?no_sso).

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

Si obtiene un error 400 y un mensaje sobre que la solicitud se ha compuesto incorrectamente ("Cannot retrieve metadata for IdP 'https://myidp.com/oam/fed' because it isn't a valid IdP for this SP") después de haber habilitado SAML en su cuenta de iSpring Cloud, significa que el valor establecido para el **URL del emisor (ID de entidad del IdP)** campo 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 funcione correctamente en su cuenta, copie la URL del texto de error y péguela en el campo **URL del Emisor (ID de Entidad IdP)**.