Cómo configurar SSO con Microsoft AD FS

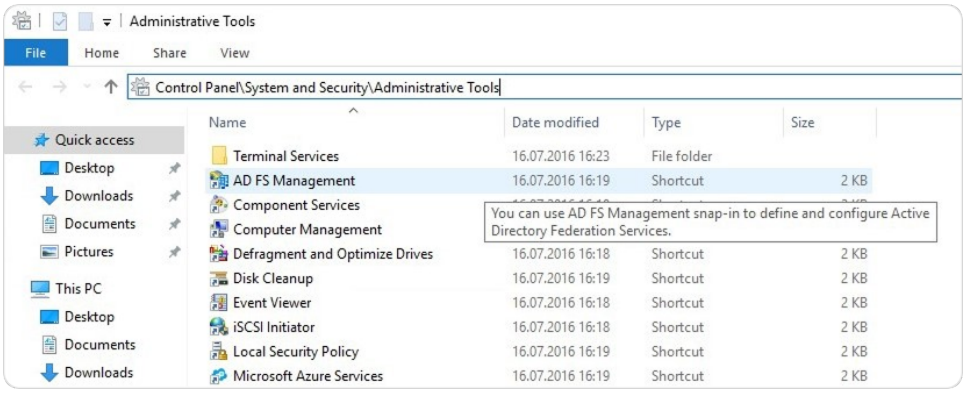
Requisitos del sistema

- 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*

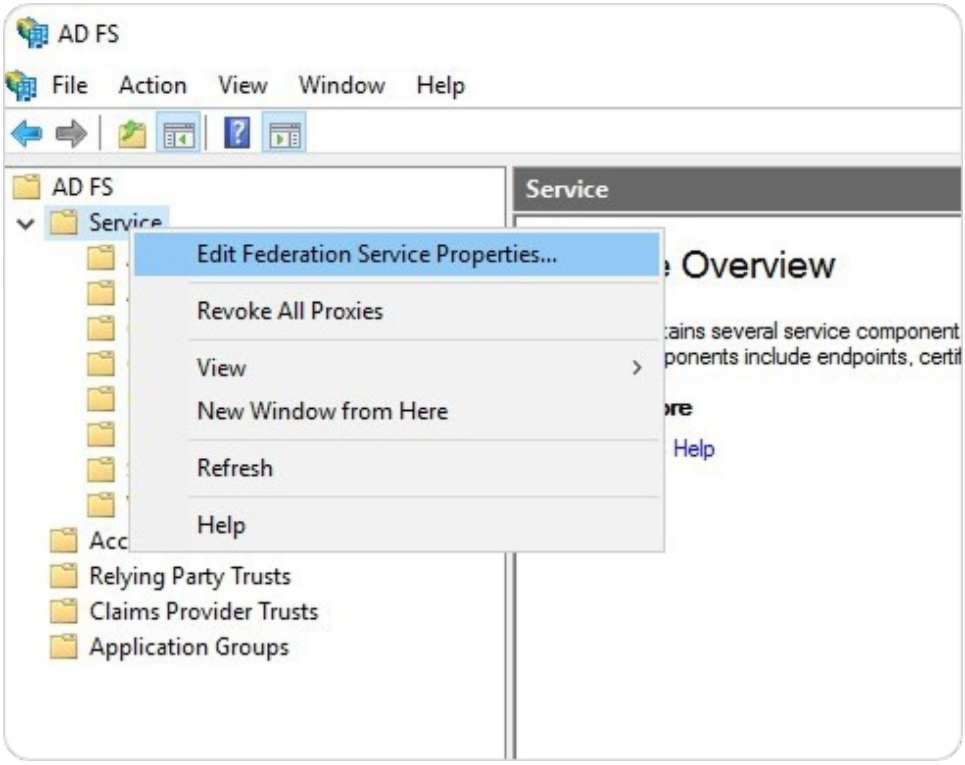
Esta guía cubre la configuración de SSO SAML mediante AD FS 4.0 en Windows Server.

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).

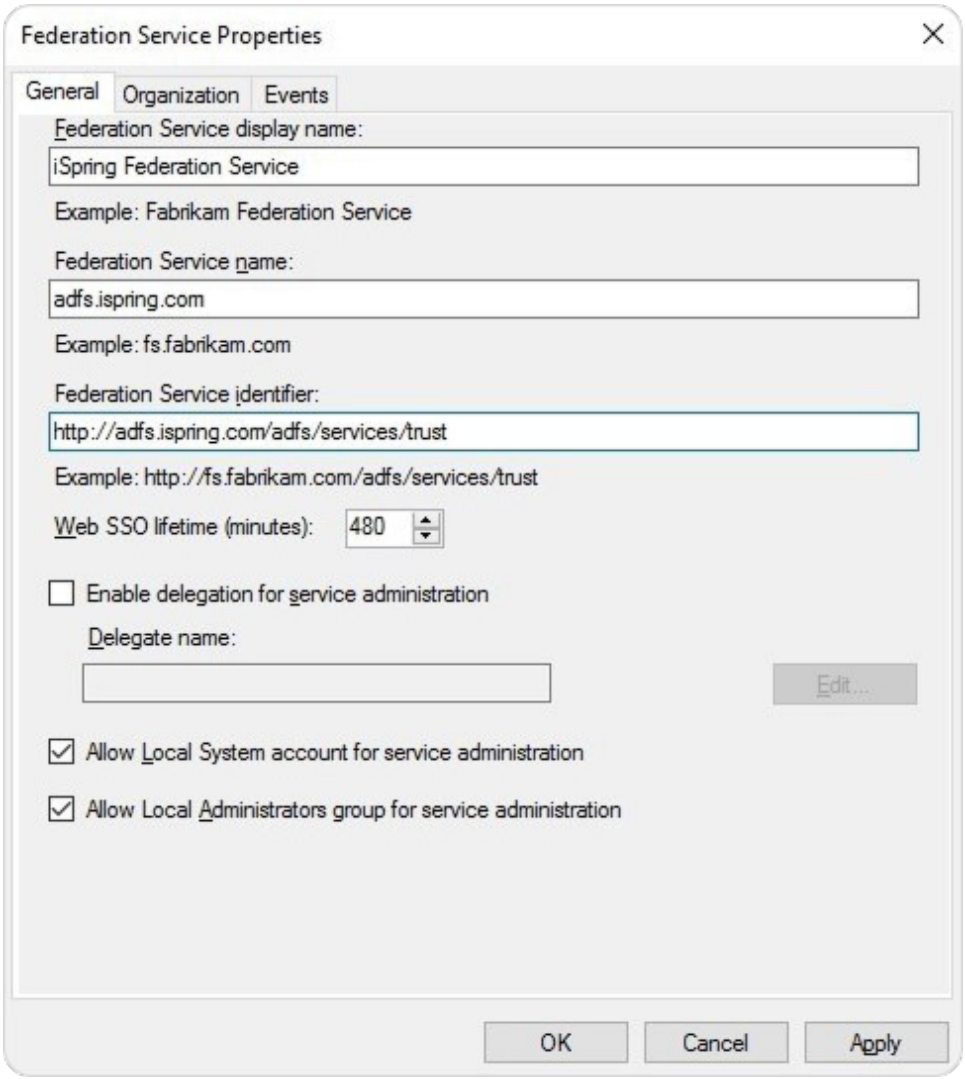


2. Haga clic derecho en **Service** (Servicio) y seleccione **Edit Federation Service Properties** (Editar propiedades del servicio de federación).



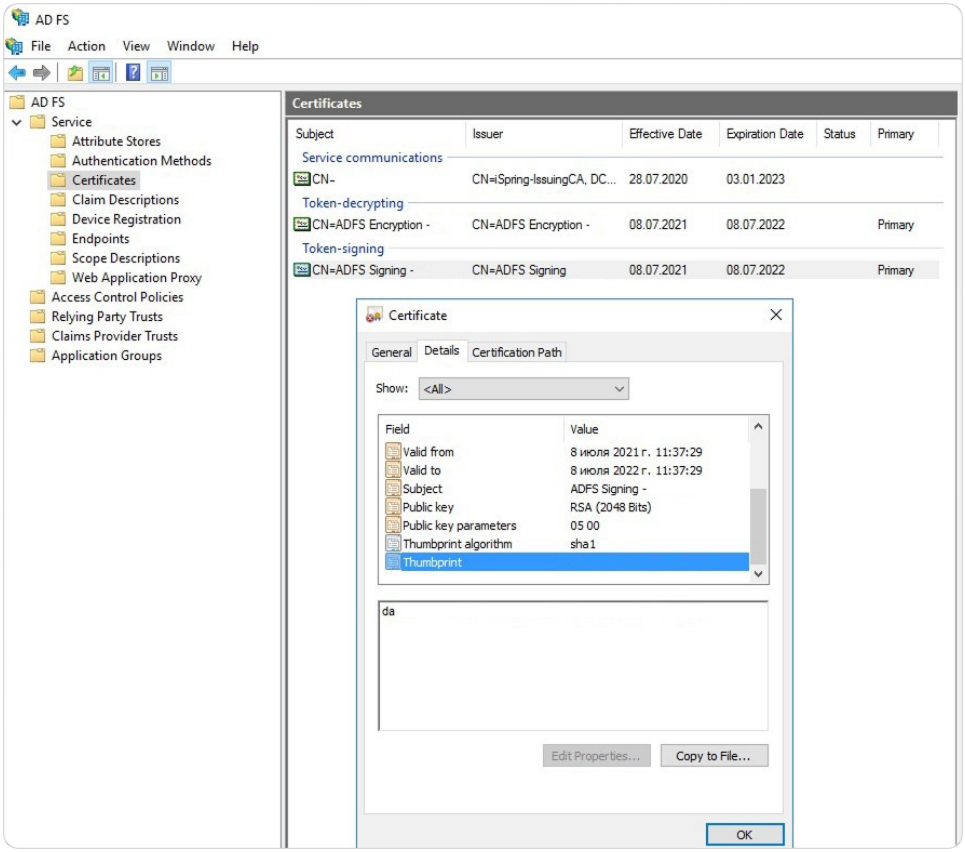
3. Verifique que los ajustes **General** (Generales) coincidan con sus entradas DNS y nombres de certificado. Tome nota del **Federation Service Identifier** (Identificador del servicio de federación), ya que se usa en los ajustes de configuración SAML 2.0 de iSpring Cloud.

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

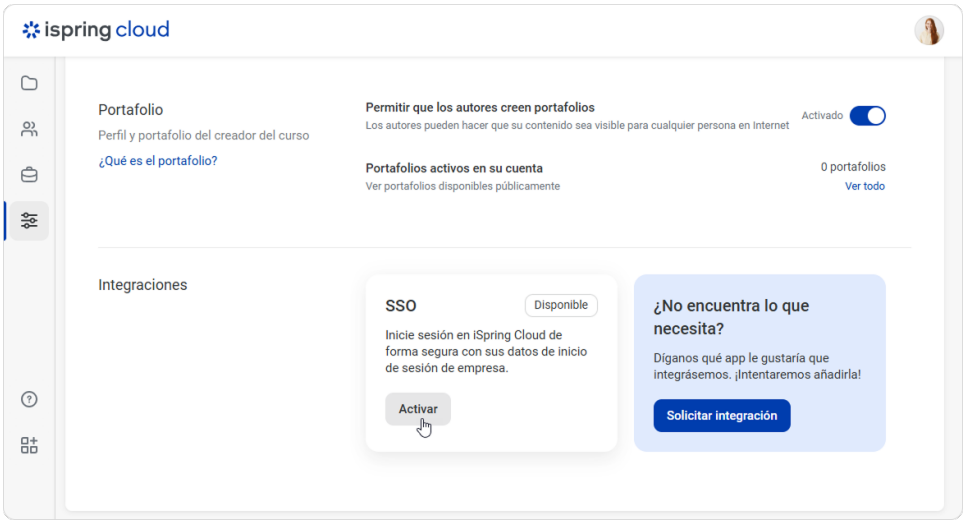


Paso 2. iSpring Cloud Ajustes

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.



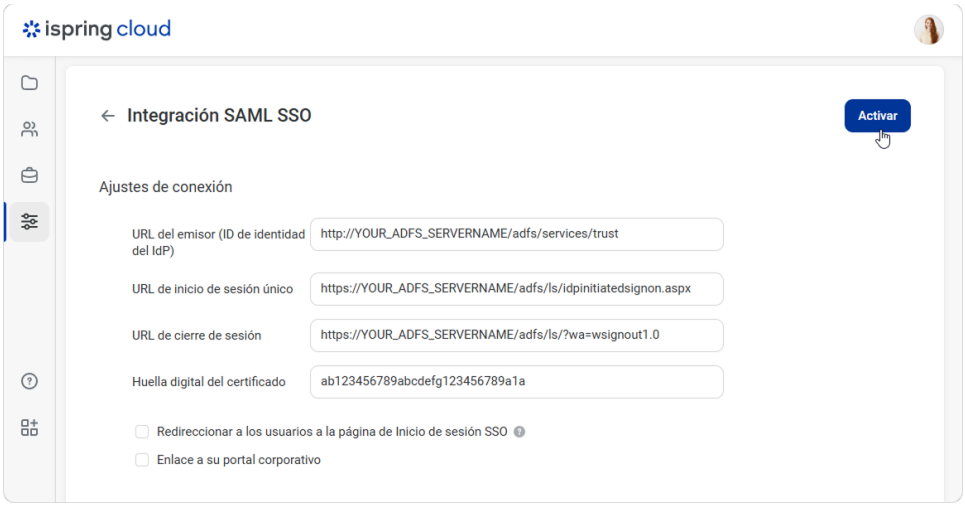
5. Inicie sesión en su cuenta de iSpring Cloud. A continuación, vaya a **Ajustes > Integraciones.** Haga clic en **Activar** en la tarjeta de **SSO.**



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)	http://YOUR_ADFS_SERVERNAME/adfs/services/trust
URL de inicio de sesión único	https://YOUR_ADFS_SERVERNAME/adfs/ls/idpinitiatedsignon.aspx
URL de cierre de sesión	https://YOUR_ADFS_SERVERNAME/adfs/ls/?wa=wsignout1.0

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

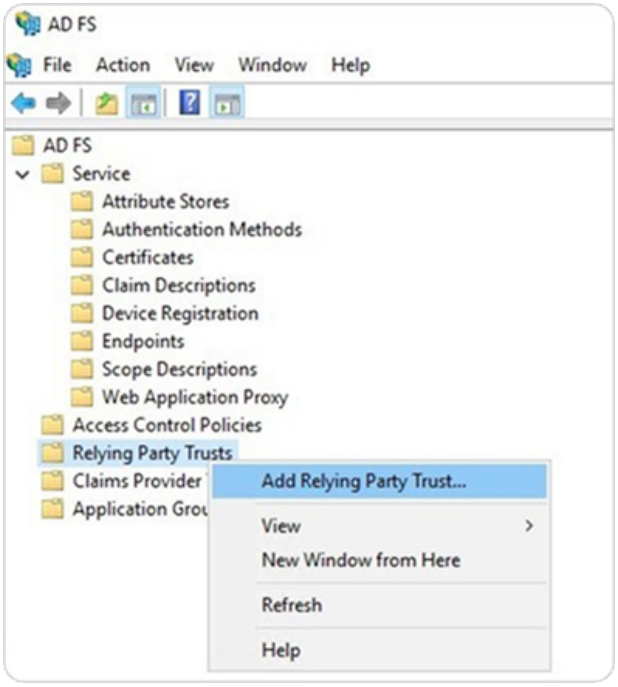


URL del emisor (ID de entidad del IdP)	La URL que identifica de forma única el servicio del proveedor de identidad. Este valor es igual al elemento **E misor** de la solicitud SAML enviada por el proveedor de identidad.
URL de inicio de sesión único	Es la ruta al script del servidor que genera solicitudes de confirmación de identificador SAML para gestionar la autorización.
URL de cierre de sesión	Es la ruta al script del servidor que genera solicitudes de confirmación de identificador SAML para gestionar el cierre de sesión.
Huella digital del certificado	Esta es una versión abreviada del certificado de clave pública 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 aquí.
Redirigir 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.ispring.com/sso/login.

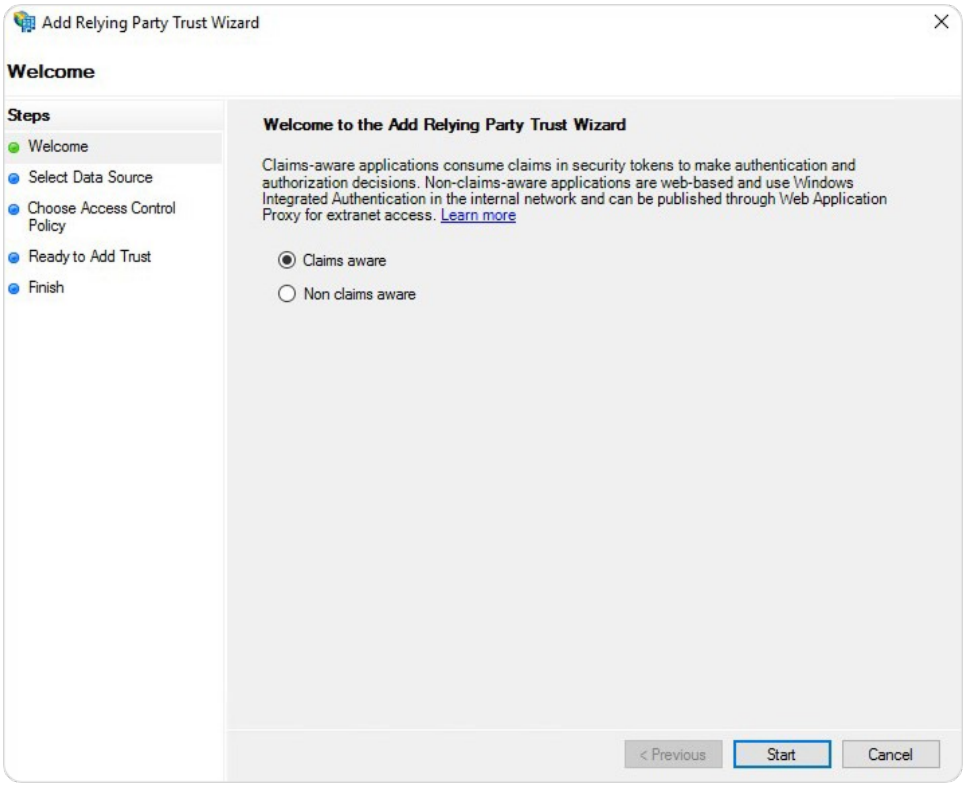
8. Haga clic en **Activar.**

Paso 3. Configuración de la parte confiable de AD FS

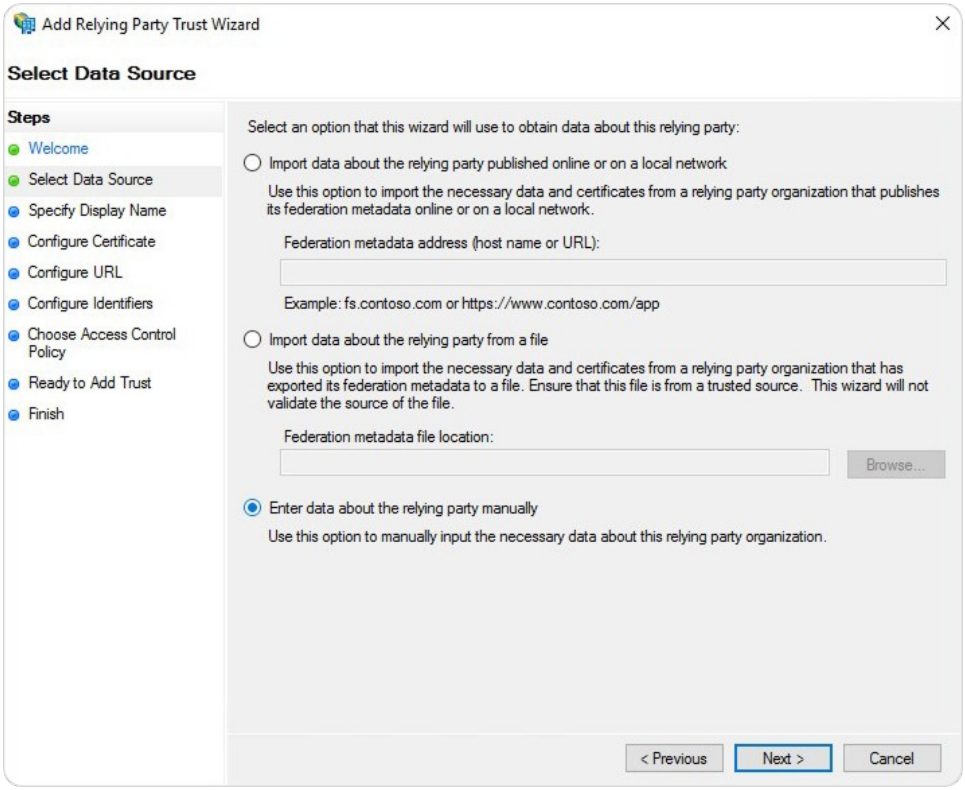
1. Vaya a la consola de administración de AD FS y seleccione **Relying Party Trusts** (Confianzas de partes confiables), haga clic con el botón derecho sobre ella y seleccione **Add Relying Party Trust** (Añadir confianza de parte confiable).



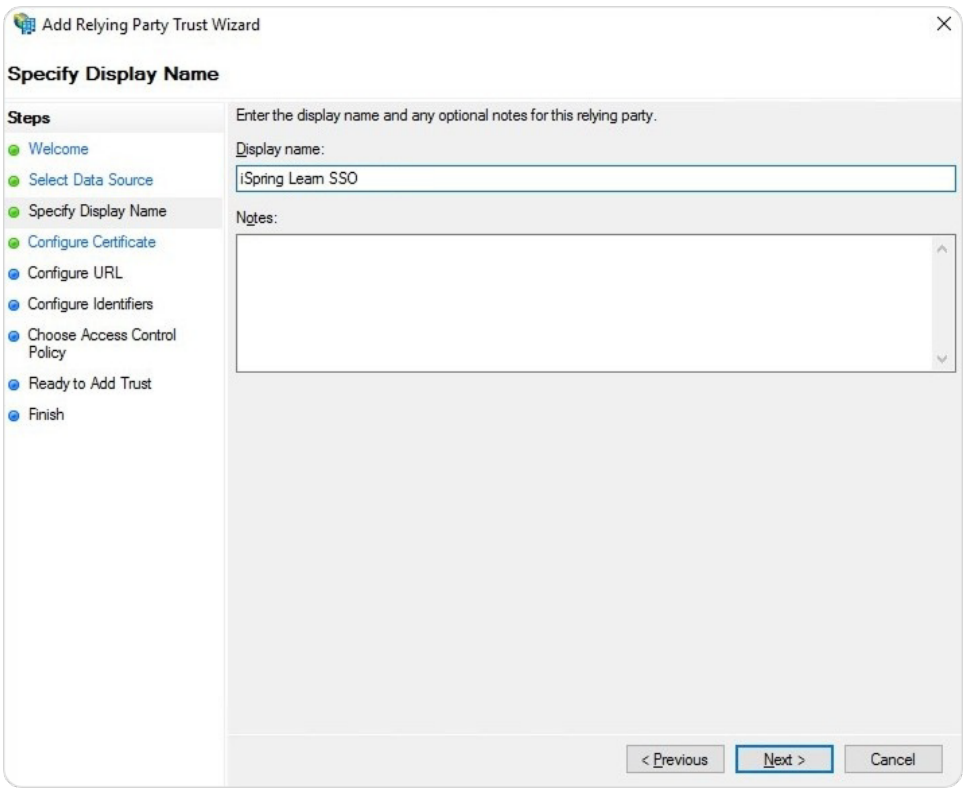
2. Seleccione **Claims aware** (Consciente de las reclamaciones) y haga clic en **Start** (Iniciar).



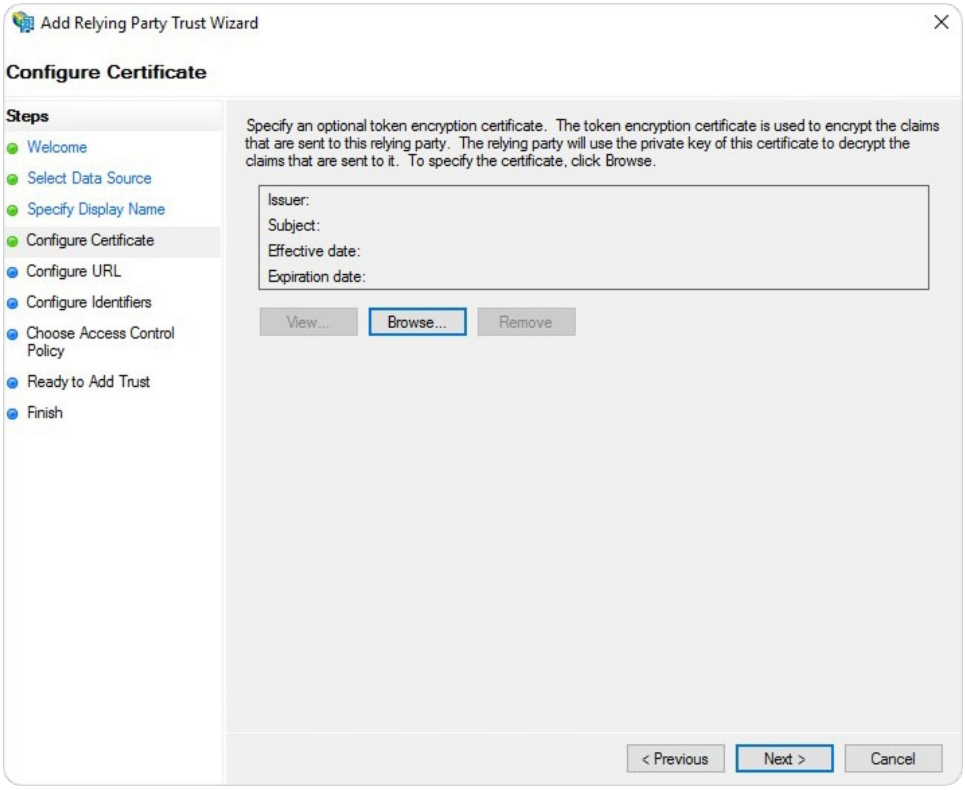
3. En la **Select Data Source** (Seleccionar origen de datos) fase, seleccione la última opción: **Enter data about the relying party manually** (Introducir datos sobre la parte confiable manualmente).



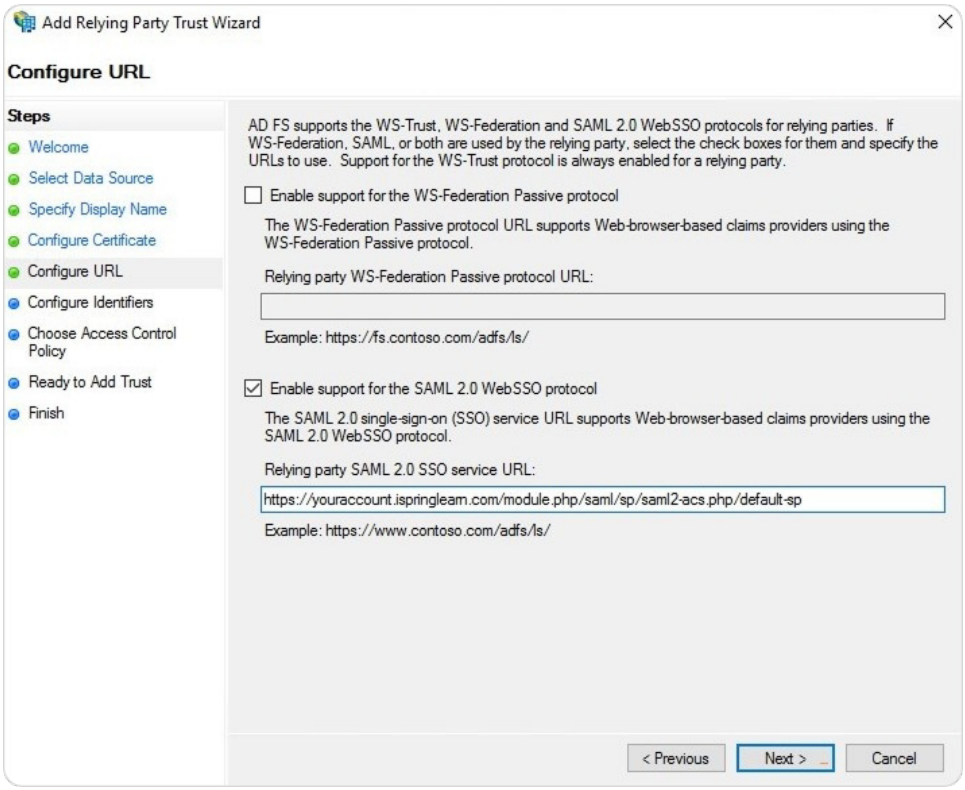
4. En la siguiente pantalla, introduzca un **Display name** (Nombre para mostrar) que pueda reconocer en el futuro. Haga clic en **Next** (Siguiente).



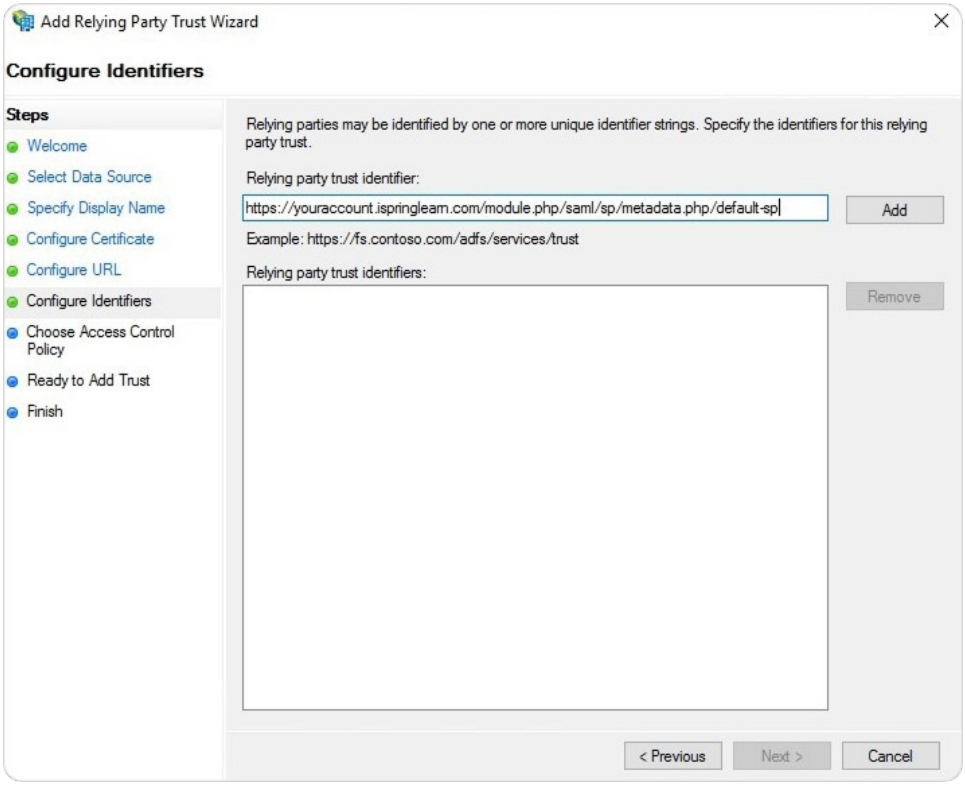
5. En la etapa **Configure Certificate** (Configurar certificado), deje los valores Predeterminadas. Haga clic en **Next** (Siguiente).



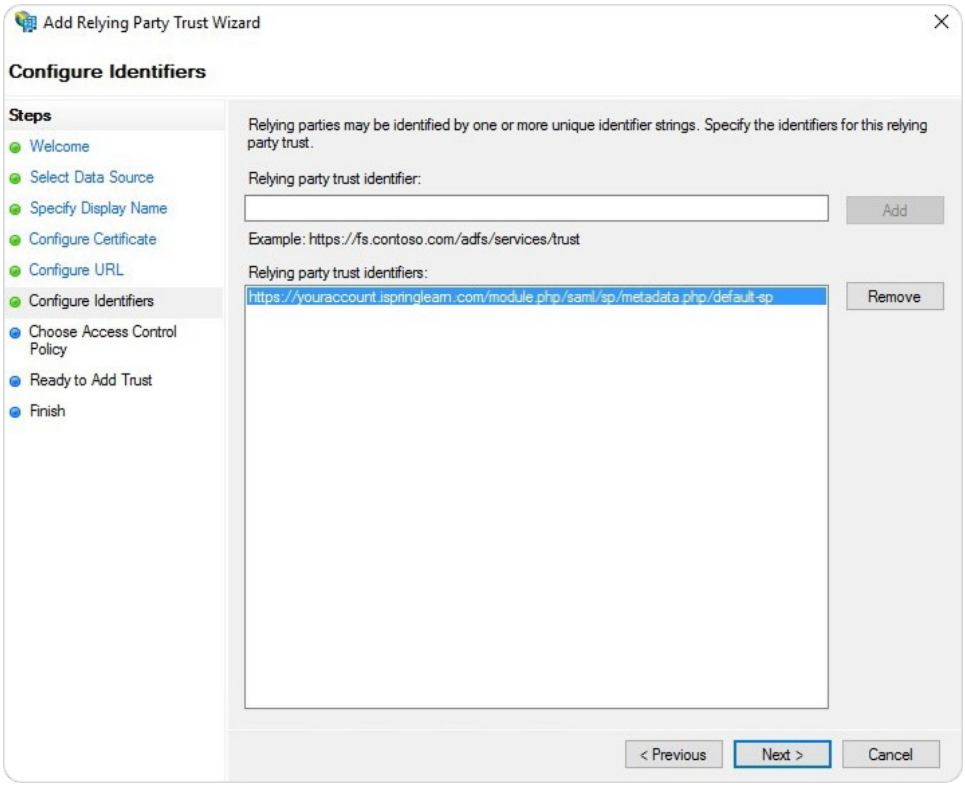
6. En la siguiente pantalla, marque la casilla **Enable support for the SAML 2.0 WebSSO protocol** (Habilitar soporte para el protocolo WebSSO SAML 2.0). La URL del servicio será: https://youraccount.ispring.com/module.php/saml/sp/saml2-acs.php/default-sp.



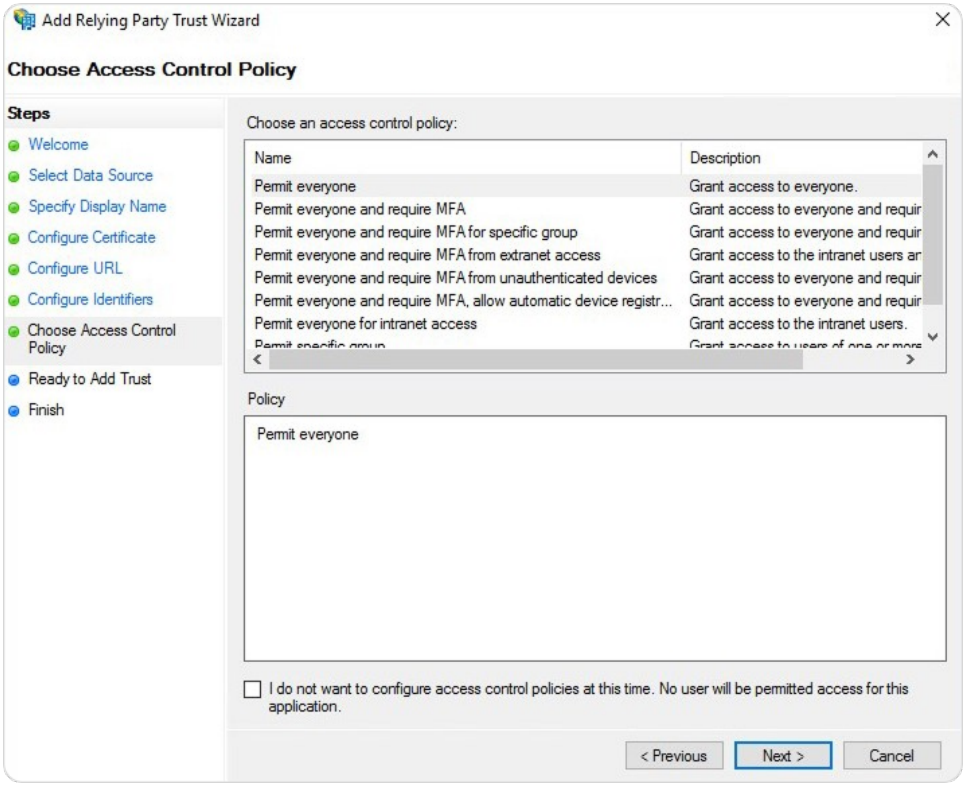
7. En la etapa **Configure Identifiers** (Configurar identificadores), añada el **Relying party trust identifier** (Identificador de confianza de parte confiable) como https://youraccount.ispring.com/module.php/saml/sp/metadata.php/default-sp. Haga clic en **Add** (Añadir).



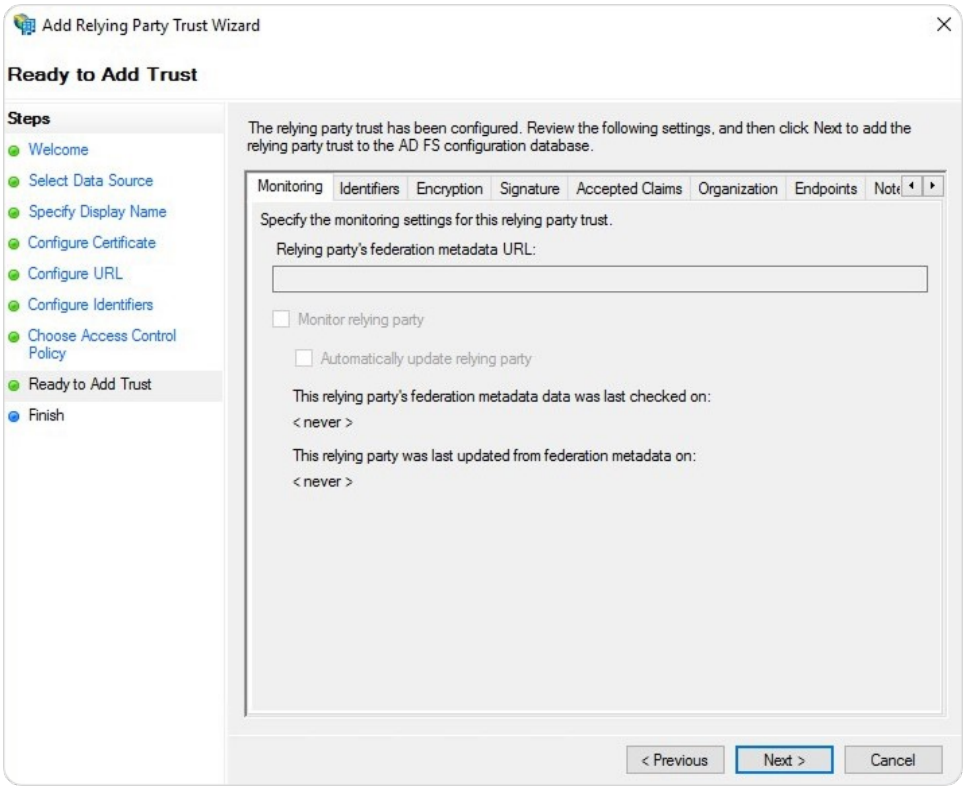
8. Luego, haga clic en **Next** (Siguiente).



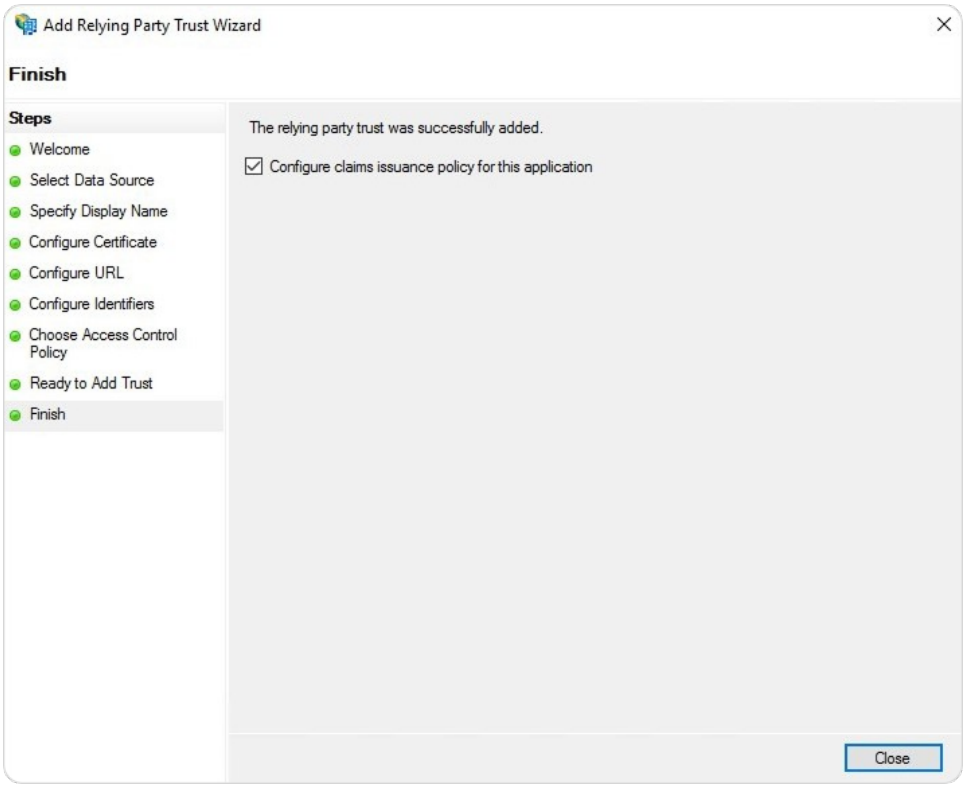
9. En el siguiente paso, elija **Permit everyone** (Permitir a todos). Haga clic en **Next** (Siguiente).



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

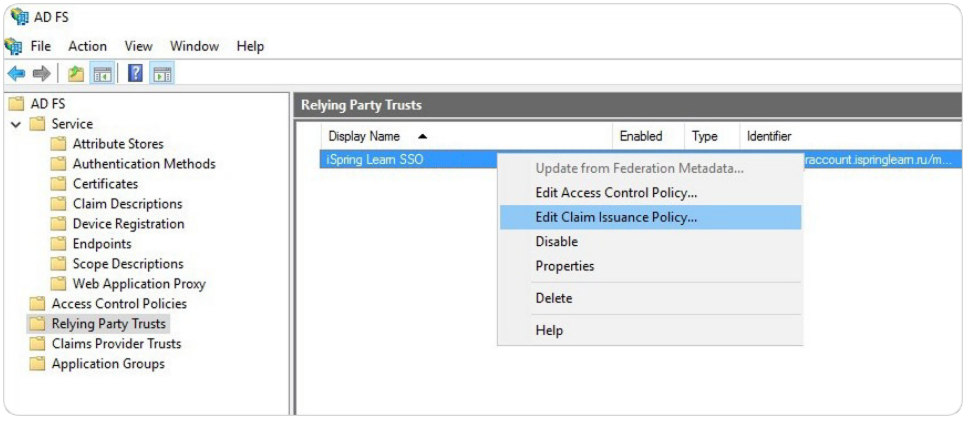


11. En el último paso, marque la casilla **Configure claims issuance policy for this application** (Configurar la directiva de emisión de reclamaciones para esta aplicación). Luego, haga clic en **Close** (Cerrar).

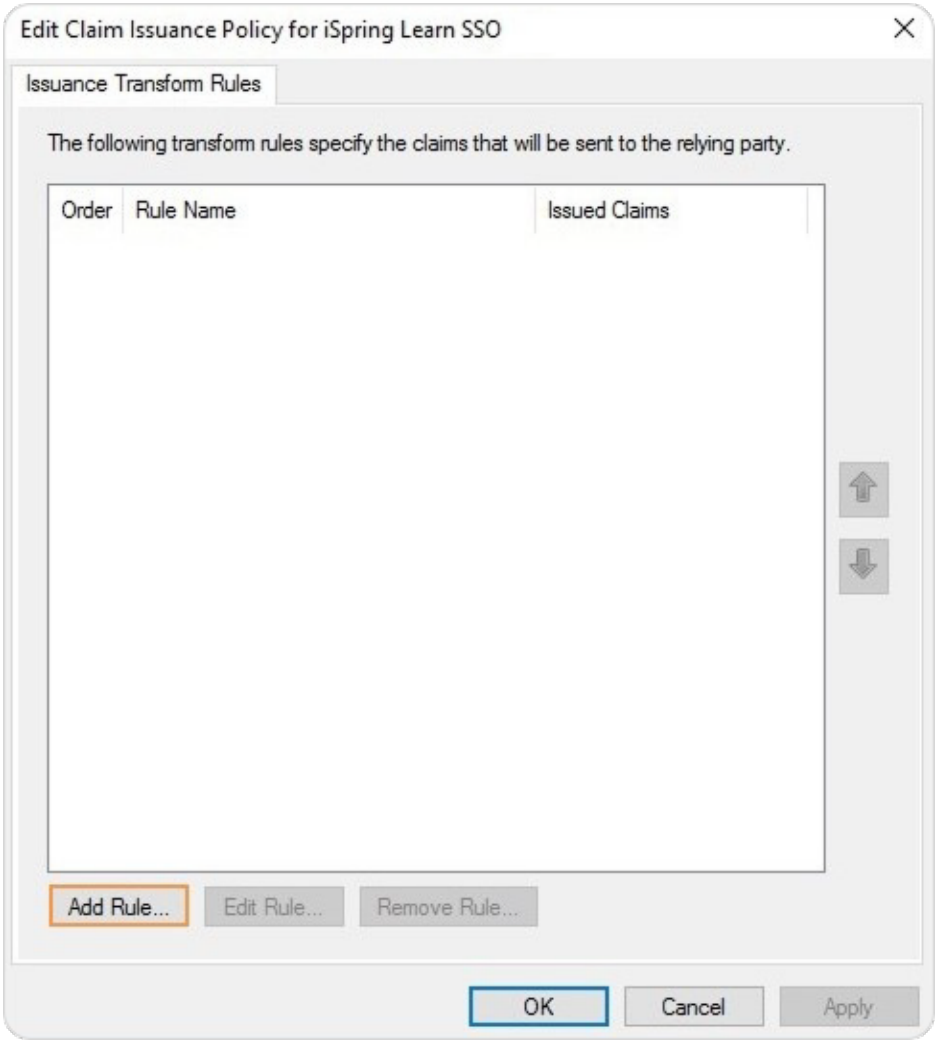


Paso 4. Creando reglas de reclamaciones

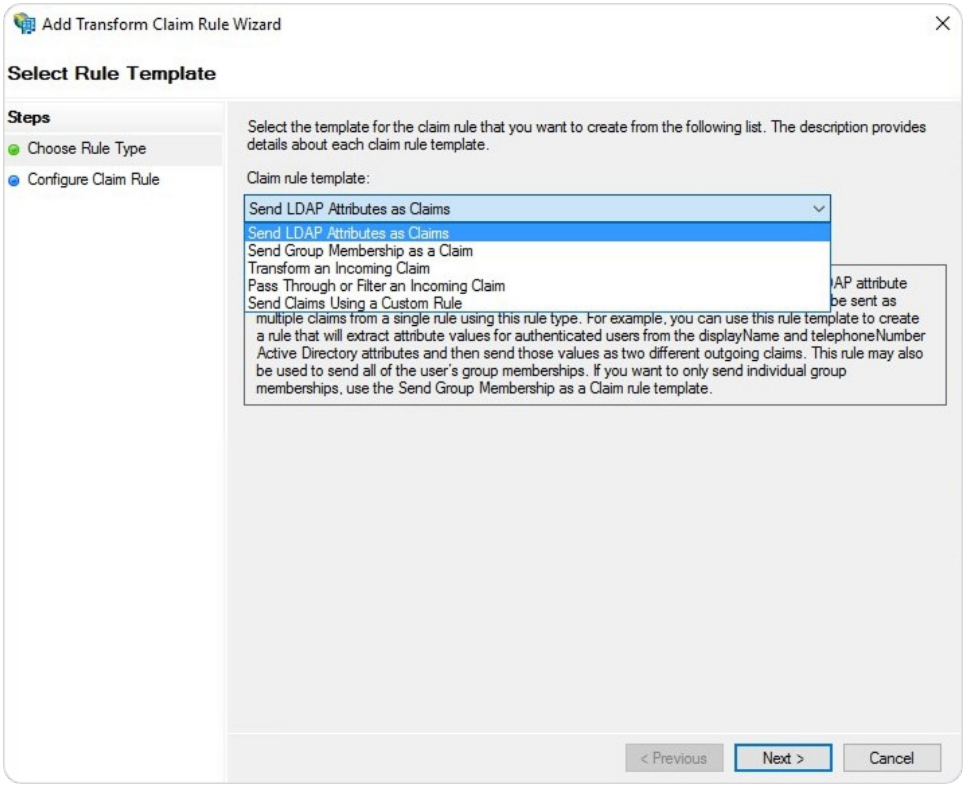
1. Abra el panel de control de AD FS. En la sección de **Relying Party Trusts** (Confianzas de la Parte Dependiente), haga clic derecho en el nombre y haga clic en **Edit Claim Issuance Policy** (Editar Política de Emisión de Reclamaciones).



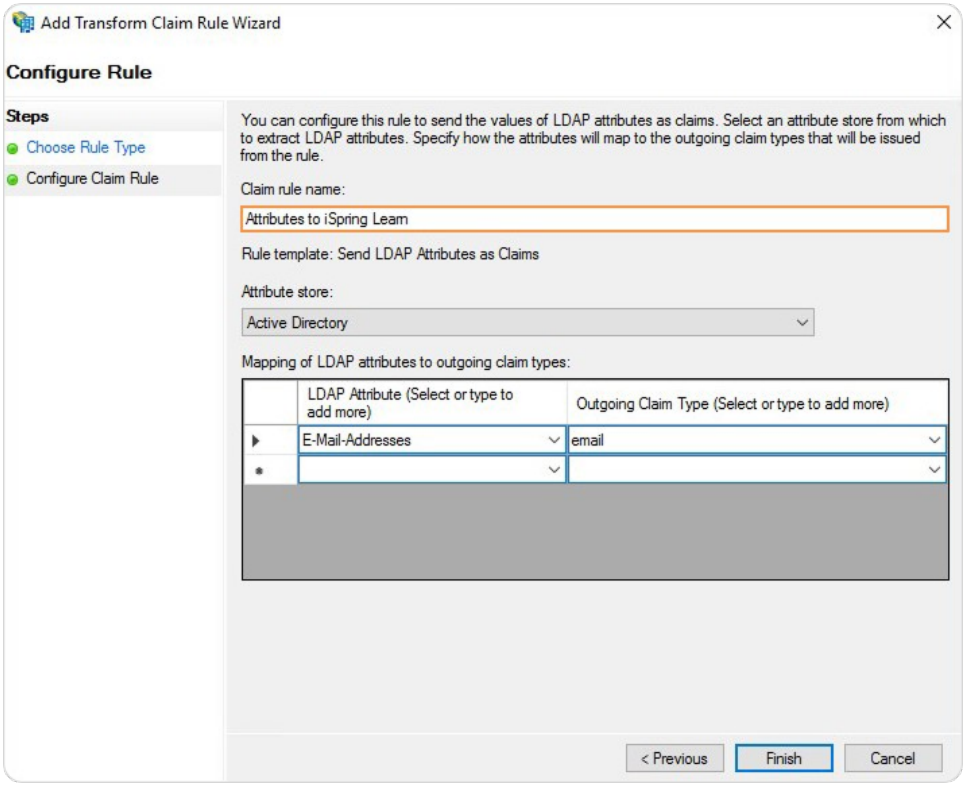
2. Añada la primera regla. Para hacer esto, haga clic en **Add Rule...** (Añadir regla...).



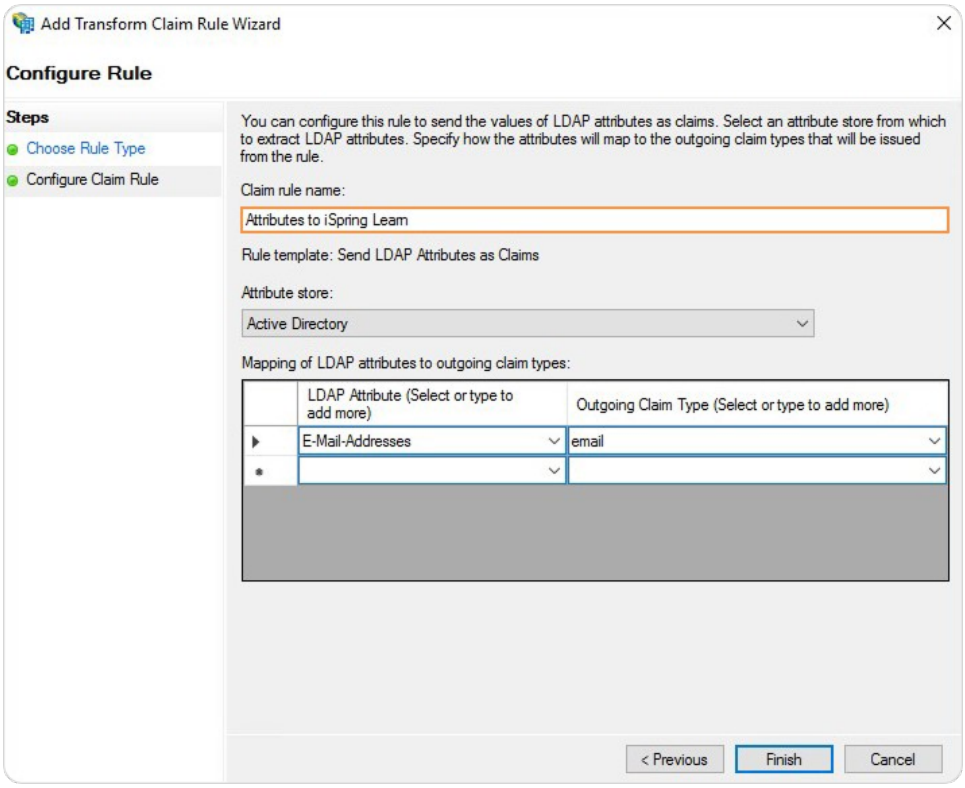
3. Seleccione **Send LDAP Attributes as Claims** (Enviar atributos LDAP como reclamaciones). Haga clic en **Next** (Siguiente).



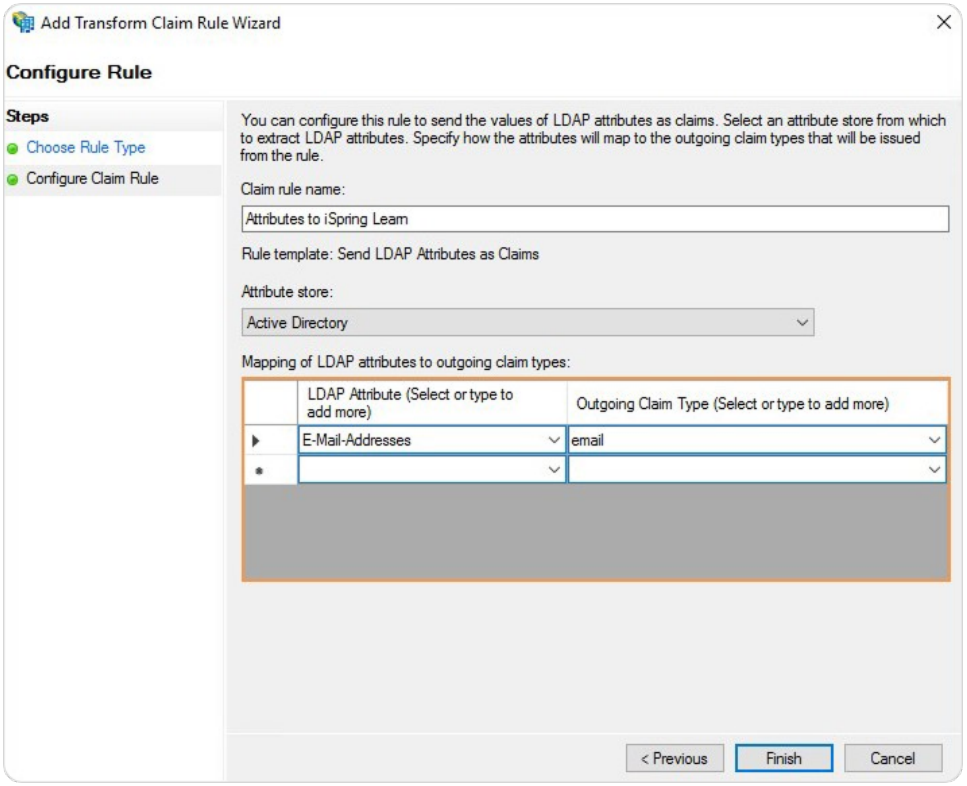
4. En el paso **Configure Claim Rule** (Configurar regla de reclamación), en el campo Nombre de la regla de reclamación, introduzca un nombre para la regla, por ejemplo, **Attributes of iSpring Cloud** (Atributos de iSpring Cloud).



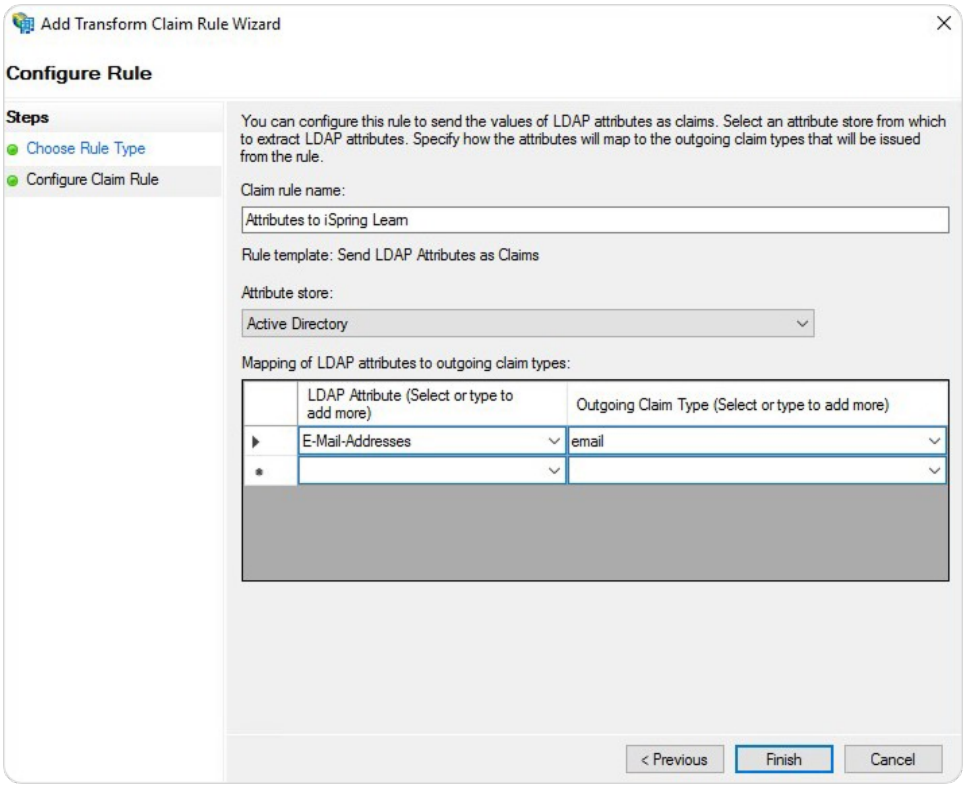
5. Elija **Active Directory** como su almacén de atributos.



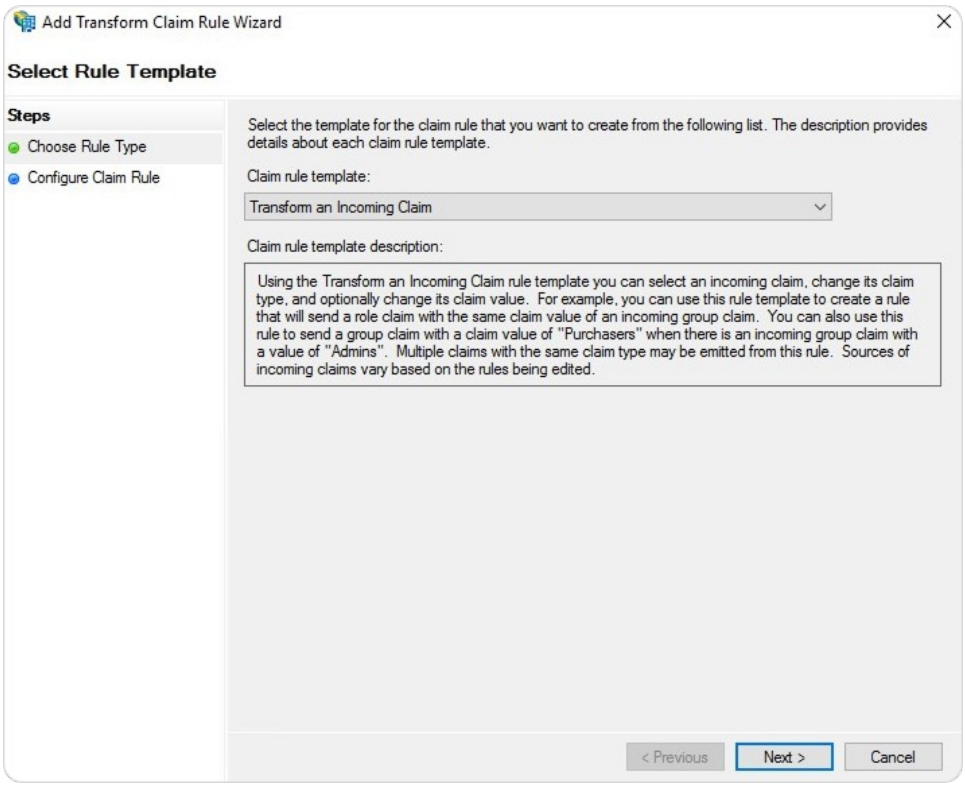
6. A continuación, seleccione estos valores:
   - En la columna **LDAP Attribute** (Atributo LDAP), establezca E-Mail-Addresses.
   - En la columna **Outgoing Claim Type** (Tipo de reclamación saliente), establezca el valor de correo electrónico, como en iSpring Cloud https://youraccount.ispring.com/settings/sso.



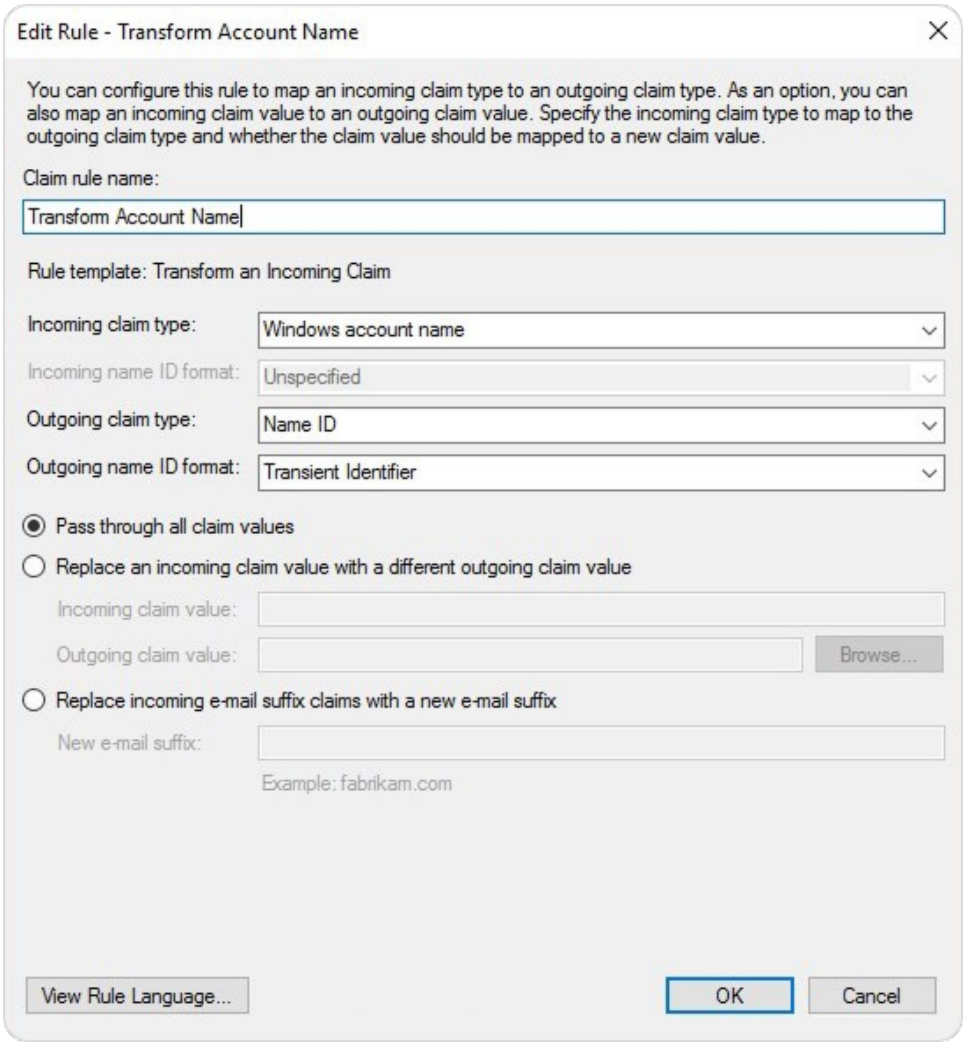
7. Haga clic en **Finish** (Finalizar) para guardar la nueva regla.



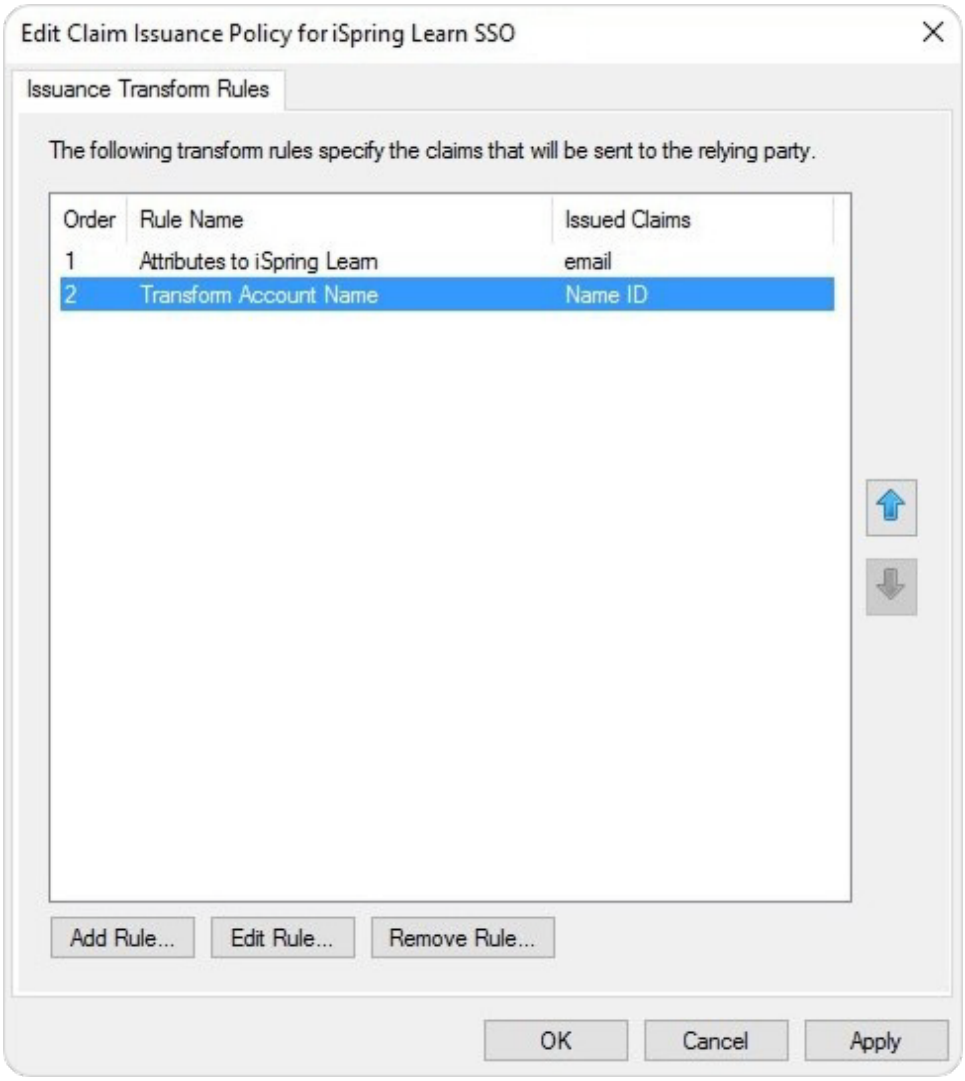
8. Luego, añada la segunda regla y seleccione **Transform an Incoming Claim** (Transformar una reclamación entrante) como plantilla.



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

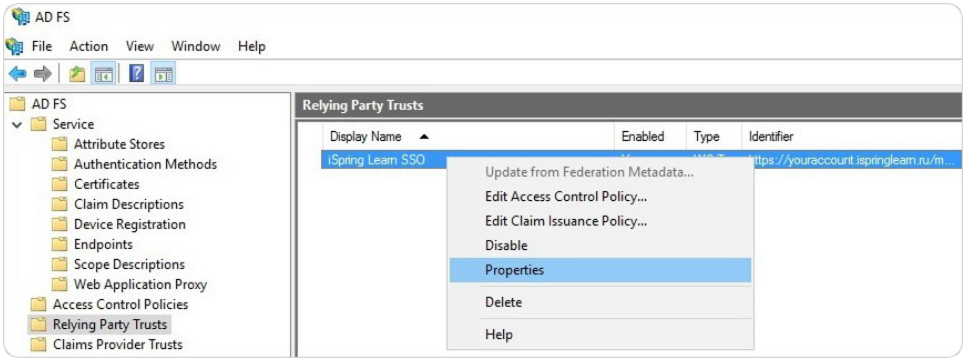
10. Haga clic en **Apply** (Aplicar) y luego en **OK** para confirmar.



Paso 5. Ajustando los Ajustes de Confianza

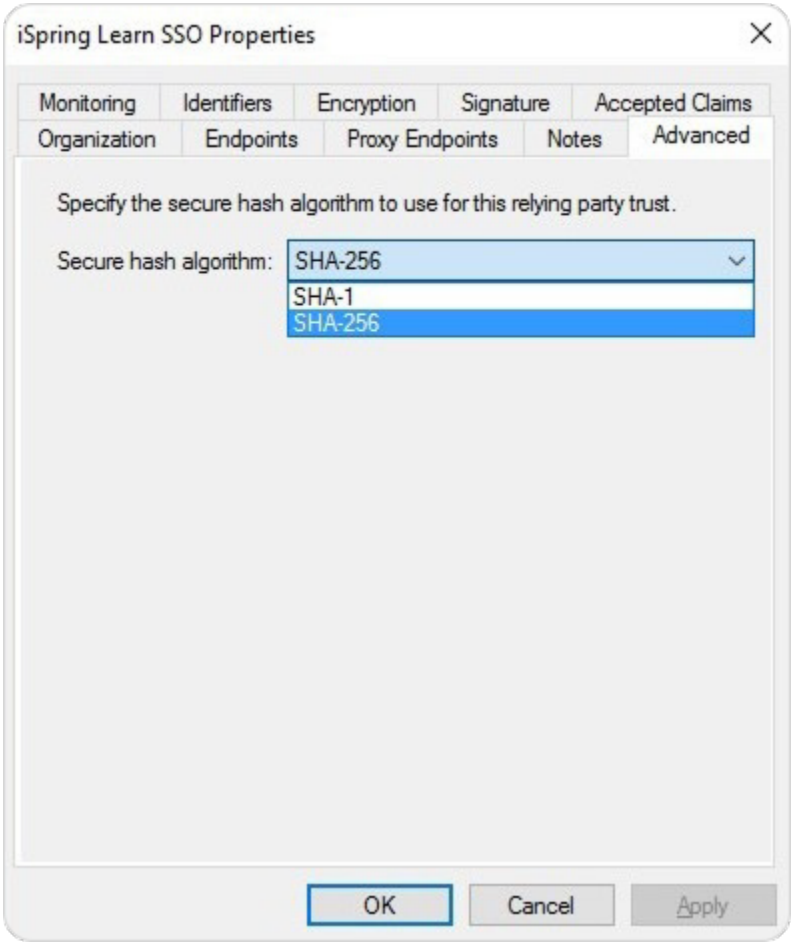
Asegúrese de que el **Secure hash algorithm** (Algoritmo de hash seguro) esté configurado en **SHA-256** en los ajustes de seguridad. Para hacer esto:

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).



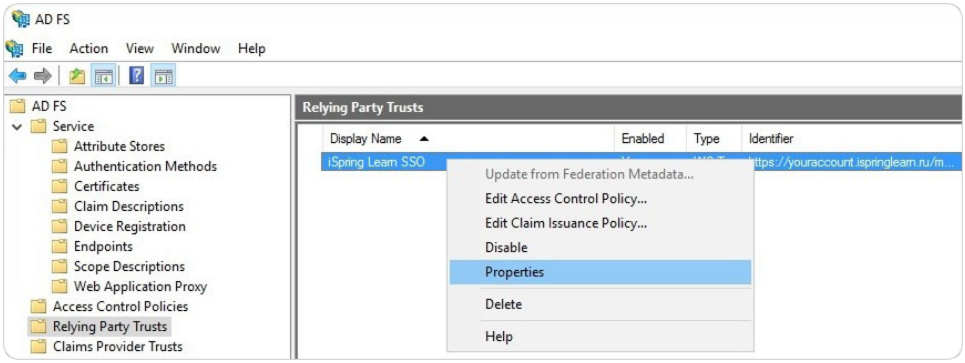
2. Vaya a la pestaña **Advanced** (Avanzado) y seleccione **SHA-256** en el campo **Secure hash algorithm** (Algoritmo de hash seguro).

3. Haga clic en .



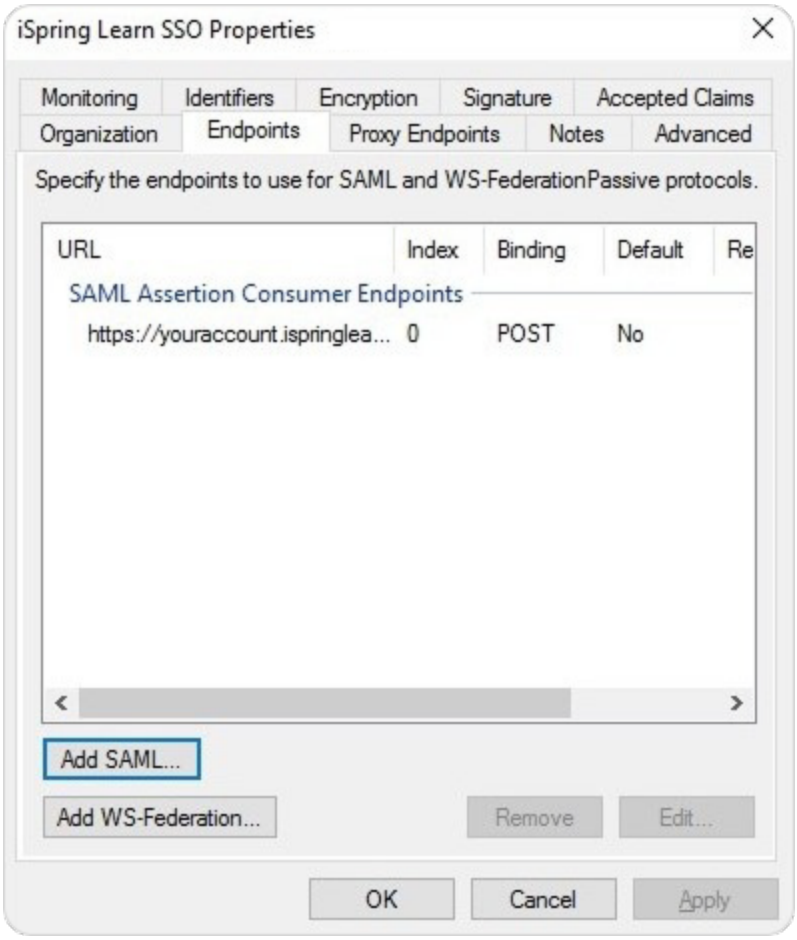
Paso 6. Punto final Ajustes

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).

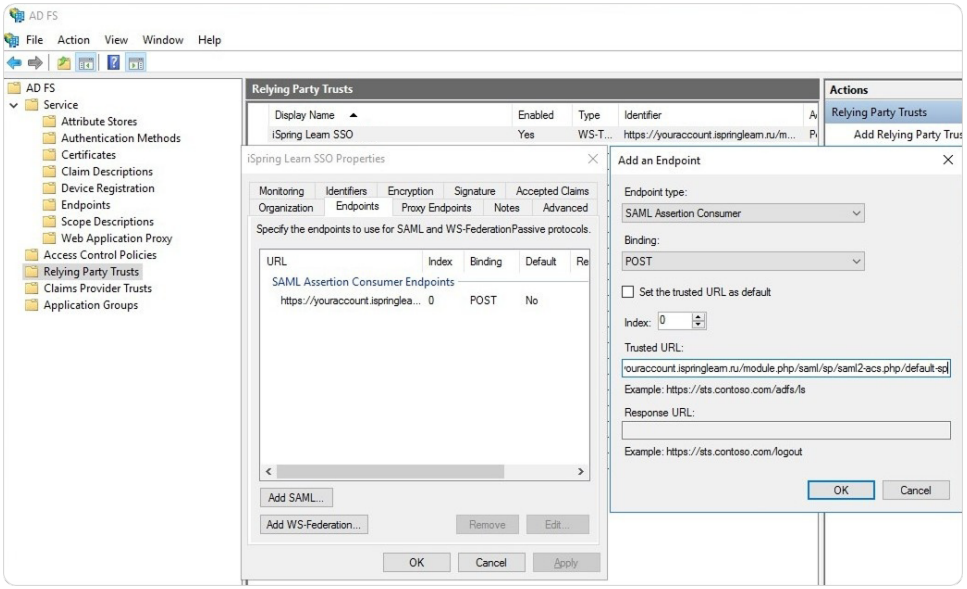


2. En la pestaña **Endpoints** (Extremo), verifica el punto predeterminado:

    - 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**.

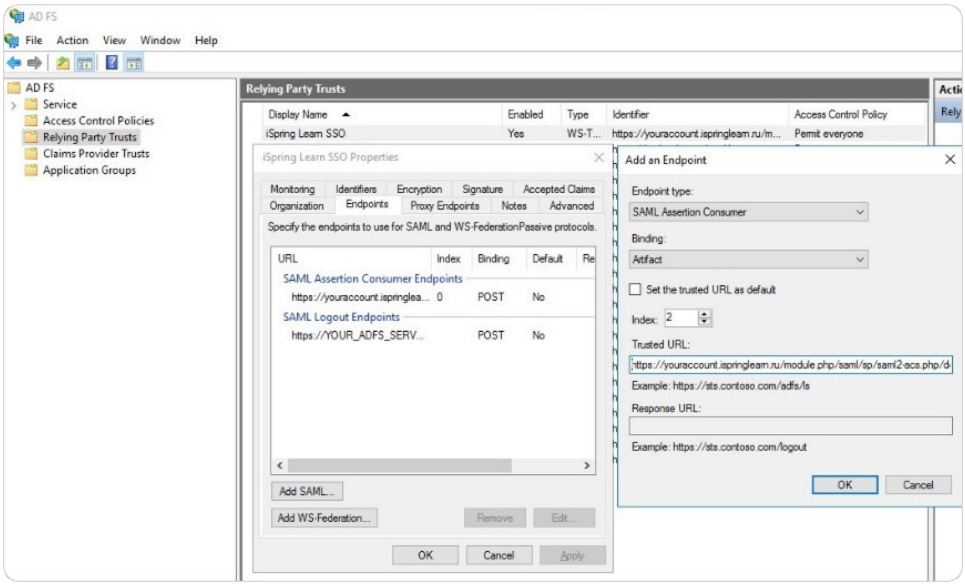


3. Luego añada 2 puntos de cierre de sesión.

    a. Para añadir un punto:

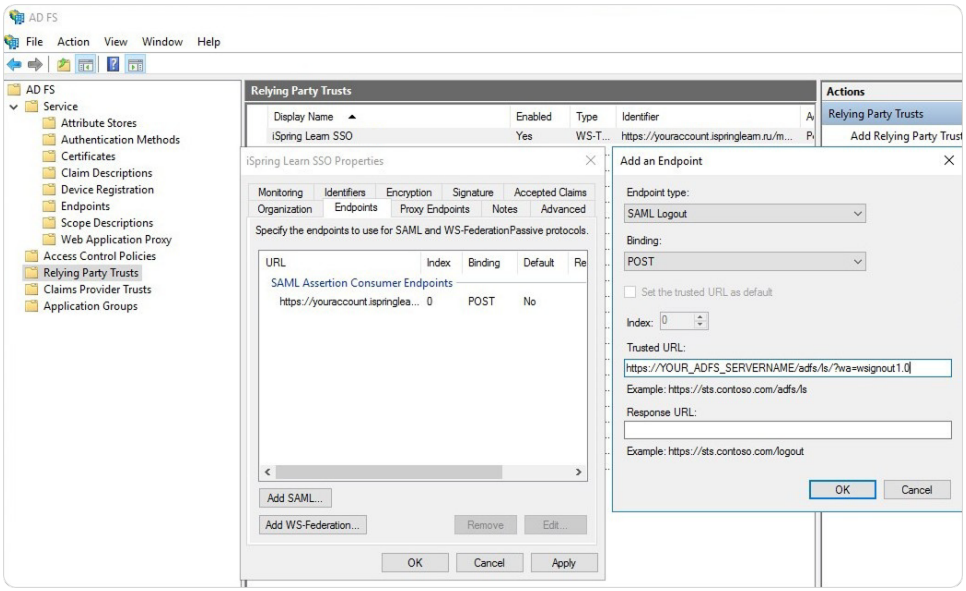
        i. Haga clic en **Add SAML** (Añadir SAML).
        ii. Para el parámetro de tipo de **Endpoint** (Extremo), seleccione **SAML Assertion Consumer**.
        iii. Para **Binding** (Enlace), seleccione **Artifact**.
        iv. Para **Index** (Índice), seleccione 2.

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

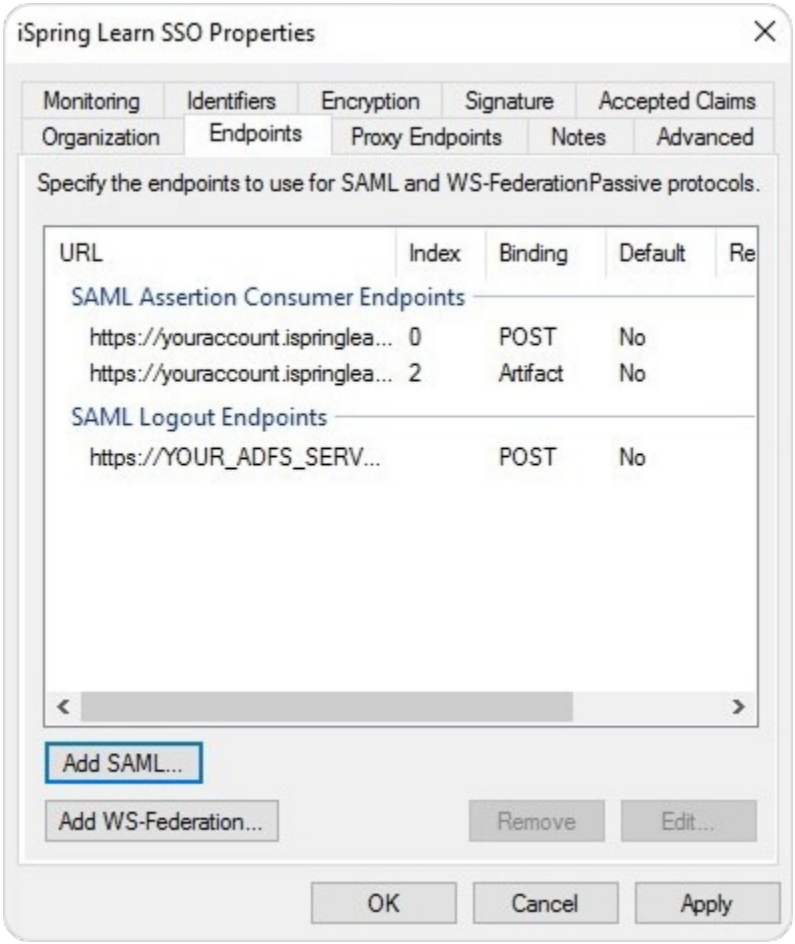


b. Añada un nuevo punto. Para hacer esto:

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.
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.



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**.

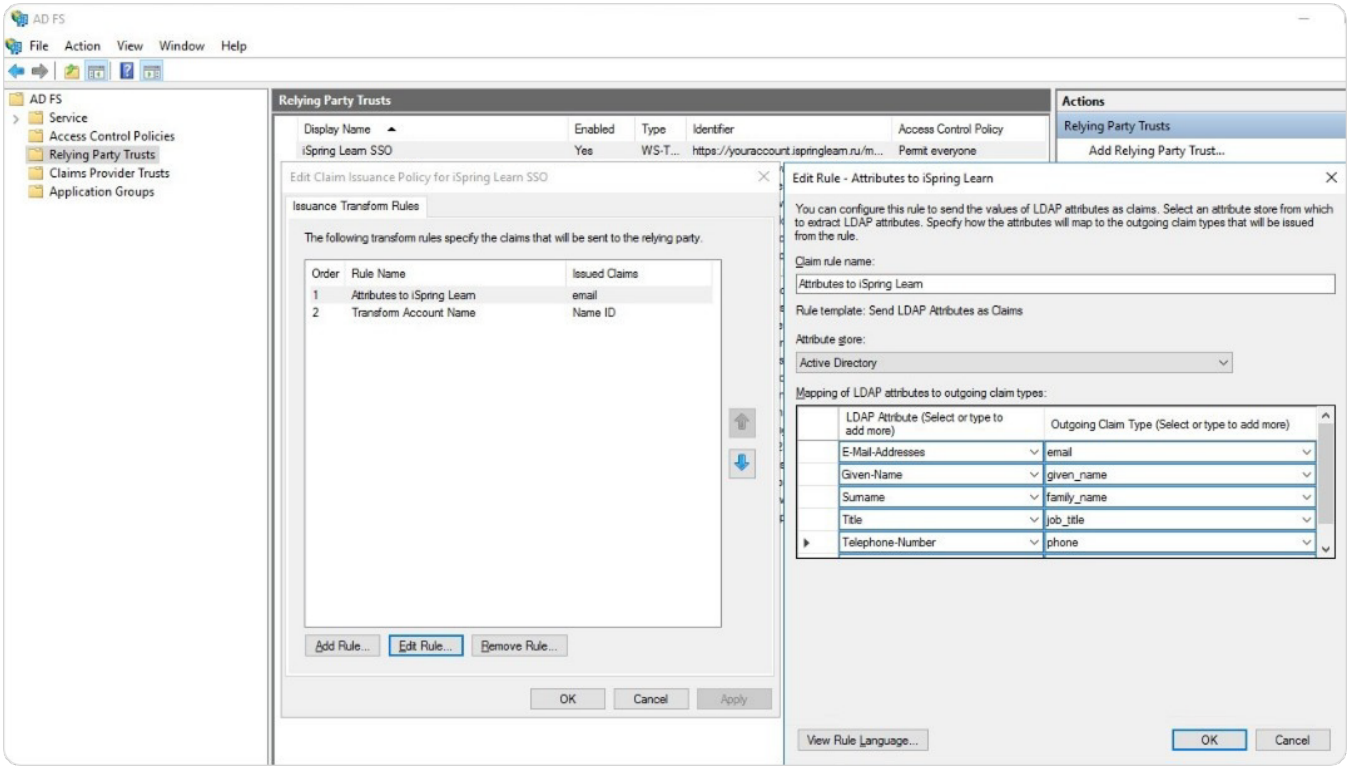
   Se abrirá la cuenta personal del usuario.

   Si se produce un error durante la configuración, envíe una captura de pantalla del error a support@ispring.es.

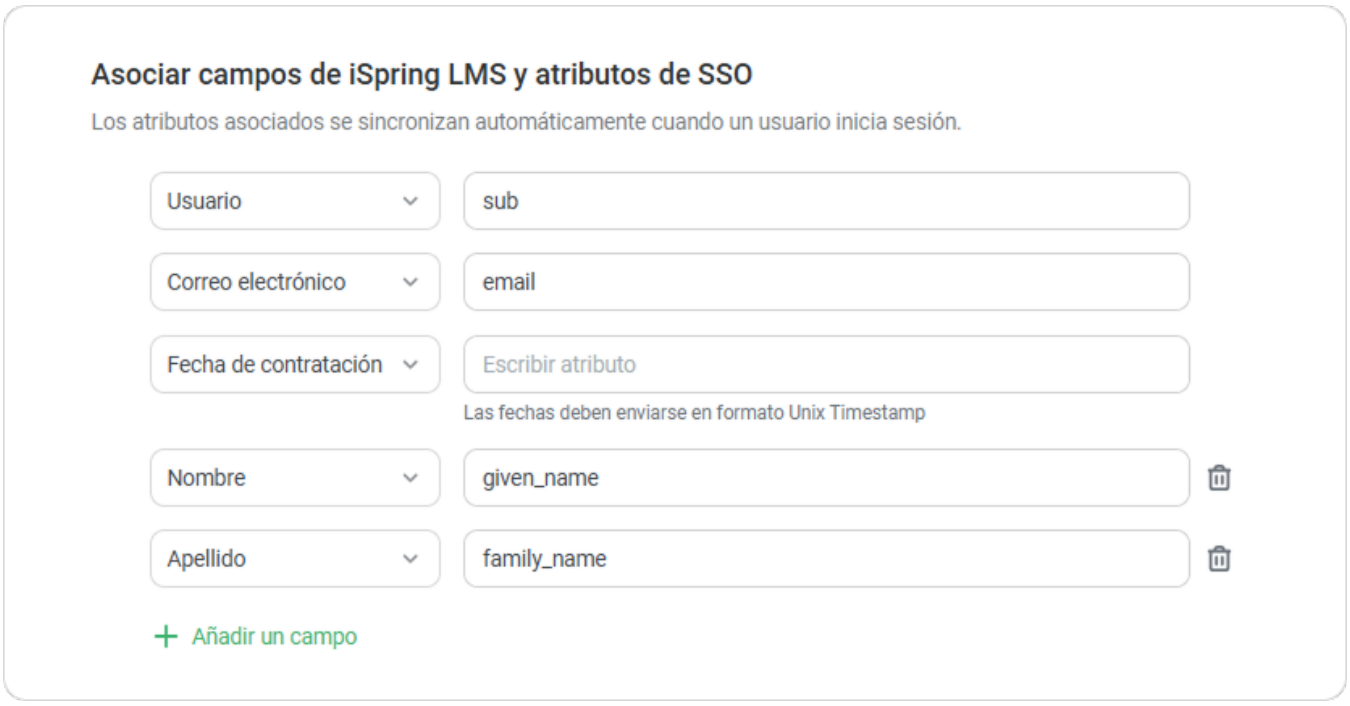
Correlación de campos de iSpring Cloud y SSO

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 Clloud y SSO.

En el lado de AD FS:



En el lado de iSpring Cloud:

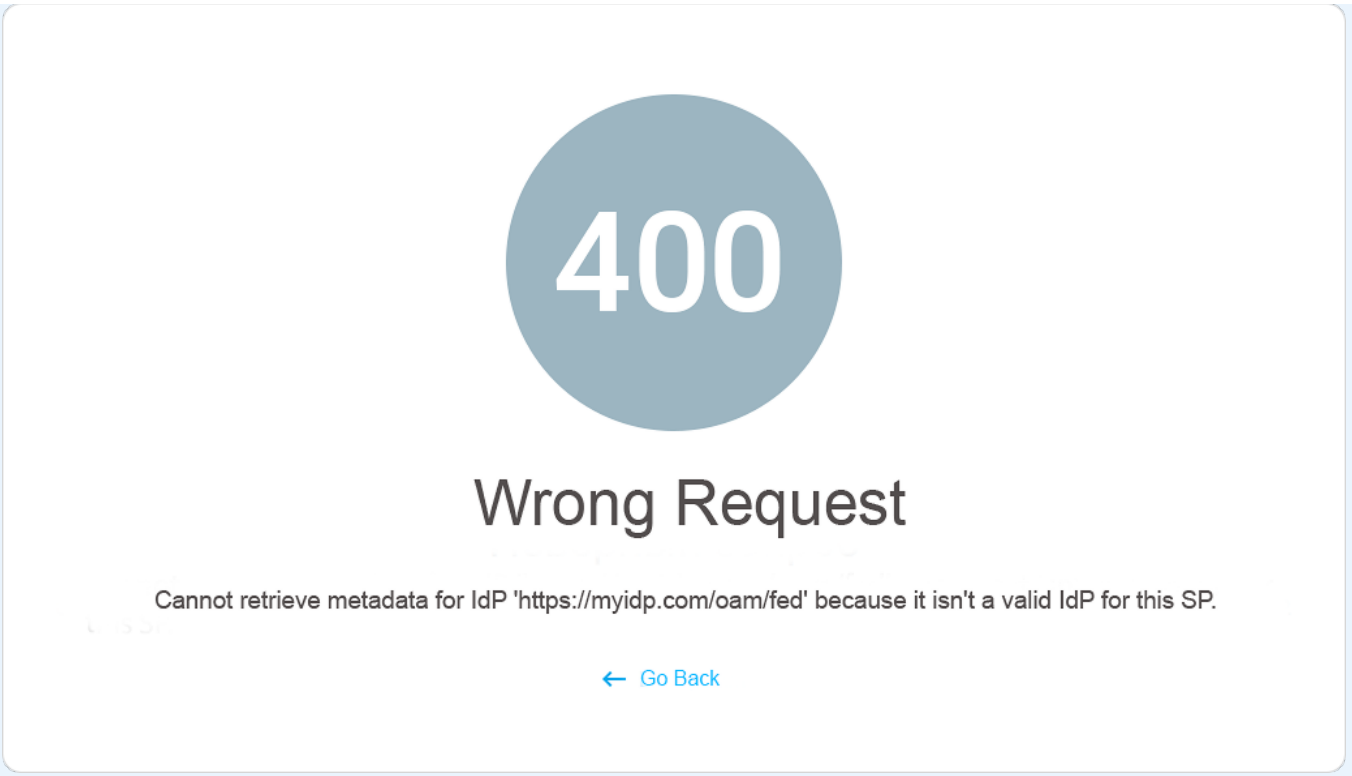


Autorización sin SAML

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**.

Ahora iniciarás 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.



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)**.