

Guía de configuración para conectar un nuevo Proyecto con el ADFS de Interworld Group.

**Para el siguiente manual existe un repositorio donde podrá encontrar todos los archivos necesarios. El repositorio está en la siguiente dirección*

<https://www.github.com/IWGDevelop/IGSIFiles>

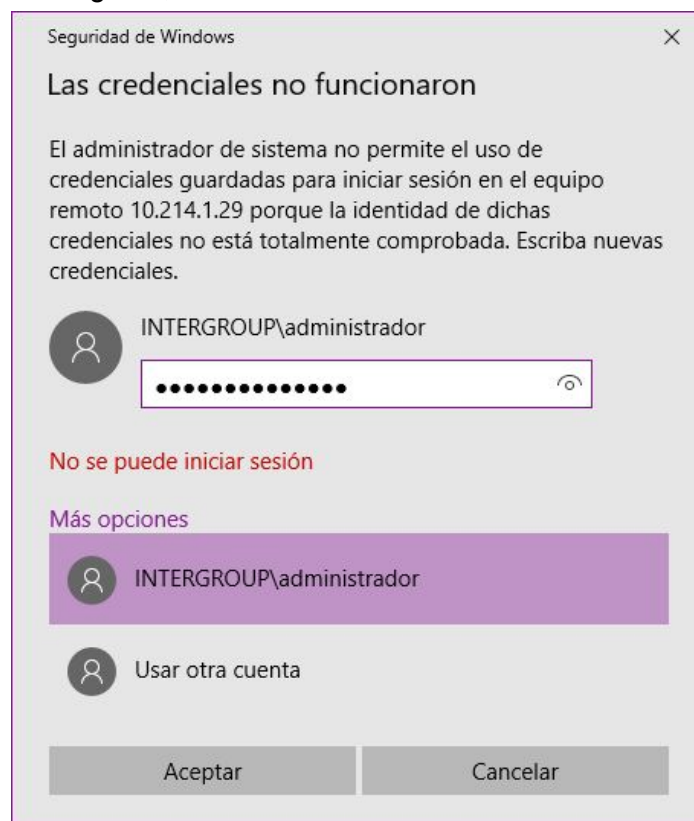
***Asegúrese de cambiar el tag `NOMBRE_DE_LA_EMPRESA` por el nombre asociado a la empresa en su nuevo proyecto.*

1. De la carpeta de Controladores, reemplace el AccountController por el que se encuentra en el repositorio. Este archivo contiene los siguientes métodos:
 - a. SignIn: Para el manejo del inicio de sesión con el WSFederation
 - b. SignOut: Para el cierre de la sesión del usuario.
 - c. SignOutCallback: Método de redirección para el cambio de estado de la sesión de un usuario.
 - d. NotAuthorized: Vista para el acceso no autorizado de un usuario.
 - e. NotLoggedIn: Recuperación de sesión al redireccionar al usuario a la página inicial (Controlador Home, Etiqueta Authorized)
2. Al reemplazar el archivo AccountController, deberá instalar el Paquete Nuget Owin.WsFederation usando el siguiente comando en el administrador de paquetes de Visual Studio
 - a. Install-Package Microsoft.Owin.Security.WsFederation -Version 3.1.0
3. Elimine el ManageController ya que no se necesitará. Además reemplace el HomeController con el del repositorio, que elimina métodos innecesarios y agrega la etiqueta Authorize para obligar al Proyecto a Autenticarse ante el ADFS.
4. Cree el CommonController que tiene métodos de uso común para todos los proyectos.
5. Con este controlador usted deberá referenciar el proyecto Iwg.Entities para obtener los datos de las entidades de los demás proyectos.
 - a. Para ello dé clic derecho en Referencias -> Agregar referencia -> Examinar y busque la ruta
“PATH_DE_CODIGO_TFS\IWG-DEV\SourceCode\Iwg.Base\Iwg.Entities\bin\Debug” (En caso de estar usando proyectos Release, busque la ruta especificada en Release)
 - b. Seleccione el archivo Iwg.Entities.dll. Dé clic en Aceptar
 - c. Se seleccionará la referencia a la anterior dll. Dé clic en Aceptar.
6. En la carpeta de vistas elimine las Vistas de la carpeta Account y elimine la carpeta Manage, ya que usan vistas que no se usarán con WsFederation. También puede eliminar las vistas Contact y About de Home, y _LoginPartial y Lockout de Shared.
7. Copie las vistas NotAuthorized, NotLoggedIn y SignOutCallback en la carpeta Account para el manejo de los métodos de seguridad y sesión del usuario.
8. Cree la carpeta para el controlador Common y copie la vista GetMenus para mostrar el menú de la Aplicación.

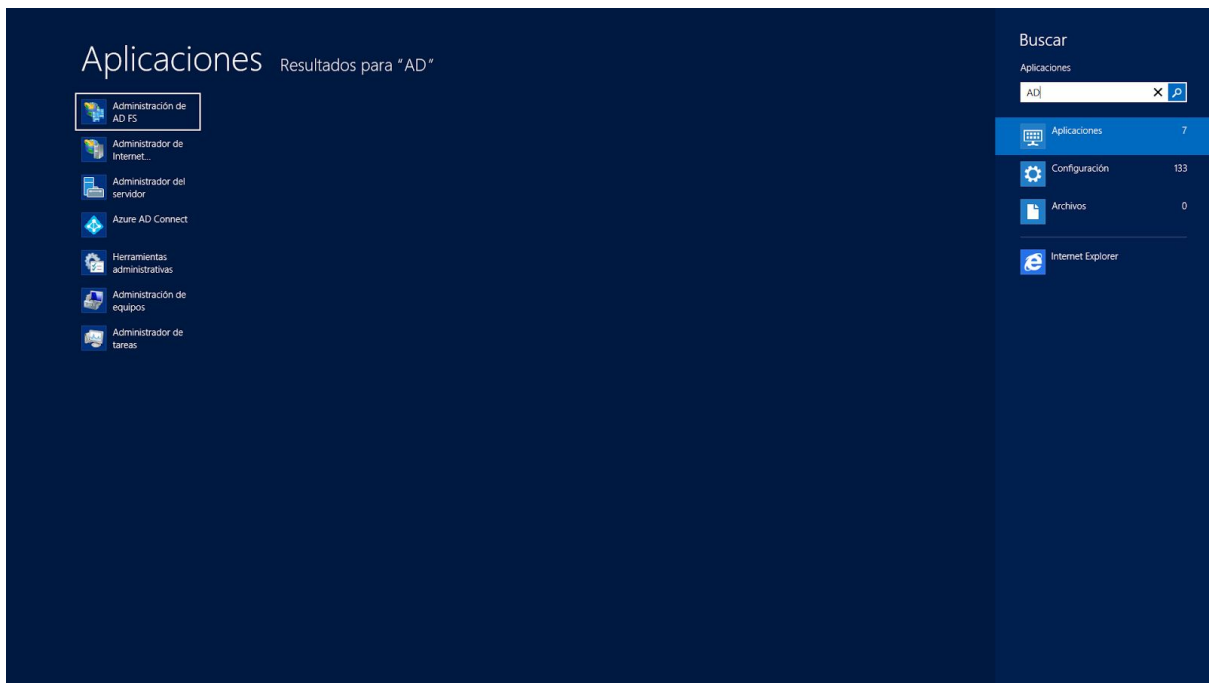
9. Reemplace la vista Index de Home que tiene los métodos para el manejo de localStorage del navegador, además de una plantilla básica del Home de la aplicación.
10. Copie la vista _LayoutIWG a Shared. Esta vista contiene la plantilla de todos los formularios y las páginas de la Aplicación.
11. Cambie la etiqueta
“COLOQUE_AQUI_EL_ID_DE_LA_EMPRESA_EN_LA_BASE_DE_DATOS” por el identificador de la empresa en la tabla “IWG_TRANSVERSE” para la obtención de los menús según el usuario y la empresa.
12. En el archivo ViewStart cambie la referencia a la vista _Layout por la vista _LayoutIWG.
13. En la carpeta App_Start elimine el archivo IdentityConfig.cs, reemplace el archivo Startup.Auth.cs y cree el archivo WebApiConfig.cs
14. Al pegar el archivo WebApiConfig.cs, deberá referenciar la dll System.Web.Http del paquete Microsoft.AspNet.WebApi.Core.5.2. La forma más fácil de hacerlo es dando clic derecho en Referencias -> Agregar referencia -> Examinar y buscando la ruta “URL_DEL_PROYECTO\IWG-DEV\SourceCode\Iwg.Base\Iwg.Entities\bin\Debug” y seleccionando la dll System.Web.Http.dll

Configuración de conexión entre Servidor ADFS y Proyecto

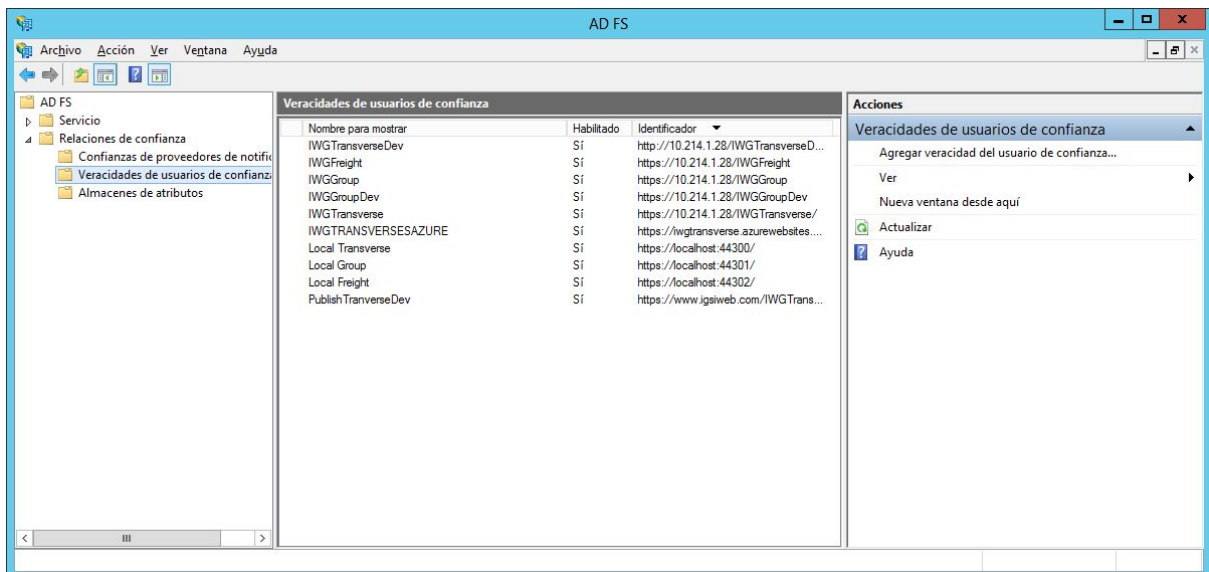
1. Ingrese al servidor ADFS de Interworld LTDA en la dirección 10.214.1.29. Para las credenciales de ingreso, contacte al administrador de la red de la compañía.



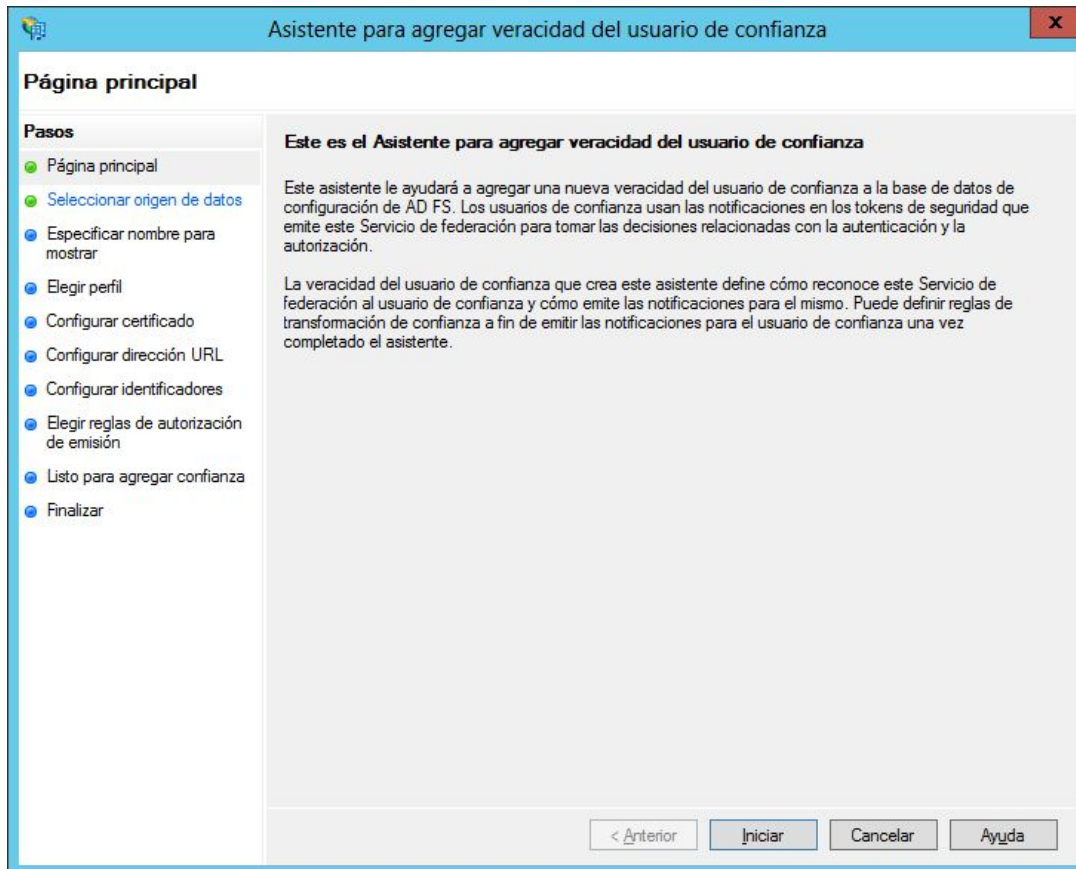
2. En inicio escriba AD y seleccione Administración de AD FS.



3. En el árbol de carpetas al lado izquierdo, abra ADFS, Relaciones de confianza, Veracidades de usuarios de confianza. Saldrán todas las aplicaciones que tienen acceso al ADFS de la compañía.



4. Dé clic en Agregar veracidad del usuario de confianza y dé clic en Iniciar



Asistente para agregar veracidad del usuario de confianza

Página principal

Pasos

- Página principal
- **Seleccionar origen de datos**
- Especificar nombre para mostrar
- Elegir perfil
- Configurar certificado
- Configurar dirección URL
- Configurar identificadores
- Elegir reglas de autorización de emisión
- Listo para agregar confianza
- Finalizar

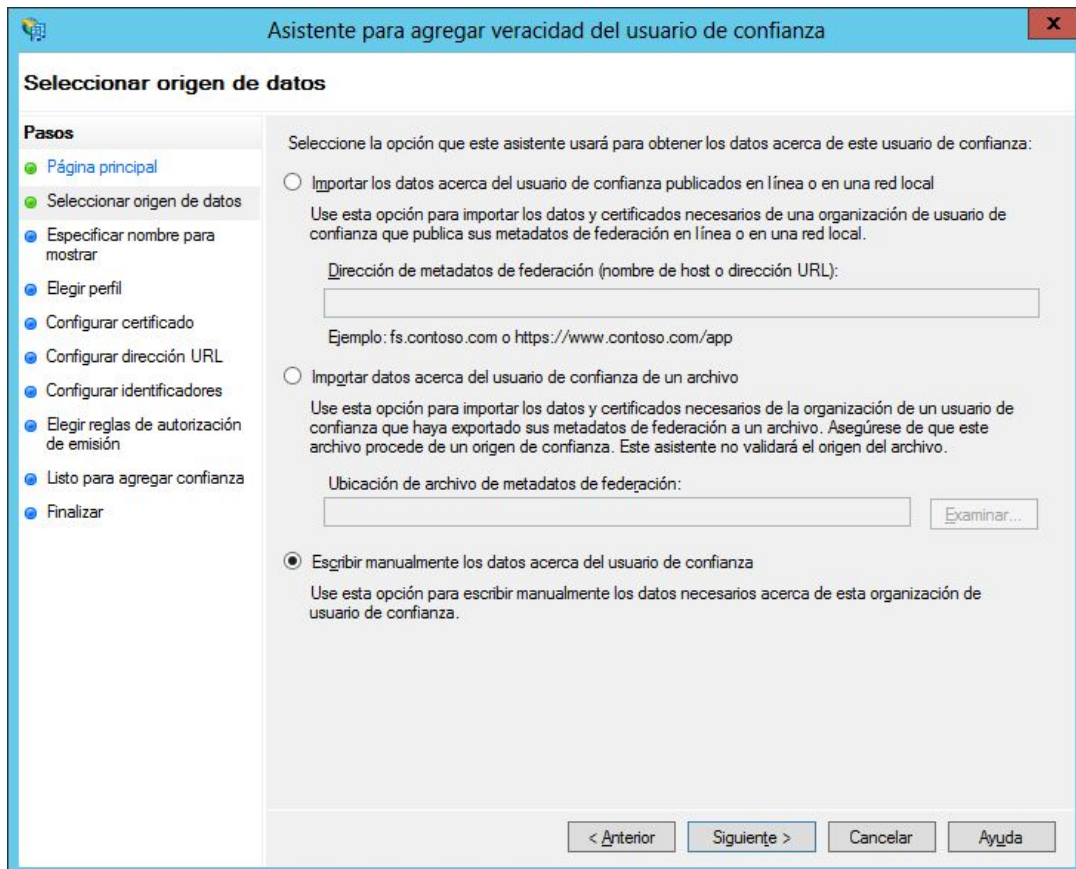
Este es el Asistente para agregar veracidad del usuario de confianza

Este asistente le ayudará a agregar una nueva veracidad del usuario de confianza a la base de datos de configuración de AD FS. Los usuarios de confianza usan las notificaciones en los tokens de seguridad que emite este Servicio de federación para tomar las decisiones relacionadas con la autenticación y la autorización.

La veracidad del usuario de confianza que crea este asistente define cómo reconoce este Servicio de federación al usuario de confianza y cómo emite las notificaciones para el mismo. Puede definir reglas de transformación de confianza a fin de emitir las notificaciones para el usuario de confianza una vez completado el asistente.

< Anterior Iniciar Cancelar Ayuda

5. Seleccione Escribir manualmente los datos acerca del usuario de confianza



Asistente para agregar veracidad del usuario de confianza

Seleccionar origen de datos

Pasos

- Página principal
- **Seleccionar origen de datos**
- Especificar nombre para mostrar
- Elegir perfil
- Configurar certificado
- Configurar dirección URL
- Configurar identificadores
- Elegir reglas de autorización de emisión
- Listo para agregar confianza
- Finalizar

Seleccione la opción que este asistente usará para obtener los datos acerca de este usuario de confianza:

☐ Importar los datos acerca del usuario de confianza publicados en línea o en una red local

Use esta opción para importar los datos y certificados necesarios de una organización de usuario de confianza que publica sus metadatos de federación en línea o en una red local.

Dirección de metadatos de federación (nombre de host o dirección URL):

Ejemplo: fs.contoso.com o https://www.contoso.com/app

☐ Importar datos acerca del usuario de confianza de un archivo

Use esta opción para importar los datos y certificados necesarios de la organización de un usuario de confianza que haya exportado sus metadatos de federación a un archivo. Asegúrese de que este archivo procede de un origen de confianza. Este asistente no validará el origen del archivo.

Ubicación de archivo de metadatos de federación:

Examinar...

☒ Escribir manualmente los datos acerca del usuario de confianza

Use esta opción para escribir manualmente los datos necesarios acerca de esta organización de usuario de confianza.

< Anterior Siguiente > Cancelar Ayuda

6. Escriba un nombre para la Veracidad del usuario de confianza

The screenshot shows the 'Asistente para agregar veracidad del usuario de confianza' (Trust User Veracity Assistant) wizard. The title bar is blue with a close button. The main window has a light gray background. On the left, a 'Pasos' (Steps) pane lists the following steps: 'Página principal' (green dot), 'Seleccionar origen de datos' (green dot), 'Especificar nombre para mostrar' (green dot, currently selected), 'Elegir perfil' (blue dot), 'Configurar certificado' (blue dot), 'Configurar dirección URL' (blue dot), 'Configurar identificadores' (blue dot), 'Elegir reglas de autorización de emisión' (blue dot), 'Listo para agregar confianza' (blue dot), and 'Finalizar' (blue dot). The main area is titled 'Especificar nombre para mostrar' and contains the instruction: 'Escriba el nombre para mostrar y las notas que desee para este usuario de confianza.' Below this, there is a text box labeled 'Nombre para mostrar:' containing the text 'Local Land'. Below that is a larger text box labeled 'Notas:' which is currently empty. At the bottom right, there are four buttons: '< Anterior', 'Siguiente >', 'Cancelar', and 'Ayuda'.

7. Seleccione Perfil ADFS

The screenshot shows the 'Asistente para agregar veracidad del usuario de confianza' (Trust User Veracity Assistant) wizard. The title bar is blue with a close button. The main window has a light gray background. On the left, a 'Pasos' (Steps) pane lists the following steps: 'Página principal' (green dot), 'Seleccionar origen de datos' (green dot), 'Especificar nombre para mostrar' (green dot), 'Elegir perfil' (green dot, currently selected), 'Configurar certificado' (blue dot), 'Configurar dirección URL' (blue dot), 'Configurar identificadores' (blue dot), 'Elegir reglas de autorización de emisión' (blue dot), 'Listo para agregar confianza' (blue dot), and 'Finalizar' (blue dot). The main area is titled 'Elegir perfil' and contains the instruction: 'Este asistente usa perfiles de configuración para ayudar a crear la veracidad del usuario de confianza. Elija el perfil de configuración apropiado para esta veracidad del usuario de confianza.' Below this, there are two radio button options. The first option is 'Perfil de AD FS' (selected), with the description: 'Este perfil es compatible con los usuarios de confianza que pueden interoperar con las nuevas características de AD FS, como el cifrado de tokens de seguridad y el protocolo SAML 2.0.' The second option is 'Perfil de AD FS 1.0 y AD FS 1.1', with the description: 'Este perfil es compatible con los usuarios de confianza que pueden interoperar con AD FS 1.0 y AD FS 1.1.' At the bottom right, there are four buttons: '< Anterior', 'Siguiente >', 'Cancelar', and 'Ayuda'.

8. No se preocupe por el certificado de Token por ahora, ya que vamos a manejar todo en localhost.

The screenshot shows the 'Asistente para agregar veracidad del usuario de confianza' (Trust User Verification Assistant) wizard. The current step is 'Configurar certificado' (Configure certificate). The left pane shows a list of steps: 'Página principal', 'Seleccionar origen de datos', 'Especificar nombre para mostrar', 'Elegir perfil', 'Configurar certificado' (selected), 'Configurar dirección URL', 'Configurar identificadores', 'Elegir reglas de autorización de emisión', 'Listo para agregar confianza', and 'Finalizar'. The main area contains instructions: 'Especifique un certificado de cifrado de token opcional. El certificado de cifrado de token se usa para cifrar las notificaciones que se envían a este usuario de confianza. El usuario de confianza usará la clave privada de este certificado para descifrar las notificaciones que se le envíen. Para especificar el certificado, haga clic en Examinar.' Below the instructions are fields for 'Emisor:', 'Asunto:', 'Fecha de vigencia:', and 'Fecha de expiración:'. There are three buttons: 'Ver...', 'Examinar...', and 'Quitar'. At the bottom are navigation buttons: '< Anterior', 'Siguiente >', 'Cancelar', and 'Ayuda'.

9. Habilite la compatibilidad con WS Federation y escriba la URL que va a usar su proyecto (El puerto lo escoge usted, asegúrese de seleccionar uno libre)

The screenshot shows the 'Asistente para agregar veracidad del usuario de confianza' (Trust User Verification Assistant) wizard. The current step is 'Configurar dirección URL' (Configure URL). The left pane shows the same list of steps as the previous screenshot, with 'Configurar dirección URL' selected. The main area contains instructions: 'AD FS es compatible con los protocolos WS-Trust, WS-Federation y SAML 2.0 WebSSO para los usuarios de confianza. Si el usuario de confianza usa WS-Federation, SAML o ambos, active las casillas correspondientes y especifique las direcciones URL que se usarán. La compatibilidad con el protocolo WS-Trust siempre está habilitada para un usuario de confianza.' There are two checkboxes: 'Habilitar compatibilidad con el protocolo WS-Federation Passive' (checked) and 'Habilitar compatibilidad con el protocolo SAML 2.0 WebSSO' (unchecked). Below the first checkbox, it says 'La dirección URL del protocolo WS-Federation Passive es compatible con los proveedores de notificaciones basados en explorador web que usan el protocolo WS-Federation Passive.' and 'URL del protocolo WS-Federation Passive del usuario de confianza:' followed by a text box containing 'https://localhost:44303/'. Below the second checkbox, it says 'La dirección URL del servicio de inicio de sesión único (SSO) de SAML 2.0 es compatible con los proveedores de notificaciones basados en explorador web mediante el protocolo SAML 2.0 WebSSO.' and 'Dirección URL de servicio SSO de SAML 2.0 del usuario de confianza:' followed by an empty text box. Examples are provided: 'Ejemplo: https://fs.contoso.com/adfs/ls/' and 'Ejemplo: https://www.contoso.com/adfs/ls/'. At the bottom are navigation buttons: '< Anterior', 'Siguiente >', 'Cancelar', and 'Ayuda'.

10. Si lo desea puede agregar más urls para la aplicación, en este caso la Url HTTP.

The screenshot shows the 'Asistente para agregar veracidad del usuario de confianza' (Trust User Veracity Assistant) wizard. The current step is 'Configurar identificadores' (Configure identifiers). The left sidebar shows the progress: 'Página principal', 'Seleccionar origen de datos', 'Especificar nombre para mostrar', 'Elegir perfil', 'Configurar certificado', 'Configurar dirección URL', 'Configurar identificadores' (current step), 'Elegir reglas de autorización de emisión', 'Listo para agregar confianza', and 'Finalizar'. The main area contains instructions: 'Los usuarios de confianza pueden identificarse mediante una o varias cadenas de identificador únicas. Especifique los identificadores para esta veracidad del usuario de confianza.' Below this, there is a text box for 'Identificador de veracidad del usuario de confianza:' with the value 'http://localhost:44303/' and an 'Agregar' button. An example is provided: 'Ejemplo: https://fs.contoso.com/adfs/services/trust'. Below that, there is a list box for 'Identificadores de veracidad del usuario de confianza:' with the value 'https://localhost:44303/' and a 'Quitar' button. At the bottom, there are navigation buttons: '< Anterior', 'Siguiente >', 'Cancelar', and 'Ayuda'.

11. Permita a todos los usuarios tener acceso a la veracidad de confianza.

The screenshot shows the 'Asistente para agregar veracidad del usuario de confianza' (Trust User Veracity Assistant) wizard. The current step is 'Elegir reglas de autorización de emisión' (Choose issuance authorization rules). The left sidebar shows the progress: 'Página principal', 'Seleccionar origen de datos', 'Especificar nombre para mostrar', 'Elegir perfil', 'Configurar certificado', 'Configurar dirección URL', 'Configurar identificadores', 'Elegir reglas de autorización de emisión' (current step), 'Listo para agregar confianza', and 'Finalizar'. The main area contains instructions: 'Las reglas de autorización de emisión determinan si se permite que un usuario reciba notificaciones para el usuario de confianza. Elija una de las opciones siguientes para el comportamiento inicial de las reglas de autorización de emisión de este usuario de confianza.' Below this, there are two radio button options. The first option is selected: 'Permitir que todos los usuarios tengan acceso a este usuario de confianza'. Below this option, there is a paragraph: 'Las reglas de autorización de emisión se configurarán para permitir que todos los usuarios tengan acceso a este usuario de confianza. La aplicación o servicio del usuario de confianza seguirán denegando el acceso al usuario.' The second option is 'Denegar a todos los usuarios el acceso a este usuario de confianza'. Below this option, there is a paragraph: 'Las reglas de autorización de emisión se configurarán para denegar a todos los usuarios el acceso a este usuario de confianza. Posteriormente, debe agregar reglas de autorización de emisión para permitir a los usuarios el acceso a este usuario de confianza.' At the bottom, there is a paragraph: 'Puede cambiar las reglas de autorización de emisión de esta veracidad del usuario de confianza seleccionando la veracidad del usuario de confianza y haciendo clic en Editar reglas de notificación en el panel Acciones.' At the bottom, there are navigation buttons: '< Anterior', 'Siguiente >', 'Cancelar', and 'Ayuda'.

12. Vea el resumen de su configuración

Asistente para agregar veracidad del usuario de confianza

Listo para agregar confianza

Pasos

- Página principal
- Seleccionar origen de datos
- Especificar nombre para mostrar
- Elegir perfil
- Configurar certificado
- Configurar dirección URL
- Configurar identificadores
- Elegir reglas de autorización de emisión
- Listo para agregar confianza
- Finalizar

La veracidad del usuario de confianza se ha configurado. Revise las opciones siguientes y haga clic en Siguiente para agregar la veracidad del usuario de confianza a la base de datos de configuración de AD FS.

Supervisión | Identificadores | Cifrado | Firma | Notificaciones aceptadas | Organización | Extremo < >

Especifique la configuración de supervisión para esta veracidad del usuario de confianza.

Dirección URL de metadatos de federación de usuario de confianza:

☐ Supervisar usuario de confianza

☐ Actualizar automático: usuario confianza

Los datos de los metadatos de federación de este usuario de confianza se comprobaron por última vez en:

< nunca >

Este usuario de confianza se actualizó por última vez a partir de los metadatos de federación en:

< nunca >

< Anterior | Siguiente > | Cancelar | Ayuda

13. Agregue la veracidad de confianza y abra el diálogo de reglas de notificación

Asistente para agregar veracidad del usuario de confianza

Finalizar

Pasos

- Página principal
- Seleccionar origen de datos
- Especificar nombre para mostrar
- Elegir perfil
- Configurar certificado
- Configurar dirección URL
- Configurar identificadores
- Elegir reglas de autorización de emisión
- Listo para agregar confianza
- Finalizar

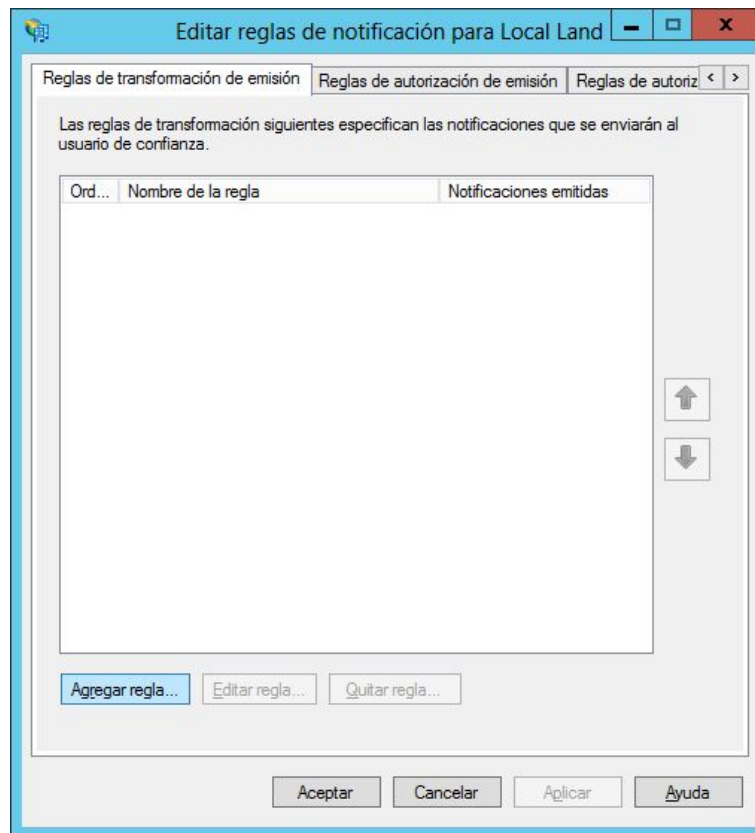
La veracidad del usuario de confianza se agregó a la base de datos de configuración de AD FS.

Puede modificar esta relación de confianza para usuario autenticado mediante el cuadro de diálogo Propiedades del complemento Administración de AD FS.

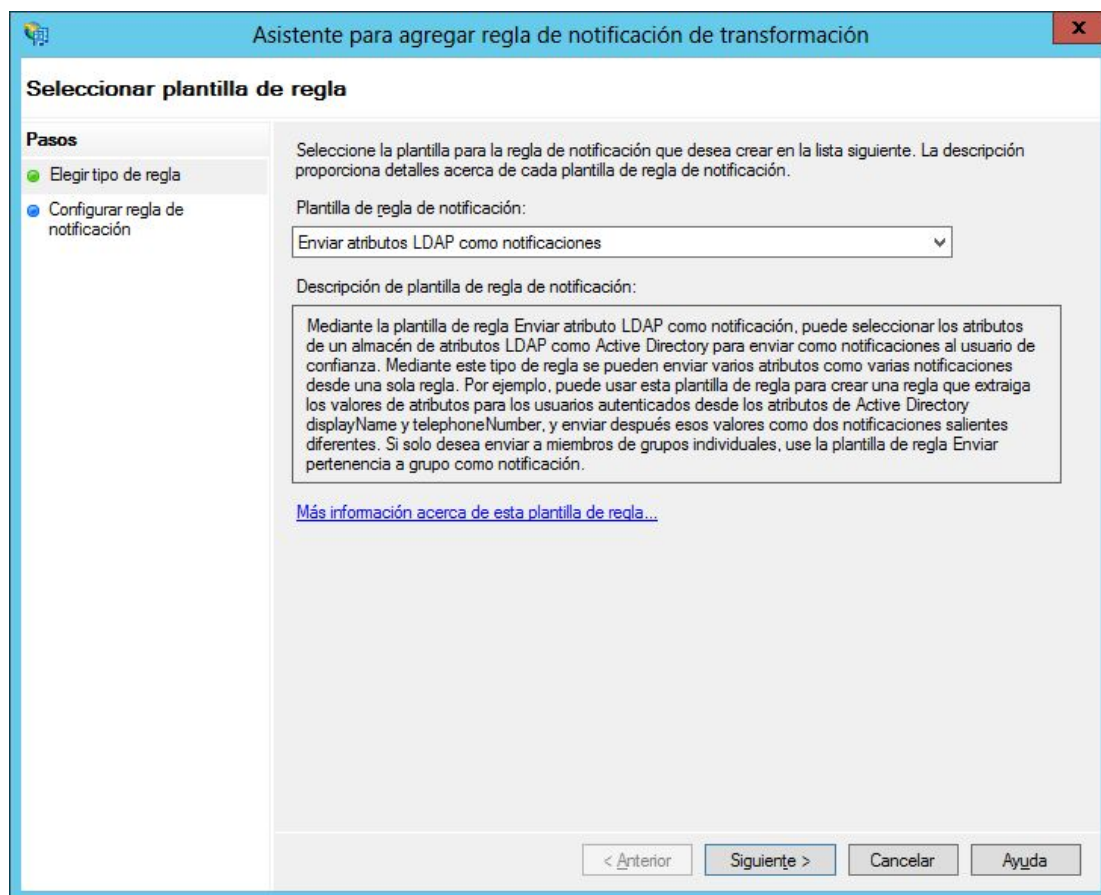
☒ Abrir el cuadro de diálogo Editar reglas de notificación para esta veracidad del usuario de confianza cuando se cierre el asistente

Cerrar

14. Dé clic en agregar regla, se le abrirá el cuadro de diálogo



15. Seleccione Enviar atributos LDAP como notificaciones



16. Escriba un nombre para la regla, seleccione Active Directory y agregue los atributos Display-Name como Nombre, E-Mail-Addresses como Dirección de correo electrónico y User-Principal-Name como UPN y dé clic en finalizar.

Configurar regla

Pasos

- Elegir tipo de regla
- Configurar regla de notificación

Puede configurar esta regla para enviar los valores de los atributos LDAP como notificaciones. Seleccione un almacén de atributos del que extraer los atributos LDAP. Especifique el modo en que los atributos se asignarán a los tipos de notificación saliente que se emitirán a partir de la regla.

Nombre de regla de notificación:
LocalLand

Plantilla de regla: Enviar atributos LDAP como notificaciones

Almacén de atributos:
Active Directory

Asignación de atributos LDAP a los tipos de notificación saliente:

| | Atributo LDAP (seleccione o escriba para agregar más) | Tipo de notificación saliente (seleccione o escriba para agregar más) |
|---|---|---|
| | Display-Name | Nombre |
| | E-Mail-Addresses | Dirección de correo electrónico |
| ▶ | User-Principal-Name | UPN |
| * | | |

< Anterior Finalizar Cancelar Ayuda

17. En Visual Studio abra el WebConfig y configúrelo de la siguiente manera

Configuración del WebConfig.

- Copie el siguiente XML dentro del WebConfig.

```
<configuration>
  <appSettings>
    <add key="ida:ADFSMetadata"
      value="https://adfs.intergroup.com/federationmetadata/2007-06/
      federationmetadata.xml" />
    <add key="ida:Wtrealm" value="https://localhost:44303/" />
    <add key="apiIWGTransverse"
      value="https://10.214.1.28/IWGServivesDev/Api/" />
    <add key="urlIWGTransverse"
      value="https://10.214.1.28/IWGTransverseDev/" />
  </appSettings>
</configuration>
```

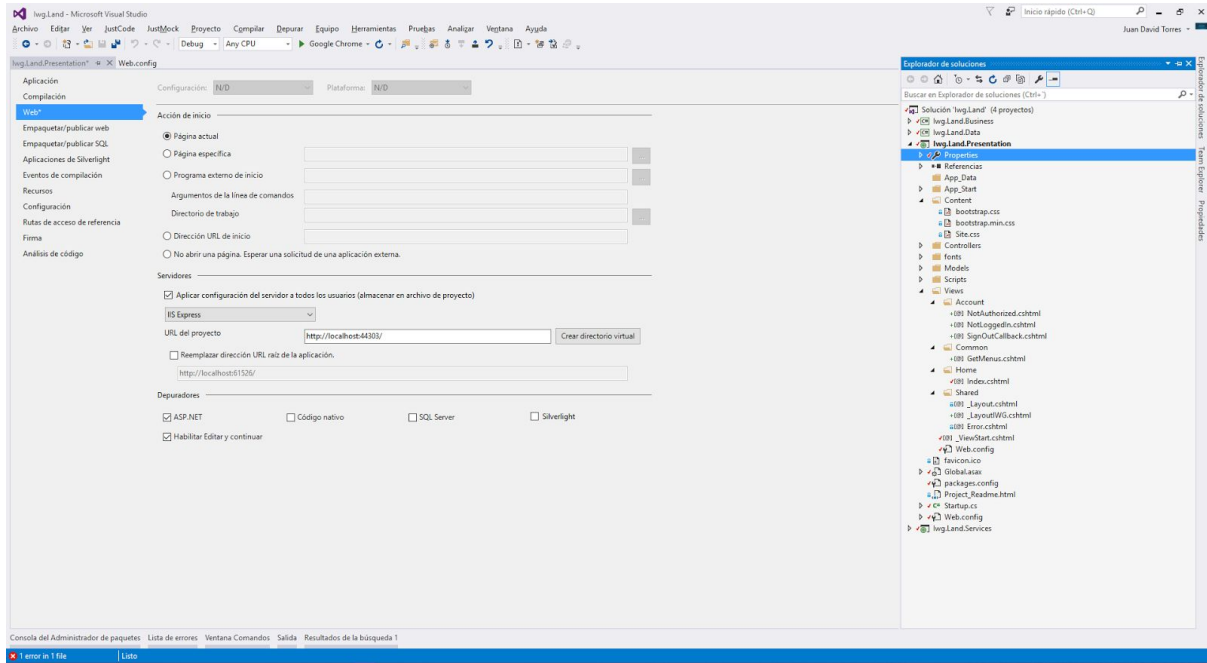
Estas son 4 llaves de configuración de la aplicación.

- a. ADFSMetadata es la referencia al archivo de configuración del ADFS.
 - b. Wtrealm es la dirección del proyecto con el que se identificará dentro del ADFS
 - c. apiIWGTransverse es la dirección de la publicación del proyecto Services de IGSi. Esta dirección debe ser la misma que configuró en el ADFS, para nuestro caso "https://localhost:44303"
 - d. urlIWGTransverse es la dirección de la publicación del proyecto Transverse de IGSi
- Elimine la etiqueta <authentication mode="None" /> dentro de <configuration> <system.web>
 - Reemplace toda la etiqueta <system.webServer> dentro de <configuration> por el siguiente XML

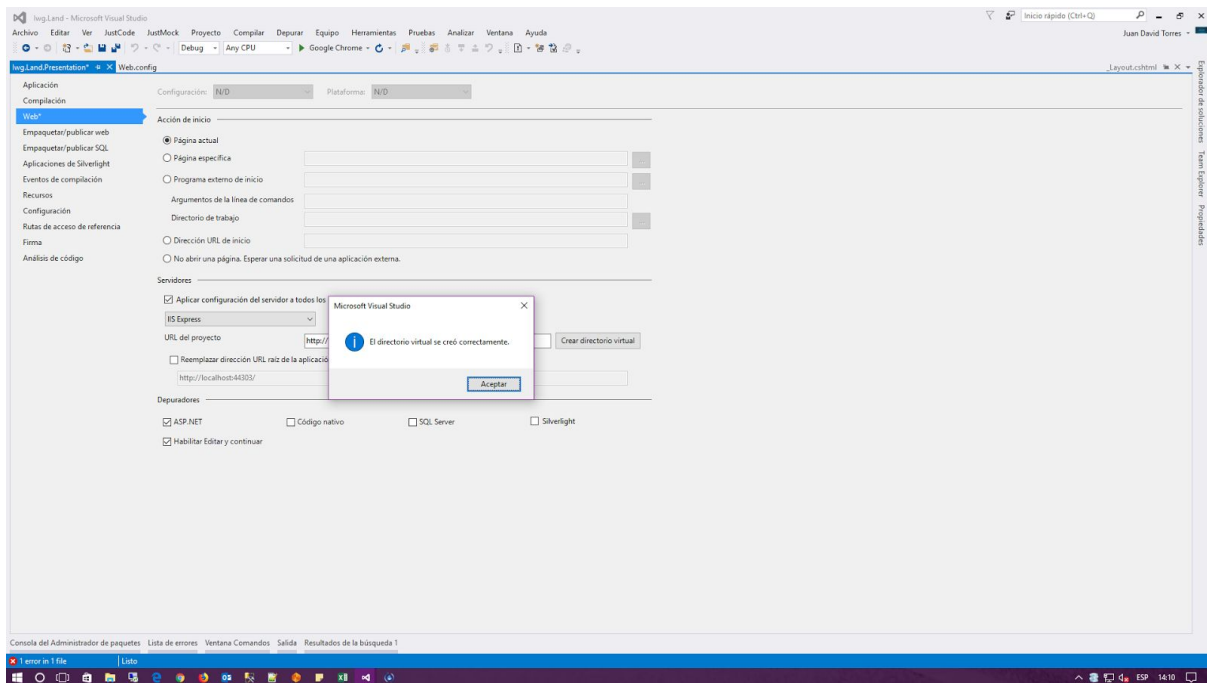
```
<system.webServer>
  <staticContent>
    <remove fileExtension=".woff" />
    <mimeTypeMap fileExtension=".woff"
mimeType="application/font-woff" />
    <remove fileExtension=".woff2" />
    <mimeTypeMap fileExtension=".woff2" mimeType="font/x-woff" />
  </staticContent>
  <validation validateIntegratedModeConfiguration="false" />
</system.webServer>
```

Configuración final de Proyecto

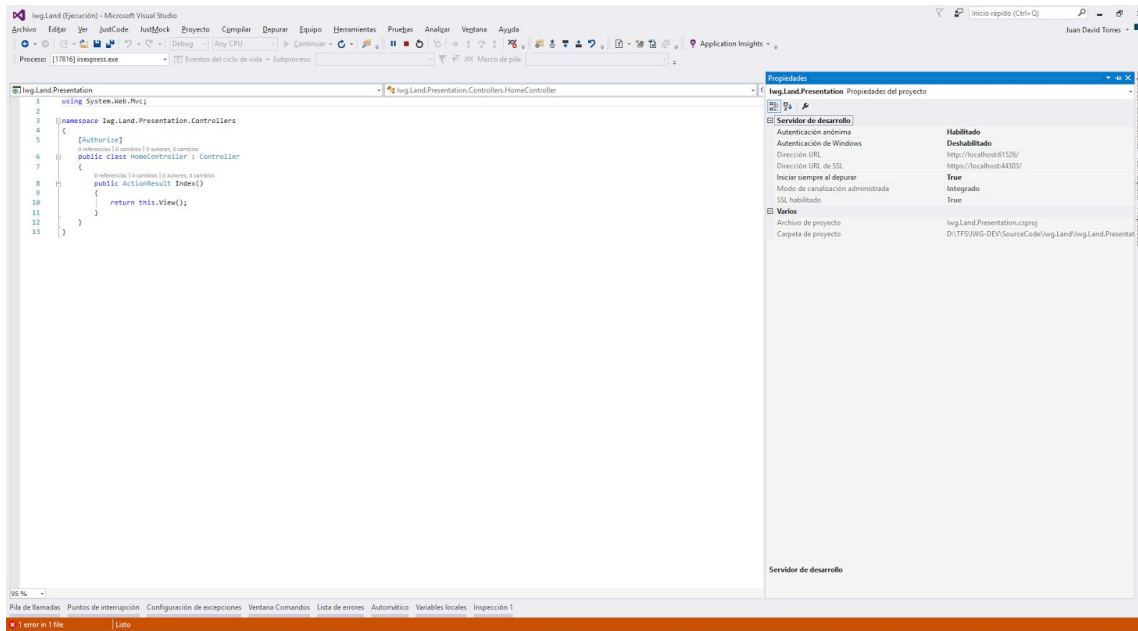
1. Abra las propiedades del proyecto y en sección Web, escriba como URL del proyecto la misma dirección que configuró en el ADFS y en el Web.Config. En nuestro caso <https://localhost:44303>.



2. Acepte la creación del directorio virtual y guarde las configuraciones.



3. Al finalizar la configuración, seleccione su proyecto Presentation y oprima F4, esto mostrará las propiedades del proyecto que deben estar de la siguiente forma



- Autenticación anónima: Habilitado
 - Autenticación de Windows: Deshabilitado
 - Dirección URL: https://localhost:xxxxx (Una dirección que Visual Studio genera para el despliegue local)
 - Dirección URL de SSL: <https://localhost:44303> (La misma que se configuró en el ADFS y en el Web.config)
 - Iniciar siempre al depurar: True
 - Modo de canalización administrada: Integrado
 - SSL habilitado: True
4. Copia y pega los bundles del archivo BundleConfig.cs
5. Por último copia y pega las carpetas Content, fonts y Scripts del repositorio a la carpeta raíz de tu proyecto, estas ya tienen los archivos básicos y necesarios para la aplicación

