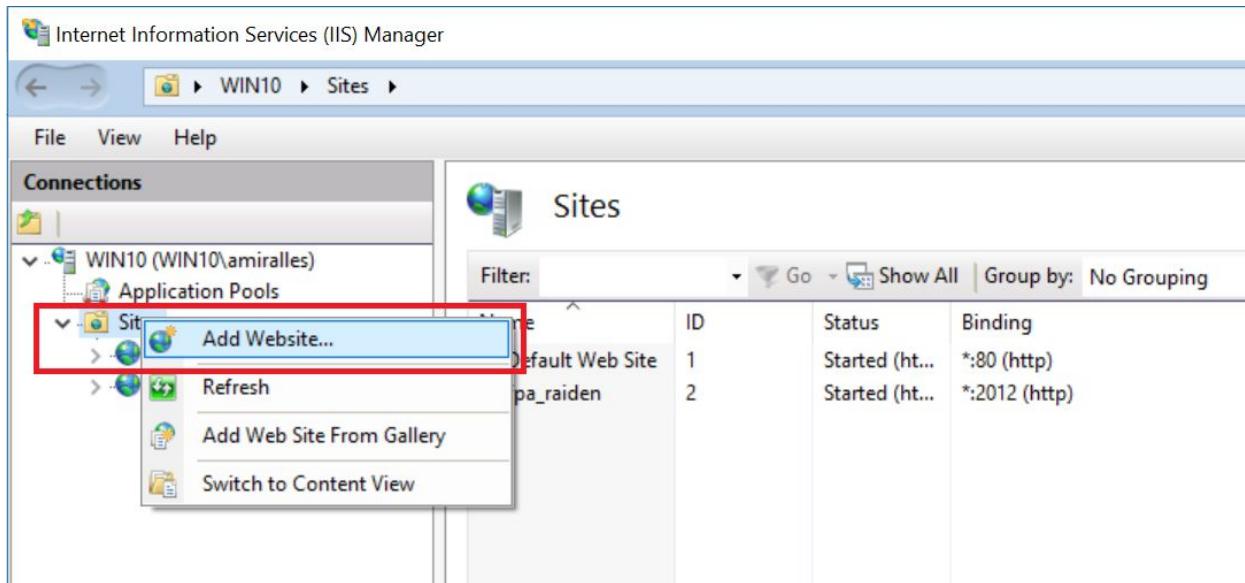


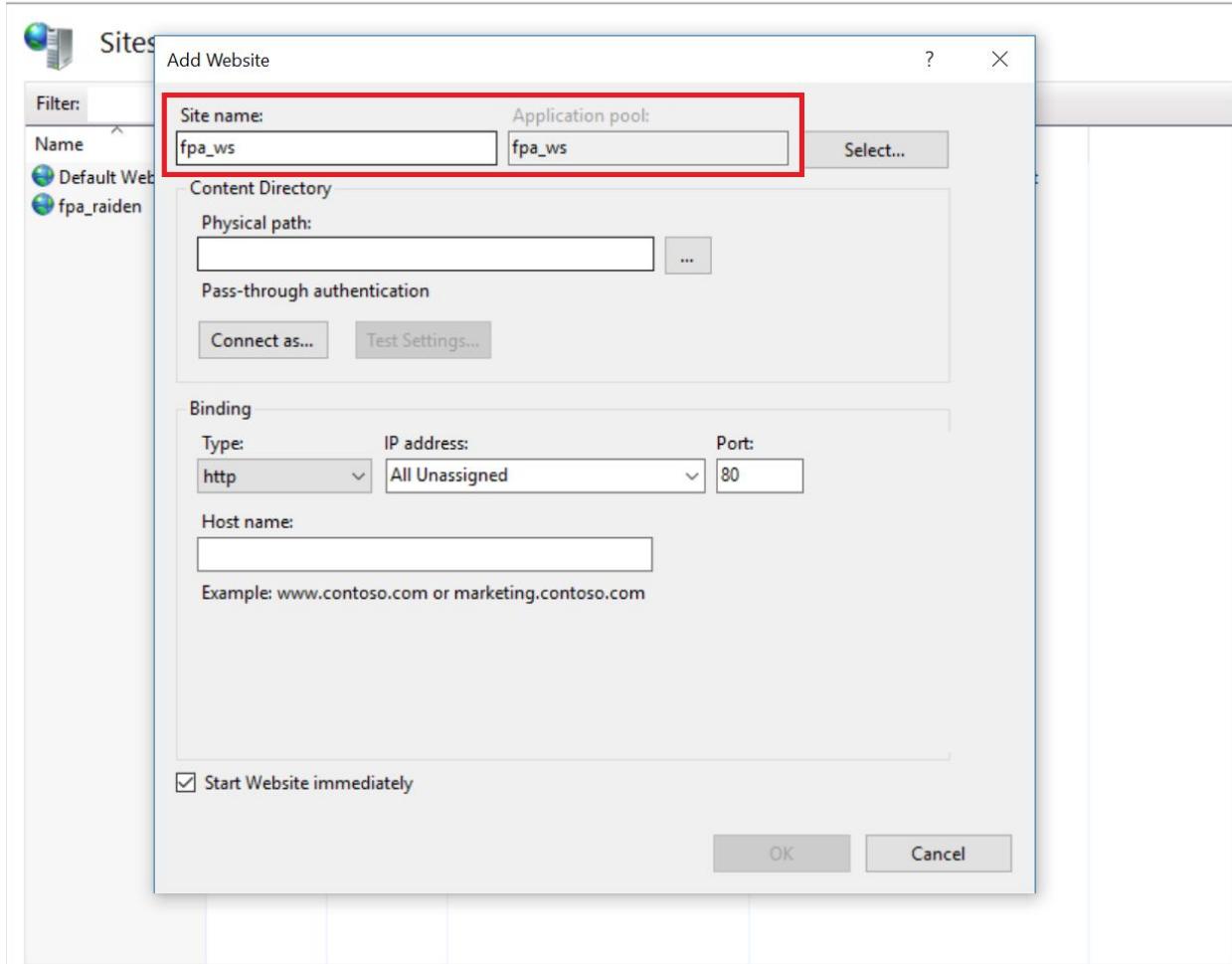
API Raiden FPA: Guía de instalación

A continuación, se detallan los pasos necesarios para instalar el servicio de integración FPA-Raiden de forma manual.

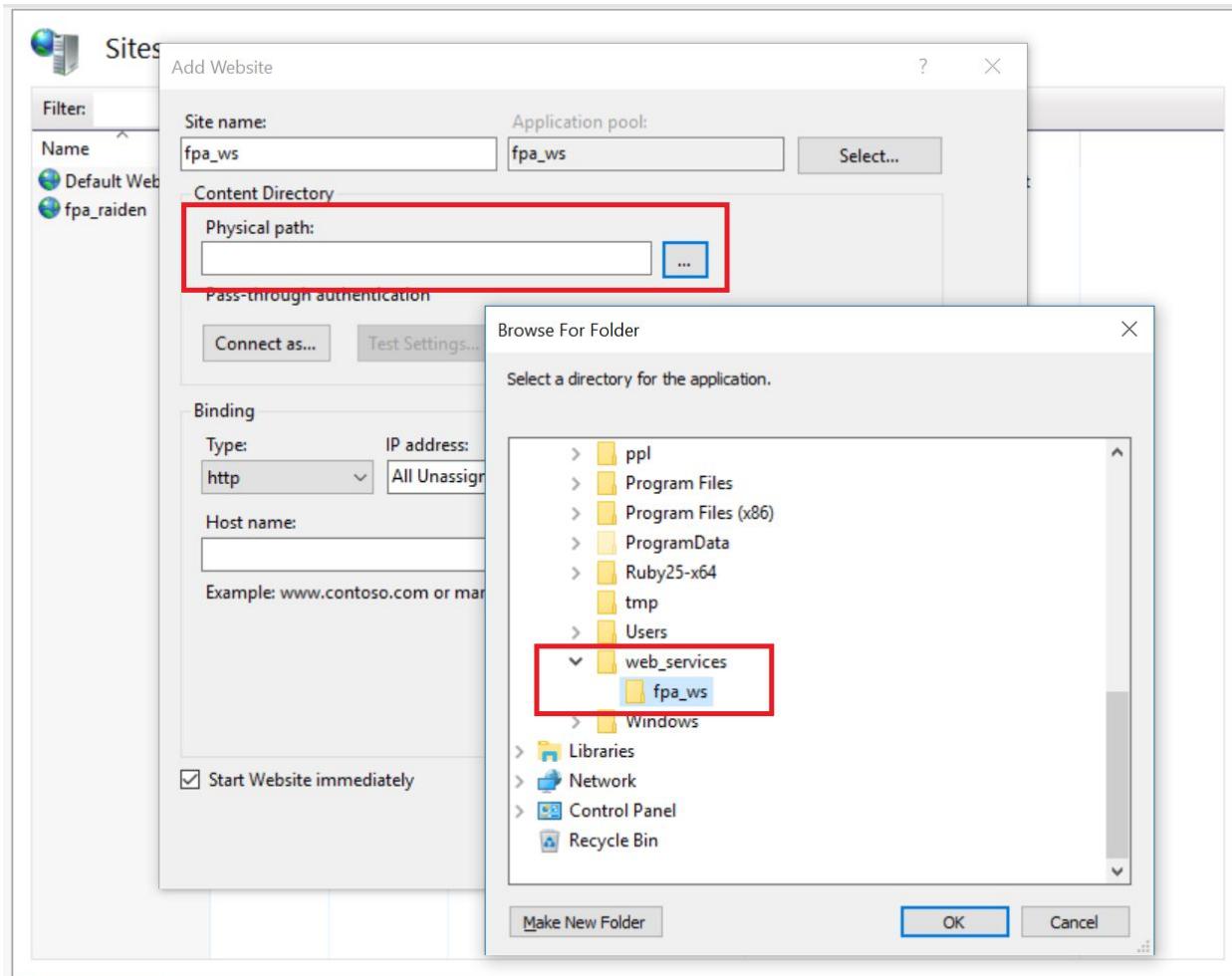
1. Crear un nuevo sitio desde la consola de administración de IIS.



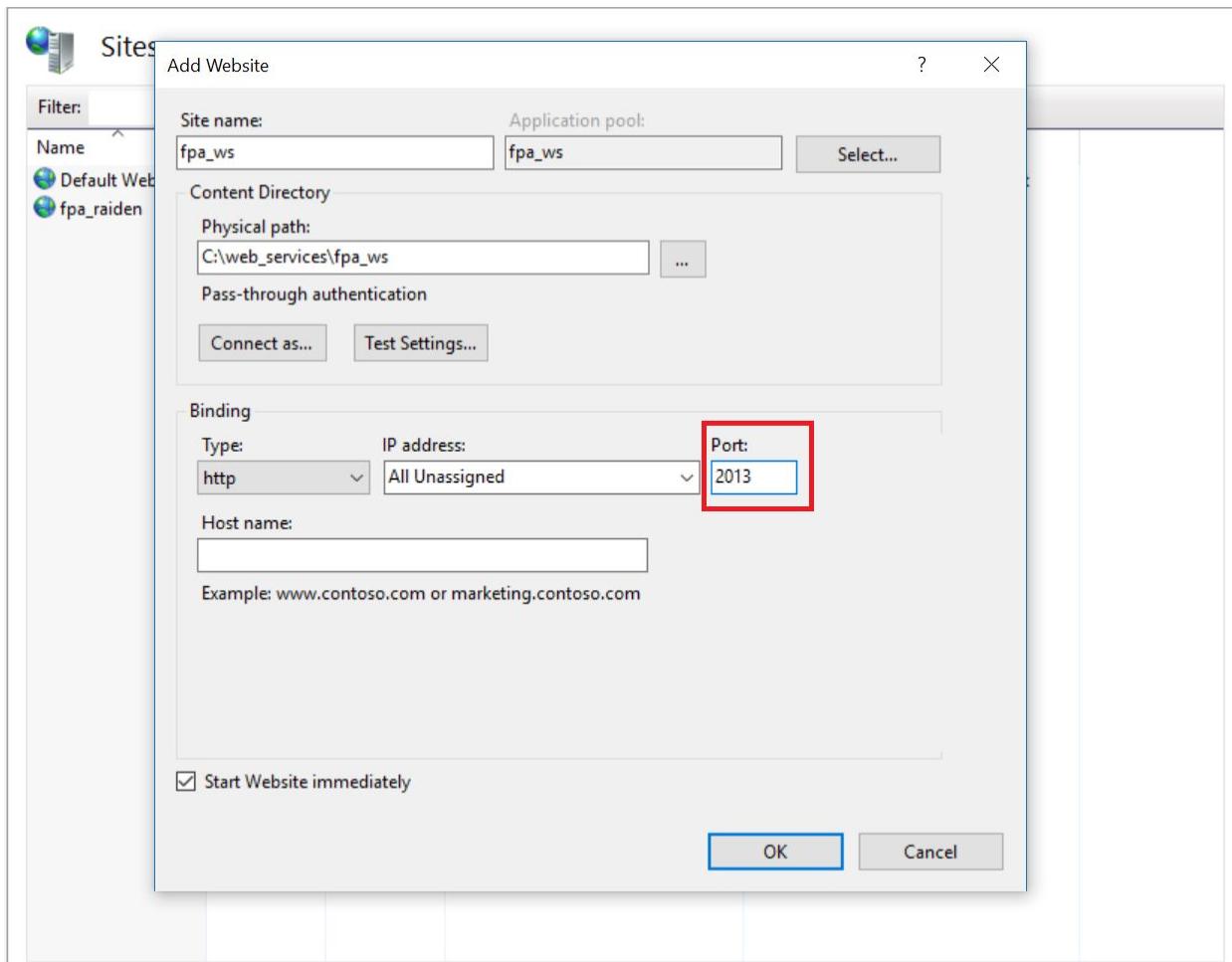
2. Ingresar el nombre del sitio web. Por ejemplo, **fpa_ws**. (En este paso también se crea de forma automática el “application pool” donde va a correr el servicio.)



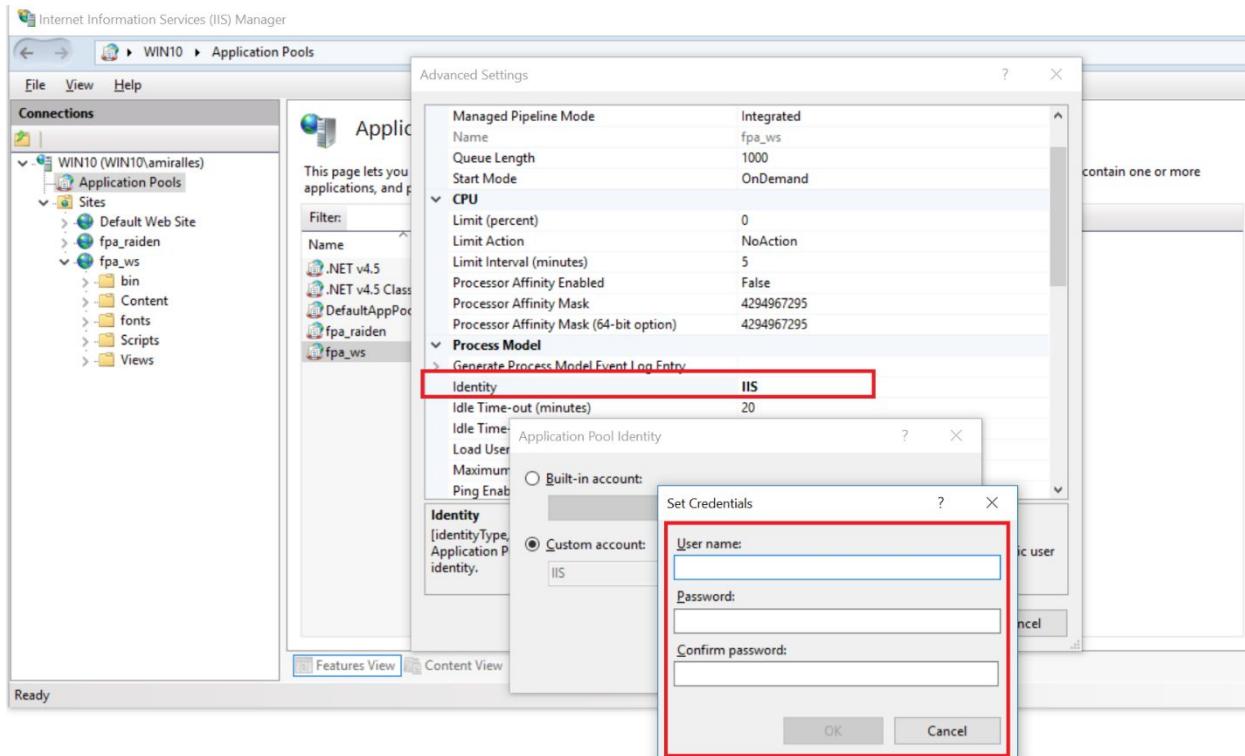
3. Especificar la ruta donde se van a publicar los archivos del sitio web.



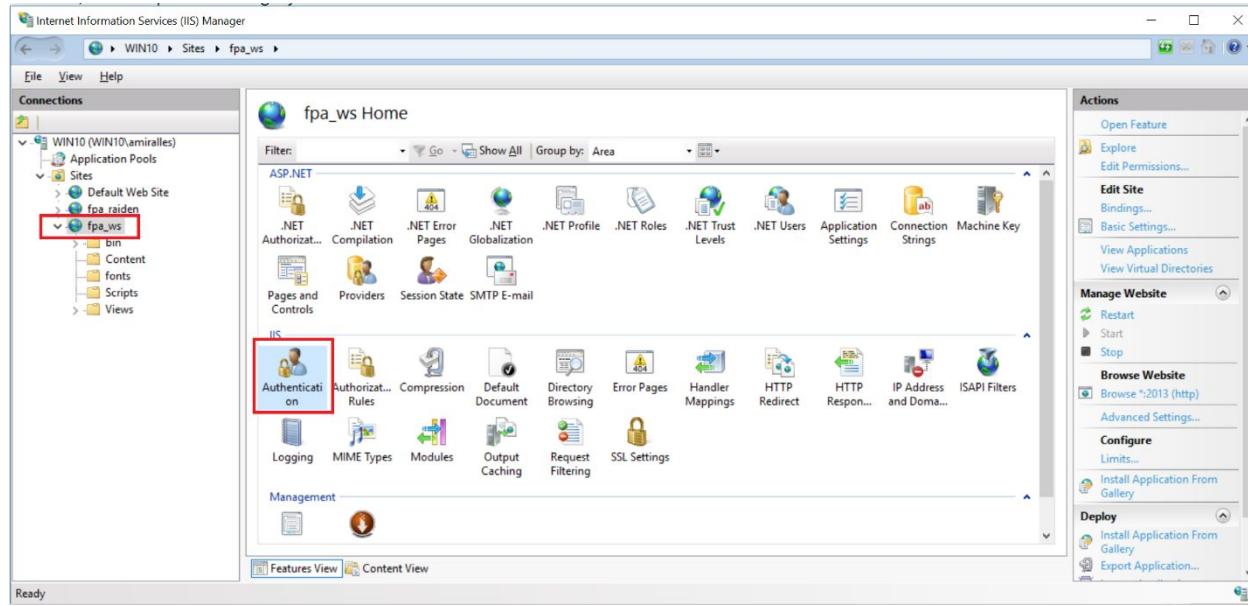
4. Especificar el puerto donde va a escuchar el servicio.



5. Extraer el contenido del archivo **fpa_ws_deploy.zip** en el directorio especificado en el **paso 3**.
6. Seleccionar el “application pool” creado en el **paso 2** y especificar la cuenta con la que va a correr el servicio.
(Esta cuenta debe tener acceso a la base de datos.)



7. Seleccionar el menú “Authentication” y activar a opción seguridad integrada.



Name	Status	Response Type
Anonymous Authentication	Disabled	
ASP.NET Impersonation	Disabled	
Basic Authentication	Disabled	HTTP 401 Challenge
Digest Authentication	Disabled	HTTP 401 Challenge
Forms Authentication	Disabled	HTTP 302 login/Redirect
Windows Authentication	Enabled	HTTP 401 Challenge

8. Editar el archivo **web.config** (Este archivo se encuentra en el directorio seleccionado en el paso 3.).

Se debe especificar:

- La cadena de conexión a la base de datos. (`connectionString`)
- El “owner” de la base de datos. (`dbo`)
- Directorio de logs. El usuario que corre el servicio debe tener permisos de escritura sobre este directorio. (`log_path`)

```
<configuration>
  <appSettings>
    <add key="webpages:Version" value="3.0.0.0" />
    <add key="webpages:Enabled" value="false" />
    <add key="ClientValidationEnabled" value="true" />
    <add key="UnobtrusiveJavaScriptEnabled" value="true" />
    <add key="dbo" value="dbo" />
    <add key="log_path" value="C:\raiden logs" />
  </appSettings>
  <connectionStrings>
    <add name="main" connectionString="server=HOST\INSTANCE;Database=DB;trusted connection=TRUE" />
  </connectionStrings>
</configuration>
```

9. Reiniciar el sitio web. Haciendo click derecho en el ítem del sitio.

10. Verificar en el directorio de logs que se genere correctamente los archivos **.log**:



11. Verificar que el servicio este funcionando correctamente accediendo a:

[http://\[host\]:\[port\]/operaciones/status](http://[host]:[port]/operaciones/status)

12. Verificar que el sitio tenga acceso a la base de datos accediendo

[http://\[host\]:\[port\]/operaciones/var?cod=ABIERTO](http://[host]:[port]/operaciones/var?cod=ABIERTO)

13. Probar el webhook emitiendo un POST request contra el método **informar**. Este es el método de la API que se debe usar desde Raiden para informarle sus operaciones a FPA.

A continuación, se pude ver un ejemplo sobre como emitir el POST request utilizando CURL:

```
curl --ntlm -u : -X POST -d '{ "idRaiden" : "RDN00001" }' http://\[host\]:\[port\]/operaciones/informar
```

Si el StatusCode de la respuesta es 200 o 400, el webhook está funcionando correctamente.

También se puede utilizar otras herramientas como Fiddler o Postman.

Otra opción es acceder a [http://\[host\]:\[port\]/operaciones/formulario](http://[host]:[port]/operaciones/formulario) desde el navegador.

En esta página se muestra un formulario HTML que realiza la llamada al webhook a través de javascript.