Integración OKTA

Control de versiones

Versión	Fecha de modificación	Responsable	Aprobador	Resumen de cambios
1.0	22/11/2023	Anjana Producto	Anjana Producto	Creación del documento. Compatibilidad con la v4.5 de todos los módulos de Anjana

Modelo de integración

Autenticación

La funcionalidad está directamente embebida en el microservicio de gestión de autenticación y autorización Zeus, se habilita y configura mediante el fichero de configuración de dicho microservicio.

Configuración de autenticación

En la propiedad *security.authentication.oidc.providers* se configuran los distintos proveedores de autenticación que se utilizan. En el caso de OKTA es necesario completar las siguientes propiedades:

1. Nombre del proveedor.
2. URL de autorización: Endpoint del servidor de autorización de la organización de Okta.
3. URL de autorización para el frontal de Anjana Data.
4. URL del token de acceso: token para el servidor de autorización de la organización de Okta.
5. Scopes: Incluye los ámbitos que le permiten realizar las acciones en el endpoint al que desea acceder. Ese ámbito ya debe existir en la colección de permisos de la aplicación y el usuario debe tener el permiso para realizar esas acciones.
6. ID de cliente: se utiliza el client_id de la aplicación Okta OAuth 2.0 que se crea cuando se registra la aplicación en la organización de Okta (Se muestra en el siguiente apartado Requerimientos).
7. Secreto del cliente: se utiliza el client_secret de la aplicación Okta OAuth 2.0 que se crea cuando se registra la aplicación en la organización de Okta.
8. Método de autenticación utilizado al autenticar al cliente con el servidor de autorización.
9. URI de redirección de inicio de sesión.
10. URI de redirección de inicio de sesión para el frontal de Anjana Data.
11. El username-claim es una propiedad custom, en este caso la dirección de correo electrónico, que se puede agregar a un token de acceso si así se desea y usarla para identificar al usuario de manera única.
12. El tipo de proveedor de autenticación de OAuth externo.

```
security:
  authentication:
    oidc:
      providers:
        okta:
          name: OKTA
          authorize-url:
https://anjanadata.okta.com/oauth2/default/v1/authorize?client_id=${s
ecurity.authentication.oidc.providers.okta.client-id}&response_type=c
ode&response_mode=query&scope=${security.authentication.oidc.provider
s.okta.scopes}&redirect_uri=${security.authentication.oidc.providers.
okta.redirect-uri}
          authorize-url-portuno:
https://anjanadata.okta.com/oauth2/default/v1/authorize?client_id=${s
ecurity.authentication.oidc.providers.okta.client-id}&response_type=c
```

```
ode&response_mode=query&scope=${security.authentication.oidc.providers.okta.scopes}&redirect_uri=${security.authentication.oidc.providers.okta.redirect-uri-portuno}
          token-url:
https://anjanadata.okta.com/oauth2/default/v1/token
          scopes: openid profile email
          client-id: 05asd1f5agfsa5g14a5g
          client-secret: ASDGQ2352kjkljjgkjjgkjglGADSG-AnGiajP
          client-authentication-method: POST
          redirect-uri: https://localhost:8443/anjana/authorized
          redirect-uri-portuno:
https://localhost:8443/anjana/authorized
          username-claim: email
          type: OKTA
```

Requerimientos

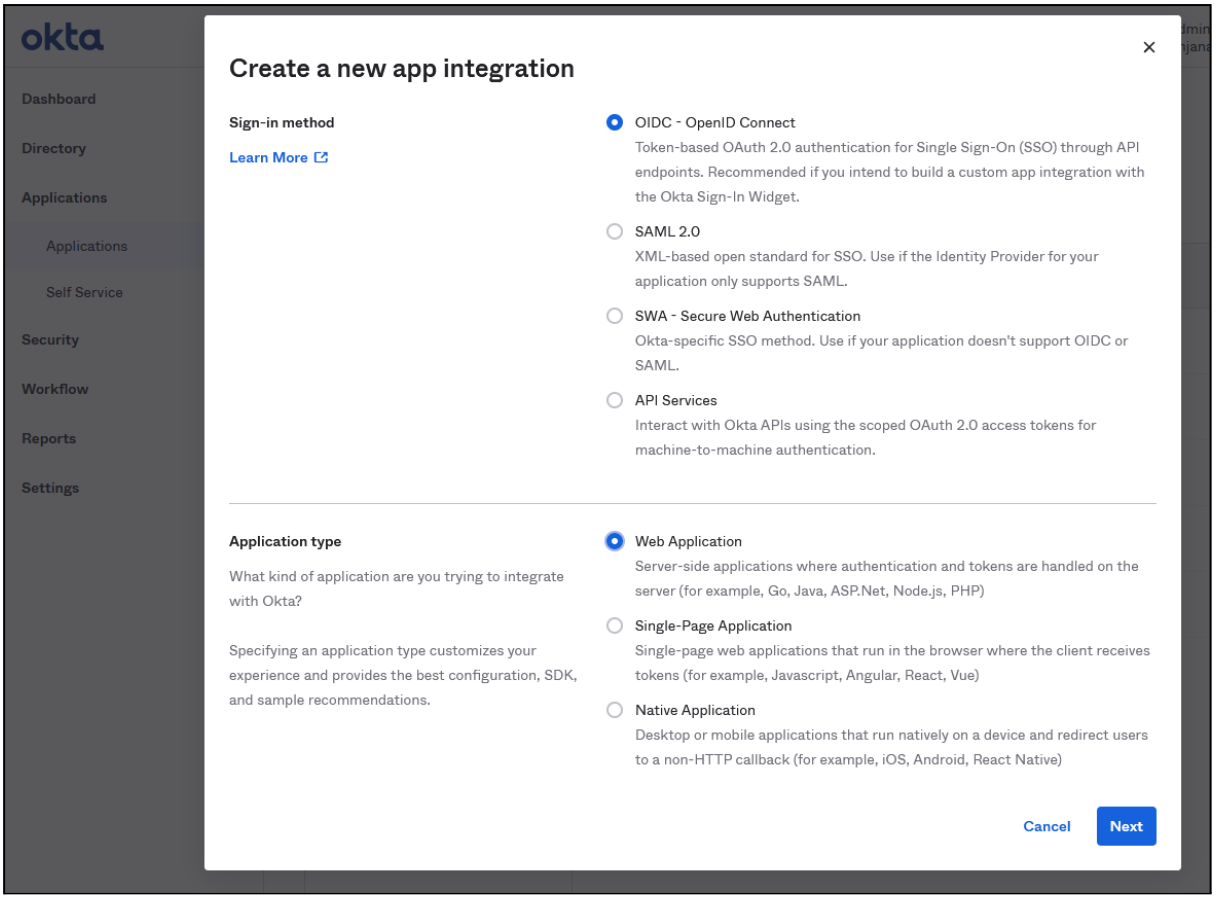
Registro de aplicación

La funcionalidad está directamente embebida en el microservicio de gestión de autenticación y autorización Zeus, se habilita y configura mediante el fichero de configuración de dicho microservicio.

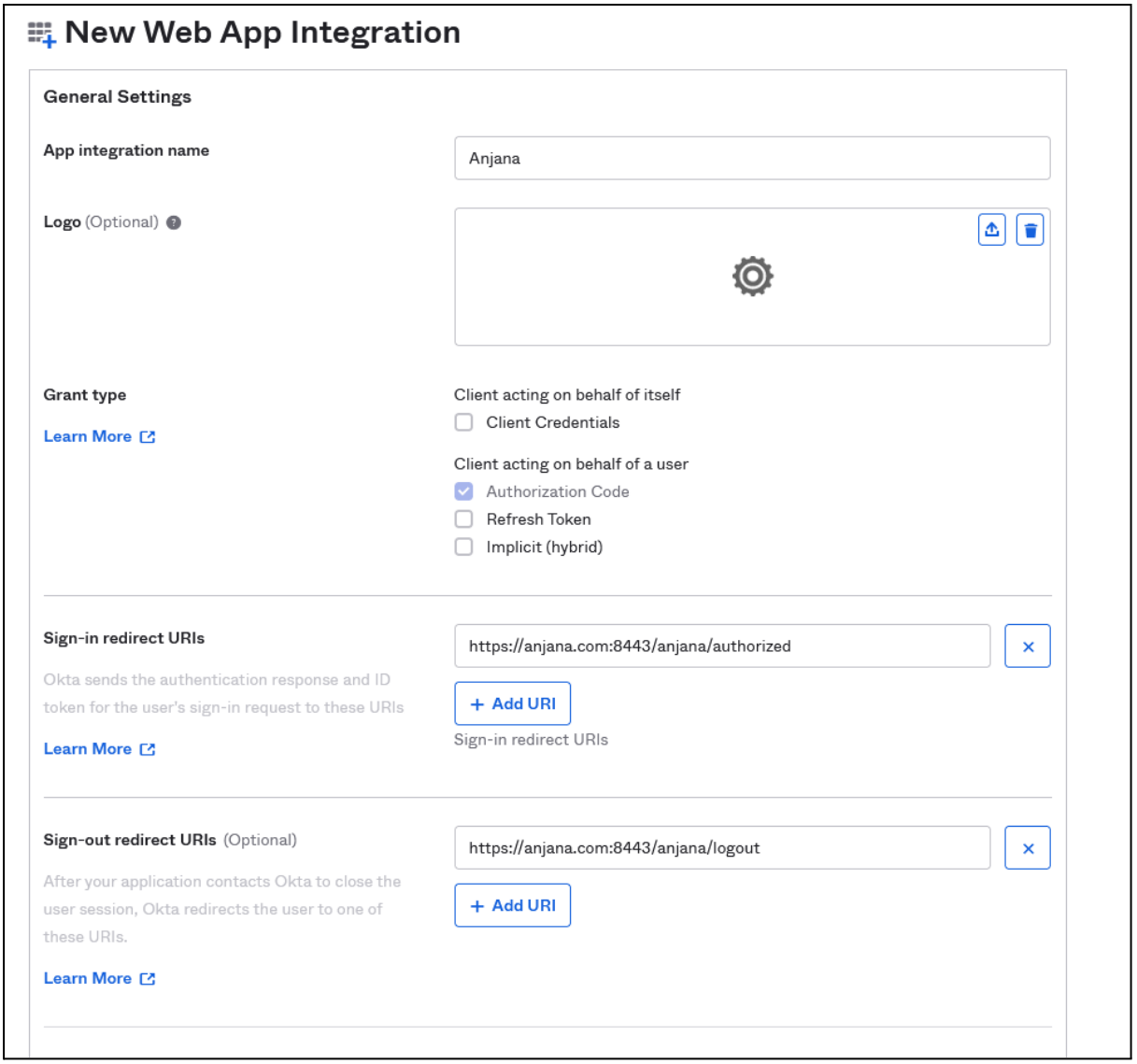
A continuación, se muestra como crear una integración de Okta para Anjana Data. Una integración representa la aplicación en la organización de Okta. La integración incluye información de configuración requerida por Anjana para acceder a Okta.

Para configurar la integración manualmente una vez dentro de la organización Okta es necesario:

1. Clicar en Crear integración de aplicaciones.
2. Seleccionar un método de inicio de sesión de OIDC-OpenID Connect.
3. Seleccionar un tipo de aplicación web (Nota: si se elige un tipo incorrecto de aplicación puede interrumpir los flujos de inicio o cierre de sesión al requerir la verificación de un client-secret, algo que los clientes públicos no tienen).



4. Ingresar un Nombre de integración de la aplicación (Anjana).
   (Nota: El código de autorización se selecciona como predeterminado y no se puede editar, ya que es un tipo obligatorio para Grant type).
5. Ingresar la URI de redirección de inicio de sesión (Sign-in redirect URIs): https://<host>:<port>/anjana/authorized
6. Ingresar la URI de redirección de cierre de sesión (Sign-out redirect URIs): https://<host>:<port>/anjana/logout


New Web App Integration
General Settings
App integration name
Anjana
Logo (Optional)
Grant type
Learn More
Client acting on behalf of itself
Client Credentials
Client acting on behalf of a user
Authorization Code
Refresh Token
Implicit (hybrid)
Sign-in redirect URIs
Okta sends the authentication response and ID token for the user's sign-in request to these URIs
Learn More
https://anjana.com:8443/anjana/authorized
+ Add URI
Sign-in redirect URIs
Sign-out redirect URIs (Optional)
After your application contacts Okta to close the user session, Okta redirects the user to one of these URIs.
Learn More
https://anjana.com:8443/anjana/logout
+ Add URI