



Integración OKTA

| | |
|--------------------------------|----------|
| Control de versiones | 2 |
| Modelo de integración | 3 |
| Autenticación | 3 |
| Configuración de autenticación | 3 |
| Requerimientos | 4 |
| Registro de aplicación | 4 |

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
```

```
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: 05asdlf5agfsa5g14a5g
  client-secret: ASDGQ2352kjdkljgkjgkjgkjlGADSG-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

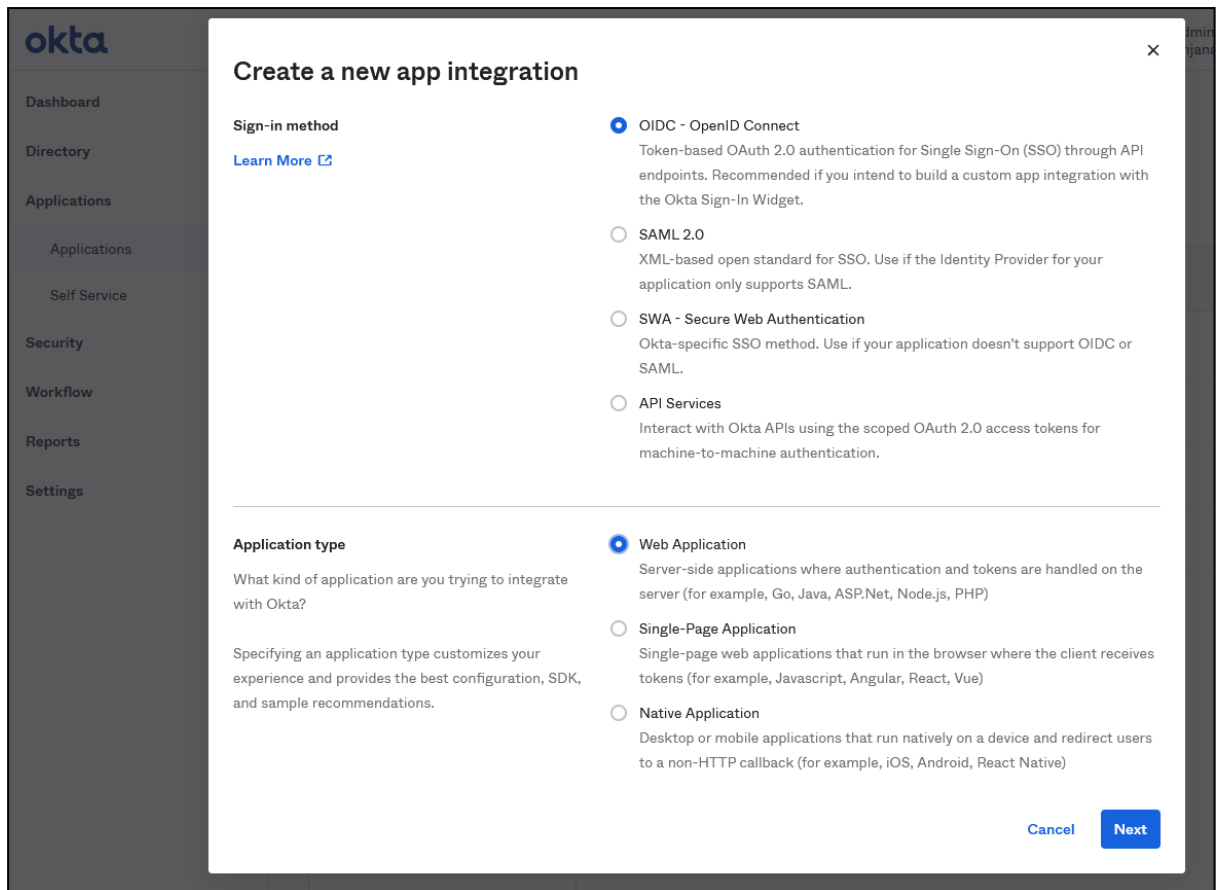
Registro de aplicación

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).



okta

Dashboard

Directory

Applications

Applications

Self Service

Security

Workflow

Reports

Settings

Create a new app integration

Sign-in method

[Learn More](#)

- OIDC - OpenID Connect**
Token-based OAuth 2.0 authentication for Single Sign-On (SSO) through API endpoints. Recommended if you intend to build a custom app integration with the Okta Sign-In Widget.
- SAML 2.0**
XML-based open standard for SSO. Use if the Identity Provider for your application only supports SAML.
- SWA - Secure Web Authentication**
Okta-specific SSO method. Use if your application doesn't support OIDC or SAML.
- API Services**
Interact with Okta APIs using the scoped OAuth 2.0 access tokens for machine-to-machine authentication.

Application type

What kind of application are you trying to integrate with Okta?

Specifying an application type customizes your experience and provides the best configuration, SDK, and sample recommendations.

- Web Application**
Server-side applications where authentication and tokens are handled on the server (for example, Go, Java, ASP.Net, Node.js, PHP)
- Single-Page Application**
Single-page web applications that run in the browser where the client receives tokens (for example, Javascript, Angular, React, Vue)
- Native Application**
Desktop or mobile applications that run natively on a device and redirect users to a non-HTTP callback (for example, iOS, Android, React Native)


[Cancel](#) [Next](#)

- 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).
- Ingresar la URI de redirección de inicio de sesión (Sign-in redirect URIs):
https://<host>:<port>/anjana/authorized
- 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

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](#) 



[+ 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](#) 



[+ Add URI](#)