Autenticación

Todos los datos dentro de la plataforma son privados de forma predeterminada. El rol público se puede configurar para exponer datos sin autenticación, o puede pasar un token de acceso a la API para acceder a datos privados.

Tokens de acceso

Hay tres tipos de tokens que se pueden usar para autenticarse dentro de Catalogo.

1. **El token temporal (JWT)** es devuelto por el punto de conexión/mutación de inicio de sesión. Estos tokens tienen un tiempo de caducidad relativamente corto y, por lo tanto, son la opción más segura de usar. Los tokens se devuelven con un token de actualización que se puede usar para recuperar un nuevo token de acceso a través del punto de conexión o mutación de actualización.
2. **El token de sesión (JWT)** también puede ser devuelto por el punto de conexión/mutación de inicio de sesión. Los tokens de sesión combinan un token de actualización y un token de acceso en una sola cookie. Estos tokens no deben tener un tiempo de caducidad corto como los tokens temporales, ya que no se pueden actualizar después de que hayan caducado.
3. **El token estático** se puede configurar para cada usuario de la plataforma y nunca caducan. Son menos seguros, pero bastante útiles para la comunicación de servidor a servidor.

Una vez que tenga su token de acceso, hay tres formas de pasarlo a la API: en el encabezado o header `Authorization` de la solicitud, como **cookie de sesión** o a través del parámetro `access_token` de consulta.

Encabezado de autorización

```
Authorization: Bearer <token>
```

Cookie de sesión

```
Cookie: directus_session_token=<token>
```

Parámetro de consulta

```
?access_token=<token>
```

> ADVERTENCIA
>
> La opción de parámetro de consulta no se recomienda en las configuraciones de producción, ya que varios sistemas pueden registrar los parámetros.

Iniciar sesión

Autenticarse como usuario.

Request

```
POST /auth/login
{
"email": user_email,
"password": user_password
}
```

Cuerpo de la solicitud

- `email`: Dirección de correo electrónico requerida del usuario.
- `password`: Contraseña requerida del usuario.
- `otp`: La contraseña de un solo uso del usuario (si MFA está habilitada).
- `mode`: Si se va a recuperar el token de actualización en la respuesta JSON o en una cookie `httpOnly`. Uno de `json`, `cookie` o `session`. El valor predeterminado es `json`.

Respuesta

- `access_token` **string**: Token de acceso temporal que se usará en las solicitudes de seguimiento. Nota: si lo usaste como modo en la solicitud, el token de acceso no se devolverá en el JSON.session
- `expires` **integer**: Cuánto tiempo pasará antes de que caduque el token de acceso. El valor se expresa en milisegundos.
- `refresh_token` **string**: El token que se puede usar para recuperar un nuevo token de acceso a través de /auth/refresh. Nota: si usaste `cookie` o `session` como el modo en la solicitud, el token de actualización no se devolverá en el JSON.

> Tiempo de caducidad
>
> El tiempo de caducidad del token se puede configurar a través de la variable de entorno ACCESS_TOKEN_TTL.

Ejemplo

```
POST /auth/login
{
"email": "admin@example.com",
"password": "c4t4l0g0"
}
```

Actualizar token

Recupere un nuevo token de acceso mediante un token de actualización.

Request

```
POST /auth/refresh
{
"refresh_token": refresh_token_string,
"mode": refresh_mode
}
```

Cuerpo de la solicitud

- `refresh_token`: El token de actualización que se va a usar. Si tiene el token de actualización en una cookie a través de `/auth/login`, no es necesario que lo envíe aquí.
- `mode`: Si se debe enviar y recuperar el token de actualización en la respuesta JSON o en una cookie `httpOnly`. Uno de `json`, `cookie` o `session`.

Respuesta

- `access_token` **string**: Token de acceso temporal que se usará en las solicitudes de seguimiento. Nota: si lo usaste como modo en la solicitud, el token de acceso no se devolverá en el JSON.session
- `expires` **integer**: Cuánto tiempo pasará antes de que caduque el token de acceso. El valor se expresa en milisegundos.
- `refresh_token` **string**: El token que se puede usar para recuperar un nuevo token de acceso a través de `/auth/refresh`. Nota: si usaste `cookie` o `session` como el modo en la solicitud, el

token de actualización no se devolverá en el JSON.

Ejemplo

```
POST /auth/refresh
{
"refresh_token": "gmPd...8wuB",
"mode": "json"
}
```

Cerrar sesión

Invalide el token de actualización, destruyendo así la sesión del usuario.

Request

```
POST /auth/logout
{
"refresh_token": refresh_token
}
```

Cuerpo de la solicitud

- `refresh_token`: El token de actualización que se va a invalidar. Si tiene el token de actualización en una cookie a través de /auth/login, no es necesario que lo envíe aquí.
- `mode`: Si el token de actualización se envía en la respuesta JSON o en una cookie `httpOnly`. Uno de `json`, `cookie` o `session`.

Ejemplo

```
POST /auth/logout
{
"refresh_token": "gmPd...8wuB",
"mode": "json"
}
```

Solicitar restablecimiento de contraseña

Solicite que se envíe un correo electrónico de restablecimiento de contraseña al usuario determinado.

Request

```
POST /auth/password/request
{
"email": user_email
}
```

Cuerpo de la solicitud

- `email` **Requerido**: Dirección de correo electrónico del usuario para el que solicitas el restablecimiento de contraseña.
- `reset_url`: Proporcione una URL de restablecimiento personalizada a la que le llevará el enlace del correo electrónico. El token de restablecimiento se pasará como parámetro.

Ejemplo

```
POST /auth/password/request
{
"email": "admin@example.com"
}
```

Restablecer una contraseña

La solicitud de un punto de conexión de restablecimiento de contraseña envía un correo electrónico con un vínculo a la aplicación de administración (o a una ruta personalizada) que, a su vez, usa este punto de conexión para permitir que el usuario restablezca su contraseña.

Request

```
POST /auth/password/reset
{
"token": password_reset_token,
"password": password
}
```

Cuerpo de la solicitud

- `token` **Requerido**: Token de restablecimiento de contraseña, tal y como se proporciona en el correo electrónico enviado por el punto de conexión de la solicitud.

- `password` **Requerido**: Nueva contraseña para el usuario.

Ejemplo

```
POST /auth/password/reset
{
"token": "eyJh...KmUk",
"password": "c4t4l0g0"
}
```

Revisión #3
Creado 22 julio 2025 19:03:35 por Luis Matos
Actualizado 24 julio 2025 13:10:27 por Luis Matos