Acceso sin conexión (Offline access)

El acceso sin conexión (Offline access) permite a los clientes obtener nuevos tokens de acceso sin requerir que el usuario vuelva a autenticarse. Es útil para sesiones de larga duración y una mejor experiencia de usuario.

- ¿Qué es el acceso sin conexión (Offline access)?

¿Qué es el acceso sin conexión (Offline access)?

El concepto de acceso sin conexión (offline access) puede variar dependiendo del contexto, nos enfocaremos en las especificaciones de OAuth 2.0 y OpenID Connect (OIDC). En este contexto, el acceso sin conexión permite a los clientes obtener nuevos tokens de acceso (access tokens) usando un token de actualización (refresh token) sin requerir que el usuario vuelva a autenticarse. Esta característica es particularmente útil para sesiones de larga duración y una mejor experiencia de usuario.

Vale la pena señalar que OAuth 2.0 no define el término “acceso sin conexión” explícitamente; solo especifica el uso de tokens de actualización para obtener nuevos tokens de acceso. Sin embargo, el término “acceso sin conexión” (junto con el scope `offline_access`) ha sido ampliamente adoptado en la industria para referirse a esta capacidad, y está oficialmente definido en la especificación OpenID Connect (OIDC) .

¿Cómo funciona el acceso sin conexión (Offline access)?

Para simplificar, usaremos los términos de OAuth 2.0 Solicitud de autorización (Authorization request) y Servidor de autorización (Authorization server) para ilustrar cómo funciona el acceso sin conexión. Sus términos alternativos en OIDC son Solicitud de autenticación (Authentication request) y Proveedor de OpenID (OP) , respectivamente.

Hay dos pasos principales involucrados en usar el acceso sin conexión:

1. **Solicitar acceso sin conexión**: Cuando el Cliente (Client) inicia una autorización (authorization request) al servidor de autorización (authorization server), incluye el scope `offline_access` para solicitar acceso sin conexión. Este scope indica que el cliente desea obtener un token de actualización junto con el token de acceso.

El soporte para acceso sin conexión puede variar entre diferentes servidores de autorización, y el servidor de autorización puede ignorar el scope `offline_access` si no lo admite. Por favor, consulta la documentación del servidor de autorización para asegurar la compatibilidad antes de usar este scope.

2. **Usar el token de actualización**: Una vez que la Concesión de OAuth 2.0 (OAuth 2.0 grant) se complete, el cliente debería recibir un token de actualización (refresh token) junto con el token de acceso (access token) . El cliente puede almacenar el token de actualización de manera segura y usarlo para enviar una solicitud de token (token request) al servidor de autorización para obtener un nuevo token de acceso cuando el token de acceso actual expire.