API access tokens and OAuth clients

Anything that calls the Alchemer Voice API needs an access token. From **Admin > Connections** you can create a personal access token (long-lived, acts as you, for your own scripts and BI tools) or an OAuth client (each user approves your app, for products used by several people or workspaces).

Before you begin

- You need the Manage connections permission, which admins have by default.

Scopes

Scope	Shown as	Grants	Available on
`api:read`	Read from API	Read access to the OData API and MCP server	Personal tokens and OAuth clients
`import`	Import data	Use of the CRM import API	Personal tokens only

A token acts as the user who created or authorised it and works in that one workspace only.

Lifetimes

Item	Value
Personal access token	1 year
OAuth access token	1 day
OAuth refresh token	1 year

Create a personal access token

1. Go to **Admin > Connections** and scroll to **Access tokens**.
2. Open the **Personal tokens** tab and click **Create token**.
3. Enter a **Name**.
4. Tick at least one scope: **Read from API** and/or **Import data**.
5. Click **Generate** and copy the token immediately. It is not shown again. If you lose it, revoke it and create a new one.

Tokens are not renewed automatically: create a new one and swap it into your tool before expiry.

Click **Revoke** to stop a token working. Tokens of a user removed from the workspace are revoked automatically. The Power BI, Microsoft Excel and Clay connection windows each create a personal token, named after the tool, every time you open them.

Create an OAuth client

1. Under **Admin** > **Connections** > **OAuth clients**, click **Create client**.
2. Enter a **Name**. Users see it when asked to approve your app.
3. Enter one or more **Callback URLs**, comma-separated. They must be absolute, use HTTPS (localhost excepted) and contain no credentials.
4. Click **Create**. The client card shows the **Client ID** and **Client Secret**. Click the secret to reveal it.

Open a client later to change its name or callback URLs, or delete it.

Authorisation flow

Alchemer Voice supports the authorisation code flow with refresh tokens, and PKCE for apps that cannot keep a secret. The authorisation and token addresses are shown under your clients.

1. Send the user's browser to the authorisation address with `response_type=code`, your `client_id`, a `redirect_uri` matching one of your callback URLs, a `state` value and `scope=api:read`.
2. The user signs in, reviews the data your app can read, and clicks **Authorize** or **Cancel**.
3. Alchemer Voice redirects to your callback URL with a short-lived code, or an error.
4. Exchange the code at the token address with `grant_type=authorization_code`, the code, client ID, client secret and redirect URI.
5. Call the API with the returned access token as a Bearer token.
6. When it expires, call the token address with `grant_type=refresh_token`, the refresh token, client ID and client secret.

Connected apps

Apps that people have authorised are listed under **Access tokens** > **Third-party connections** with creation date, user and last refresh. Click **Revoke** to cut an app off immediately.

Troubleshooting

Error	Cause

Error	Cause
`401 Unauthorized`	Token missing, expired or revoked. Refresh it or create a new one.
Missing scope	The token lacks the required scope (for example `api:read`).
Callback URL rejected	Must be absolute, HTTPS (localhost excepted), with no credentials.
"An authorization request must request at least one scope"	Add the `scope` parameter to the authorisation request.

Permissions

Managing tokens, OAuth clients and webhooks needs the Manage connections permission, which admins have by default. A token sees only what the user who created or authorised it can see.

If you need help, contact Alchemer Support.

Related Articles