# OAuth 2.0 and OpenID Setup

DEXPRO Core provides shared authentication setup for the DEXPRO apps that call external services. Two setup lists are available: one for OAuth 2.0 client-credentials connections and one for OpenID Connect connections. Both keep secrets in Business Central isolated storage so they are never shown again after entry.

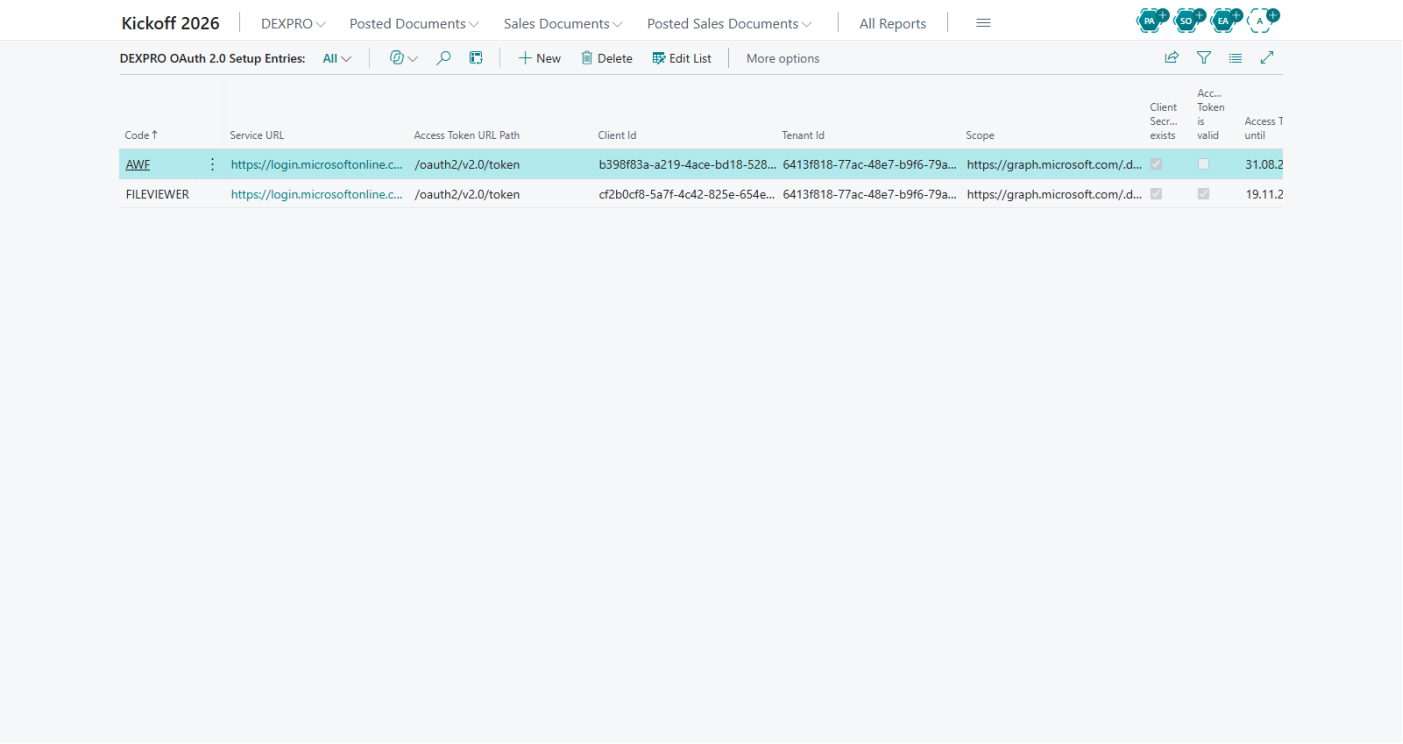
# Purpose

Several DEXPRO features connect to external services — for example the Freeze archive, the SQUEEZE tenant, Digivoice, and Microsoft Graph. These connections need to authenticate. Instead of each app defining its own credentials, Core stores the connection settings centrally and issues the tokens the apps need.

# DEXPRO OAuth 2.0 Setup Entries

The **DEXPRO OAuth 2.0 Setup Entries** page holds client-credentials connections. Each entry defines how Core obtains a token for a given service.

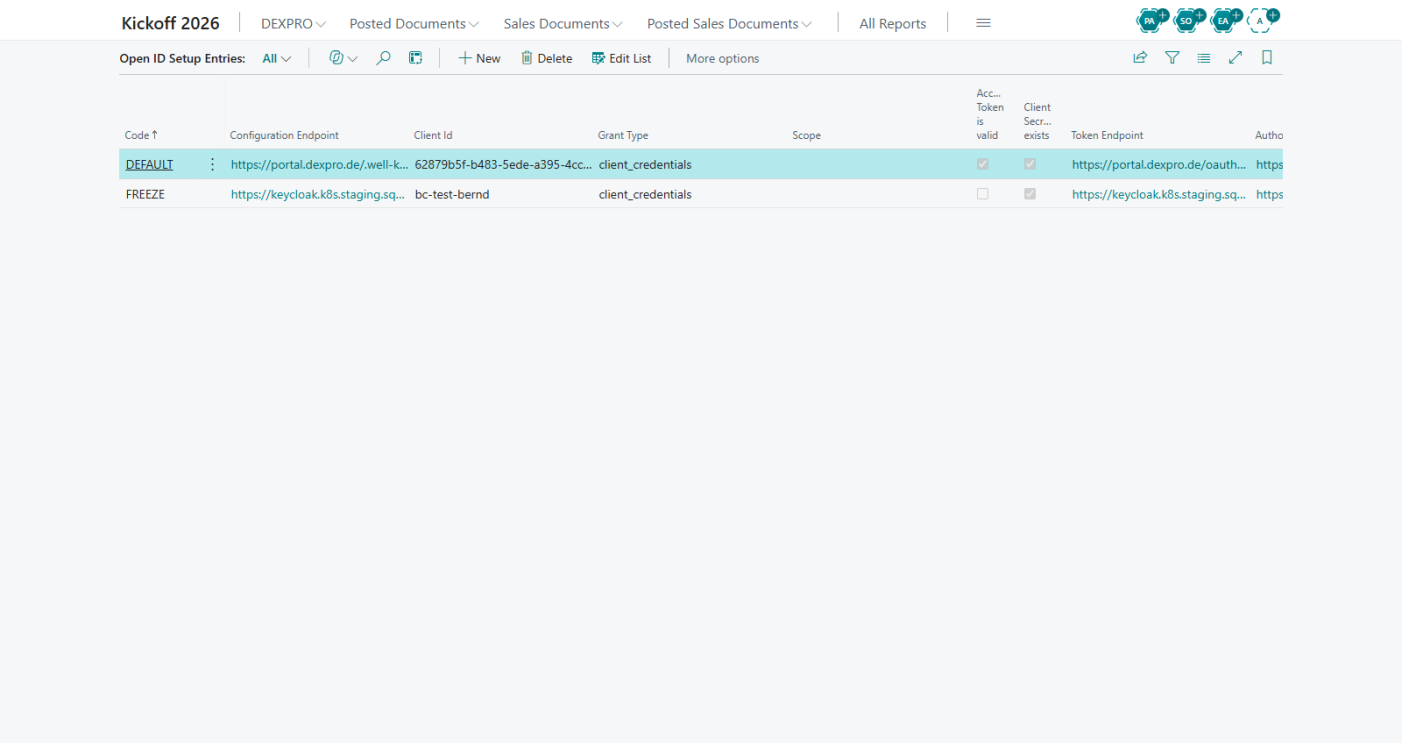
- **Service URL** — the base URL of the service to call.
- **Token Path** — the endpoint used to request an access token.
- **Client ID** — the application (client) identifier.
- **Tenant ID** — the tenant the token is requested for.
- **Scope** — the scope requested for the token.
- **Client Secret** — entered through a dedicated dialog and stored in **isolated storage**.




# Open ID Setup Entries

The **Open ID Setup Entries** page holds OpenID Connect connections.

- **OpenID endpoints** — the OpenID Connect endpoint(s) used for authentication.
- **Client ID** — the application (client) identifier.
- **Grant Type** — the OAuth grant type used.
- **Scope** — the scope requested.
- **Secret and token** — stored in **isolated storage**.




# Entering a secret

Secrets are entered through a dialog and written straight to isolated storage. They are used when Core requests tokens on behalf of the apps.

> For security, secrets are **never displayed again** after they are entered. If a secret changes, re-enter it through the dialog — you cannot read the stored value back from the page.

# Permissions

Of the DEXPRO Core permission sets, only **DEXPRO Core Admin** includes the **DEXPRO OAuth 2.0 Setup Entries** and **Open ID Setup Entries** pages and the dialog for entering a client secret. Only users with this permission set can therefore create, change or delete connections and enter secrets.

**DEXPRO Core User** grants read access to the stored connection settings only. This lets features such as the File Viewer request tokens for regular users without giving them access to the setup pages.

# Prerequisites

- The service you are connecting to must be registered and must provide the client ID, tenant ID (where applicable), scope, secret, and endpoint values.
- For Microsoft Graph connections you need a Microsoft Entra ID app registration (see "File Viewer" and "File Viewer Setup Wizard").

# Related features

- File Viewer
- File Viewer Setup Wizard
- Extensibility

---

Revision #4
Created 2026-07-22 07:21:13 UTC by Bernd Feddersen
Updated 2026-11-19 11:11:38 UTC by Bernd Feddersen