

Configuring Office 365 App Registration and Obtaining an Access Token for OneDrive on Linux

To allow the OneDrive client on Linux to access your Office 365 account, you need to create an Azure AD app registration in the Microsoft Azure portal. This app registration allows OneDrive to securely authenticate with your Office 365 account.

Prerequisites

1. **Microsoft Office 365 Account** with administrative privileges to create app registrations.
2. **Azure AD Access** for configuring app permissions.

Step 1: Create an App Registration in Azure AD

1. **Log in to Azure Portal:** Go to <https://portal.azure.com> and log in with your Office 365 credentials.
2. **Navigate to Azure Active Directory:** In the left sidebar, select **Azure Active Directory**.
3. **Go to App Registrations:** In the **Azure AD** dashboard, select **App registrations** from the sidebar.
4. **Create a New Registration:**
 - Click **New registration**.
 - **Name:** Enter a name, such as `OneDrive Linux Client`.
 - **Supported account types:** Select **Accounts in this organizational directory only**.

- **Redirect URI:** Choose **Web** and enter `http://localhost:53682/`. This is a required field for local testing, but the `onedrive` client will manage redirection internally.
 - Click **Register**.
5. **Copy the Application (Client) ID and Directory (Tenant) ID:** After registration, you'll see the **Overview** page with the **Application (client) ID** and **Directory (tenant) ID**. Copy these values to use later in the OneDrive client configuration.

Step 2: Configure API Permissions

1. **Go to API Permissions:** On your app's **Overview** page, select **API permissions** from the left sidebar.
2. **Add OneDrive API Permissions:**
 - Click **Add a permission**.
 - Select **Microsoft Graph**.
 - Choose **Delegated permissions**.
 - In the permissions search bar, type and select the following permissions:
 - `Files.Read`
 - `Files.ReadWrite`
 - `Files.Read.All`
 - `Files.ReadWrite.All`
 - `offline_access`
 - `User.Read`
 - Click **Add permissions**.
3. **Grant Admin Consent:** After adding the permissions, click **Grant admin consent for [Your Organization Name]**. This will authorize these permissions for all users in your organization. You may need to authenticate again to confirm the consent.

Step 3: Generate the Client Secret

1. **Go to Certificates & Secrets:** In your app's settings, select **Certificates & secrets** from the left sidebar.
2. **Create a New Client Secret:**
 - Under **Client secrets**, click **New client secret**.
 - **Description:** Enter a description, like `OneDrive Token`.
 - **Expires:** Choose the expiration duration (e.g., 6 months, 1 year, or 2 years). Note that you'll need to regenerate this token after it expires.
 - Click **Add**.
3. **Copy the Client Secret Value:** After saving, copy the **Value** of the client secret. This is your **Client Secret**, and you'll need it for the OneDrive client configuration. **Make sure to save it** securely, as it won't be displayed again.

Step 4: Obtain the Authorization Code

The OneDrive client needs an authorization code to generate an access token. To obtain this code:

1. **Construct the Authorization URL:** Replace `[TENANT_ID]`, `[CLIENT_ID]`, and `[REDIRECT_URI]` with your specific details in the URL below:

```
https://login.microsoftonline.com/[TENANT_ID]/oauth2/v2.0/authorize?client_id=[CLIENT_ID]&response_type=code&redirect_uri=[REDIRECT_URI]&response_mode=query&scope=offline_access%20Files.ReadWrite.All%20User.Read
```

- **[TENANT_ID]:** Your Directory (Tenant) ID from Step 1.
- **[CLIENT_ID]:** Your Application (Client) ID from Step 1.
- **[REDIRECT_URI]:** `http://localhost:53682/`.

Example URL (replace with actual IDs):

```
https://login.microsoftonline.com/12345678-1234-1234-1234-123456789abc/oauth2/v2.0/authorize?client_id=abcdefgh-ijkl-mnop-qrst-uvwxyz123456&response_type=code&redirect_uri=http://localhost:53682/&response_mode=query&scope=offline_access%20Files.ReadWrite.All%20User.Read
```

2. **Visit the Authorization URL:** Open this URL in your web browser. Sign in with your Office 365 account if prompted.
3. **Copy the Authorization Code:** After logging in, you'll be redirected to `http://localhost:53682/` with an authorization code in the URL. Copy the code from the URL; it will look something like this:

```
http://localhost:53682/?code=AUTHORIZATION_CODE
```

The `AUTHORIZATION_CODE` is what you need to proceed.

Step 5: Configure the OneDrive Client with OAuth Tokens

1. **Run the OneDrive Client:** Run the following command to configure the OneDrive client:

```
onedrive
```

This will start the interactive setup. If it detects that the client ID and secret are needed, it will prompt you for these.

2. **Provide Client ID, Secret, and Other Details:** Enter the following details when prompted:
 - **Client ID:** The Application (Client) ID you saved earlier.
 - **Client Secret:** The Client Secret you saved earlier.
 - **Tenant ID:** The Directory (Tenant) ID.
 - **Authorization Code:** Paste the authorization code you copied in Step 4.

3. **Test Syncing:** After configuration, test the OneDrive sync by running:

```
onedrive --synchronize
```

This command should successfully authenticate with Office 365 and start syncing your files.

Step 6: Configure the OneDrive Service to Use the New Tokens

To ensure that the OneDrive client uses the new tokens and starts automatically in monitor mode:

1. **Enable the OneDrive Service:** If the service is already set up as shown in the previous guide, simply start it:

```
systemctl --user start onedrive
```

2. **Enable Auto-Start:** If you haven't already, enable the OneDrive client to start on login:

```
systemctl --user enable onedrive
```

3. **Monitor Service Status:** Check the status of the OneDrive service to confirm it's running properly.

```
systemctl --user status onedrive
```

Step 7: Troubleshooting Tips

- **Invalid Token:** If the token expires, repeat the above process to generate a new authorization code.
- **Permissions Error:** Ensure that permissions were granted in Step 2. Check Azure AD's **API Permissions** to verify.
- **Service Fails to Start:** Review logs with `journalctl --user -u onedrive.service -f` to see any specific errors.

Summary

This guide provides a step-by-step solution for configuring Azure AD app registration, obtaining OAuth tokens, and setting up the OneDrive client on Linux to sync with Office 365. By following these steps, you can create a seamless integration between your Linux system and Office 365's OneDrive, enabling continuous file synchronization.

Revision #2

Created 3 November 2024 19:10:27 by Chris Deome

Updated 3 November 2024 19:14:01 by Chris Deome