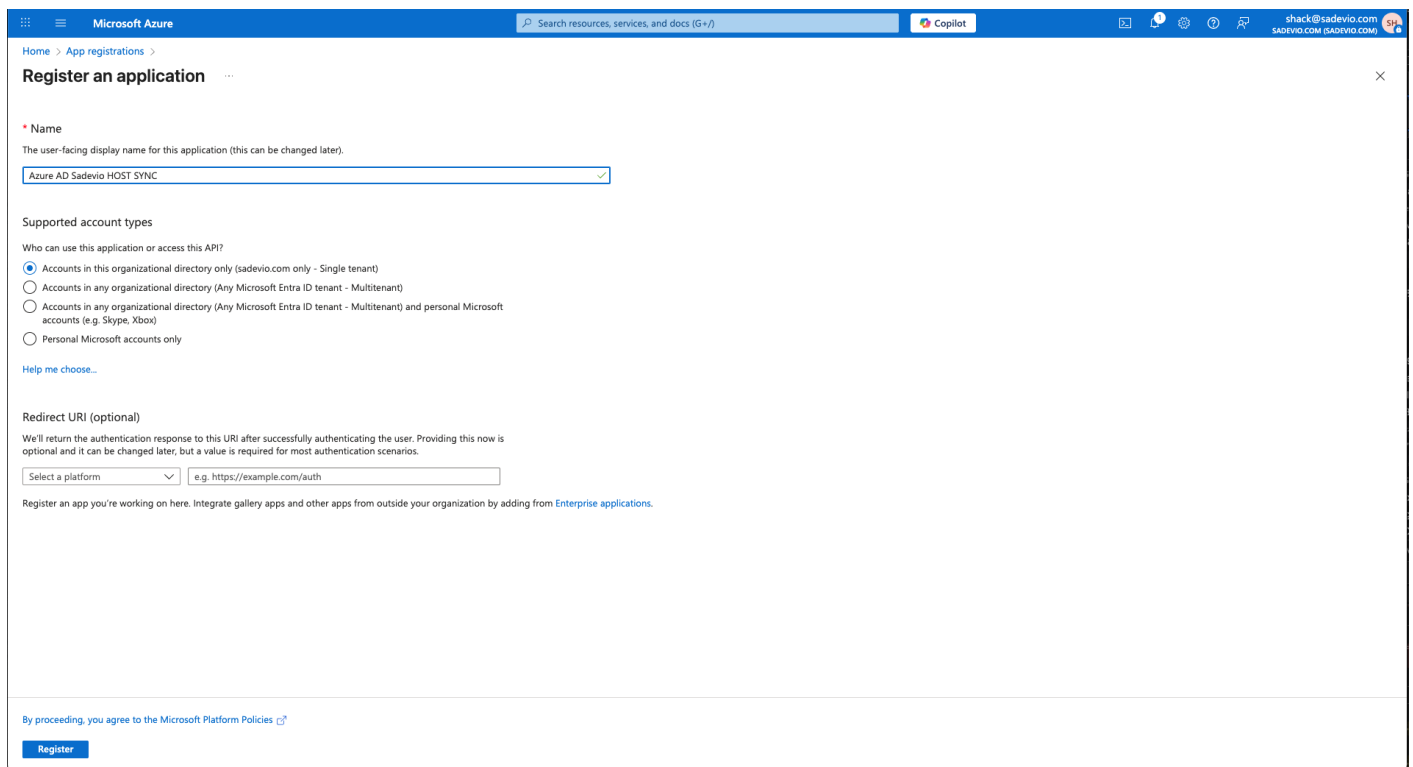


Azure Entra ID (Azure AD) – Employee synchronization

Step 1: Create an Enterprise Application

1. Go to <https://entra.microsoft.com>
2. In the left menu, click "**App registrations**"
3. Click "**+ New registration**"
4. Select "**Create your own application**"
5. Enter a name (e.g.)
6. Click **Register**



The screenshot shows the 'Register an application' page in the Microsoft Azure portal. The page is titled 'Register an application' and is part of the 'App registrations' section. It contains the following fields and options:

- Name:** A text input field containing 'Azure AD Sadevio HOST SYNC'.
- Supported account types:** A section titled 'Who can use this application or access this API?' with four radio button options:
 - Accounts in this organizational directory only (sadevio.com only - Single tenant)
 - Accounts in any organizational directory (Any Microsoft Entra ID tenant - Multitenant)
 - Accounts in any organizational directory (Any Microsoft Entra ID tenant - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox)
 - Personal Microsoft accounts only
- Redirect URI (optional):** A section with a text input field containing 'e.g. https://example.com/auth'.
- Footer:** A blue 'Register' button and a link to 'Microsoft Platform Policies'.

Microsoft Azure | Search resources, services, and docs (G+)

Home > App registrations > Azure AD Sadevio HOST SYNC

Overview | Endpoints | Preview features

Get a second? We would love your feedback on Microsoft identity platform (previously Azure AD for developer). →

Essentials

- Display name: Azure AD Sadevio HOST SYNC
- Application (client) ID: d0211111-1111-1111-1111-111111111111
- Object ID: d183ffa1-e403-4b68-89fd-ce13aab7e6c6
- Directory (tenant) ID: 8b368928-c73b-4f82-80c3-5718b55b7351
- Supported account types: My organization only

Client credentials: Add a certificate or secret
 Redirect URIs: Add a Redirect URI
 Application ID URI: Add an Application ID URI
 Managed application in L: Azure AD Sadevio HOST SYNC

Get Started | Documentation

Build your application with the Microsoft identity platform

The Microsoft identity platform is an authentication service, open-source libraries, and application management tools. You can create modern, standards-based authentication solutions, access and protect APIs, and add sign-in for your users and customers. [Learn more](#)

- Call APIs**
Build more powerful apps with rich user and business data from Microsoft services and your own company's data sources. [View API permissions](#)
- Sign in users in 5 minutes**
Use our SDKs to sign in users and call APIs in a few steps. Use the quickstarts to start a web app, mobile app, SPA, or daemon app. [View all quickstart guides](#)
- Configure for your organization**
Assign users and groups, apply conditional access policies, configure single sign-on, and more in Enterprise applications. [Go to Enterprise applications](#)

1.

Step 2: Client Secret

1. In the new app, go to **"Manage"** -> **"Certificates & secrets"**
2. Select **New client secret**
3. Give it a name which you like and an expiration date.

Microsoft Azure | Search resources, services, and docs (G+)

Home > App registrations > Azure AD Sadevio HOST SYNC

Azure AD Sadevio HOST SYNC | Certificates & secrets

Overview | Quickstart | Integration assistant | Diagnose and solve problems | Manage | Branding & properties | Authentication | Certificates & secrets | Token configuration | API permissions | Expose an API | App roles | Owners | Roles and administrators | Manifest | Support + Troubleshooting

Application registration certificates, secrets and federated credentials can be found in the tabs below.

Certificates (0) | **Client secrets (0)** | Federated credentials (0)

A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

+ New client secret

Description	Expires	Value	Secret ID
No client secrets have been created for this application.			

Add a client secret

Description:

Expires:

Start:

End:

You will need to copy the **"value"** part to **sadevio**.

The screenshot shows the Azure portal interface for an application registration named 'Azure AD Sadevio HOST SYNC'. The left-hand navigation pane is expanded to 'Certificates & secrets'. The main content area shows the 'Client secrets (1)' tab selected. Below the tab, there is a table with the following data:

Description	Expires	Value	Secret ID
Sadevio app secret	10/7/2027	lm48Q-SDkbhM3uE1-wMOURi8eHk8l3...	efaa1c7a-009f-44b6-8beb-383056addfa5

Step 3: Application permissions

1. In the new app, go to **"Manage"** -> **"API permissions"**
2. Select **"Add a permission"**
3. Select Microsoft Graph
4. Select Application permission
5. Add permission **User.Read.All**
6. Select **"Add permission"**

Request API permissions

< All APIs

Microsoft Graph
https://graph.microsoft.com/ Docs

What type of permissions does your application require?

Delegated permissions
Your application needs to access the API as the signed-in user.

Application permissions
Your application runs as a background service or daemon without a signed-in user.

Select permissions expand all

User.Read.All

Permission	Admin consent required
IdentityRiskUser	
User (1)	
<input checked="" type="checkbox"/> User.Read.All Read all users' full profiles	Yes

Add permissions Discard

Add or remove favorites by pressing Ctrl+Shift+F+F

Select now "Grant admin consent for youDomain.com"

Successfully granted admin consent for the requested permissions.

Granting tenant-wide consent may revoke permissions that have already been granted tenant-wide for that application. Permissions that users have already granted on their own behalf aren't affected. [Learn more](#)

The "Admin consent required" column shows the default value for an organization. However, user consent can be customized per permission, user, or app. This column may not reflect the value in your organization, or in organizations where this app will be used. [Learn more](#)

Configured permissions

Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The list of configured permissions should include all the permissions the application needs. [Learn more about permissions and consent](#)

+ Add a permission Grant admin consent for sadevio.com

API / Permissions name	Type	Description	Admin consent required	Status
Microsoft Graph (2)				
User.Read	Delegated	Sign in and read user profile	No	<input checked="" type="checkbox"/> Granted for sadevio.com
User.Read.All	Application	Read all users' full profiles	Yes	<input checked="" type="checkbox"/> Granted for sadevio.com

To view and manage consented permissions for individual apps, as well as your tenant's consent settings, try [Enterprise applications](#).

Add or remove favorites by pressing Ctrl+Shift+F+F

Revision #1

Created 19 January 2026 23:34:43 by Admin

Updated 19 January 2026 23:34:43 by Admin