



[Knowledgebase](#) > [For administrators](#) > [Organisation Administrator](#) > [Sync and user management](#) > [Install the Update Sync from Microsoft Entra ID](#)

Install the Update Sync from Microsoft Entra ID

Gabriel Wallén - 2025-10-10 - [Sync and user management](#)

Installing the Skolon Update Sync from Microsoft Entra ID

This guide will walk you through the process of setting up the Skolon update sync with your Microsoft Entra ID (formerly Azure AD). This secondary sync allows Skolon to fetch data from your Microsoft Entra tenant and use it to update existing users within the Skolon platform.

Important: This update sync requires that your organization either already has a primary synchronization method in place that creates the users in Skolon, or that users have been created through other means. The update sync does not create new users; it only updates existing ones.

How it Works

The Skolon update sync utilizes the Microsoft Graph API to retrieve user information from your Entra ID tenant. Specifically, it uses the following end-point:

GET <https://graph.microsoft.com/v1.0/users>

Attribute Mapping

The table below details how Skolon attributes are mapped to the corresponding attributes in your Microsoft Entra ID. Please note that some mappings can be configured further within the Skolon Data Hub.

Skolon Attribute	Entra Attribute	Comment
External Id	id	
User name	userPrincipalName, mail, otherMails	Can be configured in Skolon Data Hub.
E-mail	mail, otherEmails	Can be configured in Skolon Data Hub.
Idp identifier	userPrincipalName, mail, otherMails, onPremisesImmutableId	Can be configured in Skolon Data Hub.
First name	givenName	
Last name	surname	
City	city	
Address	streetAddress	
Zip code	postalCode	
Birth date	birthday	
Home phone number	mobilePhone	
Mobile phone number	mobilePhone	
EPPN	mail, otherMails, userPrincipalName, extensionAttribute1 - extensionAttribute15	Can be configured in Skolon Data Hub.
SSN	extensionAttribute1 - extensionAttribute15	

Configuration Steps in Microsoft Entra ID

To enable Skolon to securely connect and retrieve data from your Microsoft Entra tenant, you need to register an application within your Entra ID and provide Skolon with its credentials. These credentials will be entered into the Skolon Data Hub when you set up the update sync.

Follow these steps:

1. Register a New Application in Microsoft Entra ID:

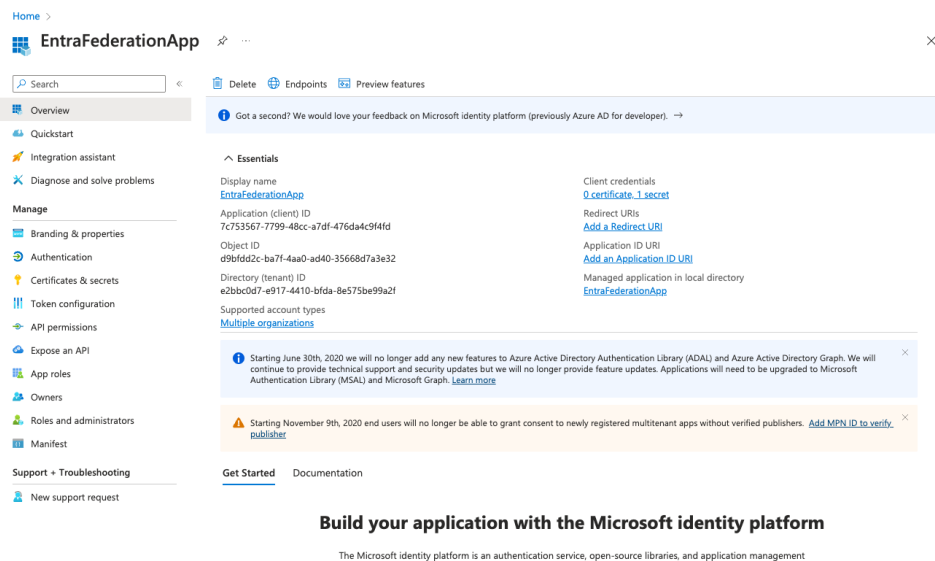
- For detailed instructions on how to register an application, please refer to the official Microsoft documentation: [How to register an app in Microsoft Entra ID - Microsoft identity platform](#)

2. Grant API Permissions:

- Once the application is created, you need to grant it the necessary permissions. The Skolon update sync requires the following permission:
 - **User.Read.All** (Application permission) - This allows the application to read the full profile of all users in your organization.

3. Obtain Application Credentials:

- You will need two pieces of information from the application you created in Microsoft Entra ID to configure the sync in Skolon Data Hub:
 - **Application (client) ID:** This is referred to as "Client Id" in the Skolon Data Hub.

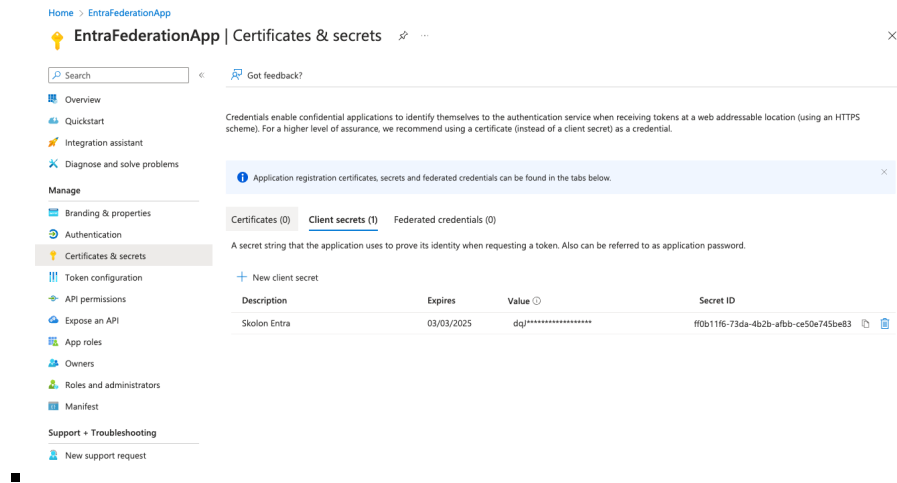


The screenshot shows the 'EntraFederationApp' configuration page in the Azure portal. The left sidebar contains navigation links: Overview, Quickstart, Integration assistant, Diagnose and solve problems, Manage (Branding & properties, Authentication, Certificates & secrets, Token configuration, API permissions, Expose an API, App roles, Owners, Roles and administrators, Manifest), and Support + Troubleshooting. The main content area displays the application's details under the 'Essentials' tab. Key information includes the Display name 'EntraFederationApp', Application (client) ID '7c753567-7799-48cc-a7df-476da4c9f4fd', Object ID 'd9bfdd2c-ba7f-4aa0-ad40-35668d7a3e32', and Directory (tenant) ID 'e2bbc0d7-e917-4410-bfda-8e575be99a2f'. Under 'Client credentials', it shows '0 certificate, 1 secret' and provides links for 'Add a Redirect URI', 'Add an Application ID URI', and 'Managed application in local directory'. Two informational banners are present: one about ADAL and Microsoft Graph deprecation (effective June 30, 2020) and another about the requirement for verified publishers for new multitenant apps (effective November 9, 2020). At the bottom, there are links for 'Get Started' and 'Documentation'.

Build your application with the Microsoft identity platform

The Microsoft identity platform is an authentication service, open-source libraries, and application management

- **Client Secret Value:** This is referred to as "Client Secret" in the Skolon Data Hub. Ensure you copy the **Value** of the client secret, not the Secret ID. **Important:** Client secret values cannot be viewed again after you leave the blade in Azure. Copy the value immediately after creation and store it securely until you can enter it into the Skolon Data Hub.



Configuring the Sync in Skolon Data Hub

Once you have the Application (client) ID and the Client Secret Value from your Microsoft Entra ID application:

1. Log in to the Skolon Data Hub together with your Skolon Representative.
2. Navigate to the section for setting up a new sync or editing an existing one.
3. When prompted, enter the **Application (client) ID** into the "Client Id" field.
4. Enter the **Client Secret Value** into the "Client Secret" field.
5. Complete any additional configuration steps as required within the Skolon Data Hub, such as customizing attribute mappings if needed.

By following these steps, you will successfully install and configure the Skolon update sync from your Microsoft Entra ID, ensuring your user data in Skolon stays up-to-date with your organization's directory. If you encounter any issues, please consult the Skolon support resources or contact our support team.