



## Installing Update Sync from Microsoft Entra ID

Skolon Support - 2025-05-07 - 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.

Home > EntraFederationApp

Search Delete Endpoints Preview features

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

New support request

Essentials

Display name  
EntraFederationApp

Application (client) ID  
7c753567-7799-48cc-a7df-476da4c9f4fd

Object ID  
d9bfdd2c-ba7f-4aa0-ad40-35668d7a3e32

Directory (tenant) ID  
e2bbc0d7-e917-4410-bfda-8e575be99a2f

Supported account types  
Multiple organizations

Client credentials  
0 certificate, 1 secret

Redirect URIs  
Add a Redirect URI

Application ID URI  
Add an Application ID URI

Managed application in local directory  
EntraFederationApp

Starting June 30th, 2020 we will no longer add any new features to Azure Active Directory Authentication Library (ADAL) and Azure Active Directory Graph. We will continue to provide technical support and security updates but we will no longer provide feature updates. Applications will need to be upgraded to Microsoft Authentication Library (MSAL) and Microsoft Graph. [Learn more](#)

Starting November 9th, 2020 end users will no longer be able to grant consent to newly registered multitenant apps without verified publishers. [Add MPN ID to verify publisher](#)

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

- **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.

Home > EntraFederationApp

EntraFederationApp | Certificates & secrets

Search Got feedback?

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

New support request

Credentials enable confidential applications to identify themselves to the authentication service when receiving tokens at a web addressable location (using an HTTPS scheme). For a higher level of assurance, we recommend using a certificate (instead of a client secret) as a credential.

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

Certificates (0) Client secrets (1) 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
Skolon Entra	03/03/2025	dqj*****	f0b11f6-73da-4b2b-afbb-ce50e745be83

## 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.