Install Outgoing Immutable ID-Sync for Microsoft Entra

Skolon Support - 2025-07-14 - Integrations

Installing Skolon's Outgoing Immutable ID-Sync for Microsoft Entra

This guide provides instructions on how to configure and install Skolon's outgoing Immutable ID-sync for your Microsoft Entra environment.

Overview

The Skolon Immutable ID-sync is an **outgoing synchronization service**. This means that Skolon securely connects to your Microsoft Entra tenant and updates the `ImmutableId` attribute for any users which are missing the `ImmutableId` attribute.

Key Features:

- **Automated Updates:** The sync automatically populates the `ImmutableId` for users in your Entra environment based on the configured settings in the Skolon platform.
- **Selective Creation:** It will only create an `ImmutableId` for users who do not already have one. Users with an existing `ImmutableId` will not be affected by this specific sync action.

Background: Why is this sync necessary?

Microsoft Entra requires the `ImmutableId` to be set for users when an external Identity Provider (IdP), like Skolon, is used for sign-in. Skolon developed this integration to streamline the process of updating these `ImmutableIds` in Microsoft Entra for customers that don’t have any `ImmutableIds` set in their environment.

When you federate a domain using the Skolon IdP (Identity Provider), users are authenticated and matched based on their `ImmutableId`. Microsoft Entra does not automatically generate these `ImmutableIds` for users. Therefore, these identifiers typically need to be manually created and aligned with the attributes used in the SAML (Security Assertion Markup Language) assertions for identification.

To simplify this, Skolon provides this outgoing sync. It retrieves a unique attribute from the Skolon database for each user and uses this attribute to create and write the corresponding `ImmutableId` in your Entra environment.

Configuration Steps in Microsoft Entra

For Skolon to successfully connect to your Microsoft Entra tenant and perform the

necessary data fetching and updates, you (the customer) must create an Application Registration within your Azure portal. Skolon will then use the credentials from this application.

You can follow Microsoft's general guidance on how to register an application in Microsoft Entra ID:

- Quickstart: Register an application with the Microsoft identity platform

Once you have initiated the app registration process, ensure the following configurations are set for the application that Skolon will use:

1. **API Permissions:**
    - On the **API permissions** page for your application:
        - Click on **+ Add a permission**.
        - Select **Microsoft Graph**.
        - Choose **Application permissions**.
        - Search for and select `User.ReadWrite.All`.
        - Click **Add permissions**.
        - **Crucially**, after adding the permission, you **must click "Grant admin consent for [Your Organization Name]"** to activate it.
2. **Client Secret:**
    - Navigate to the **Certificates & secrets** page for your registered application.
    - Under "Client secrets," click on **+ New client secret**.
    - Provide a description (e.g., "Skolon Sync Secret") and choose an expiry period. **Note the expiry date, as you will need to renew the secret before it expires to avoid service interruption.** Our recommendation is to set at least 3 years as the expiry period, and put a reminder in the calendar to renew it.
    - Click **Add**.
    - **Immediately copy the "Value" of the client secret.** This is the actual secret key, and it will not be visible again after you leave this page. **Store it securely.**
3. **Collect Necessary IDs:**
    - From the **Overview** page of your registered application, you will need to copy the following:
        - **Application (client) ID**: This will be referred to as the "Client Id" in

the Skolon Data Hub.

- **Directory (tenant) ID**: This will be referred to as the "Tenant Id" in the Skolon Data Hub.

(As referenced in the initial information, imagine a screenshot here showing where to find the "Application (client) ID" and "Directory (tenant) ID" in the Azure portal's application overview page.)

(And another screenshot here showing the "Value" of the "Client Secret" on the Certificates & secrets page.)

Configuring the Sync in Skolon Data Hub
Once you have the:

- Application (client) ID (your "Client Id")
- Directory (tenant) ID (your "Tenant Id")
- Client Secret Value (your "Client Secret")

Your Skolon representative need to enter these credentials into the Skolon Data Hub when installing the outgoing Immutable ID-sync

If you have any questions or require assistance during this process, please do not hesitate to contact Skolon support.