Fabasoft Approve

White Paper

IAM Integration

2023 December Release

Contents

1 Overview of the functionality

This app provides the “Microsoft Graph User Import” object and thereby enables the synchronization of the users assigned to Microsoft Azure Active Directory (AD) groups to teams of a Fabasoft Cloud organization by means of a background task. This allows a convenient and continuous synchronization of users between AD and the Fabasoft Cloud. The data in the screenshots in this documentation are blurred for security reasons.

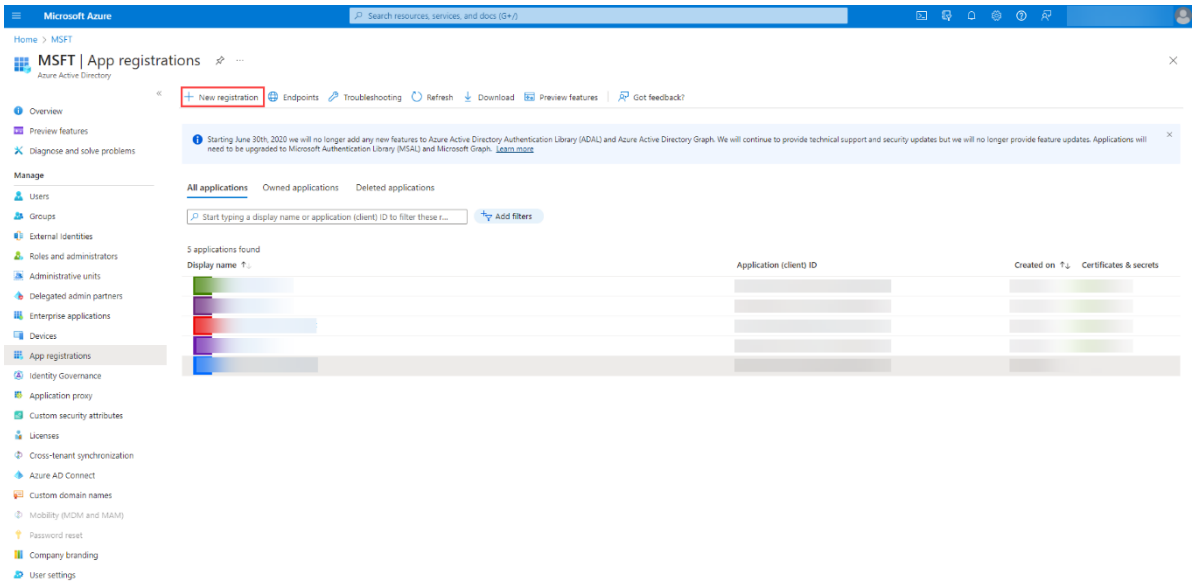
2 General procedure

In this chapter, the general procedure is explained in a concise way to get an overview. The subsequent chapters explain the steps in more detail.

- Registration of application in AD
- Configure Team of organization in Fabasoft Cloud
- Creation of Microsoft Graph User Import object

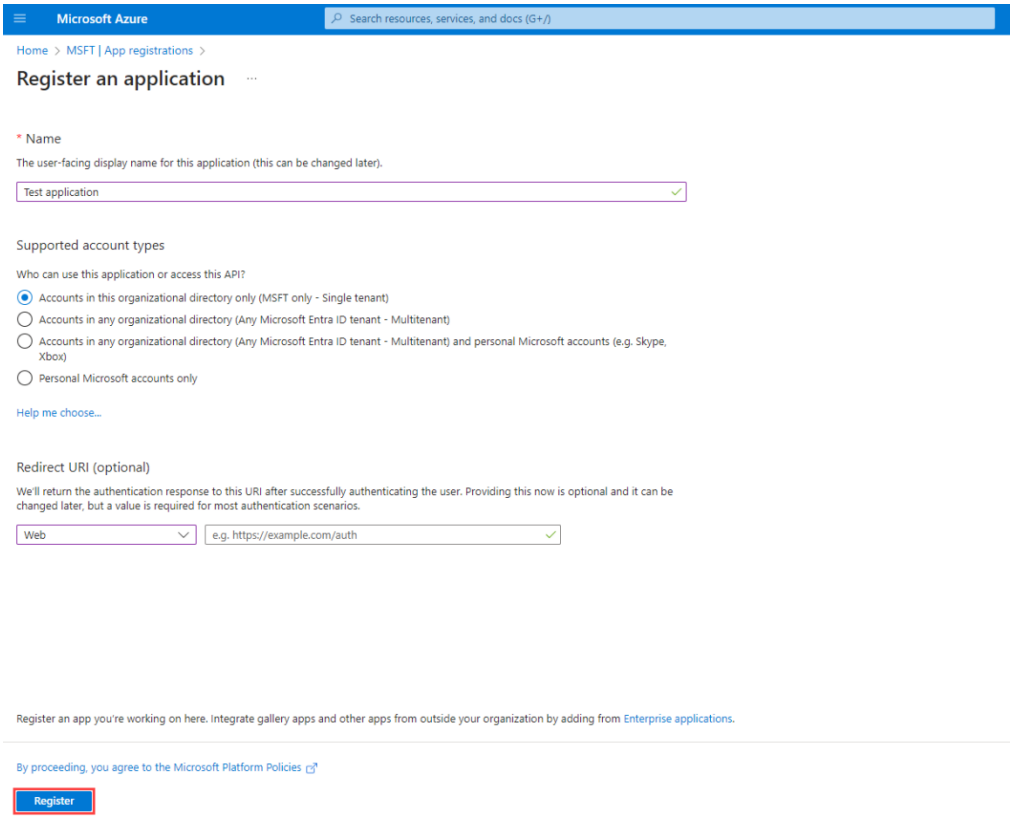
3 Registration of an application in AD

In order to use the Microsoft Graph Toolkit an application has to be registered inside the AD. This application enables the access to resources via OAuth. The registration of an application can be accomplished by clicking the “New registration” button as shown in the following illustration.

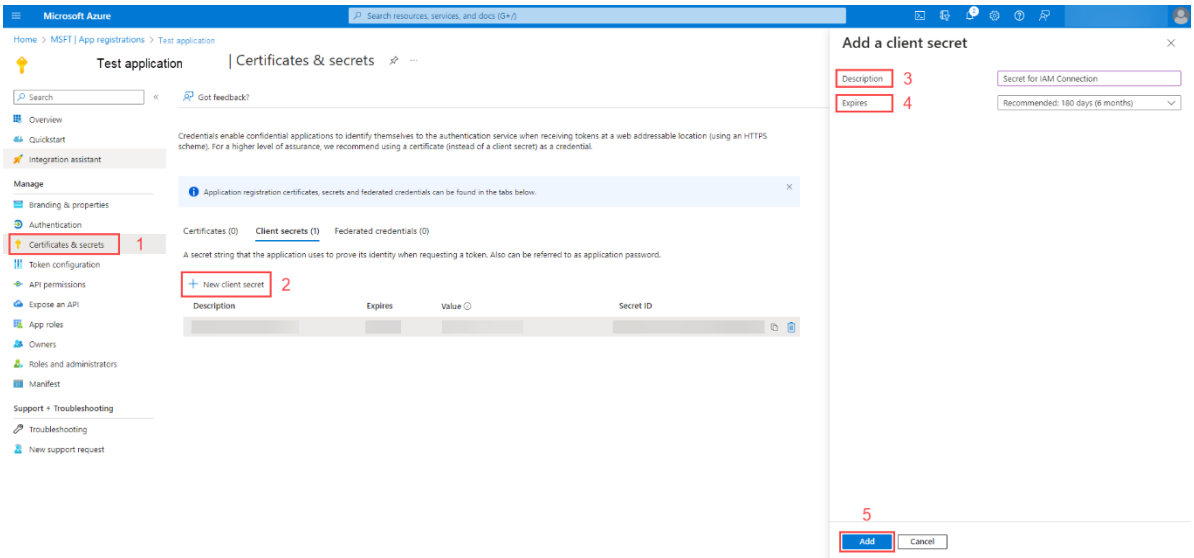


Thereafter a name for the application along with some additional information has to be provided (see the illustration below). For the “Supported account types” the option “Accounts in this organizational directory only (MSFT only - Single tenant)” has to be checked. Moreover, a “Redirect URI (optional)” has to be specified. In the dropdown menu “Web” has to be selected. The

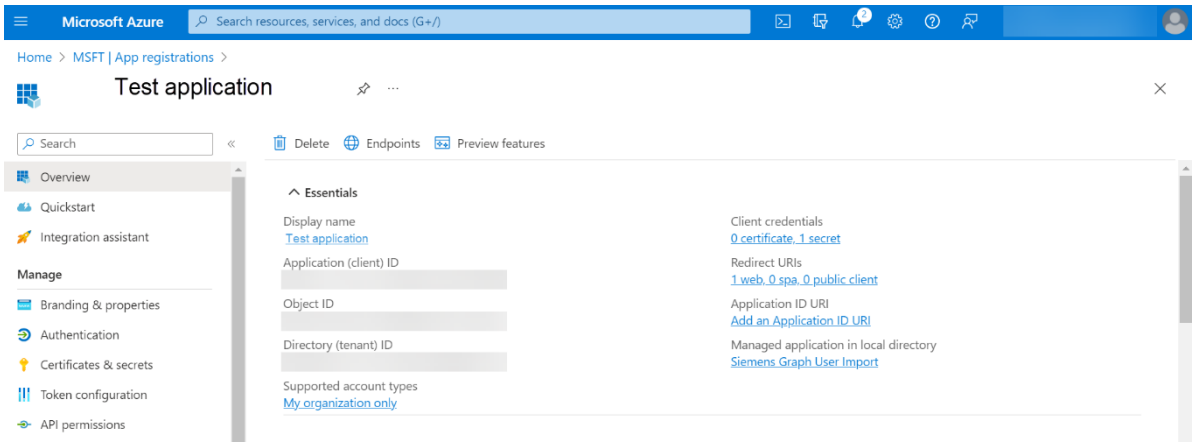
authentication response will be returned to this URI, which has to have the format shown in the following illustration.



If the registration is completed with the marked "Register" button, the application will appear in the list shown above. After the registration of the application, a Client Secret has to be generated. This can be achieved when selecting the application following the marked steps:



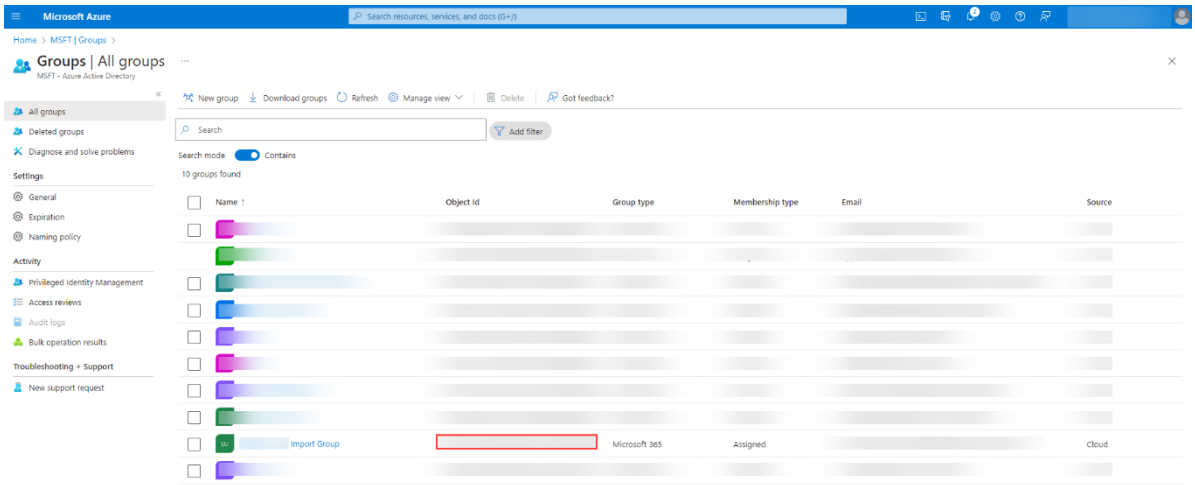
After the creation of the Client Secret, it will appear in the list of Client Secrets. In this view the value of the Client Secret can be found, which will be needed later in this example. The necessary information about the application can be viewed under the menu item "Overview" as shown in the following illustration:



For further information on creating an AD application, consider to follow the following link: [Create an AD application to use with the Microsoft Graph Toolkit]

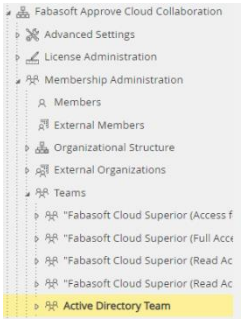
4 Configuration of a team of an organization in Fabasoft Cloud

In next step, the team inside the organization in the Fabasoft Cloud has to be configured. The “Object ID” of the Group in the AD has to be entered as “Import ID” of the respective Team of the organization in the Fabasoft Cloud. The “Object ID” can be obtained in the “Groups | All Groups” menu of the AD as shown here:

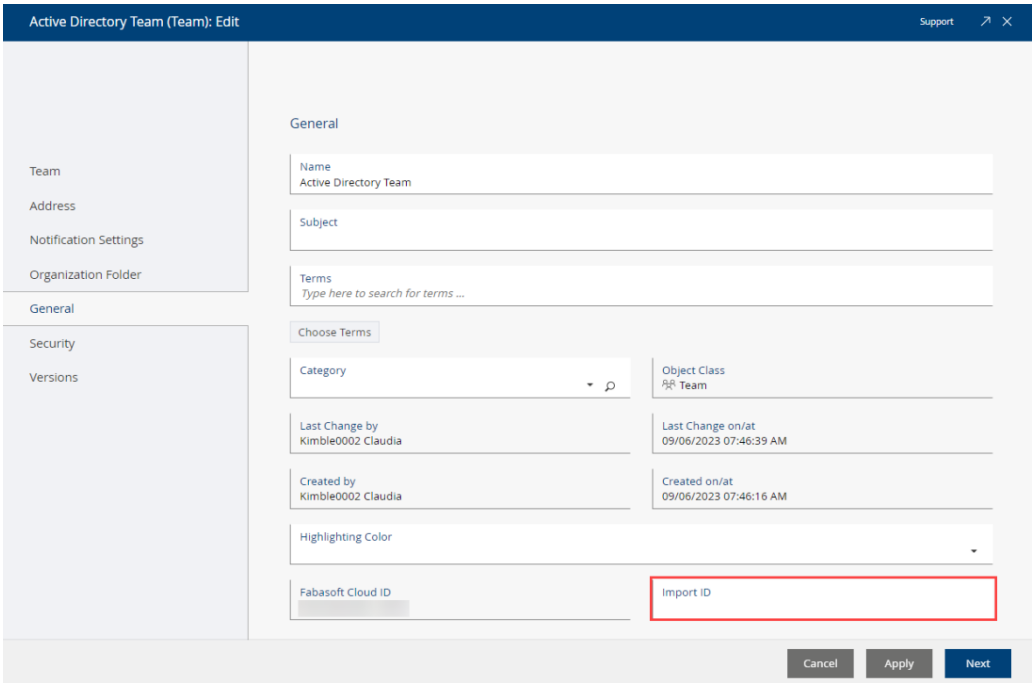


This “Object ID” has to be entered as “Import ID” in the respective team inside the organization in

the Fabasoft Cloud. The team is located inside the organization and can be accessed over the path illustrated in the following illustration.



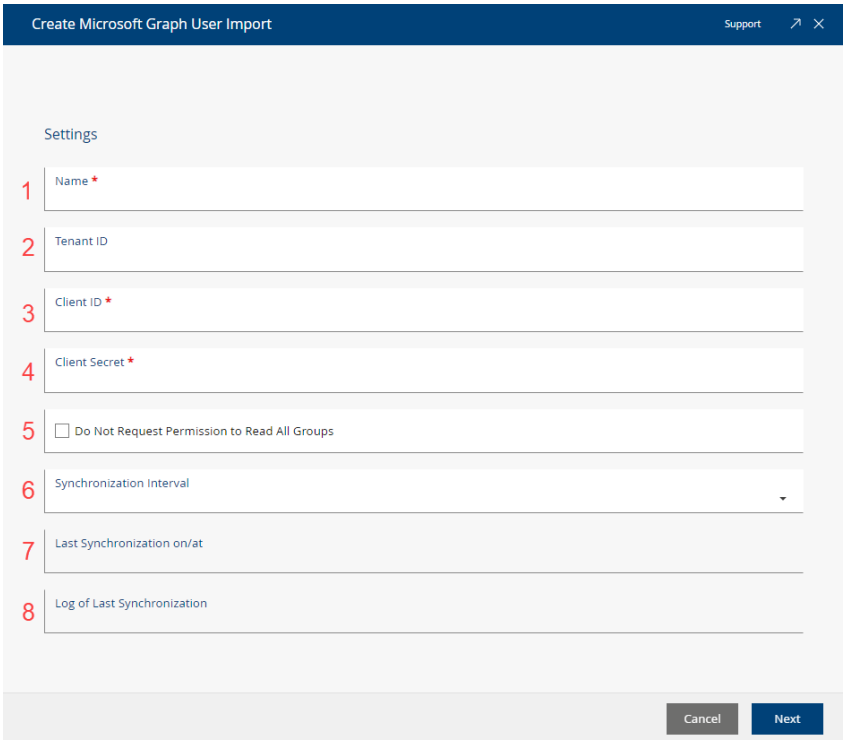
The “Import ID” can be set in the properties of the team on the “General” form page:



5 Microsoft Graph User Import Object

In the last step, a “Microsoft Graph User Import” object has to be created. This object enables the synchronization of the AD users and can be created inside in every room. In order to be able to create this object, the user has to have a “Fabasoft Approve (Full access)” license. In the "Settings"

menu page of the properties of this object, the necessary settings can be defined. Additionally, the settings can be made when creating the object during the registration of an application in the AD.



The following list explains the fields from the illustration above.

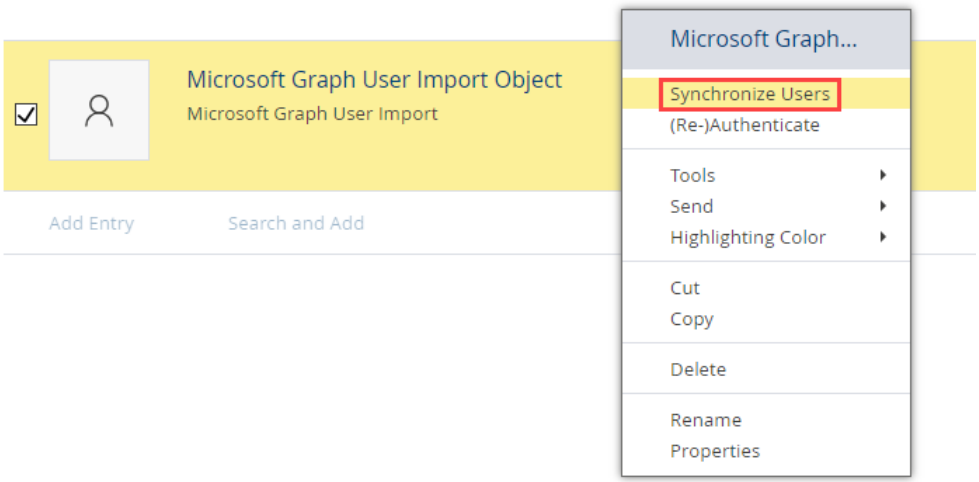
- *Attribute 1 – Name*
  The name of the "Microsoft Graph User Import" object is entered here, which has no influence on the functionality of the user synchronization.
- *Attribute 2 - Tenant ID*
  The Tenant ID is used to specify which users can log in to the application. In this case the "Directory (tenant) ID" must be entered, which can be viewed under the "Overview" menu item in the AD.
- *Attribute 3 - Client ID*
  The "Application (client) ID" shown in "Overview" has to be entered here. This is the unique identifier of the previously generated application and is needed to authenticate for the user synchronization.
- *Attribute 4 - Client Secret*
  This is the secret application key and can be created during the registration of application in AD. It is a secret string used by the application to request an OAuth-token. It is often also referred as "application password". The value (not the ID) of the Client Secret has to be entered in this input field.
- *Attribute 5 - Checkbox "Do Not Request Permission to Read All Groups"*
  By default (if the checkbox is not checked), the "group.read.all" and "offline_access" privileges are requested from Microsoft Azure Active Directory to list all groups, to read their properties and all group memberships on behalf of the signed-in user.
  In certain scenarios, Microsoft Azure Active Directory may prefer to restrict the privileges requested by the application. Therefore, if this checkbox is checked, only the "openid" and "offline_access" privileges are requested from AD. In this case, Microsoft Azure Active Directory

administrators have to take appropriate measures for the application to be allowed to retrieve group membership information and user properties.

- *Attribute 6 - Synchronization Interval*
  In this field the time interval for the automated synchronization can be set. The following intervals are available:
  - 5 Minutes
  - 15 Minutes
  - 30 Minutes
  - 1 Hour
  - 12 Hours
  - 1 Day
- *Attribute 7 - Last Synchronization on/at*
  This field displays the timestamp of the last manually or automatically started synchronization of users.
- *Attribute 8 - Log of Last Synchronization*
  In this log the number of created and updated users as well as the number of updated teams of the last synchronization is displayed.

5.1 Manual Synchronization

This button allows to initiate the synchronization of users manually as shown in the following illustration:



5.2 (Re-)Authenticate

The button "(Re-)Authenticate" is only visible when the Client ID and the Client Secret of the in the "Microsoft Graph User Import" object is set. When clicking this button, the authentication process is started. As a result of this action a new user consent is received. Before the first synchronization,

this button needs to be clicked and the user has to grant the application the permission to access the user information in the access directory.