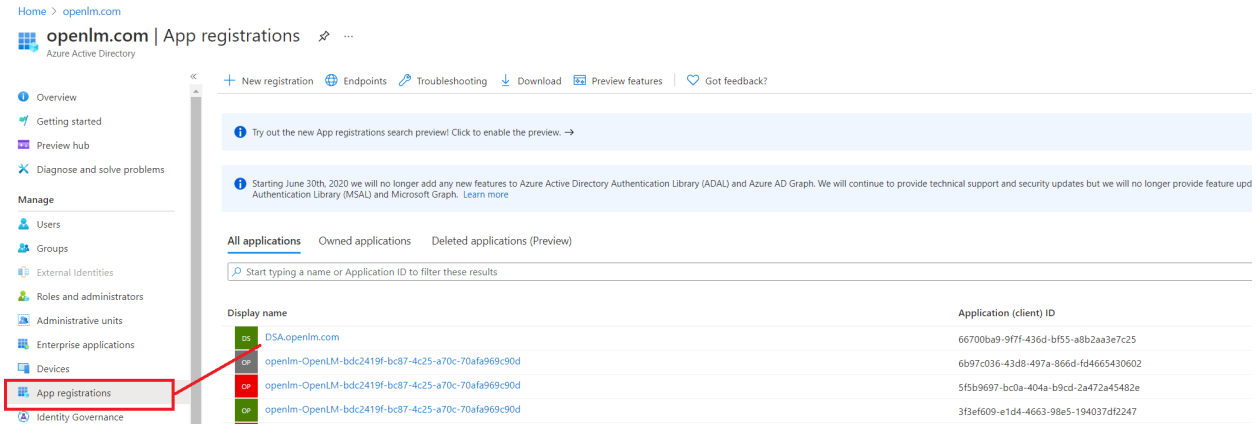
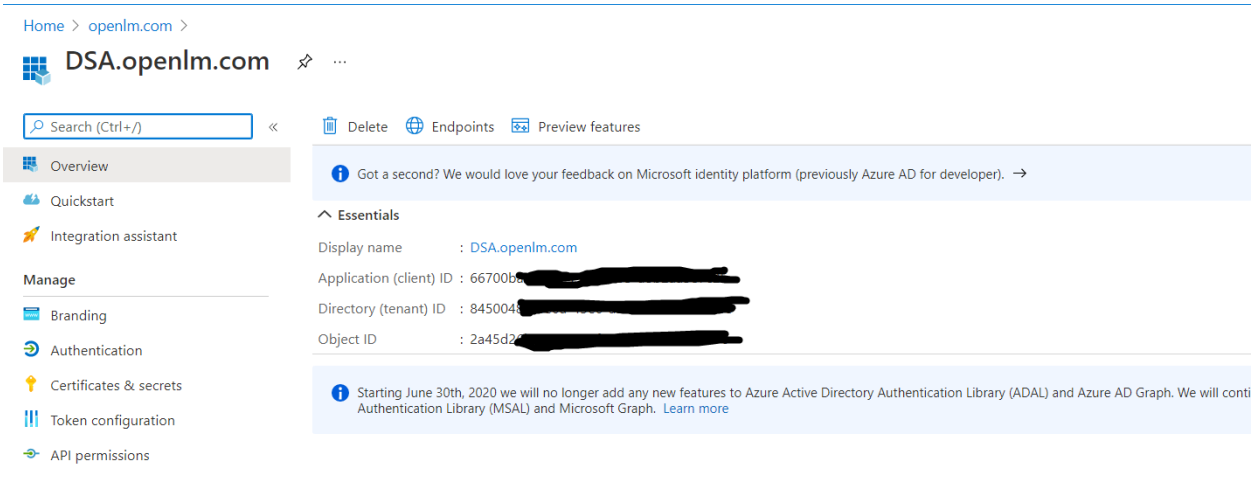
General Flow

We're using Microsoft Graph technology forgetting data from Azure AD, so users will need to make some configuration in the Azure portal:

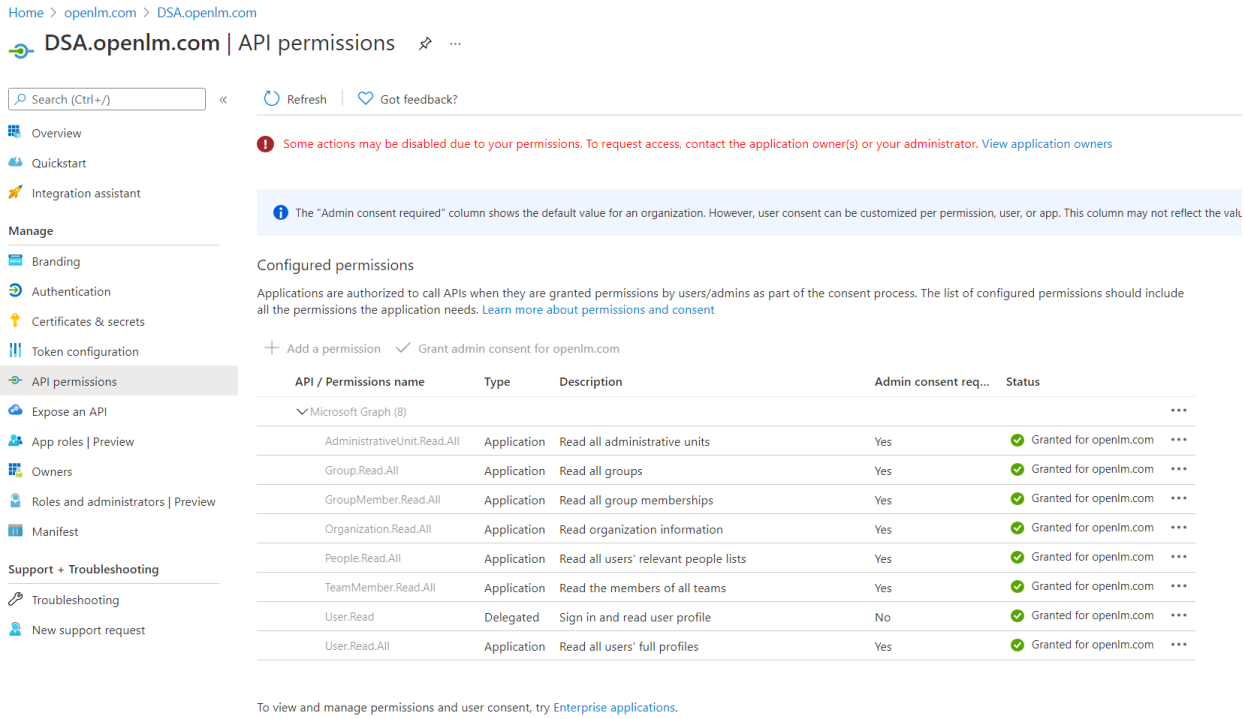
1. Register application, which will be used to grant access for his directory:



2. On registration, the parameters will be displayed: client_id, tenant_id, client_secret. The latest will be displayed only once and should be remembered by the user. These parameters should be passed in DSS UI domain settings for Azure AD (client secret will be encrypted in DSS DB). These parameters will be used by DSA to connect and authorize Microsoft Graph service, which returns data about Azure directory.



3. Permissions for application (in order DSA to be able get data):



Directory Synchronization Azure directory

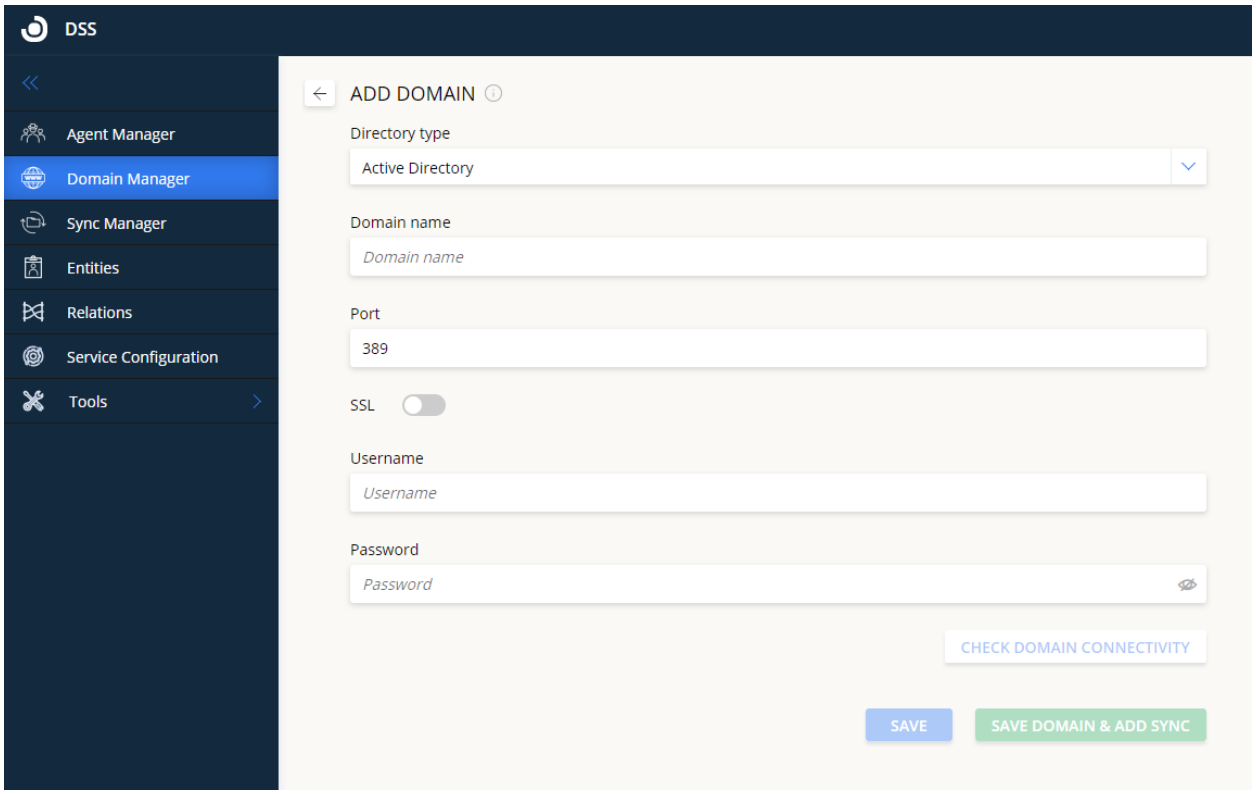
Add Domain

Add to Domain manager screen a new of directory type - Azure Directory

When **selected** update the fields below accordingly

1. Domain Name- free text
2. Directory (tenant) Id - **new**
3. Application (client) Id - **new.**
4. Client secret - **new**

The Application (client) Id And the Client Secret are used for the authentication with the Azure Directory (tenant) Id.



Keep the check domain connectivity and the save buttons...

Sync Configuration

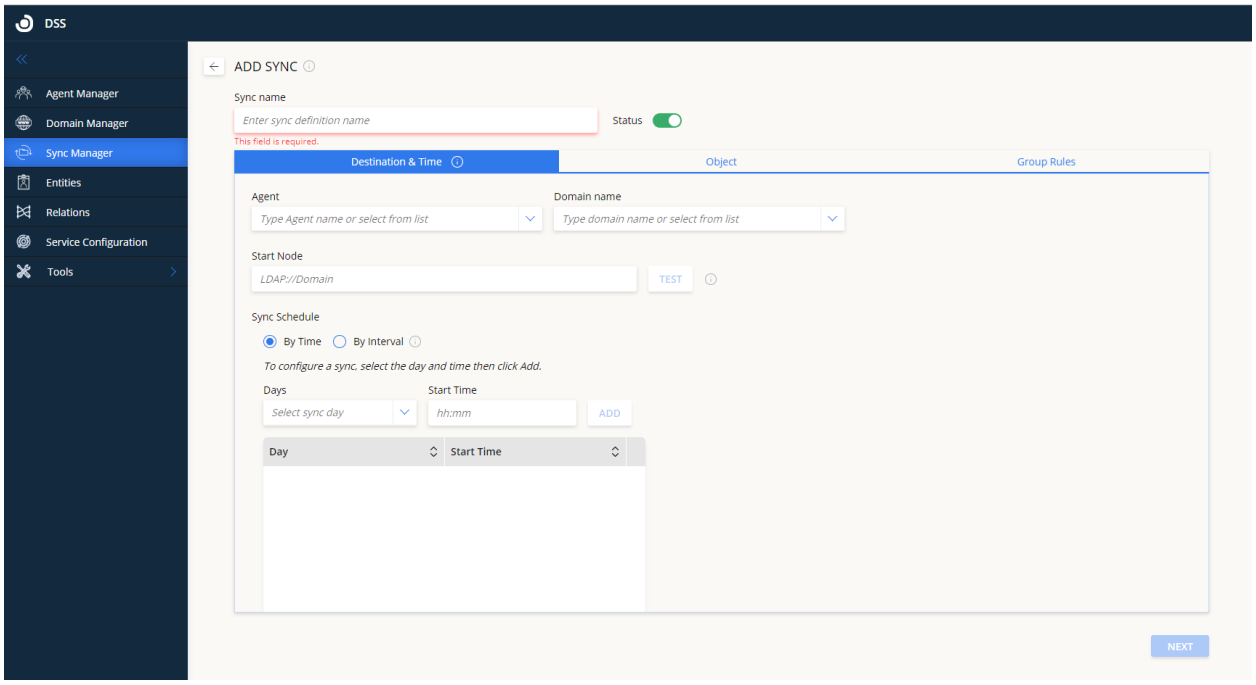
Destination & Time

Start node options: Unlike LDAP Directory the Azure structure is different: User can

1. Leave an empty value - in that case the sync will go through all users and groups (like root option in LDAP)
2. groups/**groupname -** enter the group he would like the sync to start from and synchronize from specific group. Azure groups are all open on the same level and have pointers that indicate which other groups are connected to a group.
   In that case when we use depth it will scan other groups connected to the original start group according to the search depth value was configured. Rename the start node name to Start Sync From.

Update the below text in the Info icon of the destination & time
Start Sync From: defines where the sync will start from. Leave empty to sync all the users and groups in the directory, or specify the group you would like to start from “groups/**groupname”.** Once configured, click Test to make sure the domain is valid (it might take up to 2 minutes for the test to complete)

Inline text: *Leave empty to sync all directory or enter groups/**<group name>** // (only 1 group allowed)*



Object

Object Type

In version 1 Object type “Computers” **is not supported**. Instead Azure AD has devices. But we still have to investigate it. Remove the computers option.
Update the info text of the Object tab **Sync Objects:** configure which objects to sync by (currently only users object is supported)

Sync Attribute

Azure directory default value is UserPrincipalName. Remove the CN and the SAMaccountName from DD list. User should still be able to enter any attribute he would like to sync with (free text)

Membership Filter:

When Azure directory is selected update the DD list to show 2 options

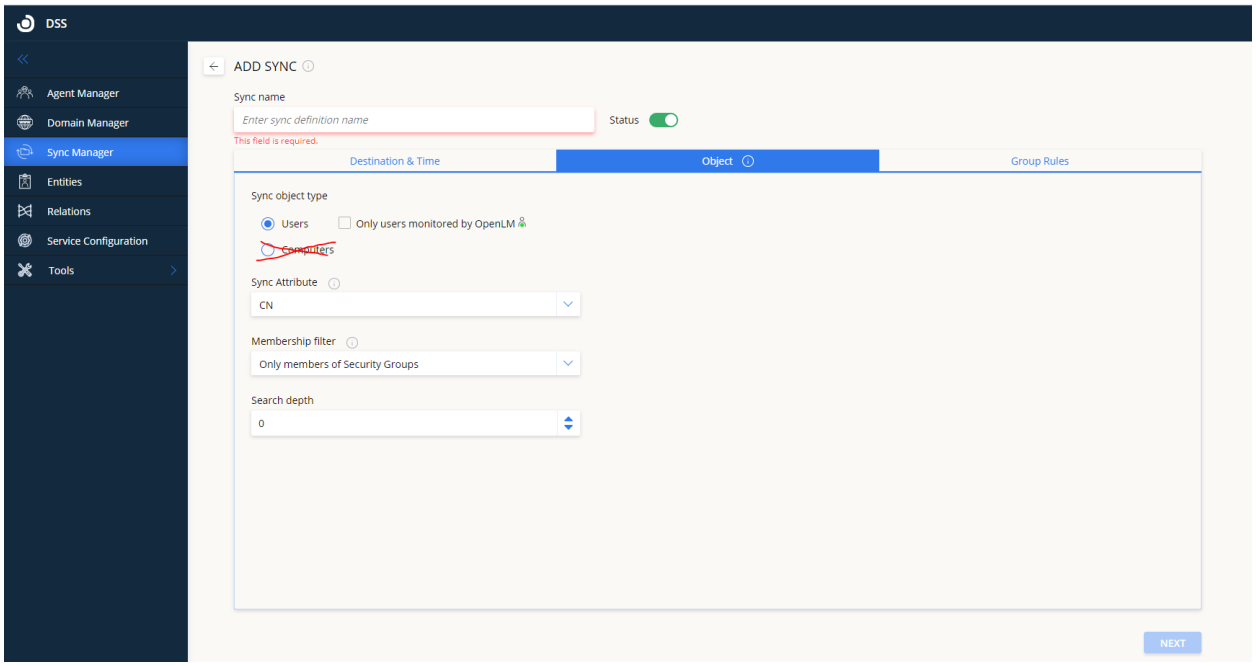
1. All Objects
2. Only members of a group

Azure AD does not have OU and instead it has Administrative units but these units can't hold other Administrative units below them. As for version 1 we won't support it.

Update the info icon of the membership filter (only when Azure Active directory is selected)
Membership filter
Choose whether to sync **all objects** or only those that belong to **a Group.**

Search depth

The Search depth is only relevant when working with "Startnode" of a group.
~~Show the search depth~~ Allow the user to fill out the search depth only when the "Start Sync From" indicates a group, if it's empty, show an error message: "Search depth has to be 0 unless you set the 'Start Sync From' group."



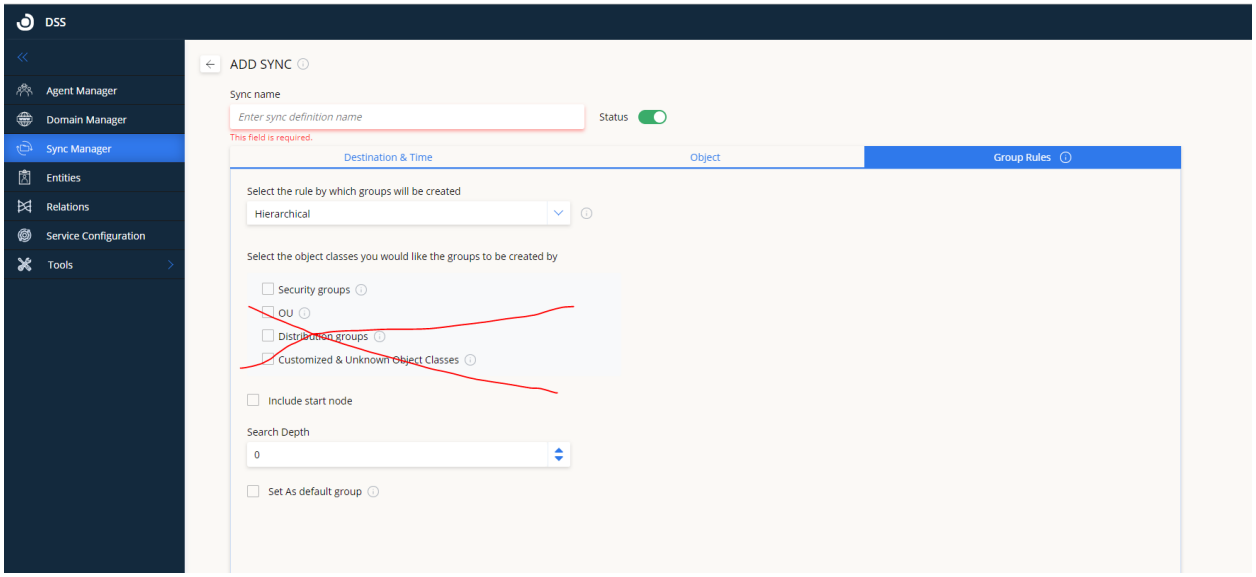
Group Rules

All group rules are supported (same list as in standard LDAP) but the hierarchy synchronization supports only **groups** so no need to have the checkbox selection.
Instead of "Select the object classes you would like the groups to be created by" write "The hierarchical group will be created according to the groups and the search depth specified below."

Remove the rest options (OU, Distribution group, customize & unknown object classes)

Include start node : change to Include start group
Search Depth - can't be higher than the Search depth was selected in the Object screen.
Set a default group - supported

Rename `Include start node` to `Include start group` (will take the users connected to the start group and add them as a Group under the start group name)



Directory sample
The directory has Groups A-E
→ indicate pointer from one group to another

A → B
B → C
C → D
C → A
D → E
E

User list :
Group A - U5, U6
Group B - U7, U8
Group C - U1, U2, U3, U4

Group D - U9, U10
Group E - U11, U12

Hierarchical structure if the sync is configured to sync from Groups\C with search depth of 3 in the group & rules

C--
- A--
  - B--
- D--
  - E

U1
U2
U3
U4
- U5
- U6
  - U7
  - U8
- U9
- U10
  - U11
  - U12