Compano Online Software
voor de bouw- & installatiebranche

Azure Authentication & Provisioning

Compano Online Software

File	COS_Azure_Authentication_And_Provisioning_[version].pdf
COS-version	L07
Date	03/03/26

Content

1 Introduction

This document describes the module Azure Single Sign-on en Provisioning.

From customer demand, the desire arose to be able to sync from a customer-own Active Directory user and groups with the Compano application in order to achieve a single sign-on. Management of users and groups that need access to the Compano application can thus be managed entirely from the customer's own Active Directory.

In COS, Azure AD is used for user authentication and provisioning; creation and synchronization of user accounts is based on user and group assignment.

1.1 Concepts

Single Sign-on
Single sign-on (SSO) is an authentication scheme that allows a user to log in with a single ID and password to any of several related, yet independent, software systems. True single sign-on allows the user to log in once and access services, including COS, without re-entering authentication credentials.

Azure Active Directory (Azure AD)
Azure Active Directory is Microsoft's enterprise cloud-based identity and access management (IAM) solution. Azure AD is the backbone of the Office 365 system, and it can sync with on-premise Active Directory and provide authentication to other cloud-based systems via OAuth.

Provisioning
Provisioning is the processes of creating an identity in a target system based on certain conditions. *De-provisioning* is the process of removing the identity from the target system when conditions are no longer met. *Synchronization* is the process of keeping the provisioned object, up to date, so that the source object and target object are similar. Azure can provide all three mentioned services.

2 Implementation of authentication

Important: Azure Authentication needs to be configured before Provisioning can be implemented.

2.1 Procedure

The procedure for setting up Azure authentication, consists of the following steps:

1. Compano will send you the: `Compano Azure Authentication Form`. This form will contain two ***Re-direct URLs*** and, in case of provisioning, one or more ***data area codes*** which you will need for your setup.
2. Customer sets it up and fills in data in the form and sends it to Compano
3. Compano configures authentication server.
4. Compano activates authentication (test site) but for the live site it only becomes active on the desired date. Compano informs customer that can be tested
5. Customer can now test login on test server; should now work with SSO

3 Configuration authentication

Important note for existing Compano user accounts

Should your Compano application already contain users and you are migrating to Azure Authentication, then care should be taken that usernames in Compano and Azure AD match.

Compano recommends using only company-issued user e-mail addresses as the user IDs for both Azure AD and the Compano application. The e-mail addresses should be based on the Active Directory domain, for instance johndoe@company.com

The configuration process consists of two steps:

I. Setting up your Azure AD for connecting with the Compano application
II. Setting up the Compano application for connecting with your Azure AD

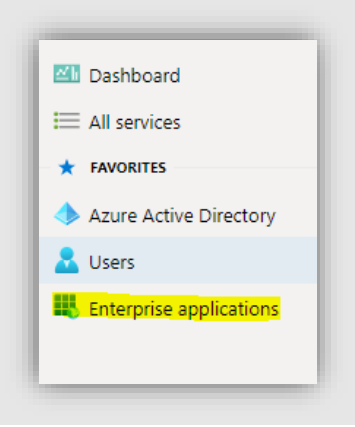
Step I will provide you with several IDs and other data which need to be sent to your Compano consultant. A *Compano Azure Authentication Form* is provided as a separate document. Please continue reading this manual and at the end fill out all the fields of this form.

After receiving this form, Compano will complete Step II, test the connection, and inform you whether it was successful.

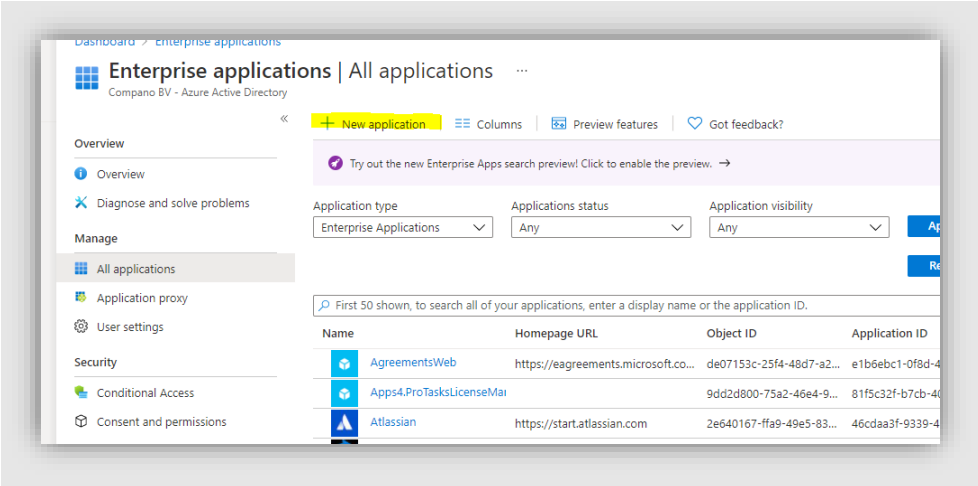
3.1 Azure Authentication setup

To prepare your Azure environment for single sign-on with the Compano application:

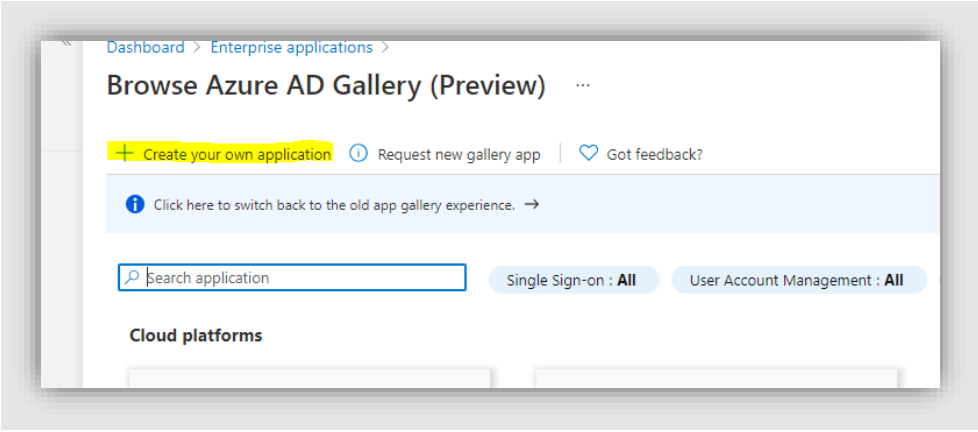
1. Go to https://aad.portal.azure.com/
2. In the left side panel menu, click on *Enterprise applications*:



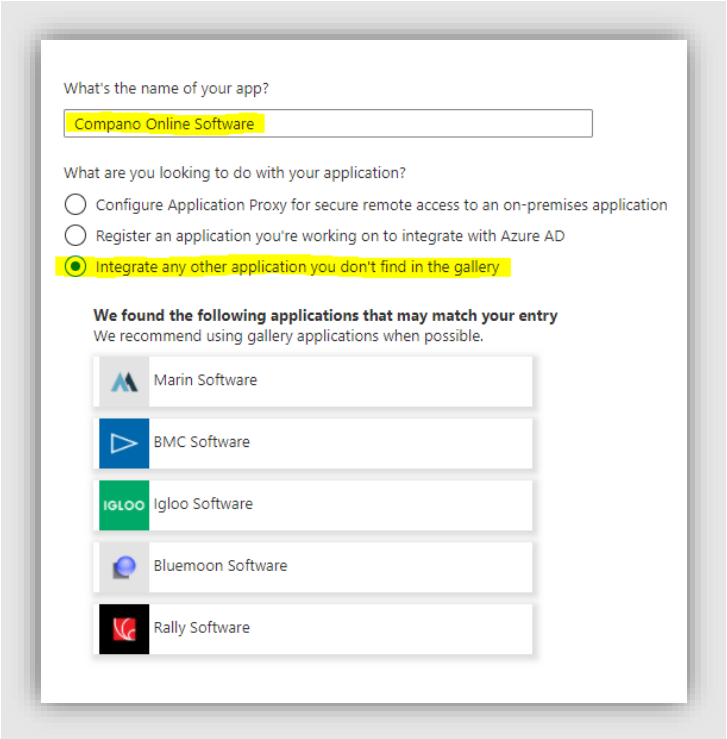
3. In the Enterprise applications screen, click on *+New application*:



4. On the next screen, click on *Create your own application*.



5. Set name and type of the application:
   - **Name of the application**: Type a name Compano Online Software
   - **What are you looking to do with your application?** Set this option to *Integrate any other application…*

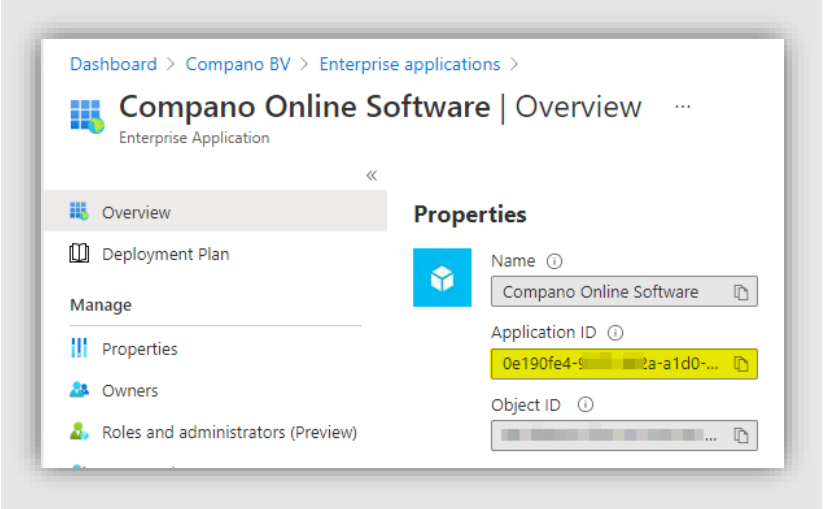


6. And create the application.

3.1.1 Application ID

The resultant application will provide you with the following authentication IDs:

- **Application ID**
- Object ID (not needed)

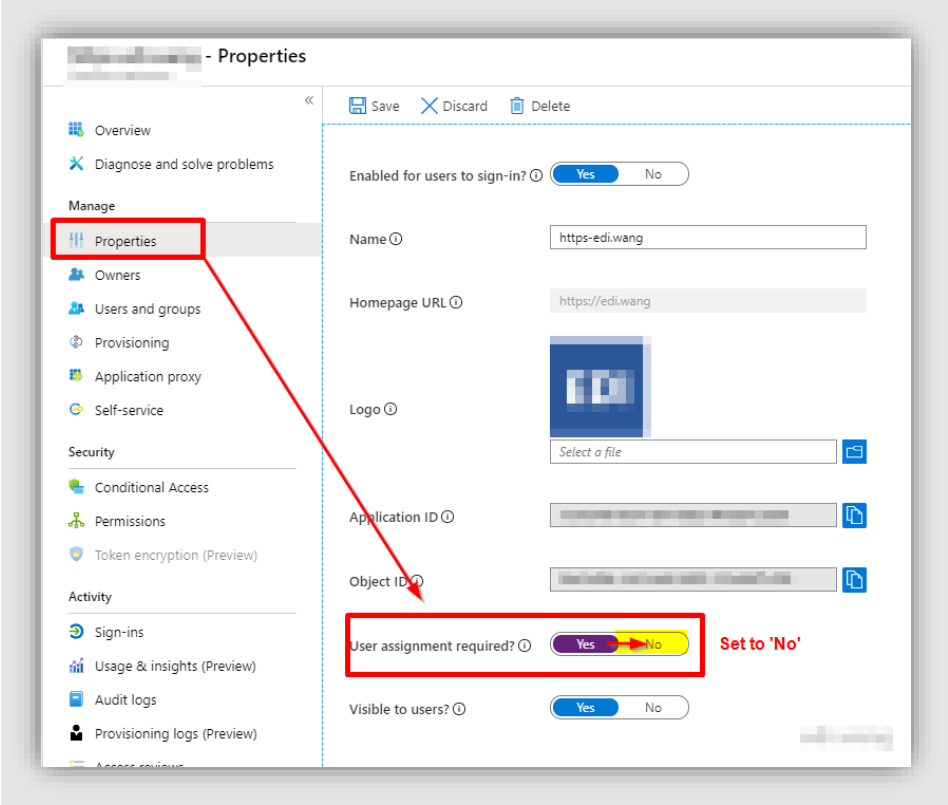


Copy the ***Application ID*** to App registration to *Appendix A: Azure Authentication Form*.

3.1.2 User assignment

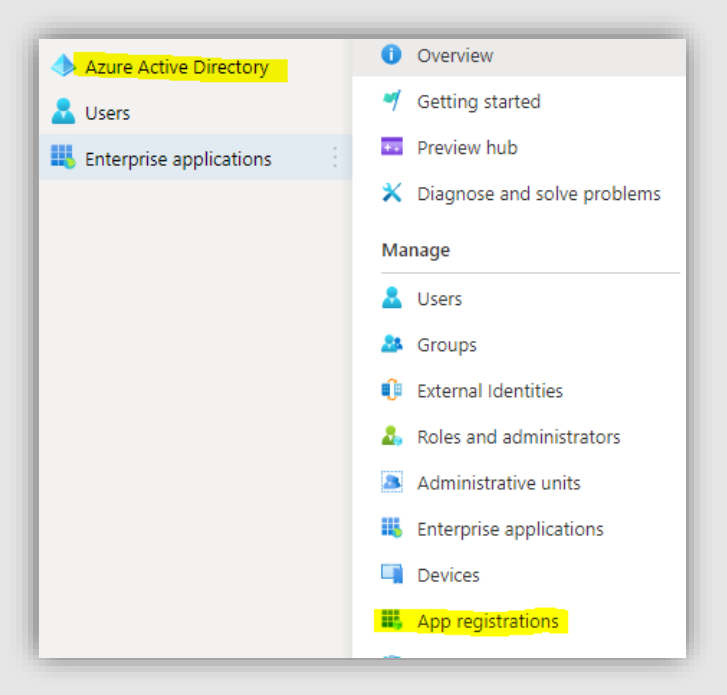
Check that the *User assignment required?* Is set to *No*.

1. Through the Azure Enterprise Application menu, go to Manage > Properties
2. Move the slider at *User assignment required?* to *No:*

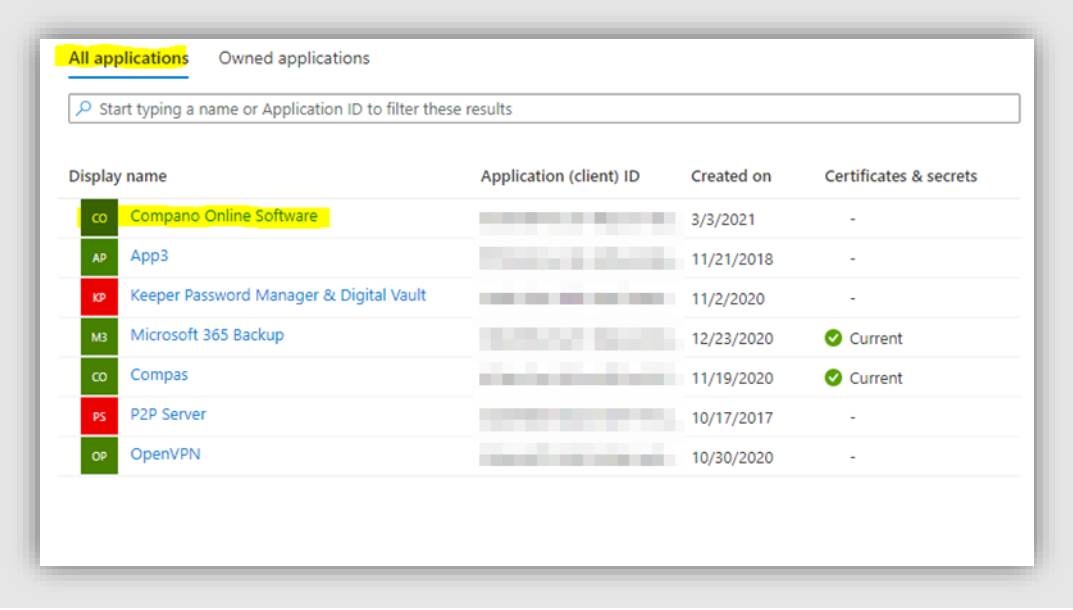


3.1.3 App registration

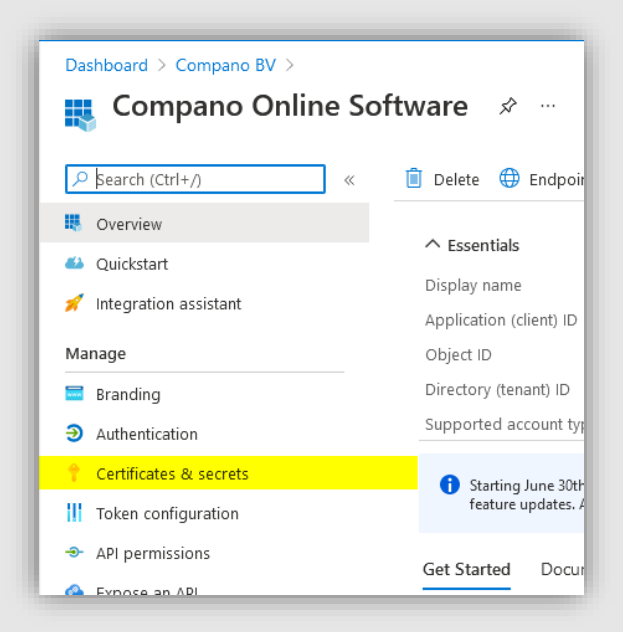
1. Now, through the Azure menu, go to *App registrations*:



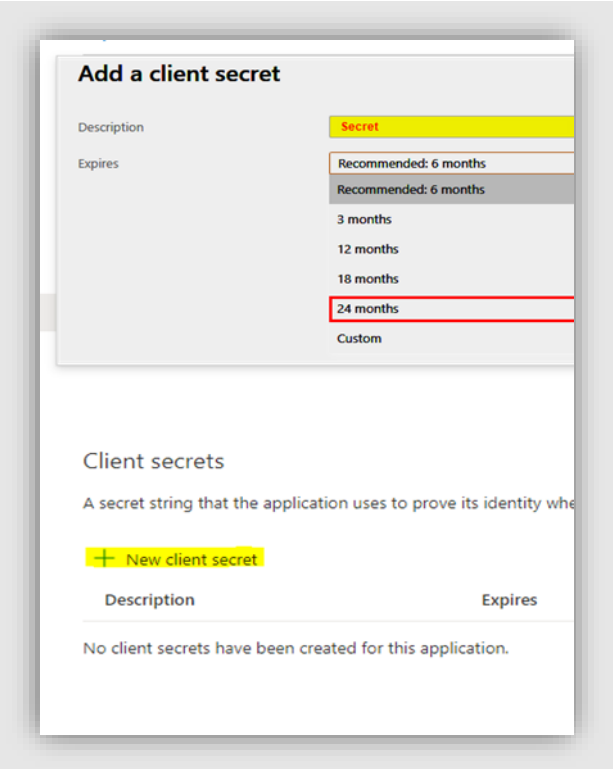
2. Click on *All applications* and select the newly created registration:



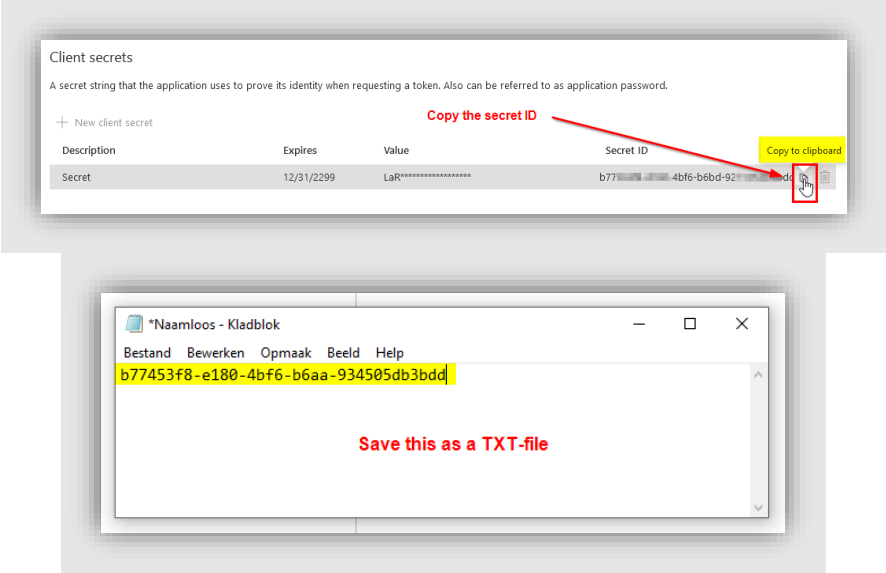
3. Using the App Registration menu, configure the application as follows:
   - Go to *Certificates & secrets*:



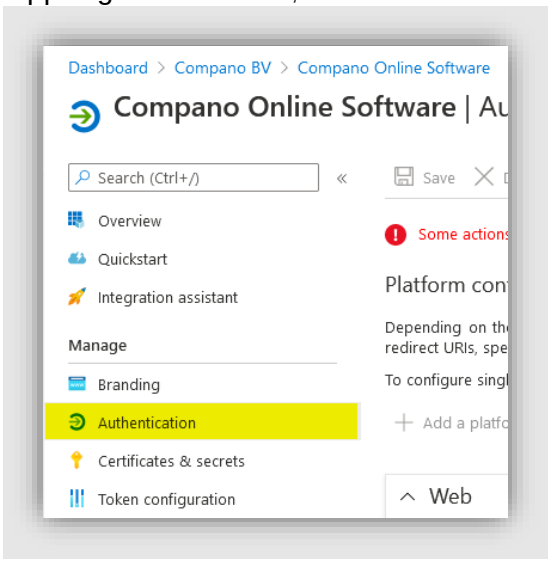
- Add a new ***client secret***:



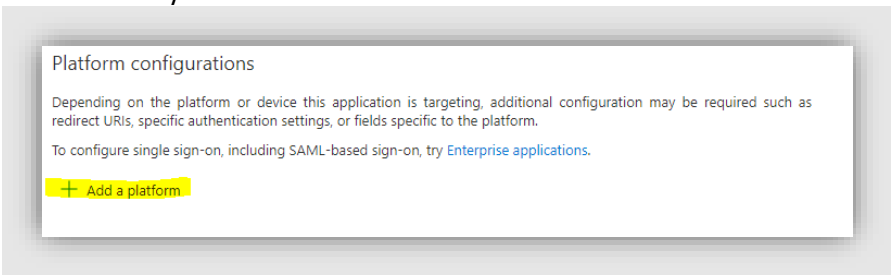
  - **Description**: Name your secret: 'secret'
  - **Expires**: Set an expiration duration (maximum 3 years custom)
- Important: Use the *Copy to Clipboard* option, to copy the ***value of the secret*** to a text-editor (for instance, ***Notepad***) and store the resultant file at a safe place (such as a password safe or digital vault), as you will need this to get access to the app registration! Warning: If you omit this step, you -will- have to create a new Client secret.



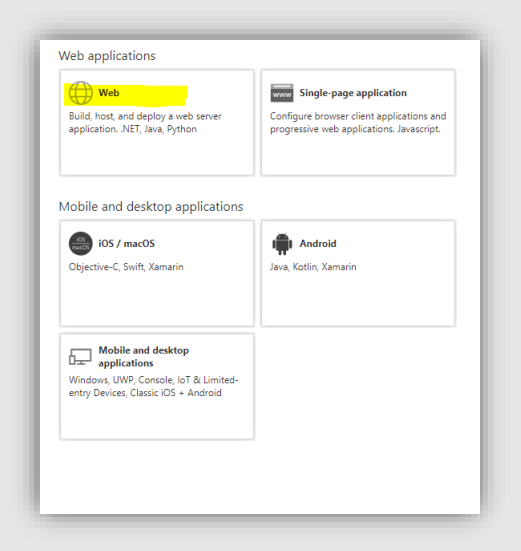
- Next, in the App Registration menu, select *Authentication*:



- Select *Add platform*:

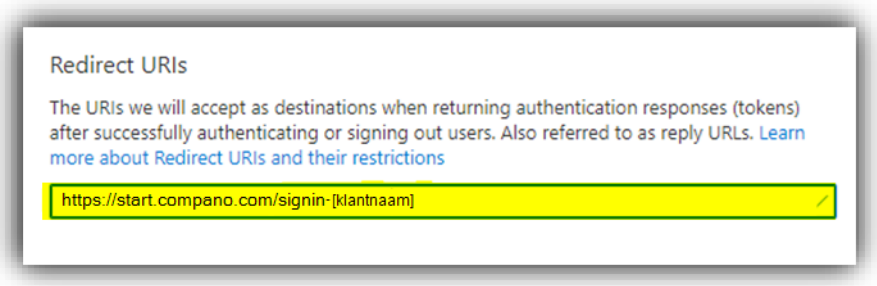


- Select web:



- Add the test *Redirect urls*:

Redirect URL (L05 and further)	https://start.compano.com/signin-[klantnaam]]



Note: Older versions of the Compano software used a different redirect URL: https://authentication.compano.com/sigin-microsoft. Please make sure to change the redirect URL when migrating to version L05 or newer.

3.2 Account(s) for Compano

Important: Once Azure Authentication has been setup, Compano employees will ***no longer have access*** to your application. To allow access to our employees for support and consultation, either:

- Create specific Compano accounts in your Active Directory for Compano employees
- Or, allow Remote Access software such as MS Teams, TeamViewer, etc.

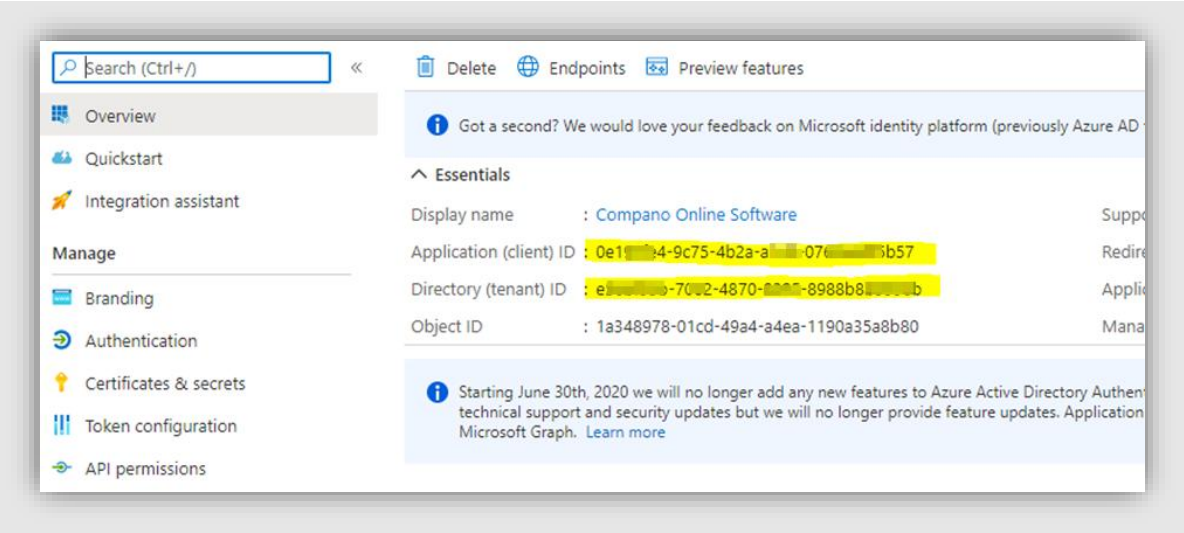
3.3 Authentication testing

Once you have filled out all information, please return the form to your Compano consultant. He or she will activate Azure authentication on your TEST-server.

Now you are ready to try-out the authentication. For this, you will need the following data:

- Application (client) ID
- Directory (tenant) ID

- Previously saved secret



Important: Please copy the IDs and secret to the Compano Azure Authentication Form and send the form to your Compano consultant.

4 Implementation Provisioning

Provisioning is the processes of creating an identity in a target system based on certain conditions. *De-provisioning* is the process of removing the identity from the target system when conditions are no longer met. *Synchronization* is the process of keeping the provisioned object, up to date, so that the source object and target object are similar. Azure can provide all three mentioned services.

5 Configuration provisioning

Important note for existing Compano user accounts

Should your Compano application already contain users and you are migrating to Azure Provisioning, then care should be taken that usernames are based on (company) e-mail addresses both Compano and Azure AD. Please contact your consultant if user names in Compano are NOT based on e-mail addresses and/or do not match your Azure AD.[1]

Compano recommends using only company-issued user e-mail addresses as the user IDs for both Azure AD and the Compano application. The e-mail addresses should be based on the Active Directory domain, for instance johndoe@company.com

5.1 Compano access

Important: Note that after setting up provisioning, Compano consultants and support will ***no longer have access*** to your application, unless you provide an Azure user account for them.

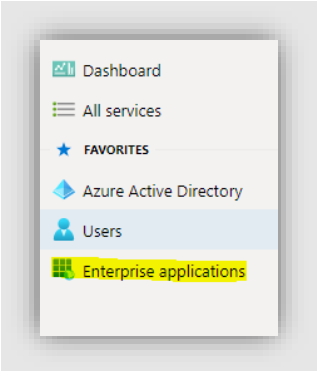
Please use the *Compano Azure Authentication Form* (separate document) to send login credentials for these accounts to your Compano consultant.

5.2 Provisioning setup

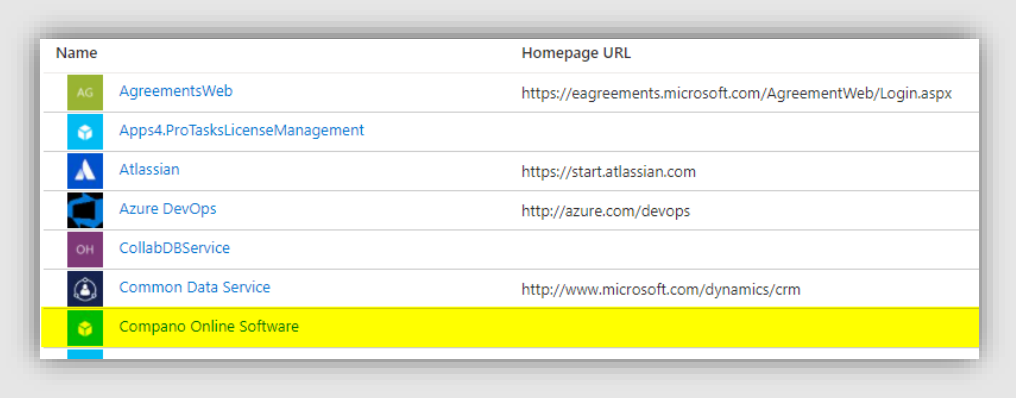
Once Azure AD Authentication has been enabled, you are ready to setup provisioning:

1. Go to https://aad.portal.azure.com
2. In the left side panel menu, click on *Enterprise applications*.

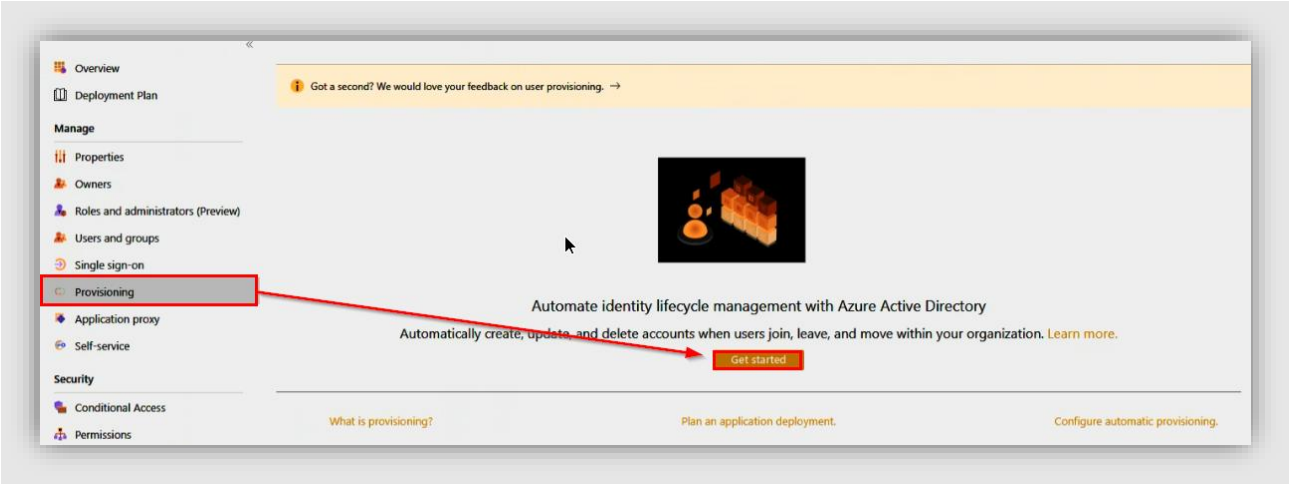
[1] Azure AD users will be synced based on the e-mail address of the user provided by Azure. If these address does ***not*** match with the existing Compano user account, a new user account will be generated; any saved layouts, filters or settings fort his user will initially be unavailabe. Contact your Compano consultant to set things right.



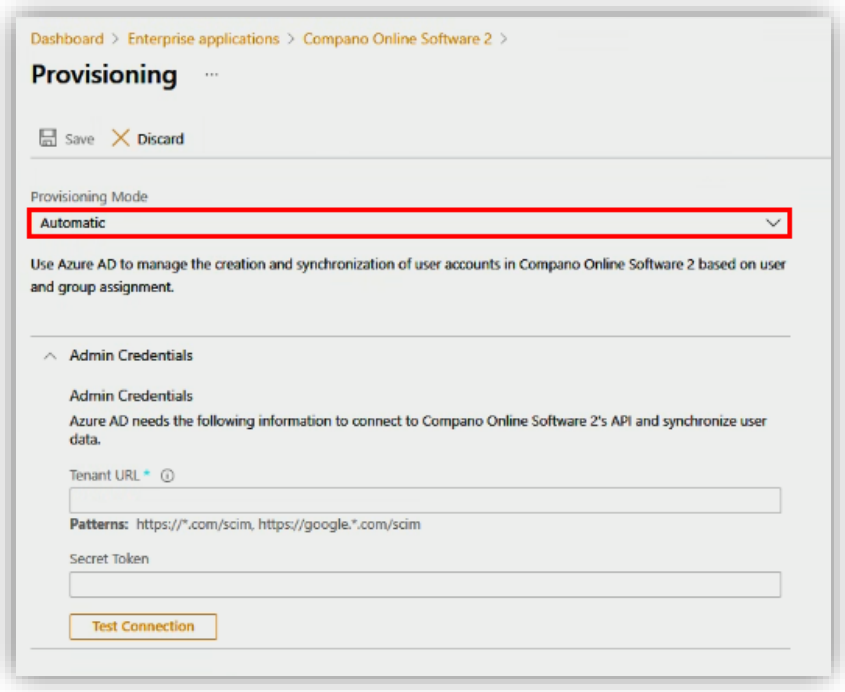
3. In the Enterprise applications screen, search for and click on *Compano Online Software*.



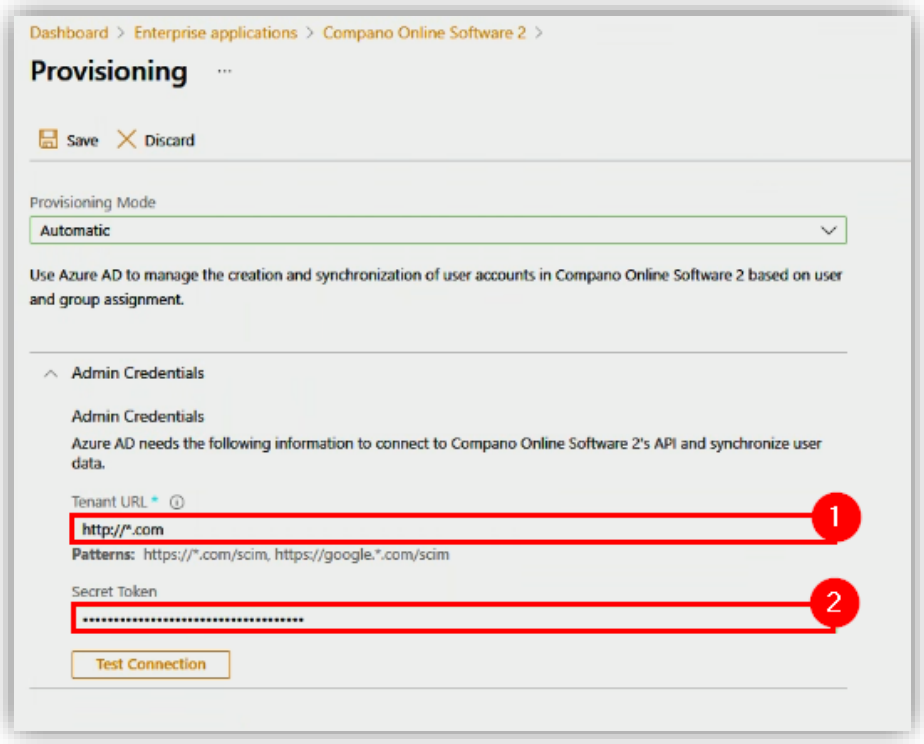
4. Next, in the application menu, click on *Provisioning*.



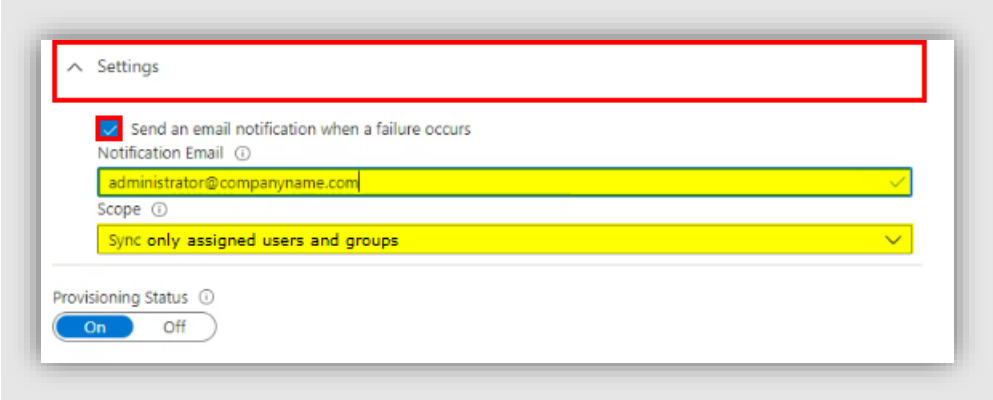
5. Next, click on *Get Started*.
6. Set the Provisioning Mode on: *Automatic*.



7. Next, open the *Admin Credentials:*
   - ***Tenant URL***: Enter the Tenant URL provided by Compano via the *Compano Azure Authentication Form*.
   - ***Secret***: Enter the Secret provided by Compano via the *Compano Azure Authentication Form*.



8. Next, open the *Settings*.



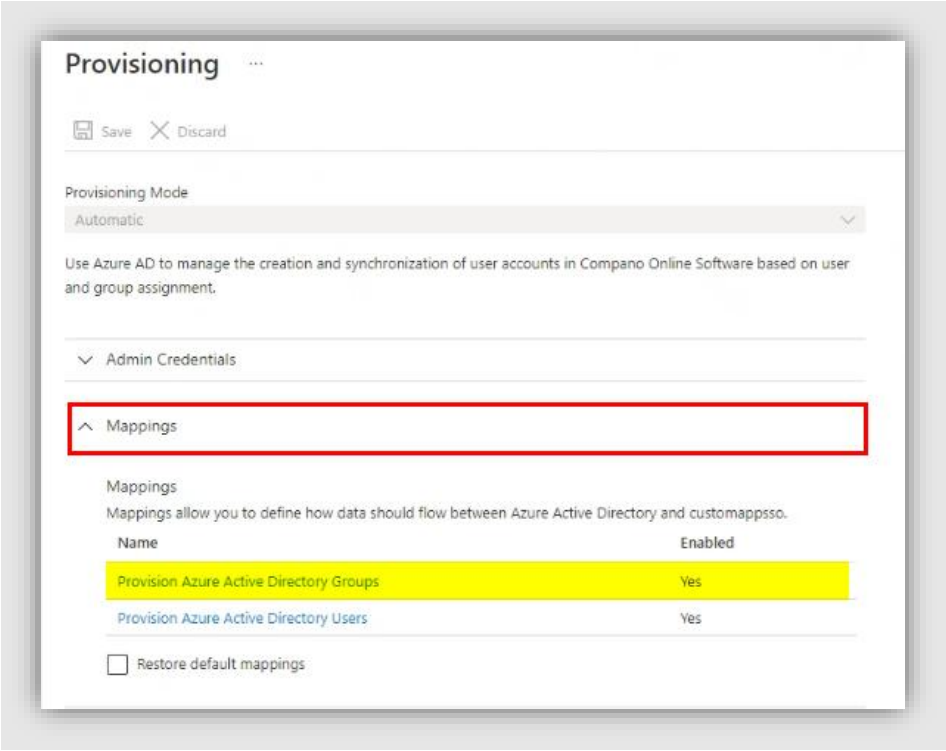
a. **Send an email notification when a failure occurs (optional)**: Check this option if you want to receive error messages for debugging.
b. **Notification Email**: Enter the e-mail address of your System Administrator.
c. **Scope**: Select *Sync only assigned users and groups*.

9. Now, save the settings you made by using the *Save* button at the top of the Provisioning page.

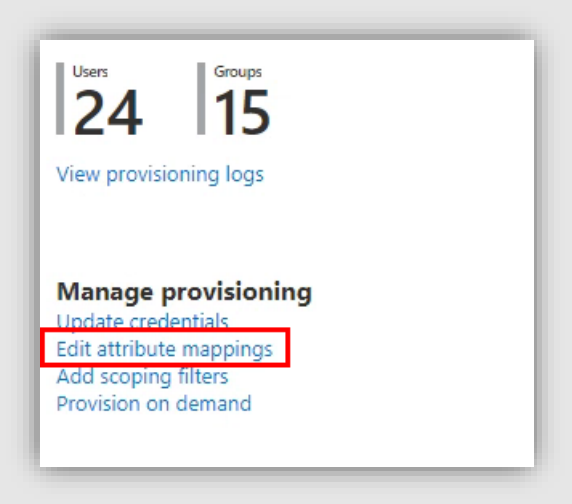
5.2.1 Mapping Groups

Next, you will need to set the mappings Groups:

1. On the Provisioning screen, open up the *Mappings* and click on *Provision Azure Active Directory Groups*.

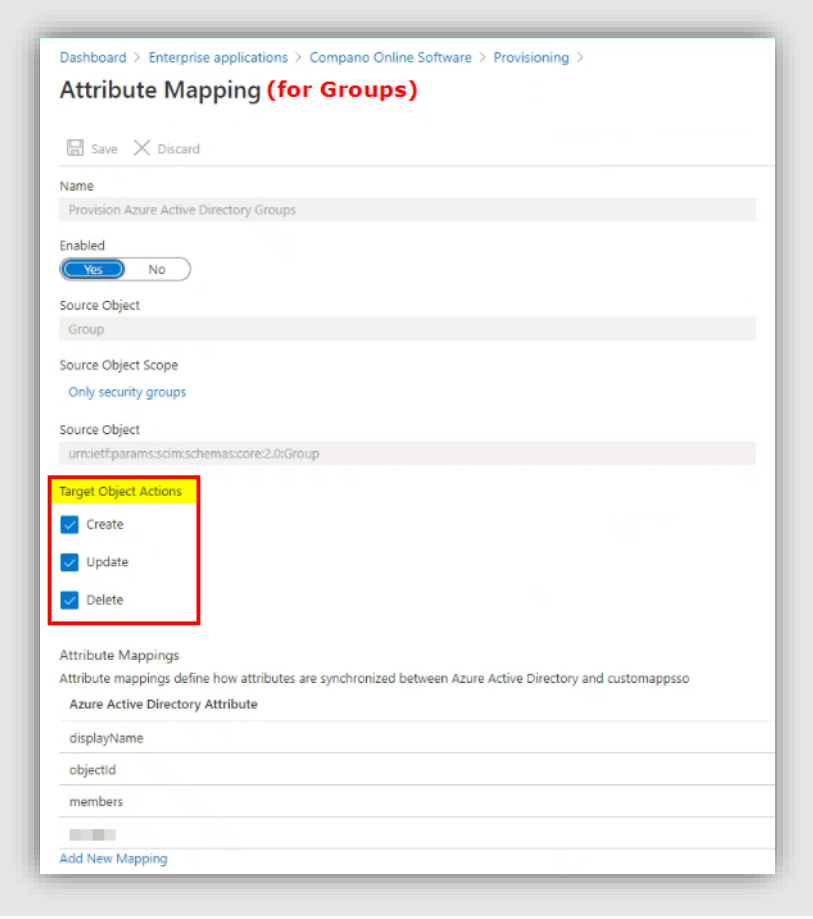


2. In the next screen, click on *Edit attribute mappings*.



5.2.1.1 Mark Target Object Actions

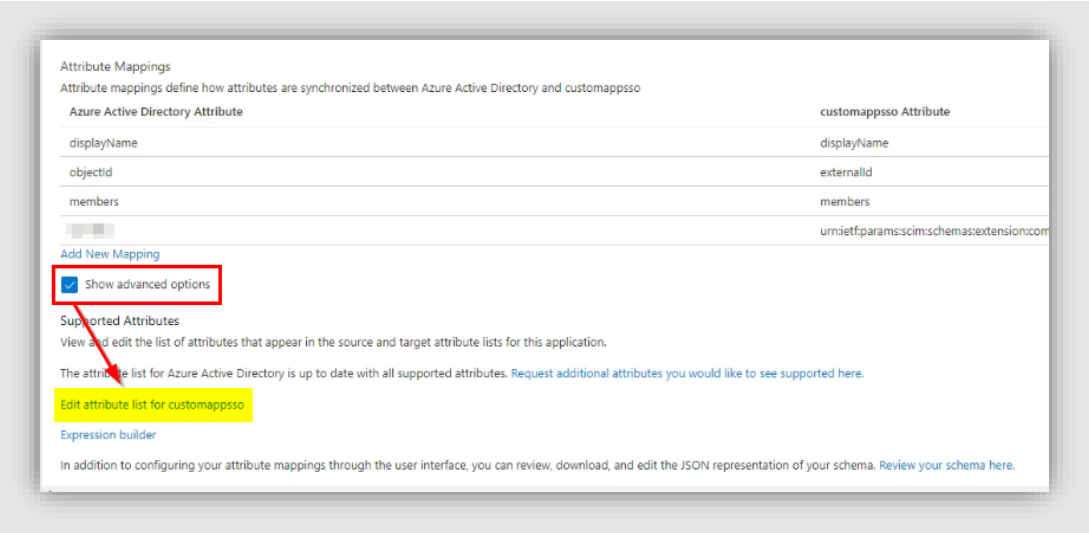
First, make sure to mark all *Target Object Actions* (`Create, Update, Delete`):



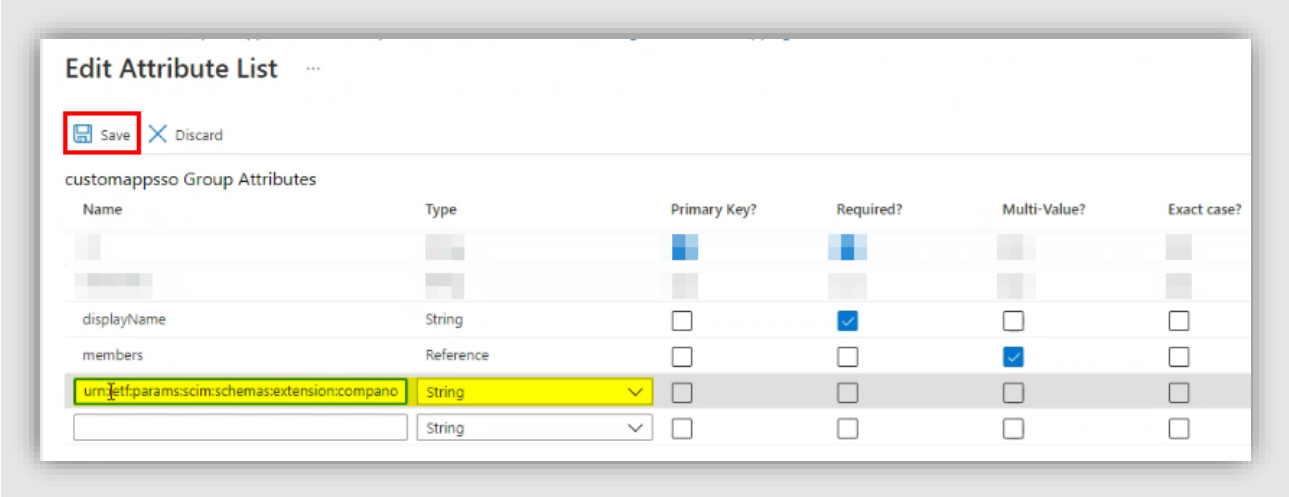
5.2.1.2 Create CustomSSO field

Next, create a CustomSSO field for the DataAreaCode. This code is needed to map your groups to the correct Compano Environment:

1. On the Attribute Mapping screen, scroll down and check the *Show advanced option* box:



2. Next, select *Edit attribute list for customappsso*, scroll down to the bottom of the attribute list:



   a. **Name (for Groups)**[2]: `urn:ietf:params:scim:schemas:extension:compano:2.0:Group:DataArea`
   b. **Type**: and enter a new field of type `String`
3. *Save* the attribute list.

5.2.1.3 Add mappings

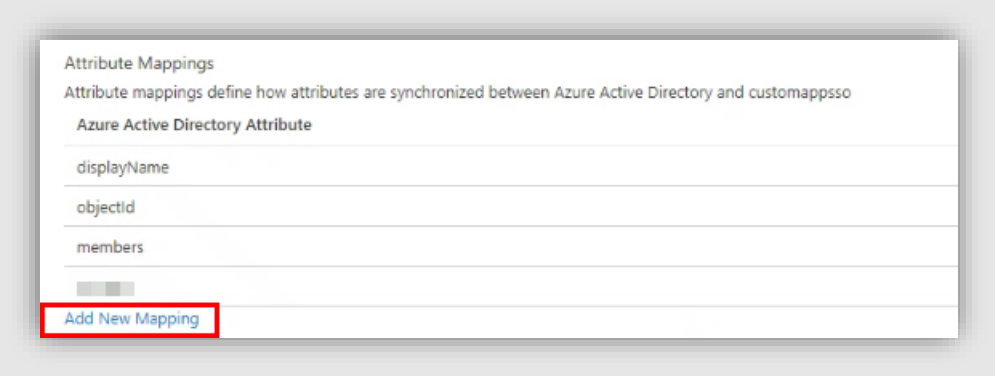
And last, you will need to add mappings for the following group attributes. Note: Check if the first three fields are present:

- displayName
- members
- objectid
- [DataAreaCode] ← New field, needs to be created

To add these mappings:

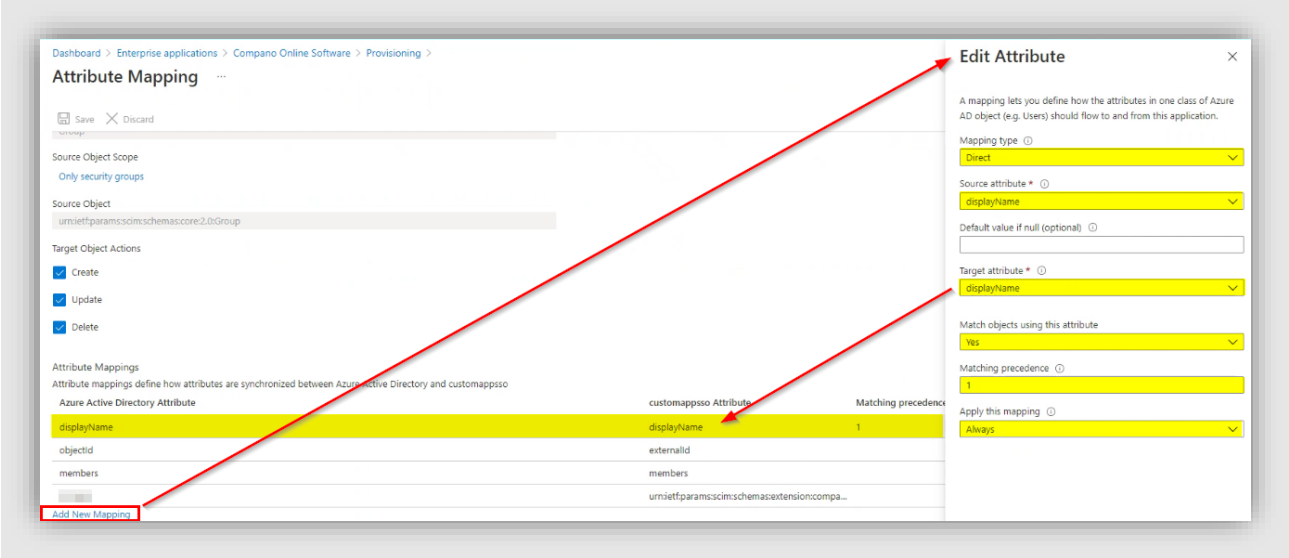
1. Return to the *Attribute mapping* (for groups) screen and click on *Add New Mapping*.

[2] This DataAreaCode is provided by Compano through the *Compano Azure Authentication Form*.



2. In the right side panel Edit Attribute, add the mappings by selecting the correct options. Important: You will need to follow the instructions for each mapping below ***precisely***:

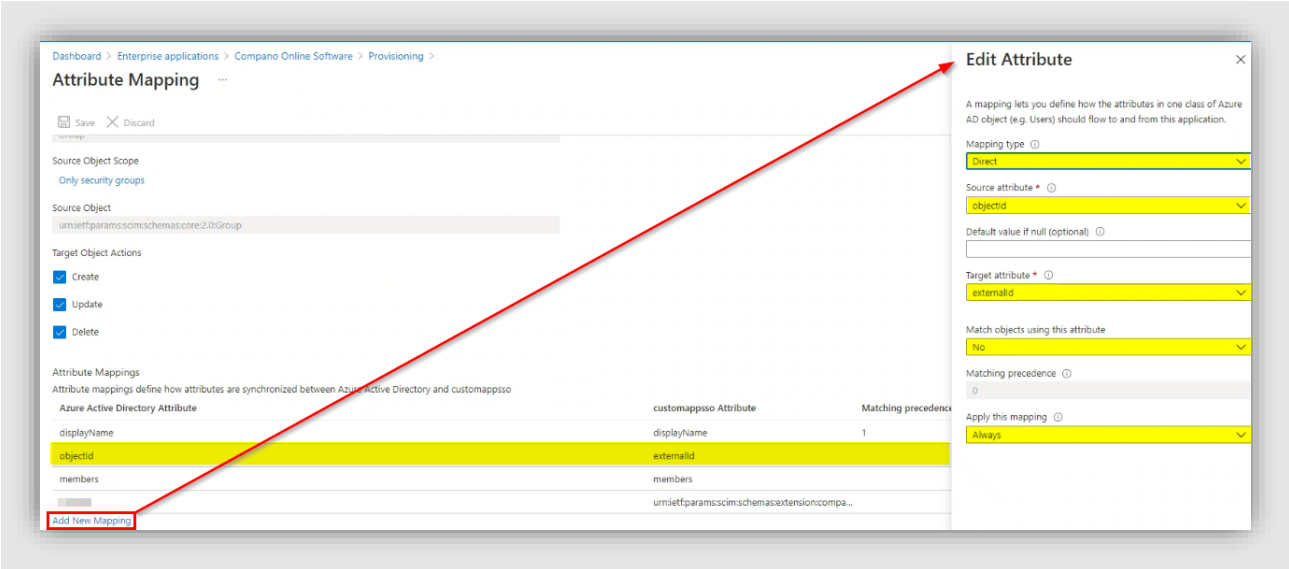
displayName



a. **Mapping type**: Select *Direct*
b. **Source attribute**: Select *displayName*
c. **Default value if null**: Leave empty
d. **Target attribute**: Select *displayName*
e. **Match objects using the attribute**: Select *Yes*
f. **Matching precedent**: Set to *1* (one)
g. **Apply this mapping**: Select *Always*

Click on *Add New Mapping* to Save and add another mapping:

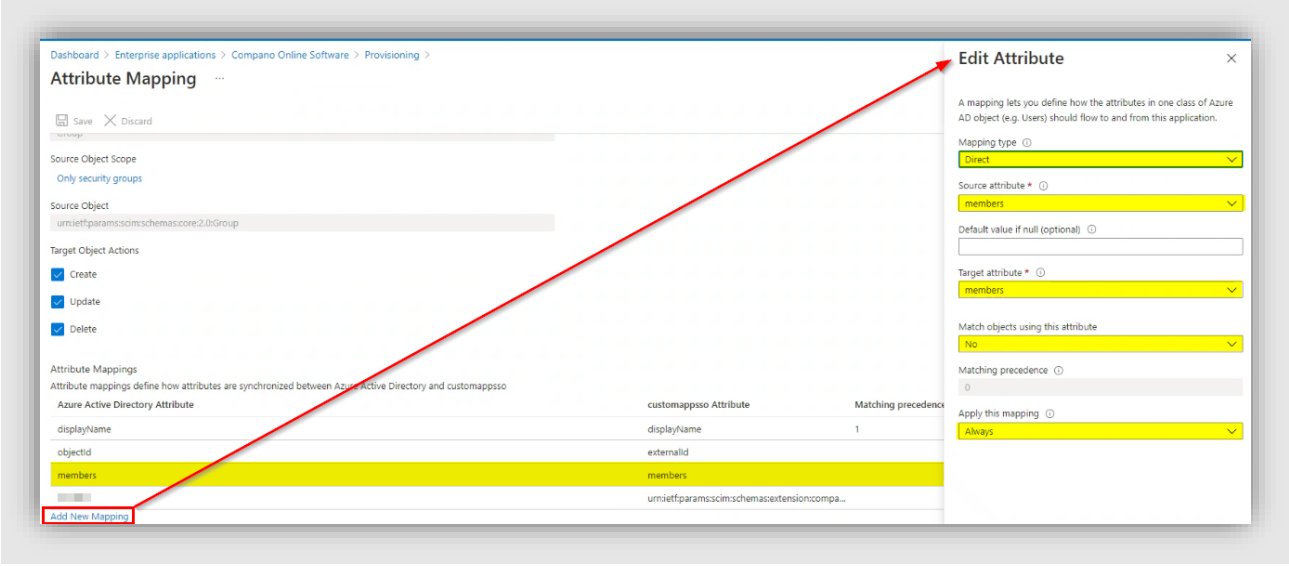
objectid



a. **Mapping type**: Select *Direct*
b. **Source attribute**: Select *objectid*
c. **Default value if null**: Leave empty
d. **Target attribute**: Select *externalid*
e. **Match objects using the attribute**: Select *No*
f. **Apply this mapping**: Select *Always*

Click on Add New Mapping to Save and add another mapping:

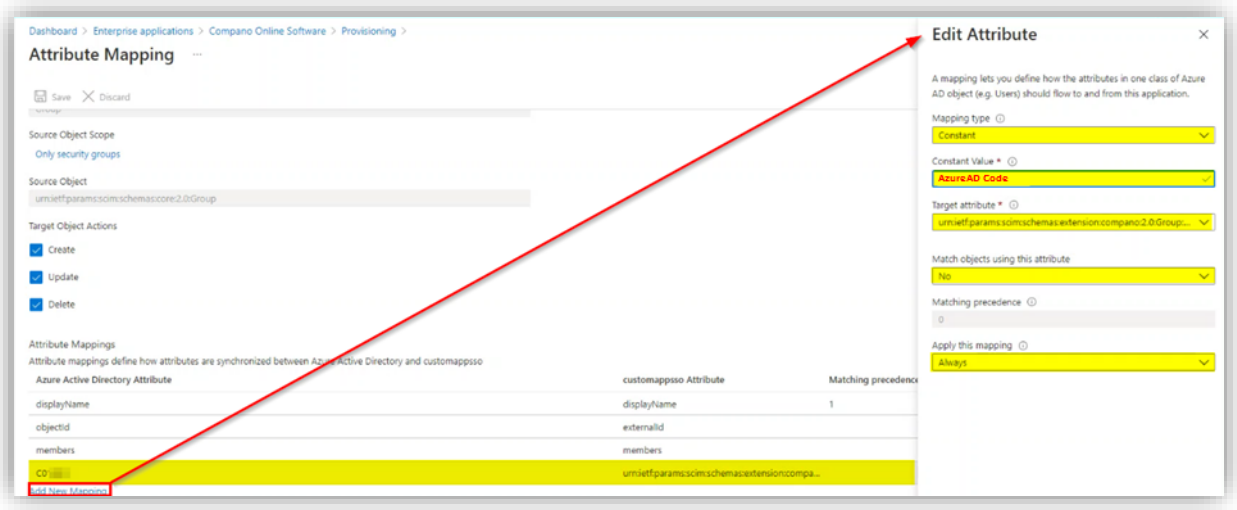
members



a. **Mapping type**: Select *Direct*
b. **Source attribute**: Select *members*
c. **Default value if null**: Leave empty
d. **Target attribute**: Select *members*
e. **Match objects using the attribute**: Select *No*
f. **Apply this mapping**: Select *Always*

Click on *Add New Mapping* to Save and add another mapping:

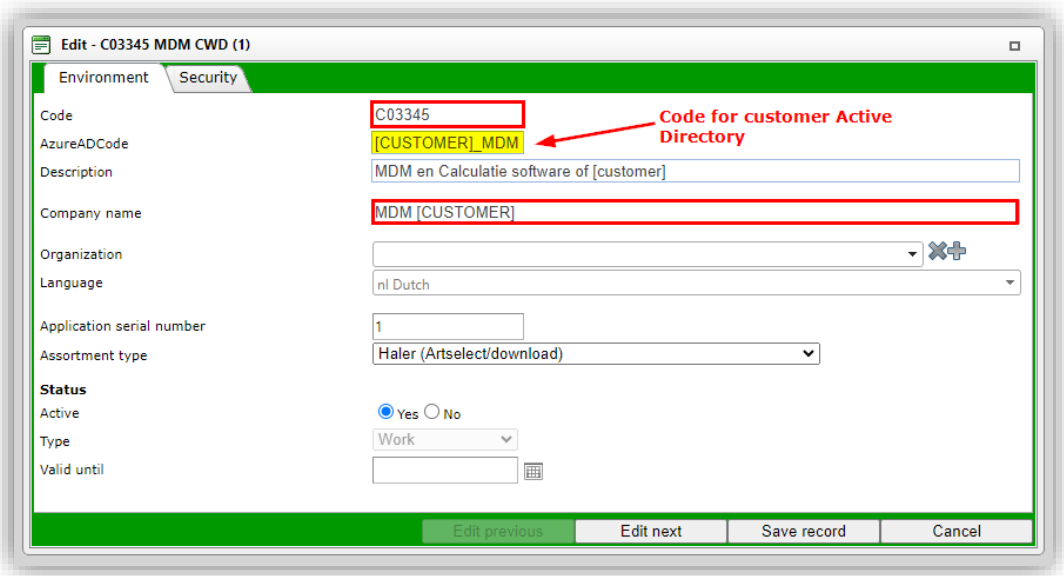
[DataAreaCode]
Next, you will need to map the [DataAreaCode] customSSO field that you created to the correct Compano environment. This is done through either the Compano contract number (L03) or the AzureAD Code (L04).



a. **Mapping type**: Select *Constant*
b. **Constant value**: Enter the either the Contract Number (L03) or the AzureAD Code (L04 and higher) as provided through the *Compano Azure Authentication Form*.
c. **Target attribute**: Select the CustomSSO field you created in paragraph *5.2.1.2:* `urn:ietf:params:scim:schemas:extension:compano:2.0:Group:DataArea`
d. **Match objects using the attribute**: Select *No*
e. **Apply this mapping**: Select *Always*

Click on *Add New Mapping* to Save.

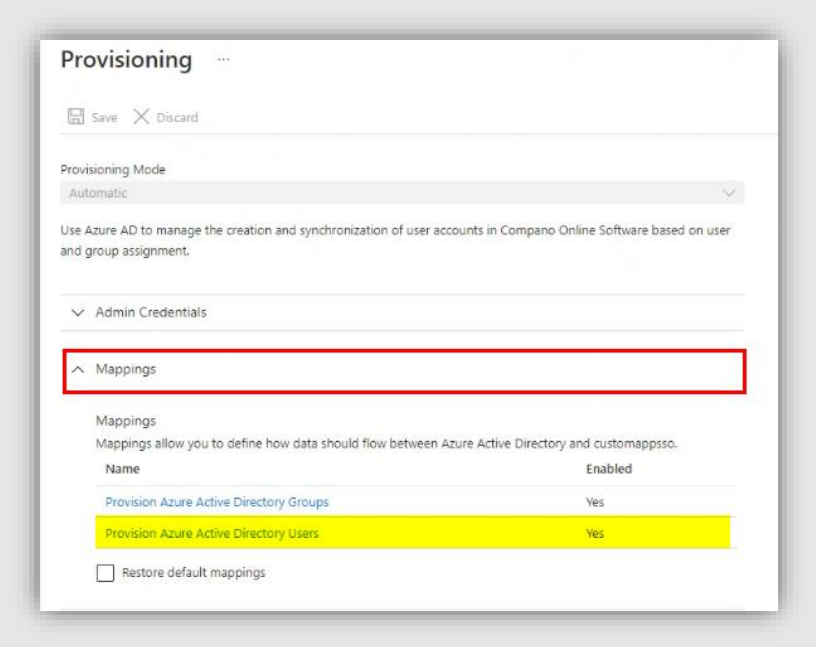
Note: The ***AzureAD Code*** is set by Compano for the application environment. This code needs to entered as the DataAreaCode at the customer's Azure Active Directory, as shown in the following example:



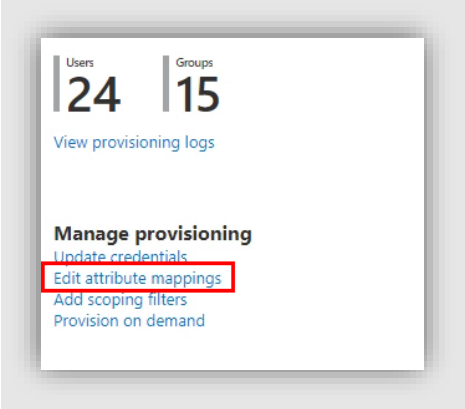
5.2.2 Mapping Users

Proceed with the settings for mapping Users:

1. On the Provisioning screen, open up the *Mappings* and click on *Provision Azure Active Directory Groups*.

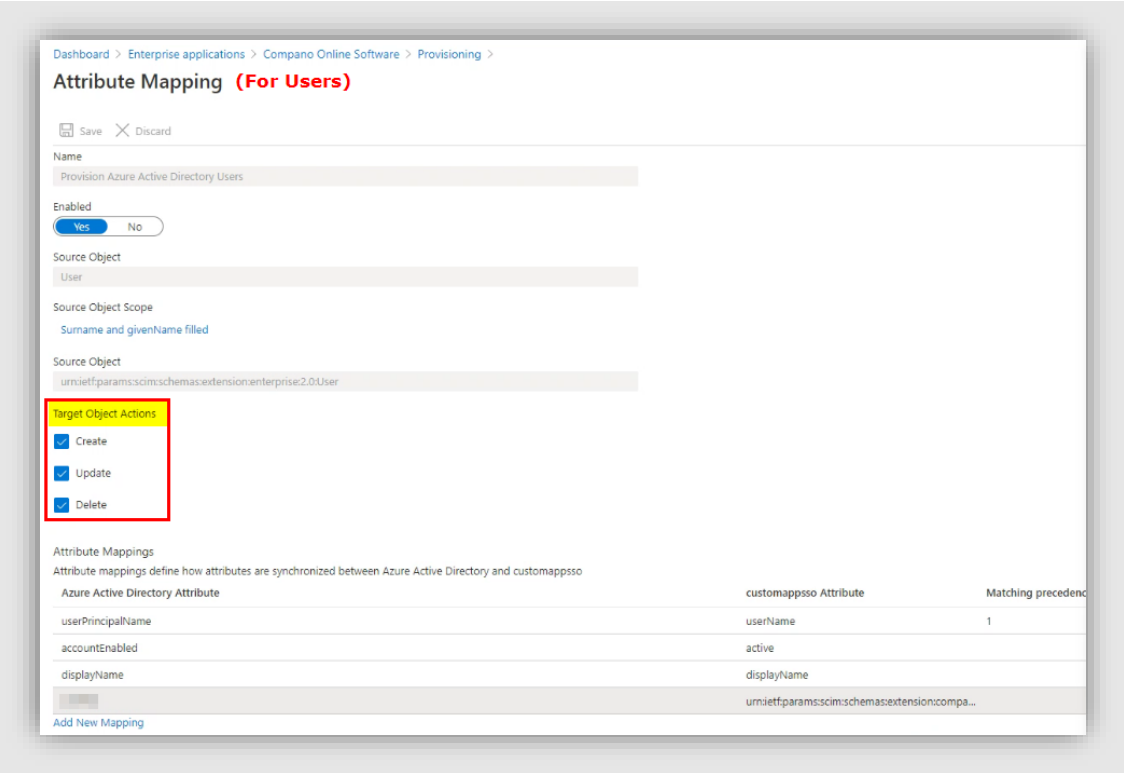


2. In the next screen, click on *Edit attribute mappings*.



5.2.2.1 Mark Target Object Actions

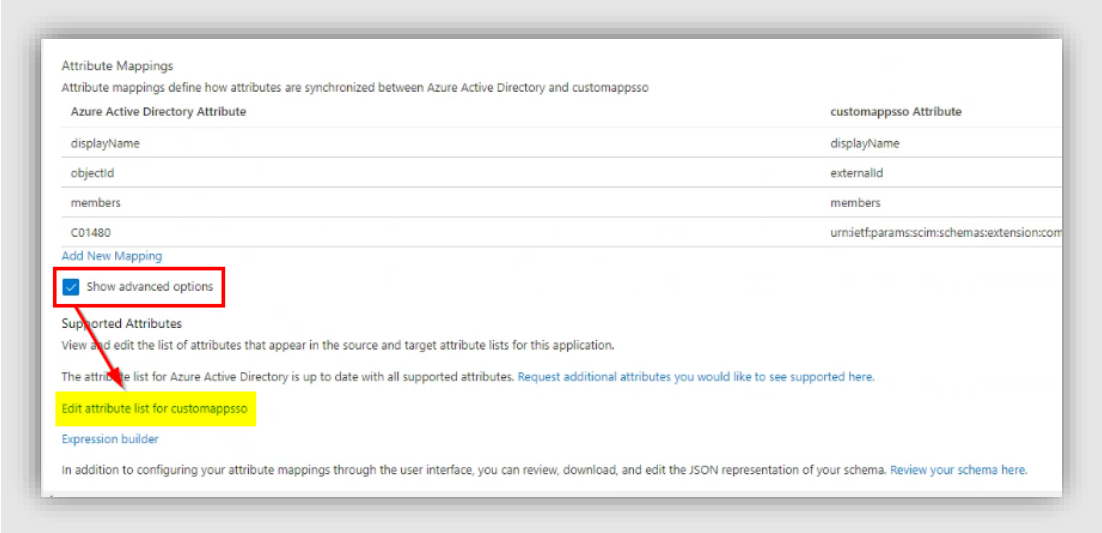
First, make sure to mark all *Target Object Actions* (`Create, Update, Delete`):



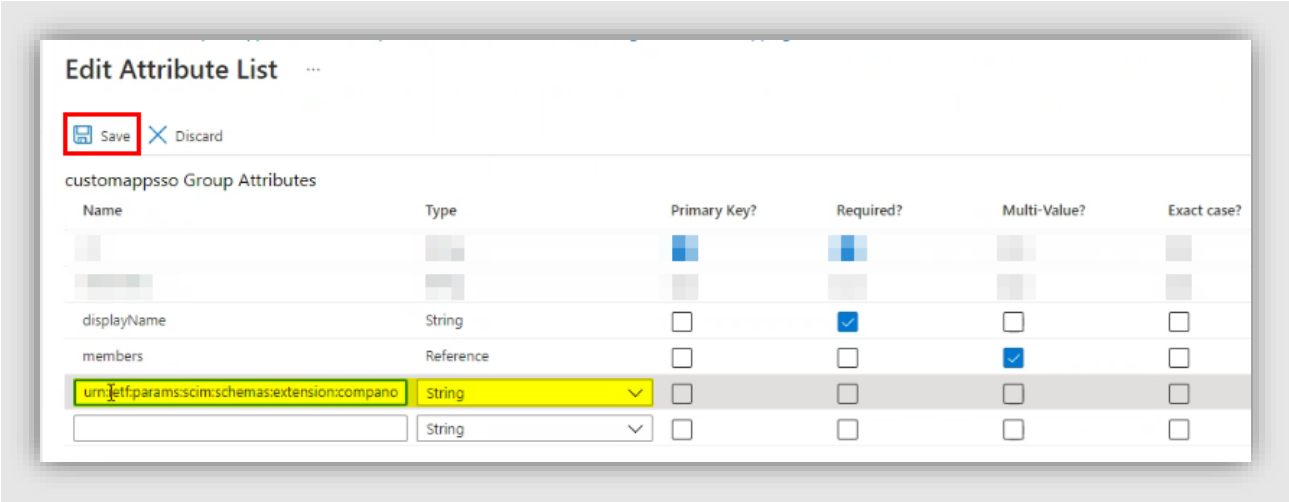
5.2.2.2 *Create CustomSSO field*

Next, create a CustomSSO field for the DataAreaCode. This code is needed to map your groups to the correct Compano Environment:

1. On the Attribute Mapping screen, scroll down and check the *Show advanced option* box:



2. Next, select *Edit attribute list for customappsso*, scroll down to the bottom of the attribute list:



a. **Name (for Users)**[3]:
`urn:ietf:params:scim:schemas:extension:compano:2.0:User:DataArea`
b. **Type**: and enter a new field of type `String`

3. *Save* the attribute list.

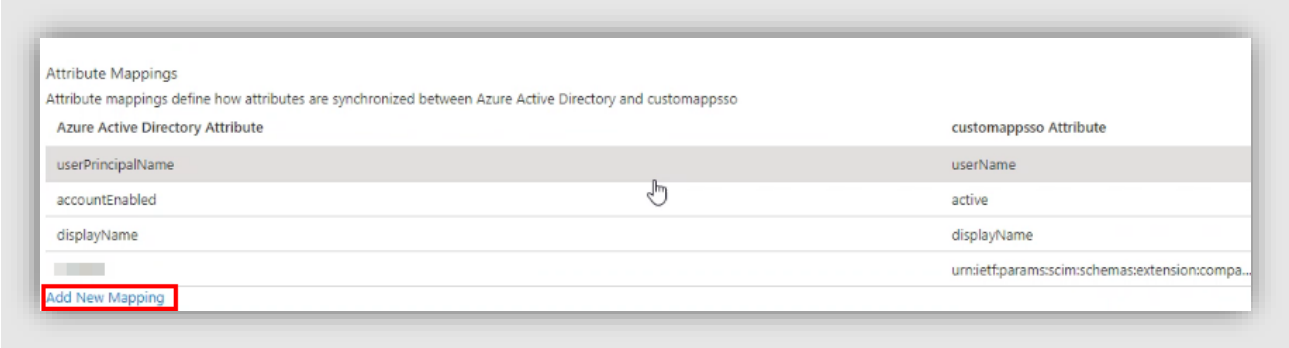
5.2.2.3 Add mappings

And last, you will need to add mappings for the following group attributes:

- userPrincipalName
- accountEnabled
- displayName
- [DataAreaCode]

To add these mappings:

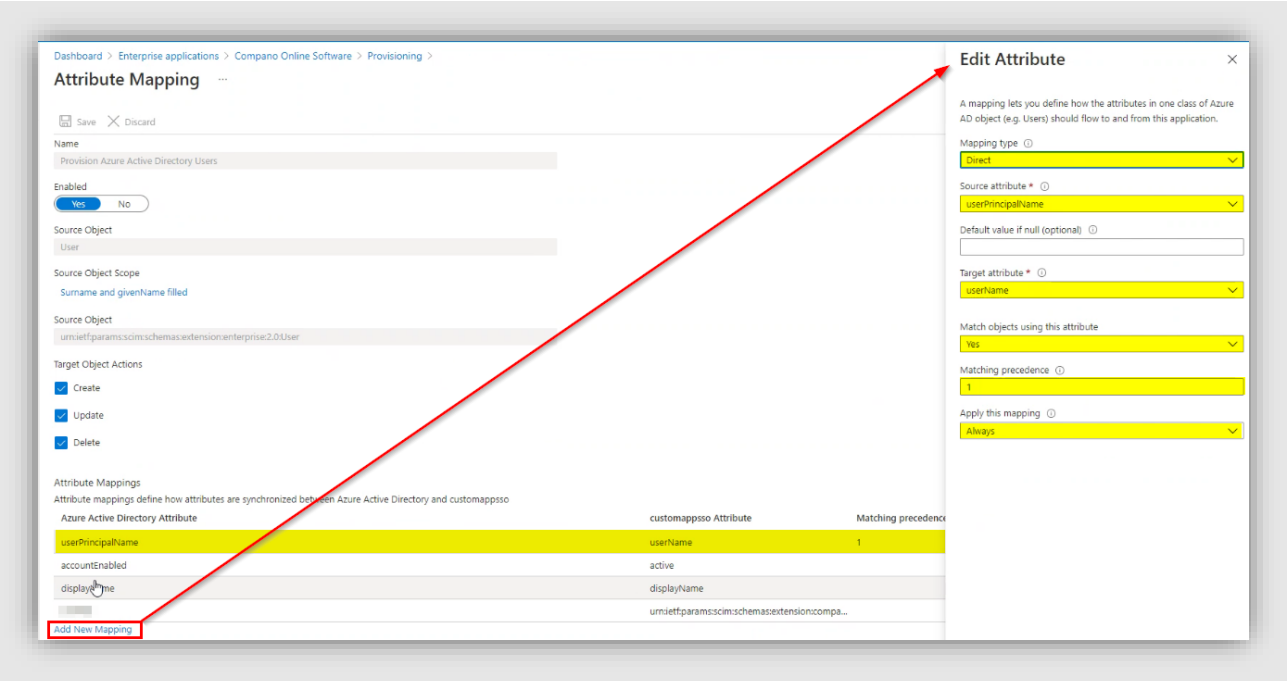
1. Return to the *Attribute mapping* (for groups) screen and click on *Add New Mapping*.



2. In the right side panel Edit Attribute, add the mappings by selecting the correct options.
Important: You will need to follow the instructions for each mapping below ***precisely***:

[3] This DataAreaCode is provided by Compano through the *Compano Azure Authentication Form*.

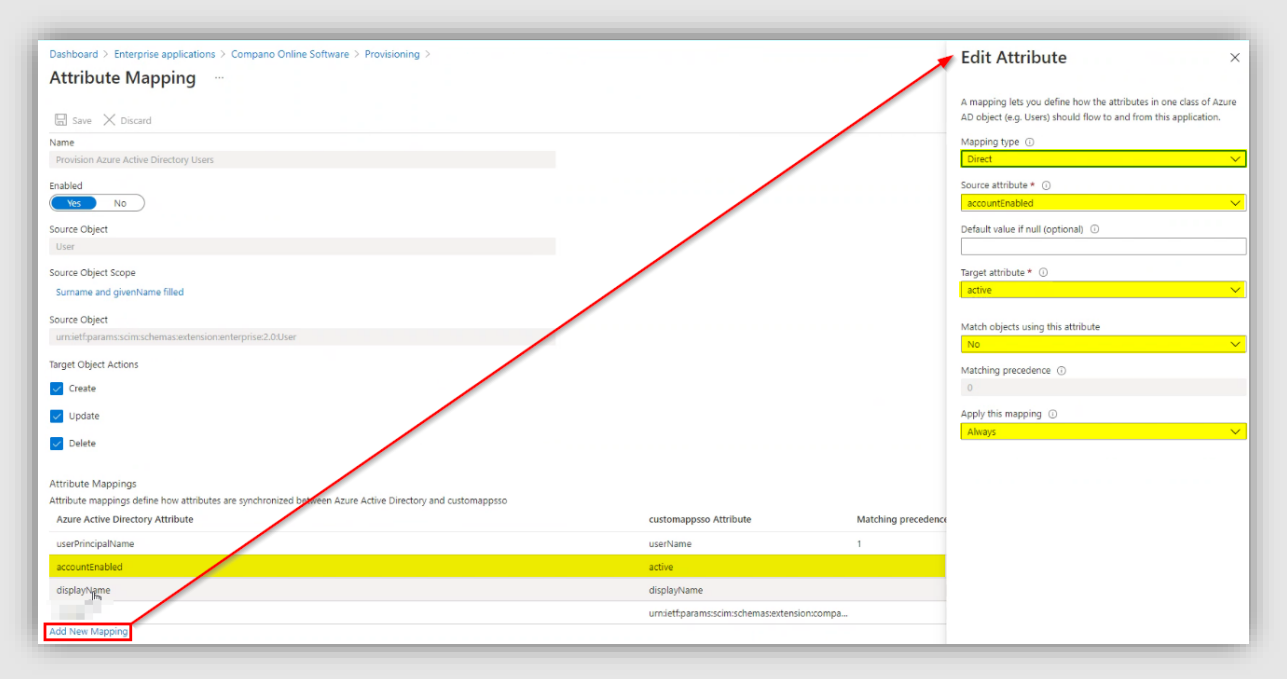
userPrincipalName



a. **Mapping type**: Select *Direct*
b. **Source attribute**: Select *userPrincipalName*
c. **Default value if null**: Leave empty
d. **Target attribute**: Select *userName*
e. **Match objects using the attribute**: Select *Yes*
f. **Matching precedent**: Set to *1* (one)
g. **Apply this mapping**: Select *Always*

Click on *Add New Mapping* to Save and add another mapping:

accountEnabled

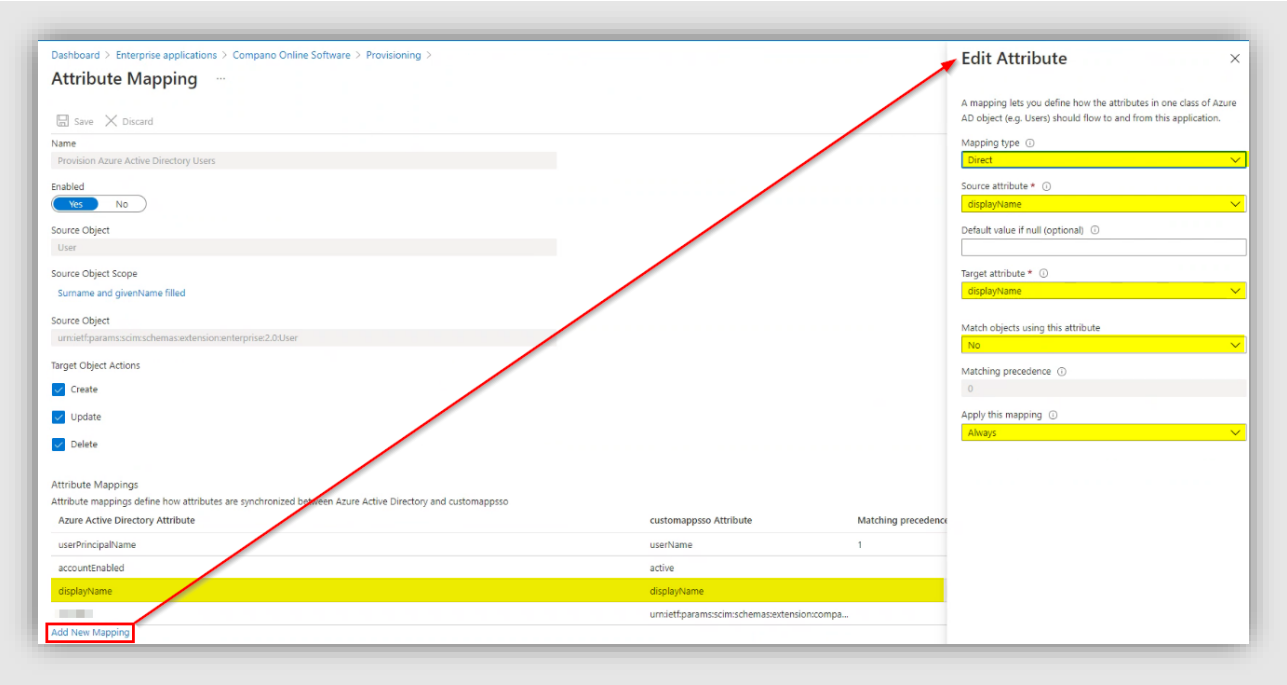


a. **Mapping type**: Select *Direct*

b. **Source attribute**: Select *accountEnabled*
c. **Default value if null**: Leave empty
d. **Target attribute**: Select *active*
e. **Match objects using the attribute**: Select *No*
f. **Apply this mapping**: Select *Always*

Click on *Add New Mapping* to Save and add another mapping:

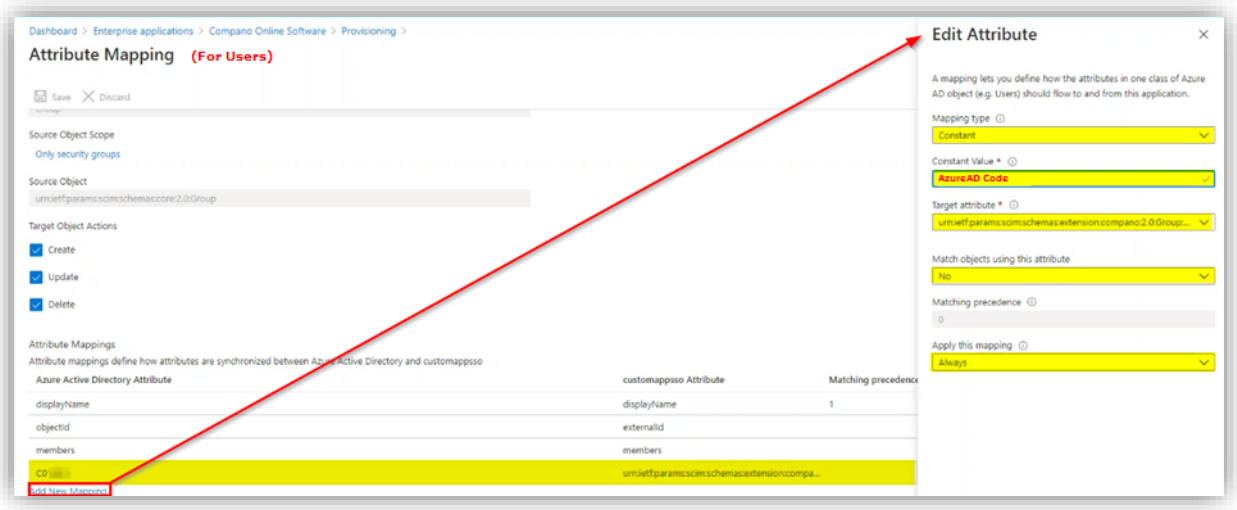
displayName



a. **Mapping type**: Select *Direct*
b. **Source attribute**: Select *displayName*
c. **Default value if null**: Leave empty
d. **Target attribute**: Select *displayName*
e. **Match objects using the attribute**: Select *No*
f. **Apply this mapping**: Select *Always*

Click on *Add New Mapping* to Save and add another mapping:

[DataAreaCode]
Next, you will need to map the [DataAreaCode] customSSO field that you created to the correct Compano environment. This is done through either the Compano contract number (L03) or the AzureAD Code (L04).



a. **Mapping type**: Select *Constant*
b. **Constant value**: Enter the either the Contract Number (L03) or the AzureAD Code (L04) as provided through the *Compano Azure Authentication Form*.
c. **Target attribute**: Select the CustomSSO field you created in paragraph 5.2.2.2: `urn:ietf:params:scim:schemas:extension:compano:2.0:User:DataArea`
d. **Match objects using the attribute**: Select *No*
e. **Apply this mapping**: Select *Always*

Click on *Add New Mapping* to Save.

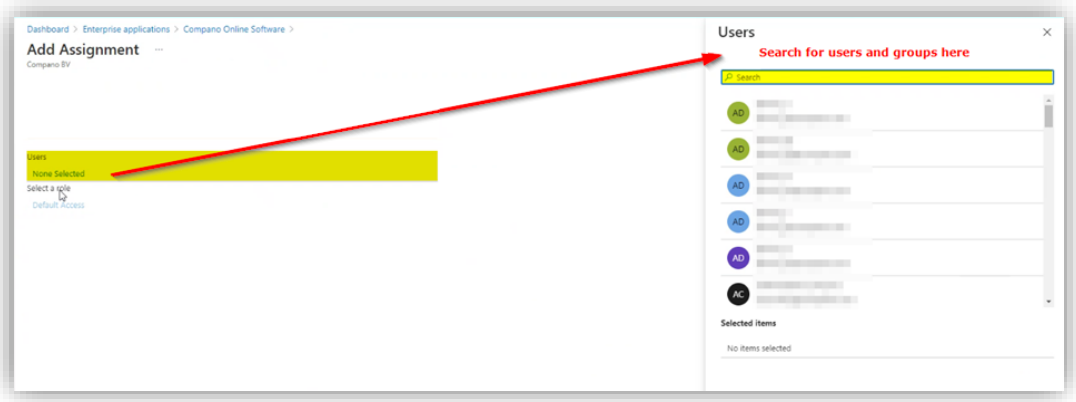
5.3 Select users and/or groups

Finish the setup by selecting users and/or groups which need to be synced to Compano Online Software.

To select users and/or groups:

1. In Azure, return to the Dashboard and select *Users and Groups* from the menu:

2. Next, click on *+ Add user/group*.
3. In the next screen, search for user(s) and group(s) in the right side panel and add them.



6 Testing provisioning

The configuration of provisioning is now finished and you are ready for testing once Compano has setup their end of the process. Please contact your Compano consultant.

Important: If you have not already done so, send the filled-out the *Compano Azure Authentication Form* (separate document) to your Compano consultant.

7 Mapping to multiple Compano environments

To sync users or groups to multiple, different Compano environments, you will need to create a customSSO attribute and map this to the Azure AD field which correctly identifies the user or groups.

Example
By setting up the correct mappings, you could map your customSSO attribute to, for instance, your Azure field `InstallationCustomers`, provided this field holds the correct identifying values for users/groups to their corresponding Compano environment. This way, user group `Janssen_Employees` could be synced to Compano environment `JanssenBV`, and user `Vries_de_J` to environment `De Vries Installatietechniek`.

Important: In case of existing groups and/or users in Compano, the values of the mapped Azure field should map ***exactly*** to the names used in Compano, otherwise groups and users will be created anew. Please contact your Compano consultant if you run into trouble.

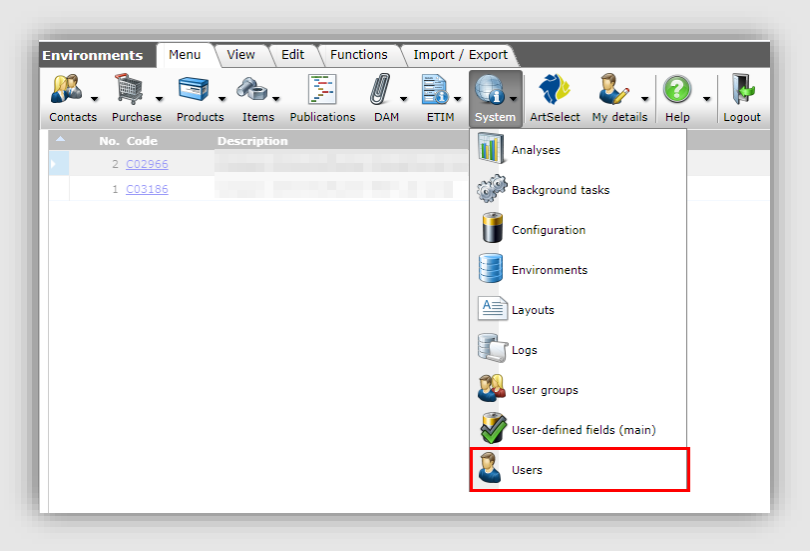
8 Filtering on AD-access

Within COS, you can easily determine which users and groups have access through single sign-on Active Directory, by setting an appropriate filter.

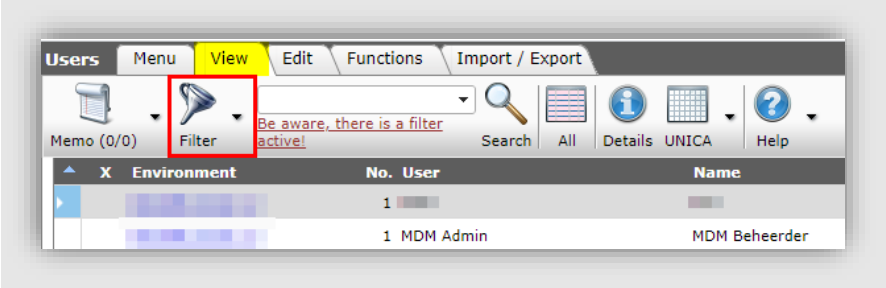
8.1 Filtering AD-users

To filter AD-users in COS:

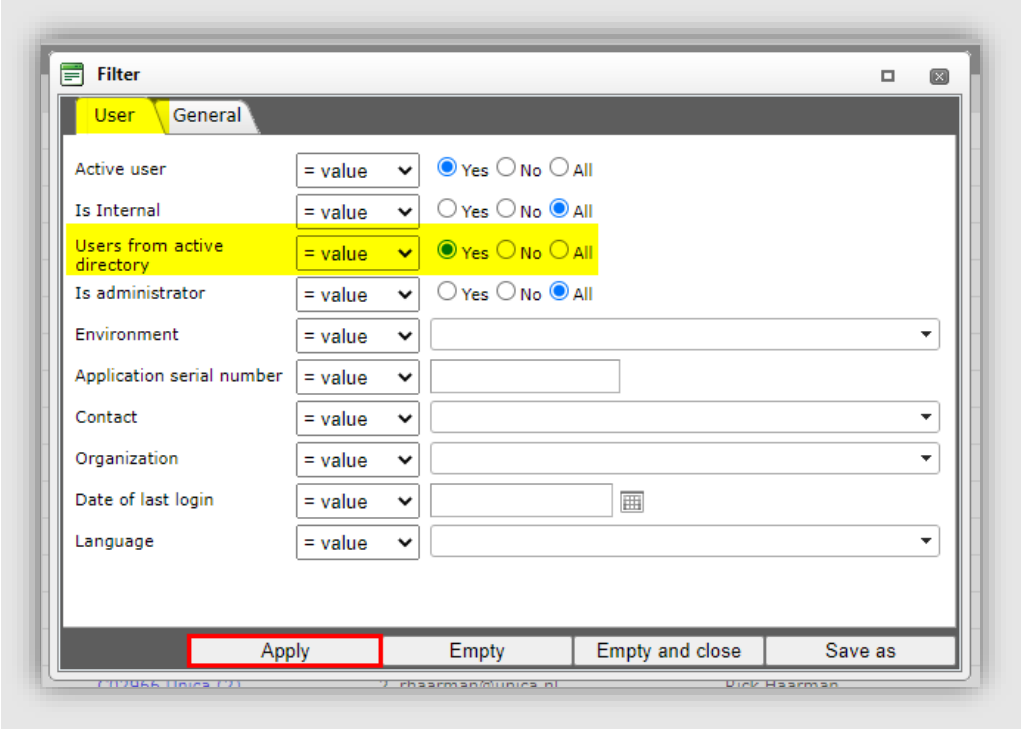
1. Through the Menu, go to *System > Users*:



2. Under View, click on the Filter button:



3. In the Filter window, set *Users from active directory* to *Yes*:

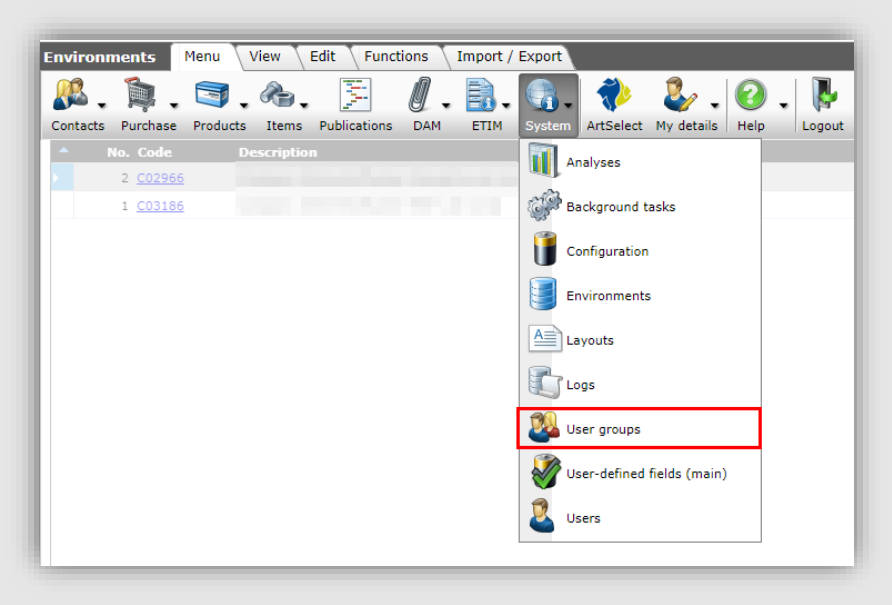


4. Apply the filter.

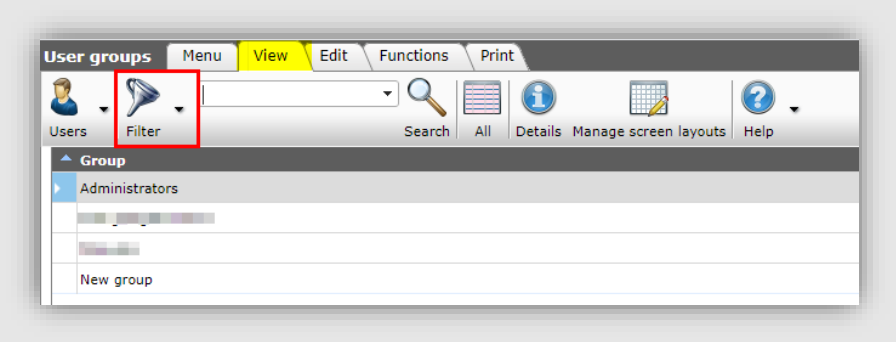
8.2 Filtering AD-groups

To filter AD-groups in COS:

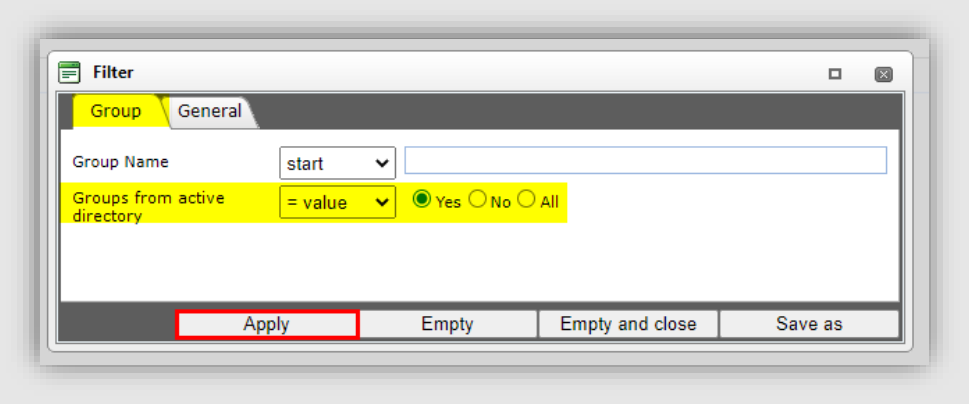
1. Through the Menu, go to *System > User groups:*



2. Under View, click on the Filter button:



3. In the Filter window, set *Groups from active directory* to *Yes*.

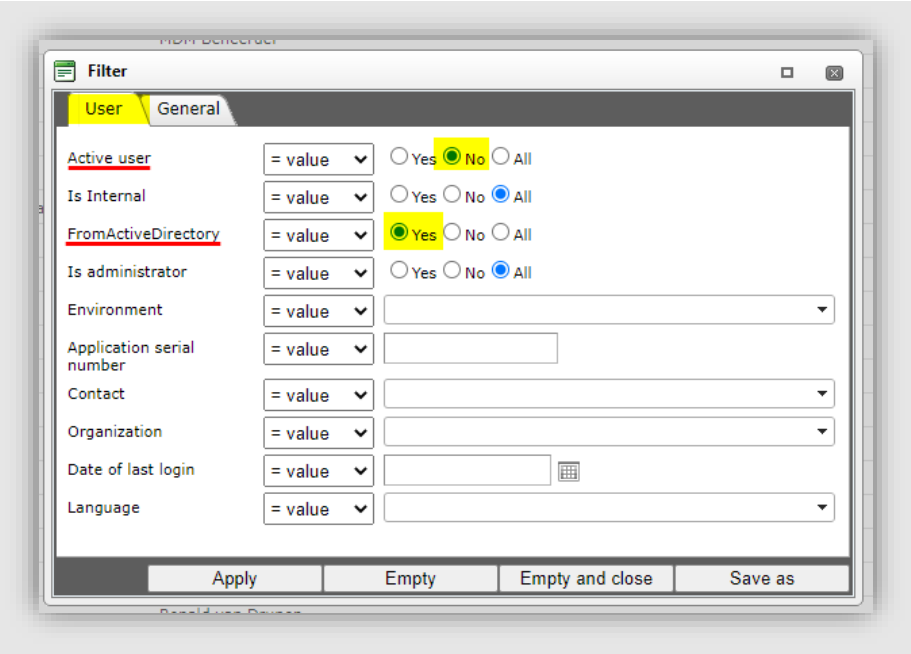


4. Apply the filter.

8.3 Filtering inactive users

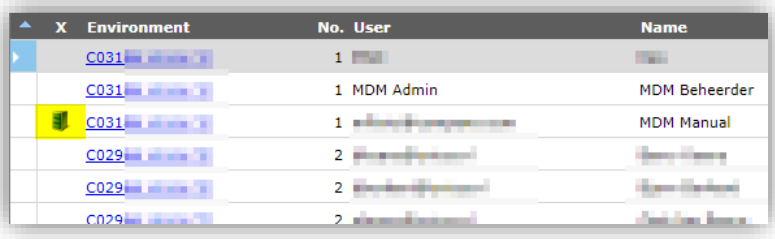
Users which are removed from your Azure AD will be ***archived*** on the next sync to Compano. These users will no longer be able to login to Compano and are considered ***inactive***.

To view inactive Azure AD users in Compano, set your filter thus:



- **Active user**: Set to *No*.
- **FromActiveDirectory**: Set to *Yes*.

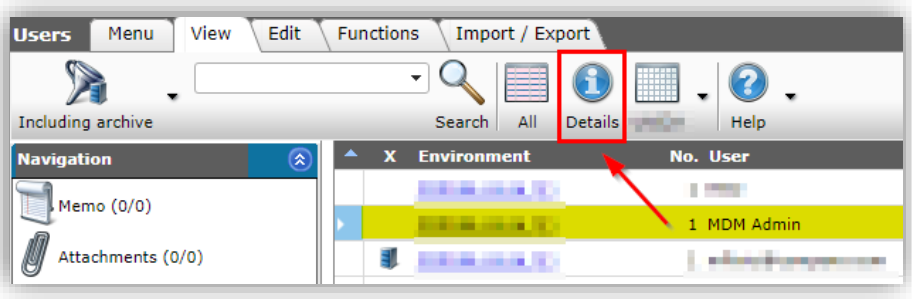
Inactive users will be identified by an archive icon next to their name:



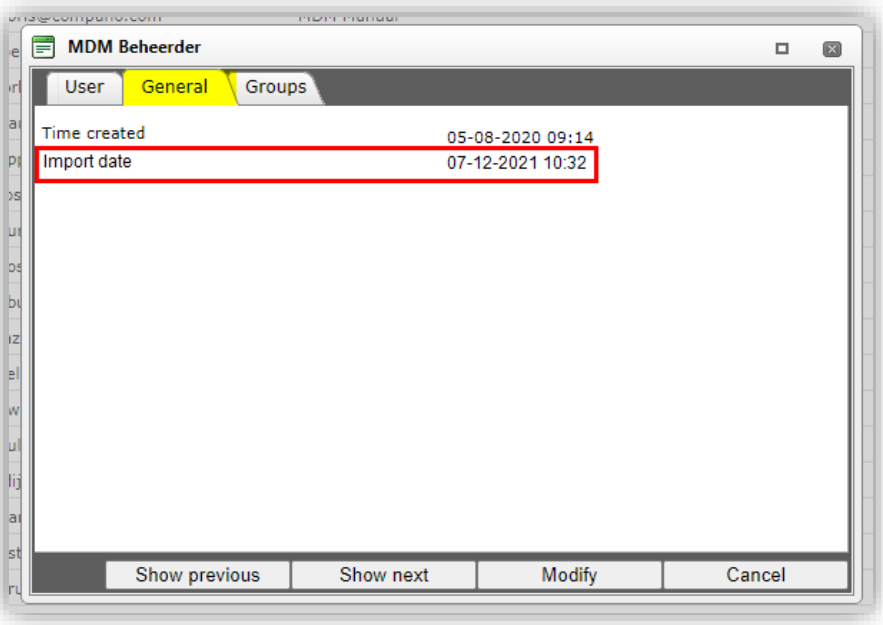
8.4 View last synced dates

By viewing the User Details, you can check when a user from you Azure AD was last synced to Compano:

1. Select users from the User overview and, under View, click on *Details*:



2. In the pop-up window, check the *Import date* on the tab *General*.


MDM Beheerder
User
General
Groups
Time created
05-08-2020 09:14
Import date
07-12-2021 10:32
Show previous
Show next
Modify
Cancel