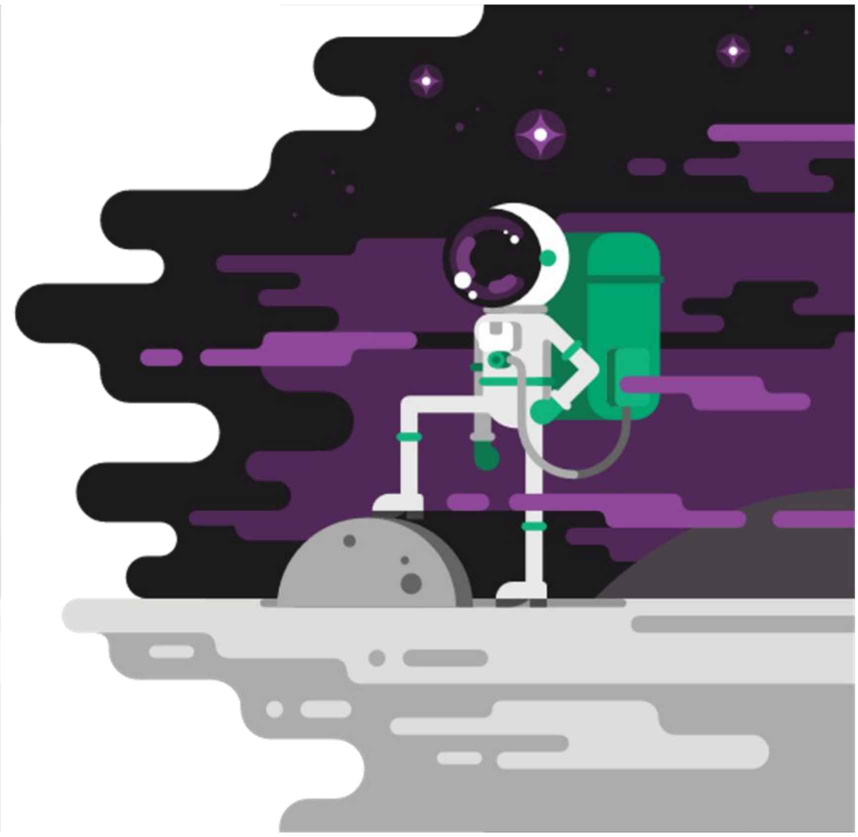


USER PROVISIONING SETUP

How to automate user management with Betr Leap

ABSTRACT

This document explains how to enable provisioning of users from Azure Active Directory to Betr Leap to automate user management.

Contents

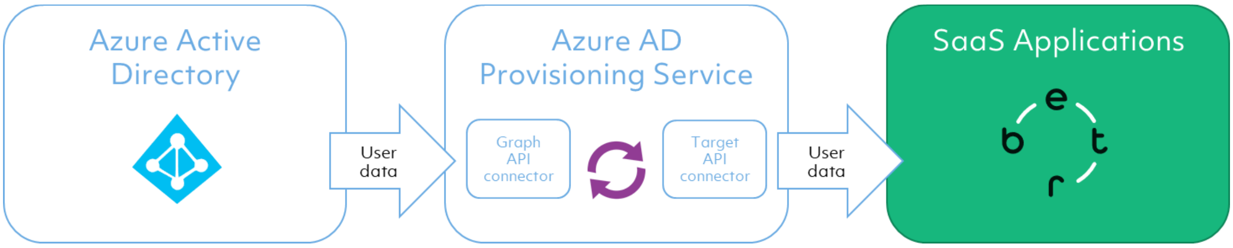
1 Introduction

Betr Leap is a SaaS application for Integrated Risk Management. Leap is using Azure Active Directory for Authentication of users. This enables Single Sign On for users using their work account. This document explains how to set up User Provisioning with Azure Active Directory to automate creation, maintenance and removal of user identities with Betr Leap.

When user provisioning is enabled, Azure Active Directory administrator will be able to control access to the application using Azure Portal.

To configure provisioning, you will create an Enterprise Application definition in Azure Active Directory defining mapping of user properties between systems.

Provisioning will add your selected users to Betr Leap and assign them to Betr Leap roles. Users added will always authenticate using your organizations Azure Active Directory. Betr Leap does not store any passwords – only the properties provisioned.



1.1 High level process

1. Enable Azure Active Directory Synchronization in Betr Leap
2. Create connector in Azure Active Directory
3. Verify Attribute Mappings
4. Add users
5. Enable provisioning

2 Enable AAD synchronization in Betr Leap

You (or the Betr Leap subscription owner) can enable provisioning and get *Provisioning URL* and *Token* using this procedure.

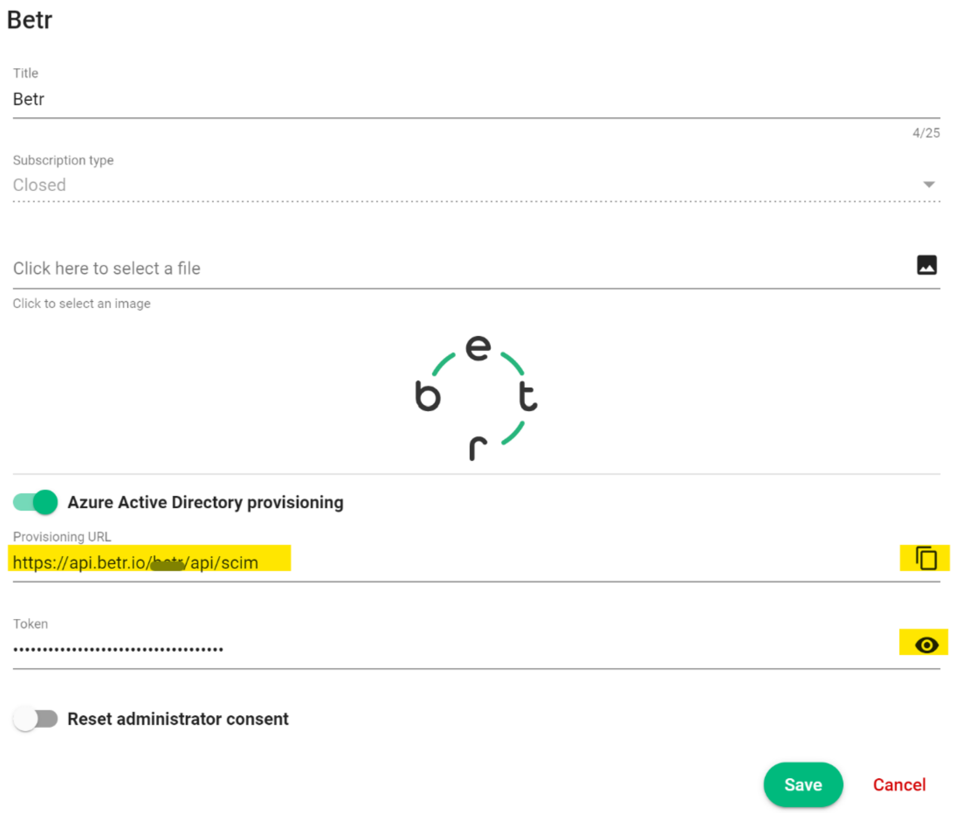
If you do not already have a Betr Leap subscription, you can create one.

IMPORTANT: You need to log in using an account from same AAD tenant you will use to set up user provisioning.

You can find steps to create your subscription in this article:
https://betr.zendesk.com/hc/no/articles/360025826392

To enable Betr Leap for user provisioning:

1. Navigate to https://leap.betr.io and sign in
2. Click your avatar image and select "Subscriptions"
3. Click the "pearl menu" on the subscription card for your subscription
4. Select Modify
5. Enable Azure Active Directory provisioning
6. Copy values from Provision URL and Token using the copy icon - you will need them later (click eye icon to make token visible)



Betr

Title
Betr
4/25

Subscription type
Closed

Click here to select a file
Click to select an image

Azure Active Directory provisioning

Provisioning URL
https://api.betr.io/[redacted]/api/scim

Token
•••••••••••••••••••••••••••••••••••

Reset administrator consent

7. Click Save to enable your Betr Leap subscription for provisioning

3 Create connector in Azure Active Directory

Azure Active Directory provides Enterprise Application registrations to enable Single SignOn, provisioning, maintenance and deprovisioning of user access to applications.

You will need Azure Active Directory administrative privileges to perform this procedure.

3.1 Add a Non-gallery Enterprise application

Betr Leap is currently not registered in Azure Marketplace. Instead we are using a custom connector (a non-gallery application) for our integration purposes.

1. Navigate to https://portal.azure.com -> Azure Active Directory -> Enterprise applications
2. Click New application
3. Select Non-gallery application
4. Give your application registration a name and click Add

5. Select Manage -> Properties
6. Set Enabled for users to sign-in to **No**
7. Set Visible to users to **No**
8. Click Save

3.2 Add roles to App registration

To be able to set access level in Betr Leap, you will add roles to the Enterprise Application registration created. To add the roles you will need to edit the manifest.

1. Right click Azure Active Directory in left menu and open in a new tab
2. Select App registrations
3. Select All applications
4. Use filter to find the app registration you just created
5. Select your app registration
6. Select Manifest
7. The "appRoles" section should be replaced with text below:

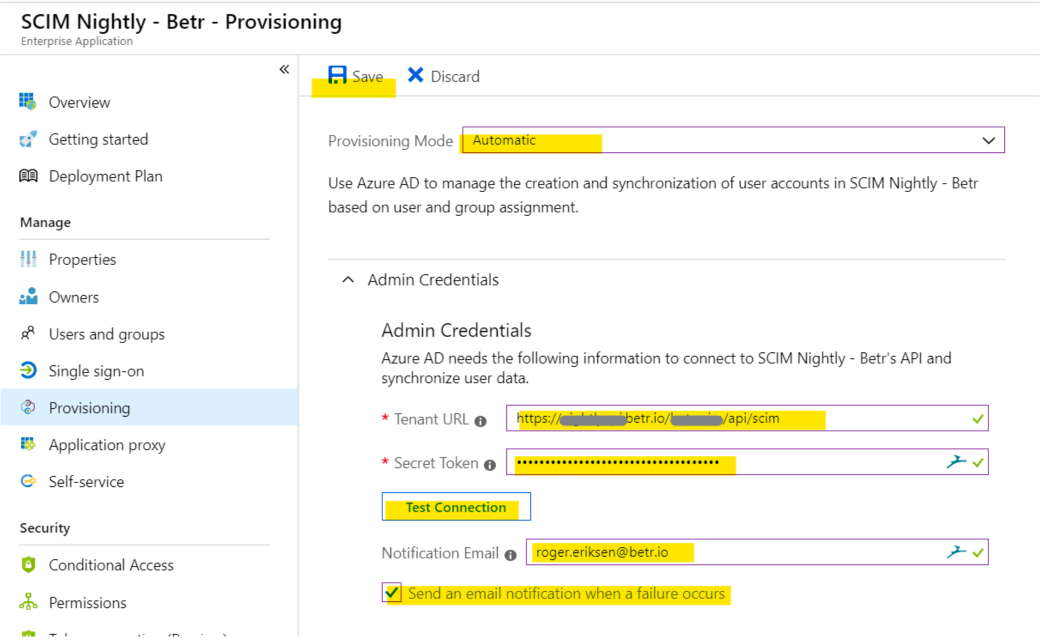
```
"appRoles": [
  {
    "allowedMemberTypes": ["User"],
    "description": "SubscriptionOwner",
    "displayName": "Subscription owner",
    "id": "de9d4c6f-b6ad-4c15-b24b-4bb97f2e6ee4",
    "isEnabled": true,
    "lang": null,
    "origin": "Application",
    "value": null
  },
  {
    "allowedMemberTypes": ["User"],
    "description": "Can create space",
    "displayName": "Space creator",
    "id": "374050e7-1e29-4fa5-893c-156ca4563e93",
    "isEnabled": true,
    "lang": null,
    "origin": "Application",
    "value": null
  },
  {
    "allowedMemberTypes": ["User"],
    "description": "Can log in to Betr",
    "displayName": "Member",
    "id": "18d14569-c3bd-439b-9a66-3a2aee01d14f",
    "isEnabled": true,
    "lang": null,
    "origin": "Application",
    "value": null
  },
  {
    "allowedMemberTypes": ["User"],
    "description": "msiam_access",
    "displayName": "msiam_access",
    "id": "b9632174-c057-4f7e-951b-be3adc52bfe6",
    "isEnabled": true,
    "lang": null,
    "origin": "Application",
    "value": null
  }
],
```

8. Save

3.3 Set Provisioning mode and Admin Credentials

Roles are now added to your Enterprise application registration. This will make you able to define user roles when adding users in a later step.

1. In Azure Portal – Navigate to Active Directory -> Enterprise applications
2. Select the application registered in “3.1 Add a Non-gallery Enterprise application”
3. Select Manage -> Provisioning
4. Set Provisioning mode to Automatic
5. Add Provisioning URL from previous section into Tenant URL field
6. Add Token from previous section into Secret Token field
7. Optionally you can add an email address to receive notifications from connector and check Send an email notification



SCIM Nightly - Betr - Provisioning

Enterprise Application

Provisioning Mode: Automatic

Use Azure AD to manage the creation and synchronization of user accounts in SCIM Nightly - Betr based on user and group assignment.

Admin Credentials

Admin Credentials

Azure AD needs the following information to connect to SCIM Nightly - Betr's API and synchronize user data.

* Tenant URL: https://[redacted]betr.io/[redacted]/api/scim

* Secret Token: ••••••••••••••••••••••••••••••••••••

Test Connection

Notification Email: roger.eriksen@betr.io

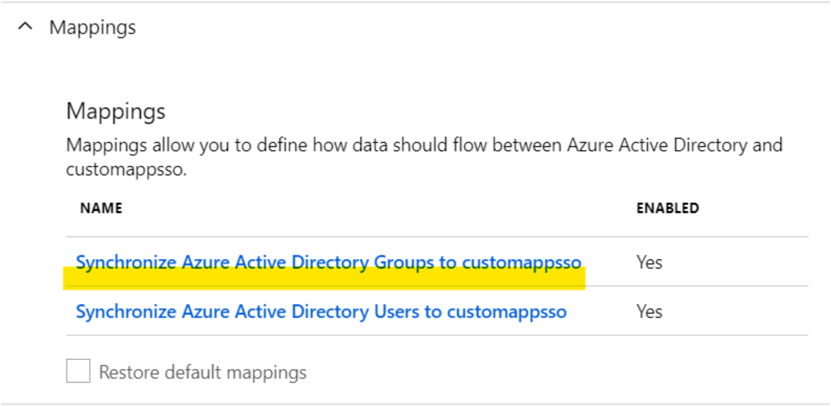
☑ Send an email notification when a failure occurs

6. Click Test Connection to verify if credentials are valid.
7. Click Save

3.4 Disable Groups synchronization

Betr Leap does not yet support provisioning groups from Azure Active Directory. This setting will prevent Azure Active Directory from trying to provision groups. You will still be able to provision users to different roles using groups as explained in *3.6 Add users or groups.*

1. Expand Mappings
2. Click Synchronize Azure Active Directory Groups to customappsso



Mappings

Mappings

Mappings allow you to define how data should flow between Azure Active Directory and customappsso.

NAME	ENABLED
Synchronize Azure Active Directory Groups to customappsso	Yes
Synchronize Azure Active Directory Users to customappsso	Yes

□ Restore default mappings

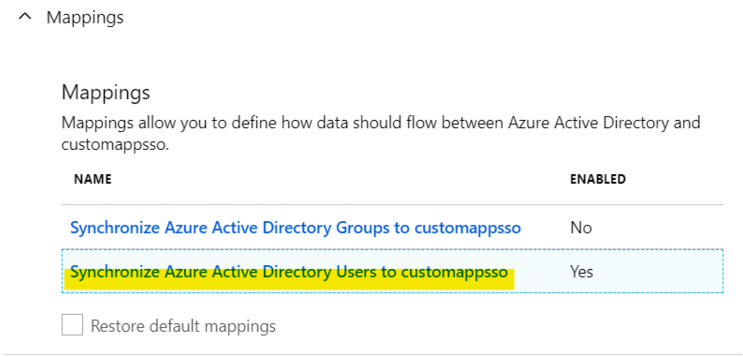
3. Set Enabled to **No**
4. Click Save

3.5 Edit User mappings between AAD and Betr Leap (customappsso)

When setting up mapping, *Source* attributes are the attributes each user object has in Azure Active Directory and *Target* attribute is the corresponding attribute for each user object in Betr Leap – also referred to as customappsso.

This section explains how to set up the mappings between Azure Active Directory users and Betr Leap users.

1. Expand Mappings
2. Click Synchronize Azure Active Directory users to customspps



Mappings

Mappings

Mappings allow you to define how data should flow between Azure Active Directory and customappsso.

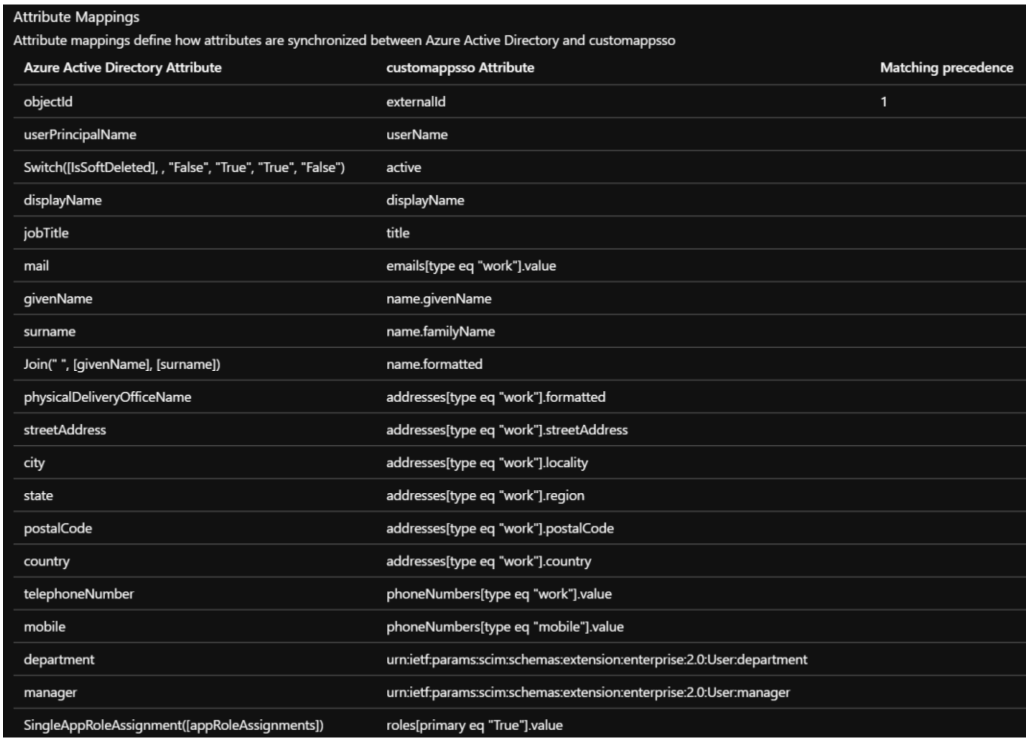
NAME	ENABLED
Synchronize Azure Active Directory Groups to customappsso	No
Synchronize Azure Active Directory Users to customappsso	Yes

□ Restore default mappings

3. Delete these mappings
   a. preferredLanguage -> preferredLanguage
   b. facsimileTelephoneNumber -> phoneNumbers[type eq "fax"].value
   c. employeeId -> urn:ietf:params:scim:schemas:extension:enterprise:2.0:User:employeeNumber
4. Edit **userPrincipalName -> userName**
   Change Matching precedence to "*2*"
5. Edit **mailNickname -> externalId**
   Change to *objectId* -> externalId
   Set "Match objects using this attribute" to Yes (Matching precedence = 1)
6. Edit **userPrincipalName -> userName**
   Set "Match objects using this attribute" to No.
7. Add new mapping
   Set *Mapping type* to **Expression**

Enter value **SingleAppRoleAssignment([appRoleAssignments])** in *Expression* field
Set *Target attribute* to **roles[primary eq "True"].value**

The result of your changes should look like this:



Attribute Mappings

Attribute mappings define how attributes are synchronized between Azure Active Directory and customappsso

Azure Active Directory Attribute	customappsso Attribute	Matching precedence
objectId	externalId	1
userPrincipalName	userName	
Switch([IsSoftDeleted], , "False", "True", "True", "False")	active	
displayName	displayName	
jobTitle	title	
mail	emails[type eq "work"].value	
givenName	name.givenName	
surname	name.familyName	
Join(" ", [givenName], [surname])	name.formatted	
physicalDeliveryOfficeName	addresses[type eq "work"].formatted	
streetAddress	addresses[type eq "work"].streetAddress	
city	addresses[type eq "work"].locality	
state	addresses[type eq "work"].region	
postalCode	addresses[type eq "work"].postalCode	
country	addresses[type eq "work"].country	
telephoneNumber	phoneNumbers[type eq "work"].value	
mobile	phoneNumbers[type eq "mobile"].value	
department	urn:ietf:params:scim:schemas:extension:enterprise:2.0:User:department	
manager	urn:ietf:params:scim:schemas:extension:enterprise:2.0:User:manager	
SingleAppRoleAssignment([appRoleAssignments])	roles[primary eq "True"].value	

8. Save your changes
9. Set Provisioning Status to "On" – if not already On.

3.6 Add users or groups

This section explains how to add users and set roles for users to be provisioned to Betr Leap.

Betr Leap has three types of roles, each giving users different permissions; *Subscription owner*, *Space creator* and *Member*.

Members can

- Become a member of and contribute in a Space
- Contribute using Tell
- Attend surveys using Ask
- Can be promoted to a Space owner

Space Creators can

- Everything a member can do
- Create new Spaces and become owner of the Space

Subscription owner can

- Everything a Member and Space Creator can do
- Enable/disable Azure Active Directory provisioning
- Take ownership of any Space
- Change Subscription logo and description

IMPORTANT: Due to limitations in current Betr Leap version, a user can not be assigned more than one role. If using groups to assign roles, you need to make sure that user will not be a member of multiple roles!

You can add both Azure Active Directory Users and Groups to Betr Leap roles.

From your “non-gallery” application definition:

1. Select Users and groups
2. Click Add user
3. Click Users and groups to add users
4. Click Select Role to define role for selected users/groups
5. Click Assign to assign users/groups to role

3.7 External users

Enabling provisioning will disable any user management in Betr Leap. If you need to allow external users to access your Betr Leap subscription, you will need to add external users as guests in you Azure Active Directory. You can assign guest users any role in Betr Leap.

Only users from other Azure Active Directory tenants are supported.

3.7.1 Adding Guests users

To add guest users to your Azure Active Directory:

https://docs.microsoft.com/en-us/azure/active-directory/b2b/add-users-administrator

3.7.2 Guest/external user sign in

When using the default URL to sign in to Betr Leap, user will always authenticate with his/her Azure Active Directory tenant. For an external user to sign in to your Betr Leap subscription you will need to authenticate with you tenant. Currently we do not provide a way to select what directory to use when signing in. To find the sign in URL for external users:

1. Sign in to your Betr Leap subscription
2. When signed in you need to get the subscription name part of the URL. This will be the last part of your URL after signing in: https://leap.betr.io/en/subscription/<*subscription name*>
3. Guest user sign in URL will be https://leap.betr.io/en/login/<*subscription name*>
4. Guest user will sign in using his/her own username/password.

3.8 Enable synchronization

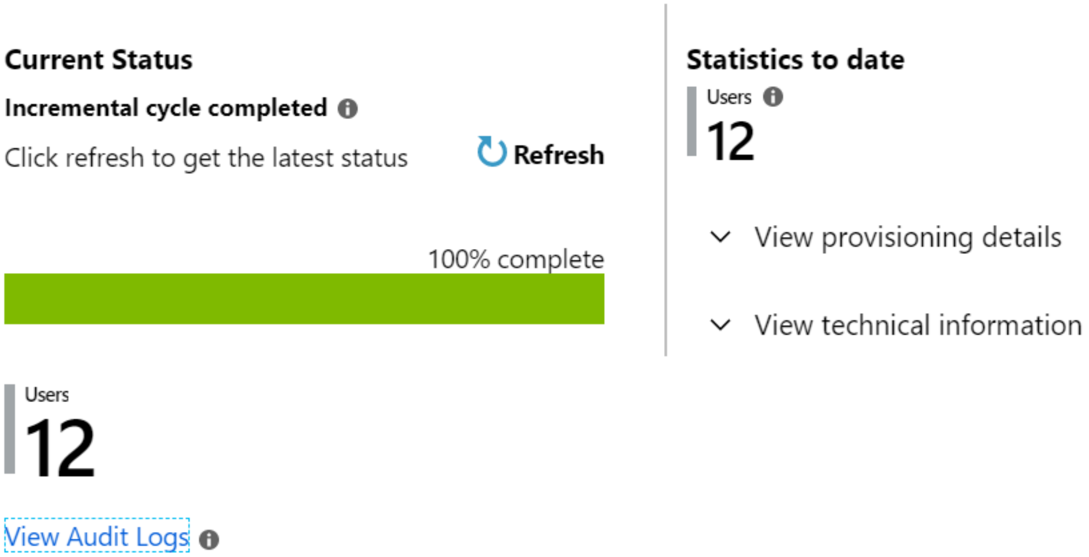
When Attribute Mapping is confirmed by Betr, you can enable Provisioning.

1. Select Provisioning
2. Under Settings, set Provision Status to On

3. Click Save

3.9 Verify synchronization

It will take Azure Active Directory some time to start your synchronization job, depending on number of users, number of groups etc. Within Provisioning you can check status of synchronization and also open Audit logs to view synchronization details:



Current Status

Incremental cycle completed

Click refresh to get the latest status

Refresh

100% complete

Users

12

View Audit Logs

Statistics to date

Users

12

View provisioning details

View technical information

3.10 Hide app registration from users

Any application registered in your Azure Active Directory will be made available to users from both Office 365 (https://account.activedirectory.windowsazure.com/) and Azure portal (https://account.activedirectory.windowsazure.com/).

To avoid the Enterprise App registration used for provisioning to be visible for users, you should hide this from the end user. This can be achieved using this procedyre:

https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/hide-application-from-user-portal#hide-an-application-from-the-end-user

4 Resources

Automate user provisioning and deprovisioning to SaaS applications with Azure Active Directory

https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/user-provisioning