

# Azure AD SCIM Provisioning for ZERO

## Quick Setup Guide

1. Sign in with a privileged administrator role at <https://Portal.Azure.com>
2. Go to **Azure Active Directory**
3. Select **Enterprise Applications** on the left-hand side.
4. Select **Add New Application** (Microsoft currently is not approving gallery app changes until at least January 2021).
5. Select Non-gallery Application under **Add your own app**
  - a. Name: ZERO SCIM Integration
  - b. Click **Add** (near bottom)
6. Select **Provisioning** on left side
7. Click **Get Started**
8. Change mode to automatic
9. Complete credentials:
  - a. Enter tenant url: <https://api.teamzero.com/scim/v2/>
  - b. Enter Secret token: [provided by ZERO]
  - c. Enter notification email to receive any provisioning errors
  - d. Check box for "Send an email notification when a failure occurs"
  - e. Click **Test Connection**
10. Click **Save** (near top) after a successful test.
11. Select your application name in the breadcrumbs near the top.
12. Select **"Edit attribute mapping"**
  - a. Expand Mapping section
  - b. Select **Provision Azure Active Directory Groups**
    - i. Verify it matches the group mapping below
  - c. Select **Provisioning** at top
  - d. Select **Provision Azure Active Directory Users** underneath Mapping
    - i. Update to the User Mapping below.
      1. Note: various entries will need to be removed and added.
    - ii. Add the mapping for ObjectID (required)
      1. Mapping Type: Direct
      2. Source attribute: objectID
      3. Target attribute: externalId
      4. Leave match object using this attribute: no and apply this mapping: always
      5. Click Ok
    - iii. Add the mapping for companyName (if desired)
      1. Mapping Type: Direct
      2. Source attribute: companyName
      3. Target attribute: urn:ietf:params:scim:schemas:extension:enterprise:2.0:User:organization
      4. Leave match object using this attribute: no and apply this mapping: always
      5. Click **Ok**
    - iv. Click **Save**

1. Review and approve any extra message if you want the your settings to change
  - e. \*\* Additional capabilities are available in mapping related to filters and various advanced settings that may be helpful to experienced enterprise accounts.
13. Select provisioning in top bread crumbs
14. Ensure scope is set as **“Only assigned users and groups”**
15. Toggle Provisioning Status from “Off” to **“On”**
16. Click **Save**
17. Click **ZERO SCIM Integration** in top breadcrumbs
18. Go to **“Users & Groups”** on left hand menu to configure your users and groups
19. If you do not want users to see they have provisioned, select Properties on the left hand side and change **“Visible to users?”** to **no**.

## Admin Credentials

Tenant URL: <https://api.teamzero.com/scim/v2/>

Secret Token: Provided by ZERO support team

## Settings

Scope: “Sync only assigned users and groups”.

Setting sope to “All users and groups” may create more groups than expected in ZERO based on your AD setup.

## Mapping

*Azure AD attributes can be changed to what fits best with your setup, but we recommend that the attributes highlighted in green are left as is.*

### User mapping

Azure AD Attribute	customappsso Attribute	Required	
userPrincipalName	userName	Yes	Email address. This is used to login to ZERO
Not([IsSoftDeleted])	active	Yes	Activate/Remove
jobTitle	title	No	Job Title
givenName	name.givenName	Yes	First Name
surname	name.familyName	Yes	Last Name
telephoneNumber	phoneNumbers[type eq “work”].value	No	Phone
department	urn:ietf:params:scim:schemas:extension:enterprise:2.0:User:department	No	Department Name (for reports)

(add the mappings below)			
objectId	externalId	Yes	
companyName	urn:ietf:params:scim:schemas:extension:enterprise:2.0:User:organization	No	Company Name (for reports)

If any attribute is updated at Azure AD - it will update at ZERO on the next interval cycle. The interval cycle is variable and not in ZERO control. You may be able to manually send a user update through Azure provisioning.

## Group mapping

Azure AD Attribute	customappsso Attribute	
displayName	displayName	Team Name in ZERO
objectId	externalId	This attribute is tracked with the team in ZERO. By default, ZERO will work off an active group that matches the displayName. This externalId allows group names to be controlled and changed by SCIM.
members	members	These use are synced via SCIM and added to the team

If any group is updated at Azure AD - it will update at ZERO on the next interval cycle. The interval cycle is variable and not in ZERO control. You may be able to manually send a user update through Azure provisioning.

## Basic Description

*Assumes app scope is set to "Sync only assigned users and groups"*

## Group syncing

Groups are synced as "**Teams**" in the Zero app. The Group name becomes the Team name, and any members of the Group in AD become members of the Team in Zero. Those users are synced as described below.

If a user is added/removed from a synced Group, this will also reflect in the Zero Teams. A user can still be added/removed from teams in Zero. This will not affect the user in AD, and there may be scenarios where AD will overwrite this.

- It is currently unclear if an AD resync event will remove manually added users.
- If the user is added into a new group in active directory, it will add the user to the new group



- If a user is added to a new group in AD that they were previously manually added to, no impact is expected to the end user.

Previously synced groups that are removed from the provisioning app will cause the corresponding team to be archived in Zero. All of the data will still be available to review. If the group is readded to the provisioning app, it will be unarchived.

If a team is manually created and then a team with the same name is created in Active Directory, the manually created team will be “taken-over” and controlled by Active Directory

## User syncing

Users will be synced if they are added directly to the Zero app in Azure. They are also synced if assigned to a group that is assigned to Zero.

Display Name		Object Type
<input type="checkbox"/>	 <b>SCIM Sync</b>	Group
<input type="checkbox"/>	 <b>Scim Team 2</b>	Group
<input type="checkbox"/>	 <b>Tim Hamilton</b>	User

In the example above, Tim Hamilton and any users that are a member of the “SCIM Sync” and “Scim Team 2” groups will be synced with Zero.

When a new user is assigned to the app in AD, a user profile is created in Zero matching that user. Any changes to the user’s synced attributes (from User mapping settings) in AD will also be carried over in the Zero app. All users will be given the “Member” role in the Zero app when created through provisioning. There’s currently no way to manage the user’s role in Zero through AD.

- User roles may be manually changed in ZERO and users will remain with any manually assigned role in ZERO. Once a user role is changed - it will never be modified by AD.
- If a user is removed through SCIM provisioning and later added back to an organization, the user will begin as the “Member” role.

If a previously synced user is deleted in AD, or is no longer assigned to the Zero provisioning app, they will be deactivated in Zero. Their data will still be available, but they will not be able to log in to Zero. If the user is reassigned to the provisioning app, their account will be restored.

## Group Deletion and Changes

If a user is removed from a group and does not exist in any other group in AD, that user will be deactivated regardless of if they have other teams in ZERO. The user can be added as a user in the provisioning app in addition to groups to prevent this problem or they can be manually reactivated.

If a group is deleted and a user account only exists in that one group in AD, that user will be deactivated regardless of if they have other teams in ZERO. The user can be added as a user in the

provisioning app in addition to groups to prevent this problem or they can be manually reactivated.

#### **Version History**

1.0	15 July 2020	Initial Release
1.1	29 July 2020	Removed User mapping “active” group type.
1.2	03 March 2021	AccountEnabled setting for users when doing user and group mapping