SAVANCE WORKPLACE

Microsoft Azure AD Integration Setup

Phone: 248-478-2555
Fax: 248-478-3270
Email: support@savance.com
www.savanceworkplace.com

© 2024 | Savance

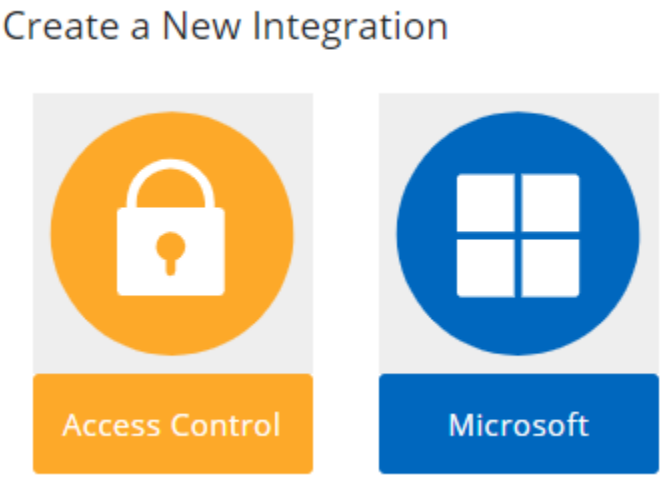
Overview

For the Active Directory (AD) integration, Savance Workplace calls information from AD and does all of the work for syncing with AD. This means that anything done in AD will also be reflected eventually in Savance Workplace. However, this may occur automatically depending on how often the sync interval is set to be. (For example if the sync user interval is set to 1, Savance Workplace and AD will sync every hour.) Note: While Savance Workplace and AD should sync automatically if the option is selected, changes in AD may take time to reflect within Savance Workplace.

AD will auto add users who are added to groups that have had all its users synced. Savance Workplace won't auto add users added to partially full groups. This way a user can be in multiple groups, but we're recommending they add an SW Sync group and put users they want to sync into it. Users can also be automatically removed if they have also been removed from AD as well.

Create the Integration

Log into Savance Workplace via Web, and click the “Admin” option. On the left hand side of the page, you should see “Integrations”, and a drop-down menu will appear. This should reveal “User & Access Control Integrations”, which you want to click to be able to create your AD Integration. Click the blue lock with “Microsoft” written underneath to begin creating your integration.



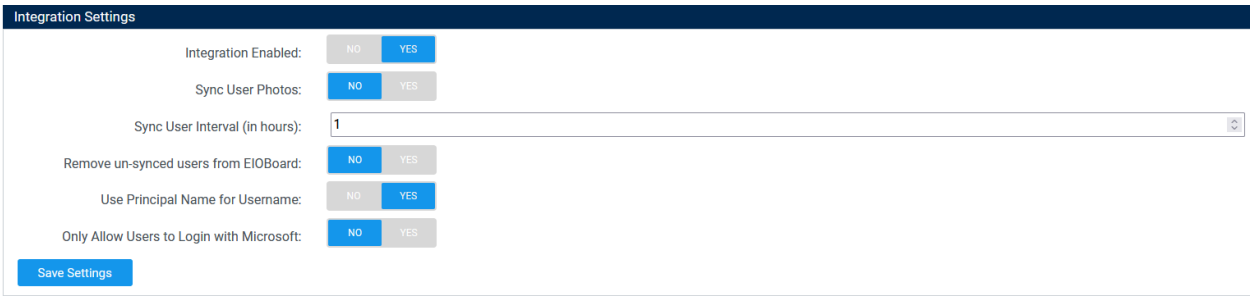
Name the integration something appropriate for your organization and click Create.

Configure the Integration

The following settings are available at this time for Microsoft Integrations.

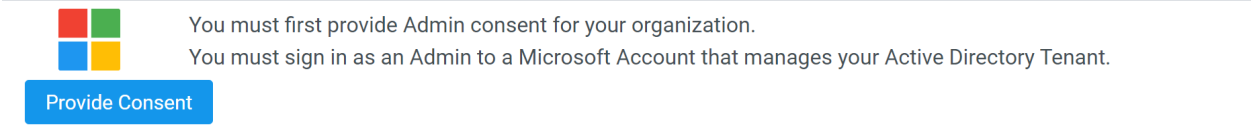
- Integration Enabled: Toggling this to No will disable the integration. Disable the integration if you no longer want to allow SSO for your users.
- Sync User Photos: Whether you sync User Pictures to the 'Pic' field of their user account
- Sync User Interval: How many hours between each automatic sync (Note: may be longer in actuality due to not starting the timer for the next sync until the current sync is finished)
- Remove unsynced users from Savance Workplace: Removes a user from Savance Workplace if they're removed from Azure AD or unchecked from the Template
- Use Principal Name for Username: Uses the Principal Name for Username. Can be useful if you change people's emails in Azure without changing their username
- Only Allow Users to Login with Microsoft: Disables logging in with a Savance Workplace username and password, requiring Microsoft Authentication (Note:

Requires syncing in Users and having at least one synced in account as an admin before this setting can be turned on)



Grant Savance Workplace Permission

The first time you create an integration you will be asked to Grant consent on behalf of your organization to give Savance Workplace permission to view user data. Click Provide Consent and when prompted log into the Microsoft account that manages your Azure AD or Office 365 account. You will be asked to consent to some permissions. If these permissions ever change you will be asked to consent again. Should you ever feel the need, you can revoke these permissions from your Azure AD portal by going to Enterprise Applications and deleting the Savance Workplace app. This will, of course, prevent the integration from functioning.



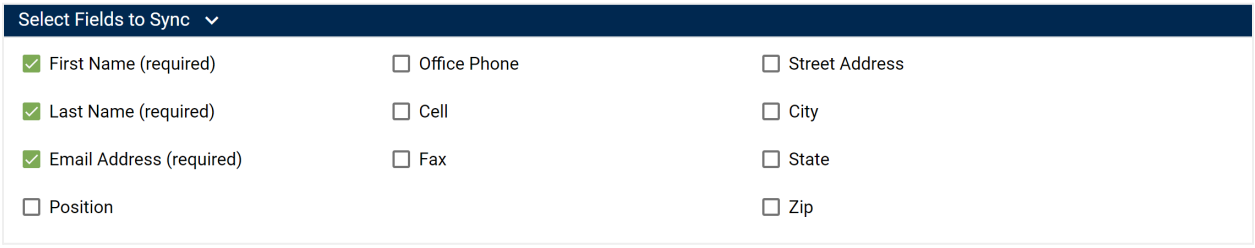
Configure Integration Settings

After granting permission, you can configure the main integration settings.

Configure Fields to Sync

By expanding the section under “Select which Fields to Sync” you can choose which fields will be imported from Microsoft to Savance Workplace. First Name, Last Name,

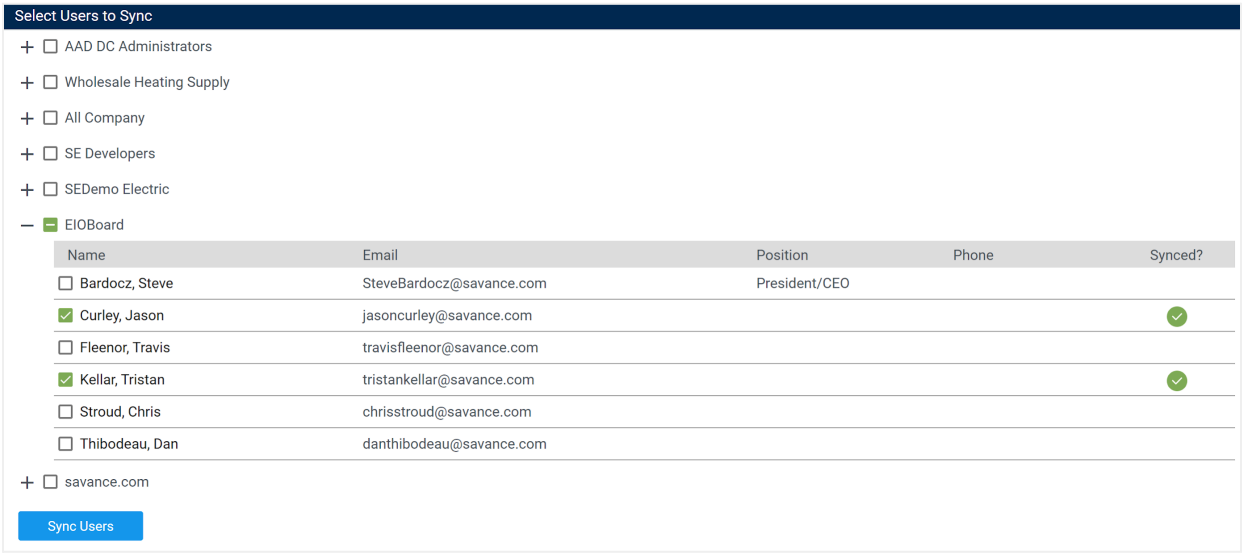
and Email Address are required as they are needed to identify unique users in Savance Workplace.



Note: The Address and location fields can be found in Savance Workplace as “Home City”, “Home Address”, etc.

Select Users to Sync

A list of user groups will appear. Users are not loaded until expanding one or more of these groups. There will always be a group that represents your whole organization, usually the name of your domain. Once the user groups are expanded, you can select which users individually that you want to sync. Clicking the checkbox next to the group name will select or deselect all users in that group. Users in multiple groups will be shown selected multiple times, however will only get synced once.



After a Sync is Complete

Results of the sync will be shown. The possible results are as follows:

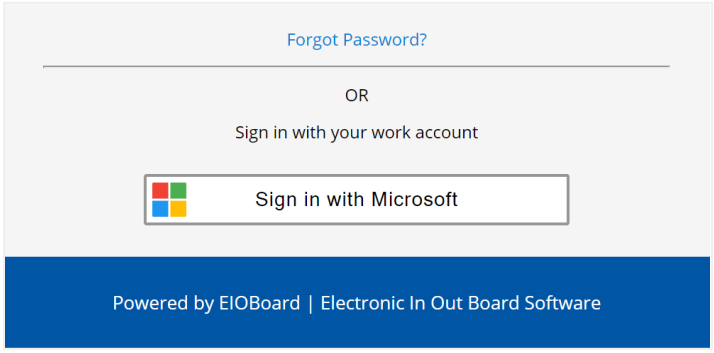
- New User Added
    - A new User was created in Savance Workplace. That user will now be able to log in using the Sign In with Microsoft button on the Savance Workplace Web Login page.
- Unmodified
    - No changes were made to the User's profile in Savance Workplace
- Modified
    - If a synced field was found to be different in Microsoft than in Savance Workplace, that field will be updated in Savance Workplace.
    - Note that if the Sync User Photos option is Yes, then the photo will be updated every time and will show as Modified.
- Error
    - An Error occurred. The user may have still been added to Savance Workplace however may need to be resynced for all fields to be imported properly or for SSO to function. Contact support if errors persist.

After a Successful Sync, the fields you had selected and the users you had selected will be saved. When returning to this page in the future, when you expand a group that had a user previously synced it will automatically select them.

Signing in to Savance Workplace with Microsoft

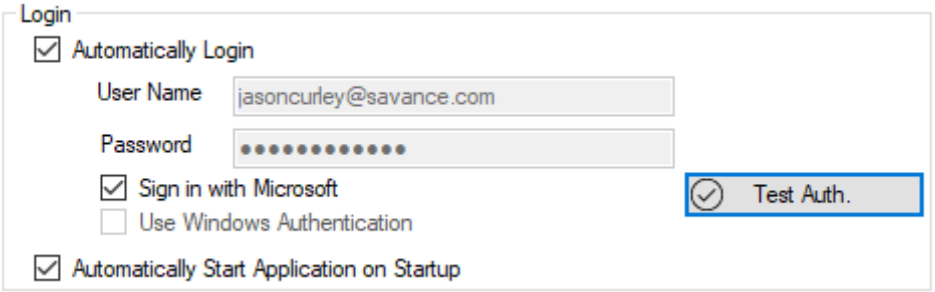
On the Login page, click the button to Sign In with Microsoft. You will be prompted to log into a Microsoft account. If your user has been synced with Microsoft then you will

be logged into Savance Workplace. Note that the Remember Me checkbox is respected if you want to stay logged into Savance Workplace.



Signing in Via The Desktop App (v10.3.5 or higher only)

In Settings on the General tab, check the box to Sign in with Microsoft. After Testing Auth. or Applying settings, you will be prompted to log into your Microsoft account. Once you are logged in, if you close and reopen the app, your credentials will be saved.



Deleting Cached Credential

If you are experiencing issues with your Microsoft login, clearing the cached credential may help. This can be done by navigating to the AppData folder. By default this is located at:
C:\Users\{user}\AppData\Roaming

Exit the Savance Workplace app and delete the file eioboard.msalcache.bin3 located in AppData. Then restart Savance Workplace. You should be prompted to log into Microsoft again.

Using on an OnPrem Account

❏ Contact Savance with the URI for your Savance Workplace website

If you are using an OnPrem account, please contact Savance with the redirect URI you wish to use. If you are hosting Savance Workplace locally, a port number would be required; however, you do not need to provide a port number in any other case. Make sure your firewall is opened, and after contacting Savance, you will have the necessary credentials needed to fully set up your integration.

❏ Copy the env.js from the VMSuite folder

You may also need to add an env.js file to the Savance Workplace website folder, one level above the ManageIntegrations Folder. The env.js file can be copied from the VMSuite folder. This should only be necessary if the website is hosted at the default and not a /EIOBoard virtual directory.

❏ Add your EIOBoard sites as the Redirect URI in the web.config

You will also need to edit the web.config in both eioboard web and the API. There are two settings, “AzureRedirectUri” and “AzureRedirectUriMobile”:

```
<add key="AzureRedirectUri" value="http://localhost/EIOBoard/Login.aspx" />
<add key="AzureRedirectUriMobile" value="http://localhost/EIOBoard/Mobile/MobileLogin.aspx" />
```

The redirect URIs specified there should match the case of the redirect URIs added by Savance on your behalf.

For Savance: Adding Redirect URLs

Log into the Azure Portal for the Savance account using an admin user.
https://portal.azure.com/
Navigate to Azure Active Directory → App Registrations → EIOBoard → Authentication
Add the following redirect URIs:
https://{public name or ip of customer hosted EIOBoard site}/ManageIntegrations/

https://{public name or ip of customer hosted EIOBoard site}/ManageIntegrations
https://{public name or ip of customer hosted EIOBoard site}/login.aspx
https://{public name or ip of customer hosted EIOBoard site}/Login.aspx
https://{public name or ip of customer hosted EIOBoard site}/VMSuite/SelfCheckIn/#/
https://{public name or ip of customer hosted EIOBoard site}/Login.aspx?SelfCheckIn=1
https://{public name or ip of customer hosted EIOBoard site}/Mobile
https://{public name or ip of customer hosted EIOBoard site}/mobile/MobileLogin.aspx
https://{public name or ip of customer hosted EIOBoard site}/Mobile/MobileLogin.aspx

Related Error Message: AADSTS50011

The Azure AD integration attempts will give this error if the redirect URL is not whitelisted on the EIOBoard Enterprise application. Savance must approve any redirect URLs.

References: AADSTS50011: Reply URL error only for Office 365 Users - Microsoft Q&A
AADSTS50011: Reply Azure Integration URL error

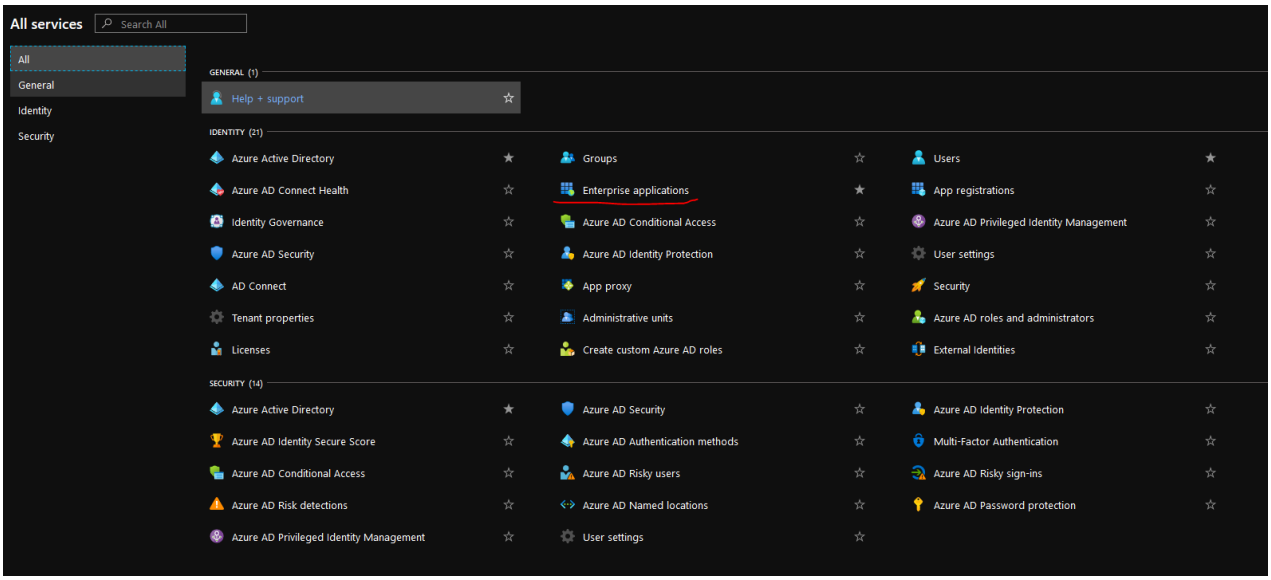
Security Concerns

EIOBoard makes calls to the Microsoft Graph API to receive information about users in your organizations. It is required that you grant consent for the following set of permissions.

API / Permissions name	Type	Description
Microsoft Graph (9)		
Group.Read.All	Delegated	Read all groups
Group.Read.All	Application	Read all groups
GroupMember.Read.All	Delegated	Read group memberships
GroupMember.Read.All	Application	Read all group memberships
offline_access	Delegated	Maintain access to data you have given it access to
User.Read	Delegated	Sign in and read user profile
User.Read.All	Delegated	Read all users' full profiles
User.Read.All	Application	Read all users' full profiles
User.ReadBasic.All	Delegated	Read all users' basic profiles

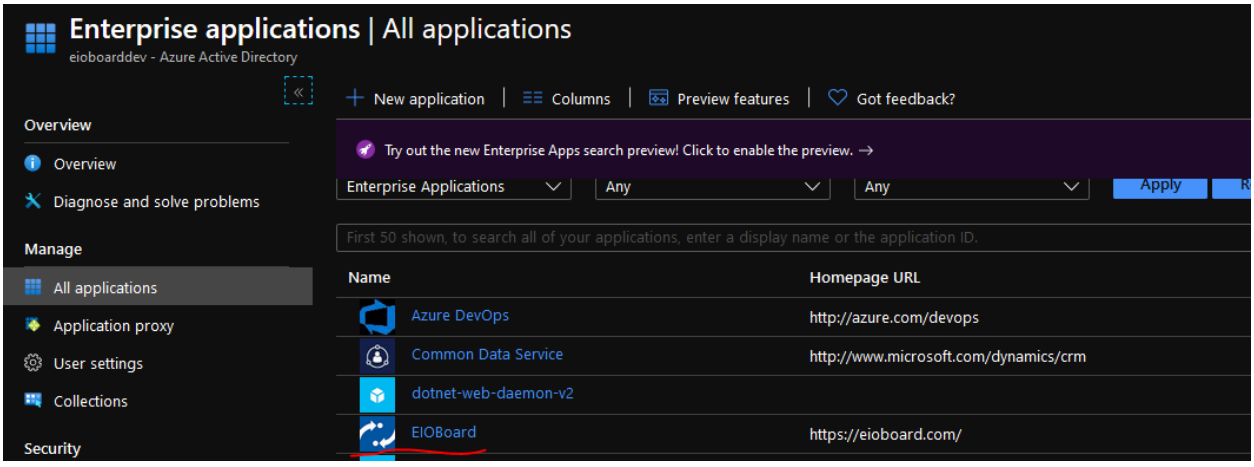
Note that some permissions appear twice as either Delegated or Application. The distinction is that EIOBoard uses Application level permissions to get user info and group info when Syncing users. The Delegated permissions are usd to validate a user when they use the Microsoft Authentication for Single Sign On.

As an Administrator, you can grant permission on behalf of your organization. If any of these permissions change, you will be notified and required to grant permission again.

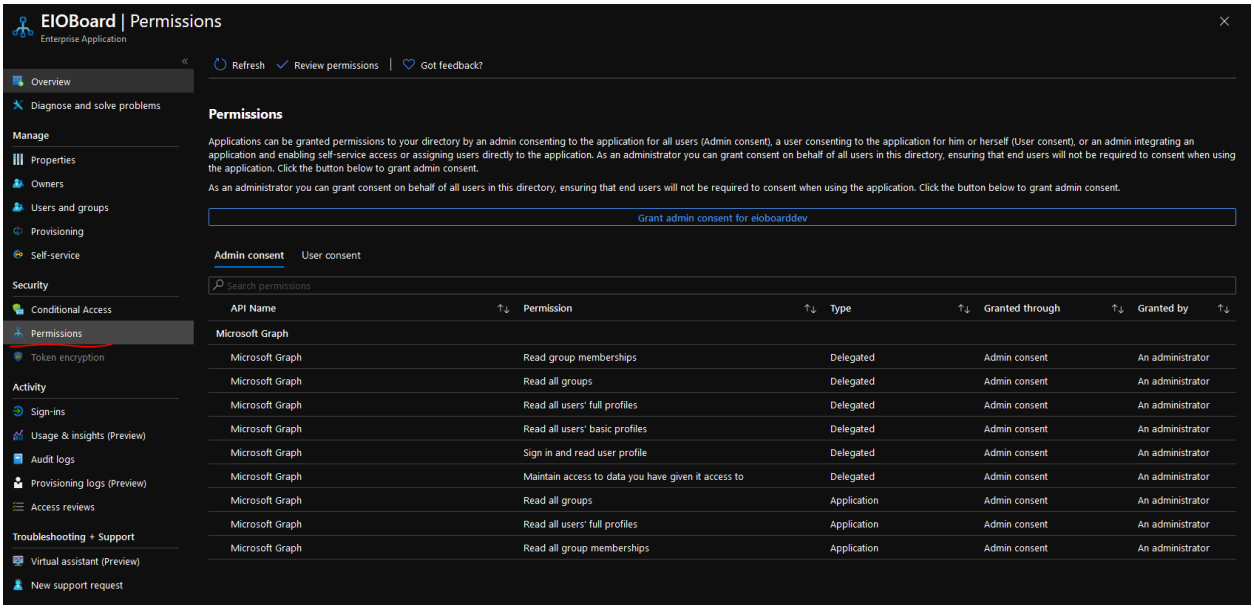


You can view these permissions from the Azure AD portal after giving consent. To do so, log into your Azure AD portal as an admin and navigate to Enterprise Applications:

EIOBoard will be listed:

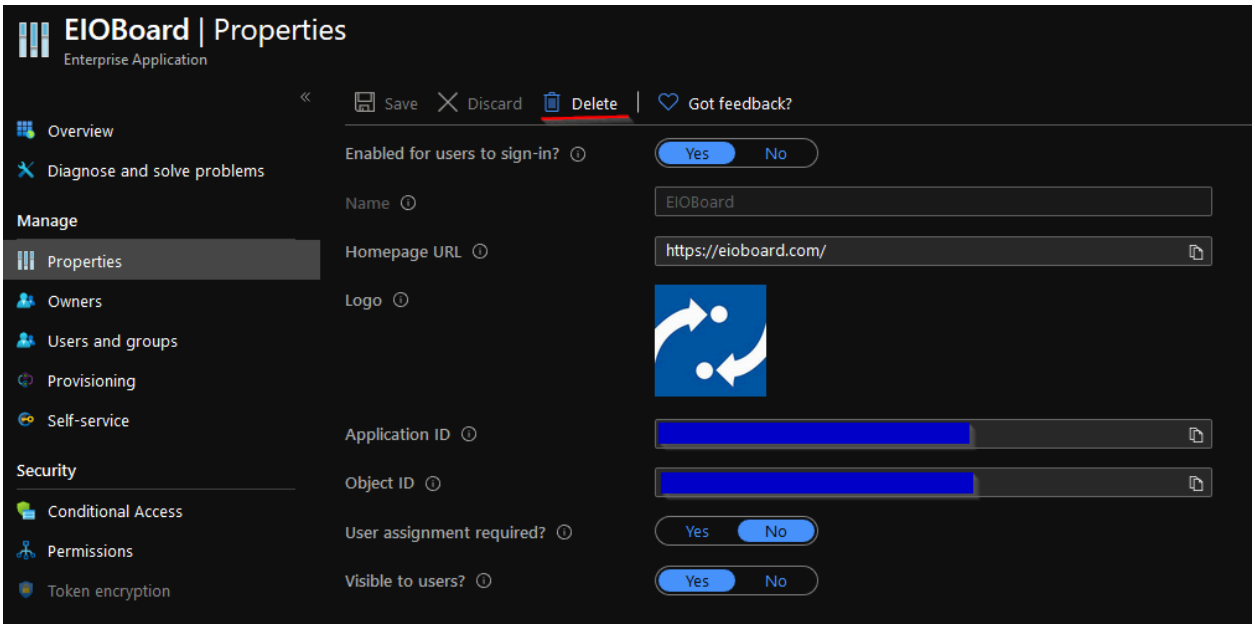


Select it and then select Permissions:



If there are issues you may need to provide admin consent again. You can do so by clicking “Grant admin consent for <you org>”.

You can revoke these permissions by navigating to the Application’s Properties and Deleting the Application.



Doing so will cause the integration to stop functioning, however, and may cause problems. The integration may need to be re-added in EIOBoard to restore functionality.

API Calls That Are Made

You can try these API calls yourself using the Microsoft Graph Explorer: https://developer.microsoft.com/en-us/graph/graph-explorer

- https://login.microsoftonline.com/organizations/v2.0
  - This is the Microsoft Oauth2.0 endpoint.
  - It is used to log users and admins into their Microsoft accounts.
- https://graph.microsoft.com/v1.0/me
  - This is used for Single Sign On, after a user has logged in with their Microsoft credentials. This matches the User's ID in EIOBoard and is to make sure the user has been Synchronized with EIOBoard.
  - The result of this API call looks like this:

```
{
    "@odata.context": "https://graph.microsoft.com/v1.0/$metadata#users/$entity",
    "businessPhones": [
        "+1 412 555 0109"
    ],
    "displayName": "Megan Bowen",
    "givenName": "Megan",
    "jobTitle": "Auditor",
    "mail": "MeganB@M365x214355.onmicrosoft.com",
    "mobilePhone": null,
    "officeLocation": "12/1110",
    "preferredLanguage": "en-US",
    "surname": "Bowen",
    "userPrincipalName": "MeganB@M365x214355.onmicrosoft.com",
    "id": "48d31887-5fad-4d73-a9f5-3c356e68a038"
}
```


- https://graph.microsoft.com/v1.0/groups?$select=id,displayName
    - This retrieves the list of Groups in your organization.
    - Example output (truncated):

```
{
    "@odata.context": "https://graph.microsoft.com/v1.0/$metadata#groups(id,displayName)",
    "value": [
        {
            "id": "02bd9fd6-8f93-4758-87c3-1fb73740a315",
            "displayName": "HR Taskforce"
        },
        {
            "id": "06f62f70-9827-4e6e-93ef-8e0f2d9b7b23",
            "displayName": "Video Production"
        },
        {
            "id": "0a53828f-36c9-44c3-be3d-99a7fce977ac",
            "displayName": "Marketing Campaigns"
        },
        {
            "id": "1381c058-2ee8-41ce-a005-aae7d91fe086",
            "displayName": "Ideas"
        },
        {
            "id": "13be6971-79db-4f33-9d41-b25589ca25af",
            "displayName": "Business Development"
        },
        {
            "id": "14d0da09-90ed-4ec6-a7b1-8e234e542fff",
            "displayName": "Quality Assurance"
        },
        {
```


- https://graph.microsoft.com/v1.0/groups/{groupId}/members{filter}
    - This gets the members of a Group.
    - Filter in this case is "?$select=id,displayName,userPrincipalName,givenName,surname,accountEnabled,birthday,businessPhones,city,companyName,country,department,employeeId,faxNumber,jobTitle,mail,mobilePhone,officeLocation,postalCode,state,streetAddress"
    - Example output (truncated):

- https://graph.microsoft.com/v1.0/users/{userId}/photo/$valuehttps://graph.microsoft.com/v1.0/users/{userId}/photos/{size}x{size}/$value
    - These will be used if the Sync User Photos option is turned on to get the user's profile picture when Syncing Users.

Troubleshooting

Clicking Manage shows a file list

If after creating an integration clicking Manage takes you to a file list, you may need to go to IIS, click the ManageIntegrations folder, then double click Default Document. You may need to add "index.html" if it not already there.

Clicking Manage briefly shows an error then goes back to Admin

You may need to add an API user for "MannedVMSuite", then log out and log back in and try again.

After syncing a user, it says your Admin may need to grant permission

You may need to disabled TLS 1.0 and 1.1 and/or enable TLS 1.2 on the server.