Identity management

SSO + user provisioning in Logiqc for Azure AD

This manual describes how to configure the Logiqc platform as an enterprise application in an Azure Active Directory and provision users.

**Contents**

[Audience & Scope 3](#_Toc158647092)

[Quick-start steps 3](#_Toc158647093)

[Configuration notes 4](#_Toc158647094)

[Prepare your Logiqc for SSO and User provisioning. 5](#_Toc158647095)

[Create Logiqc as an Enterprise Application 6](#_Toc158647096)

[Configure SSO with Logiqc 7](#_Toc158647097)

[Authenticate Logiqc with Azure AD 8](#_Toc158647098)

[Add users to the Logiqc Enterprise Application 13](#_Toc158647099)

[Set up automatic user provisioning with Logiqc. 14](#_Toc158647100)

[Provision users in Logiqc 18](#_Toc158647101)

[Activating new user accounts post SSO implementation. 22](#_Toc158647102)

[User login after SSO and User provisioning has been configured. 23](#_Toc158647103)

[Appendix 24](#_Toc158647104)

# Audience & Scope

This manual has been written for:

* **Logiqc users who have the appropriate administrative permissions to:**
  + Create and edit users, roles, and teams
  + Edit System Settings
* **IT/Network Administrator** - the person within your organisation who manages your Azure Active Directory (AAD)

Both roles have specific responsibilities in implementing and configuring Single Sign On (SSO) and provisioning users. Configuring SSO and setting up User provisioning should be performed by someone sufficiently qualified or experienced with identity management configurations.

# Quick-start steps

1. Read the Configuration notes

**Logiqc platform**

1. Prepare the Logiqc platform for SSO and User provisioning.

**Azure AD**

1. Create Logiqc as a non-gallery application.
2. Configure SSO with Logiqc.
3. Authenticate to Logiqc.
4. Add users to the Logiqc Enterprise Application.
5. Set up automatic user provisioning with Logiqc.
6. Provision users in Logiqc.

**Logiqc platform**

1. Confirm successful user provisioning of users in Logiqc.
2. Understand how to activate Logiqc user accounts post SSO implementation in Logiqc.
3. Understand the process of logging into Logiqc via a non-provisioned user account (external IT admin).

# Configuration notes

**Pre SSO implementation**

* The person who will configure your Azure AD and manage the provisioning of users will require permissions to edit system settings in the Logiqc platform. If this person is not a Logiqc user (e.g., External IT provider), a user account can be created for them using the free External user licence. Refer to the following article:

[Setting up an account for external administrators and auditors](https://knowledgebase.logiqc.com.au/setting-up-an-account-for-external-administrators-and-auditors)

* Provide a list of users from your organisation to the person responsible for implementing Single Sign-On (SSO) and User Provisioning.
* Existing Logiqc user accounts – Ensure that you perform the necessary user account checks as outlined in the upcoming section of this manual, titled 'Preparing your QMS for SSO and User provisioning'.
* New Logiqc user accounts – ensure you have sufficient user licences in your Logiqc platform for the number of users you will be provisioning.
* There is no system downtime required for the Logiqc platform during SSO configuration and user provisioning. This work can be scheduled at a time that suits your organisation.

**Post SSO implementation**

* **New Logiqc user accounts** – When provisioned user accounts are added to the Logiqc platform, they will be inactive. To activate a user account, follow the instructions provided in this manual (P21). It's important to understand that inactive user accounts do not consume Logiqc licenses. A licence is assigned once you activate a user account.
* **Existing Logiqc user accounts** – After provisioning existing Logiqc user accounts, these users will be able to authenticate themselves by using their AAD user account when accessing the Logiqc platform. This means they no longer need to log into the platform using a local Logiqc username and password.
* **Adding new users once SSO has been implemented** – To add new users to your platform, your IT Admin will add their AAD account to the Logiqc Enterprise application in AAD. Once provisioned, the users will have an inactive status in the Logiqc platform and will be marked as 'Awaiting activation'. The account is now ready to be activated.
* **Removing users once SSO has been implemented** – Your IT Admin will remove your user from the Logiqc Enterprise application in AAD. This will deactivate their Logiqc account and prevent access to the platform.
* **External user access post SSO implementation**. – For external users such as auditors or network administrators who won’t have access to Logiqc via SSO, local accounts can be added using the external user licence. Once these accounts have been set up, the user must access Logiqc locally. To log into the platform locally, add "/login" to the end of the Logiqc URL. E.g. <https://YOUR_URL.logiqc.com.au/login>. This will take the user to the Logiqc login screen where they will login using the Logiqc username and password that has been provided.

# Prepare your Logiqc for SSO and User provisioning.

## For the Logiqc System Administrator.

* Set up an account for your IT administrator with the required administration permissions:
  + ‘Create and edit users, roles, and teams’.
  + ‘Edit System Settings’
  + ‘Edit API keys’.

For instructions on setting up an external user account, click on the following article: [Setting up an account for external administrators and auditors](https://knowledgebase.logiqc.com.au/setting-up-an-account-for-external-administrators-and-auditors)

Note: Once SSO and User provisioning has been successfully implemented, you can disable this access.

* **Provisioning existing Logiqc user accounts**:
  + Check current Logiqc user accounts to ensure these accounts all have a valid and unique email address.
  + Ensure no users are sharing the same email address – e.g., reception@ admin@.
  + Ensure users email addresses in their Logiqc user account are an exact match to their AAD email address.
  + Clean up your user account list by deactivating any old user accounts you won’t be provisioning.

To edit user accounts read the following article: [Working with users](https://knowledgebase.logiqc.com.au/working-with-users).   
**Note: If a user’s Logiqc email address does not match their AAD email address, their account will not be provisioned and a second duplicate account will be added**. The provisioning process compares the email address in AAD against the email address in the users Logiqc account.

* **Provisioning new user accounts**:

There is no need for you to manually create user accounts in the Logiqc platform. The process of adding new users is handled by your IT admin through the user provisioning process explained in this manual. All you have to do is provide your IT admin with a list of users who need access to the Logiqc platform.

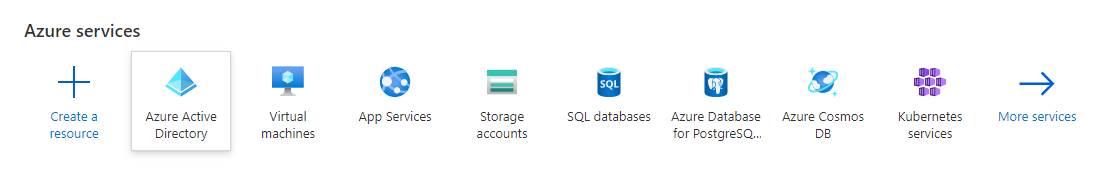
## For IT Admins who will be performing the SSO and User provisioning configuration

* The Logiqc product delivery team have configured the platform to enable SSO and User provisioning.
* You should be provided with a Logiqc external user account which will allow you to access the areas of the platform required to connect Logiqc to your Enterprise application. To log into the platform, enter the customers Logiqc URL and enter the username and password of your Logiqc account.
* You should be provided with a list of users who will require access to the Logiqc platform. These users will be added to the Logiqc Enterprise Application you will create in your AAD.
* You should only provision these user accounts. Do not provision other AAD objects such as faxes, servers, or other objects. Accounts cannot be deleted from the platform once they are added.
* Ensure you understand how to log into the platform locally once you have enabled SSO in the platform’s system settings (P12).

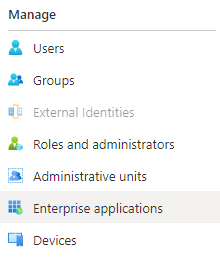
# Create Logiqc as an Enterprise Application

For the IT Manager or the person within your organisation who manages your Azure Active Directory

1. Log into <https://portal.azure.com/>
2. Sign into your Microsoft account
3. Open the Azure Active Directory (AAD)

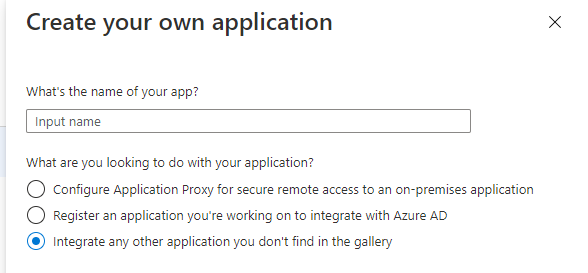
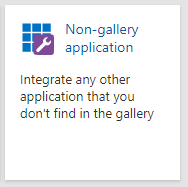


1. Open **Enterprise applications**



1. Create your own application

Select **Create your own application** or switch to **Old app gallery experience** and select **Non-gallery application**

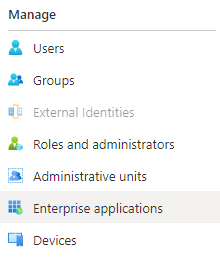


OR

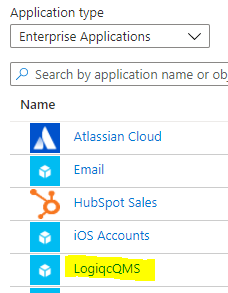
1. Name the application e.g., **Logiqc** and select **Create/Add**

# Configure SSO with Logiqc

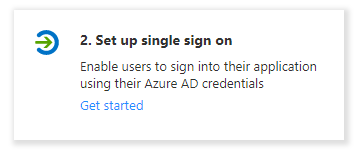
1. From the Azure Active Directory (AAD) window, select**Enterprise Applications**



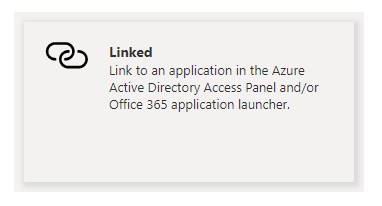
1. Click on the application you added



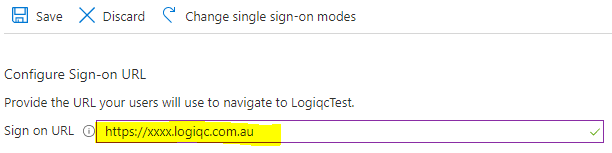
1. Select Set up single sign on



1. Select Linked

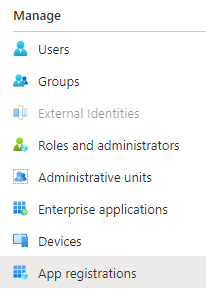


1. Set the **Sign-on URL** to the homepage of the Logiqc platform and select **Save**Note: This is your Logiqc URL address and must include - **https://** as its prefix (See example below)

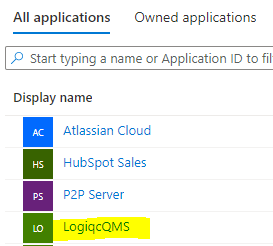


# Authenticate Logiqc with Azure AD

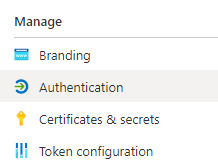
1. Navigate back to the AAD and select **App registrations.**



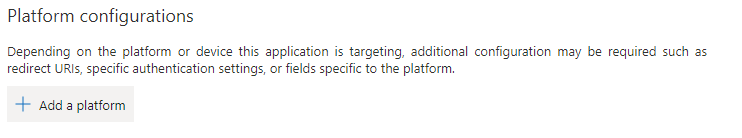
1. Select the **All applications** tab and click on your application.



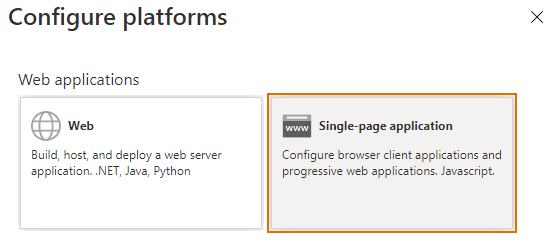
1. Under Manage in the left hand nav, select **Authentication.**



1. Select **Add a platform**.

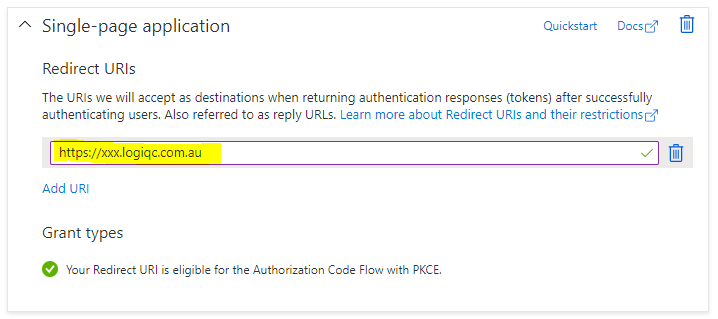


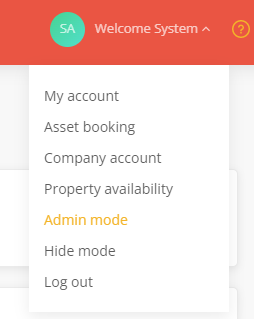
1. Select **Single-page application***.*



1. Enter the Redirect URI with the homepage of the site and select **Configure**.

This is your Logiqc URL and must include - **https://** as its prefix.

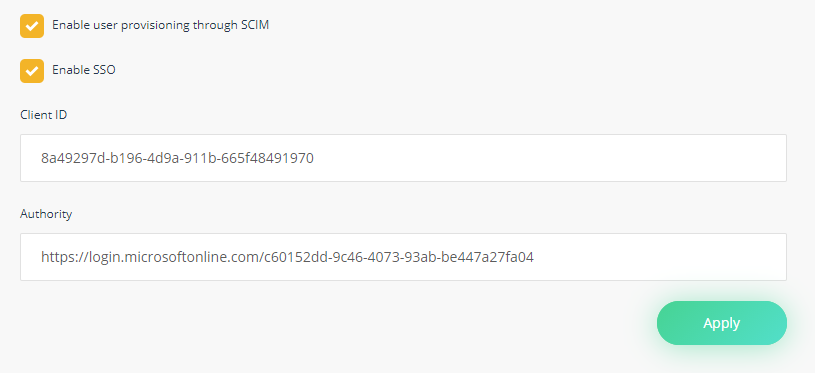


1. Log in to the Logiqc platform.
2. Under the Administrator menu select **Admin mode**  
   
3. From the account menus on the right, select **System settings**.

Graphical user interface, text, application

Description automatically generated

1. Check the following boxes located at the bottom of the page:
   1. **Enable user provisioning through SCIM.**
   2. **Enable SSO** and then enter the Client ID and Authority*.*



The **Client ID** can be found in the Overview of your Logiqc Enterprise Application under **Application ID**. Copy this to the **Client ID** field in Logiqc.

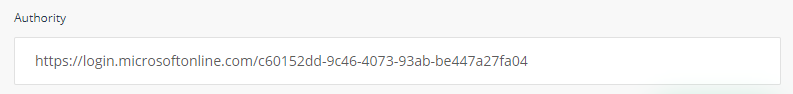
Graphical user interface, application

Description automatically generated

The Authority field can be found in the **Overview** the AAD. This is the **Tennant ID**.

Graphical user interface, application

Description automatically generated

The *Authority* is the *Tenant ID* prefixed with the following URL <https://login.microsoftonline.com/>. Example: 

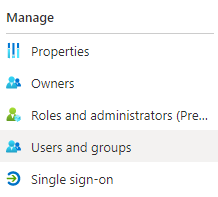
1. Ensure you click Apply to save your changes in Logiqc.



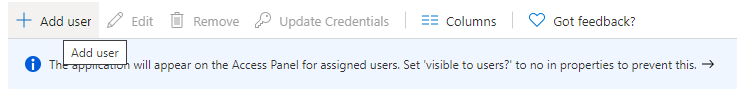
|  |
| --- |
| **IMPORTANT NOTE**: Once Single Sign-On (SSO) has been enabled in the Logiqc platform, you will only be able to authenticate and access the platform using your Azure Active Directory (AAD) credentials. However, if you need to access the platform locally, simply add "/login" to the end of the Logiqc URL and log in using your Logiqc user account. E.g. https://YOUR\_URL.logiqc.com.au/login |

# Add users to the Logiqc Enterprise Application

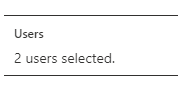
1. Open the Logiqc **Enterprise application** within AAD and select **Users and groups** to manage users.



1. Select *Add user*

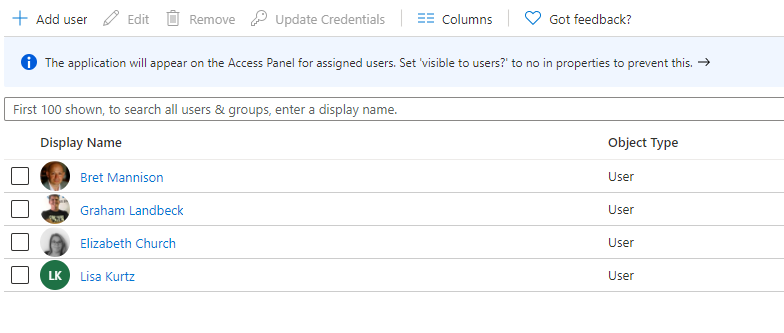


1. Click on **Users** and the user list will appear on the right-hand pane.
2. Select the users you wish to add and click **Assign**.





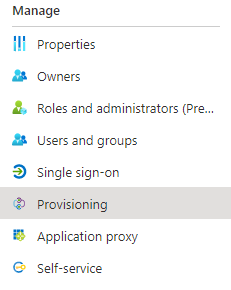
Users will be added with the default role of User. This is the only role that can be manually assigned. Note that the **Default access** role will be automatically assigned when the user has logged in.



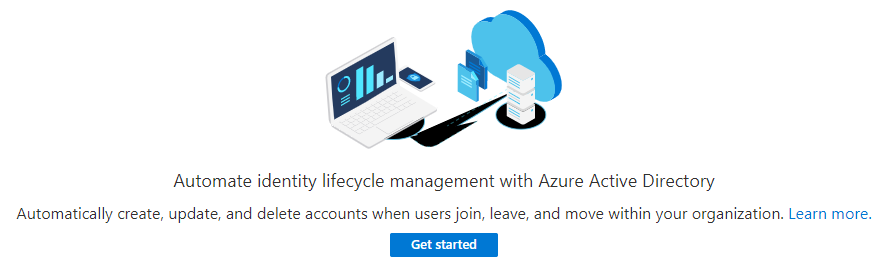
# Set up automatic user provisioning with Logiqc.

User provisioning allows user accounts to be automatically added to Logiqc from configured users in the Azure AD Logiqc Enterprise application.

1. Select **Enterprise applications**.
2. Select your application
3. Under **Manage** on the left hand nav, select **Provisioning**.



1. Open **Provisioning** in the Logiqc Enterprise application and select **Get started***.*

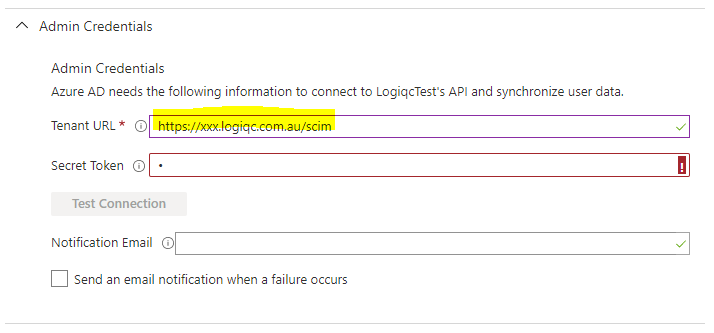


1. Select **Automatic** for the Provisioning Mode.

Graphical user interface, text, application

Description automatically generated

1. Enter the **Tenant URL**and **Secret token** (API Key).



The **Tenant URL** is the scim endpoint for your Logiqc e.g., https://xxx.logiqc.com.au/scim

The **Secret Token** value is the API key token value created in Logiqc.

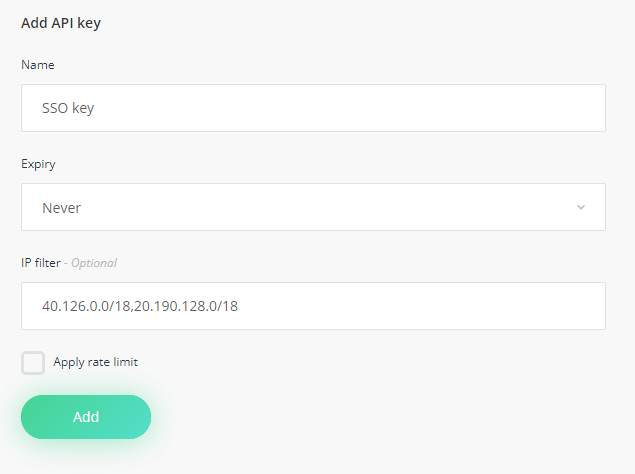
## Generating the secret token (API key) in your Logiqc

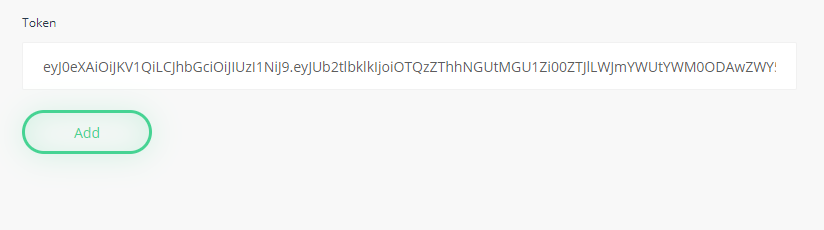
1. Log into Logiqc.
2. Select **Admin mode** via the Account menu (top right)
3. Under the Administrator menu, select **API keys***.*

Graphical user interface, application, email

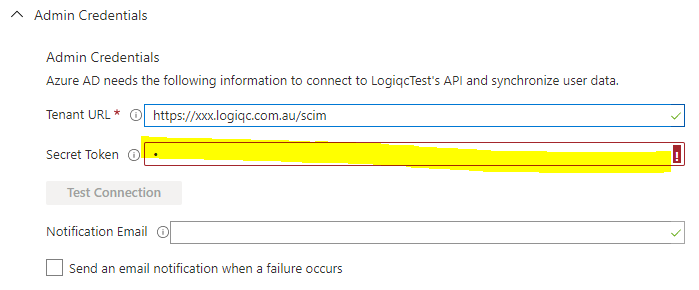
Description automatically generated

1. To create your key:
   1. Name the key.
   2. Set the expiry to **Never**.
   3. Add the following value to the IP filter - **40.126.0.0/18,20.190.128.0/18**
   4. Leave the rate limit unchecked.
   5. Click **Add**



1. When the token key is generated, copy the token string 
2. Add to the **Secret token** field in the **Admin Credentials** in AAD

Under **Test Connection**, you can add an email address under **Notification Email** and tick *Send an email notification when a failure occurs.*

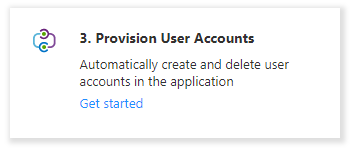


1. Click **Save**

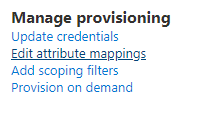
# Provision users in Logiqc

## Configure the Mappings

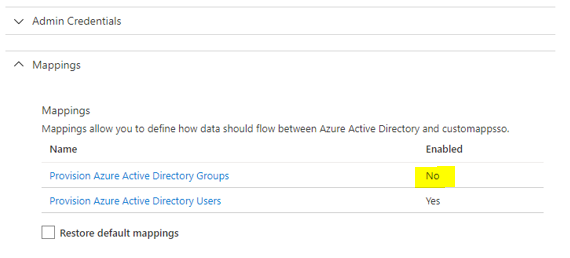
1. From within your application select **Provision User Accounts**



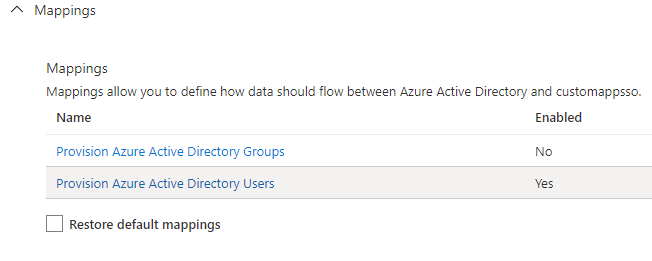
1. Under Managing provisioning, select **Edit attribute mappings.**



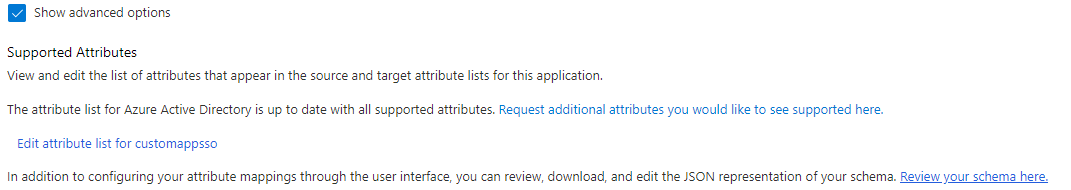
1. Select **Provision Azure Active Directory Groups** and disable it and save your changes.



1. Select **Provision Active Directory Users.**



1. Select **Show advanced options** and then select **Review your schema here.**

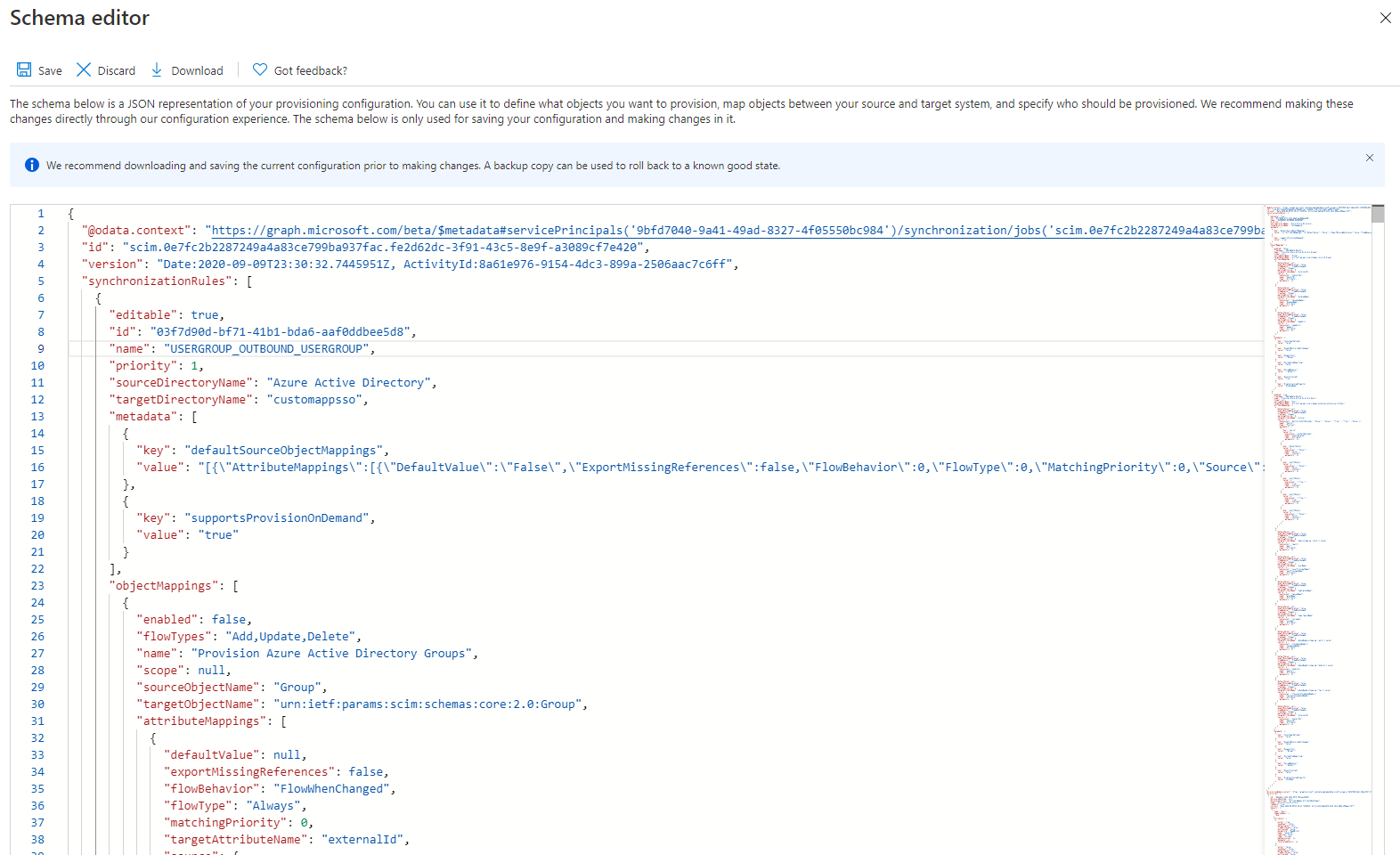


1. Double-click on the schema.json icon below (Open in a text editor) and copy the contents. The schema.json file is embedded in this document and will open in your default editor.



1. Paste the contents of schema.json into the *Schema Editor* and select *Save*

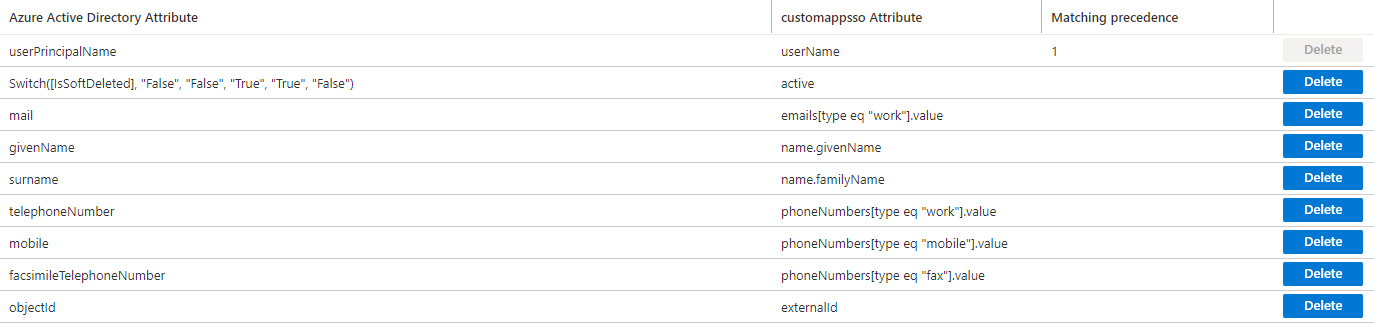
Note: Remove the existing contents first and then paste in the new content.



1. **Save** your changes.

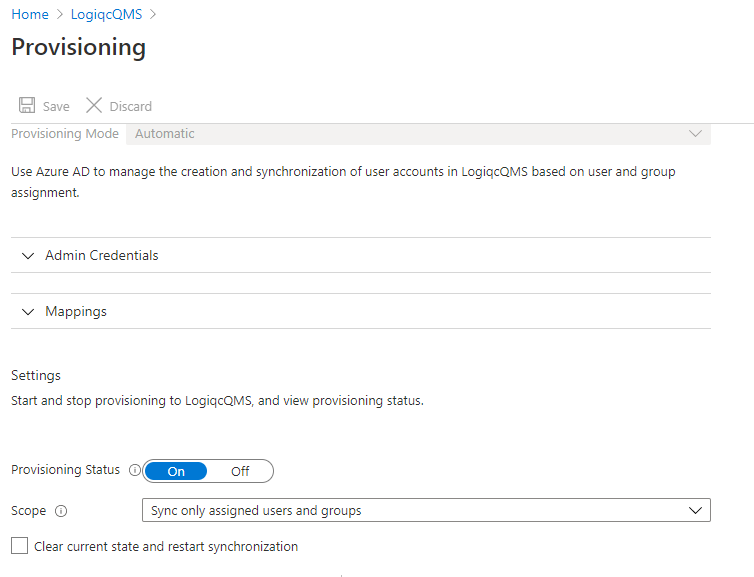


1. The resulting Attribute Mappings should look like this: Note: You may need to refresh to see the updated attribute mappings.

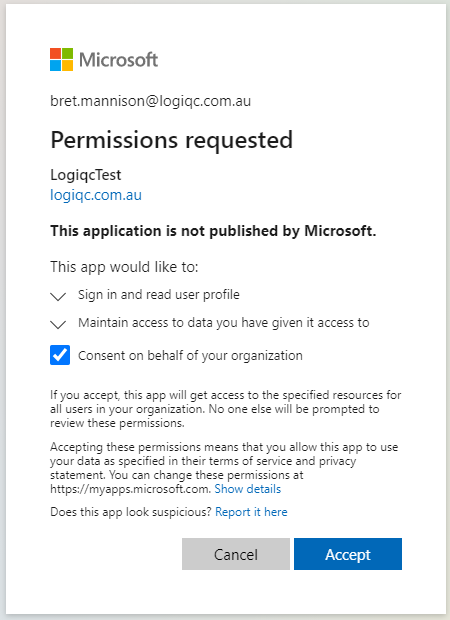


Existing users will be matched using the user’s external ID, username or email address. The external ID would be set if the user has been linked to SSO previously (or was previously provisioned).

1. Navigate back to **Provisioning** and ensure provisioning status is **ON**

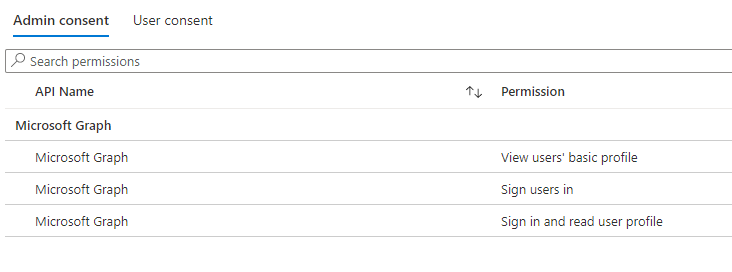


1. **Save** your settings.
2. Go to your Logiqc and log out (if still logged in) and then log back in.
3. Check the box **Consent on behalf of your organisation** and select **Accept.**



1. To check the permission levels have been applied, navigate to your Logiqc application under Enterprise applications. Go to **Security** and select **Permissions.**

The Logiqc application will need the following permissions:



Alternatively, these can be configured in the API permissions for the application in App registrations.

**Refer to the Appendix for instructions.**

# Activating new user accounts post SSO implementation.

When you have implemented SSO, there is no need for you to manually create user accounts in the Logiqc platform. The process of adding new users is handled by your IT admin through the user provisioning process. All you have to do is provide your IT admin with a list of users who require access to the Logiqc platform.

When Provisioned User accounts are provisioned into the platform, they will be ‘inactive’. To activate a user account, follow the instructions below.

**Note**: Inactive user accounts do not consume Logiqc user licenses. A user licence is assigned once you activate a user account. **Required admin permissions**: 'Create and edit users, roles, and teams'.

**To activate a provisioned user:**

1. Switch to **Admin mode** via your user account menu.
2. Select **Users** under the Administration menu.
3. Select the toggle 'Show inactive users'.
4. Find the user account you wish to activate.  Their status will be 'awaiting activation - Yes'.
5. Open their user account and set their account status to **Active**.  You will then need to edit the following fields in their account.
   1. Licence
   2. Position
   3. Roles
   4. Teams
   5. Business areas
6. **Save** your changes.

**Note:** The email address, username and password fields cannot be edited.

Once the user account has been activated and set up, provide the user with your Logiqc platform's web address (URL).  They will authenticate via your company network account to access the platform.

**To remove a provisioned user:**

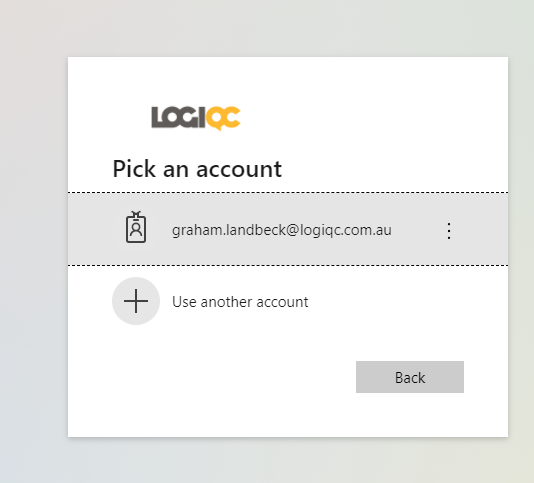
To remove a user, your IT administrator should remove the user from the Logiqc enterprise application in your organisations Azure Active Directory.  The user account will immediately be set to inactive, preventing the user from accessing the Logiqc platform.

Any assigned tasks and responsibilities will need to be managed.

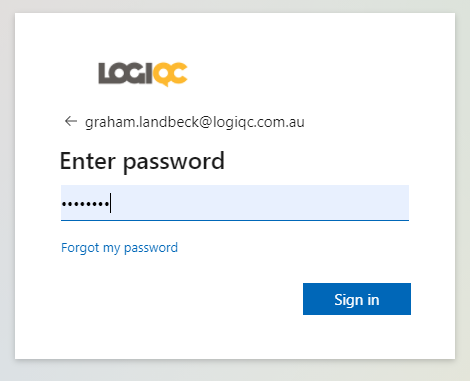
**Note:** For existing Logiqc user accounts that have been provisioned as part of SSO implementation, the active user accounts do not need any further action as described above. Users accounts remain active with all the assigned account details.

# User login after SSO and User provisioning has been configured.

1. When a user connects to your organisations Logiqc URL, they will be asked to authenticate via their AAD user account.



1. The password will be their AAD user account password.

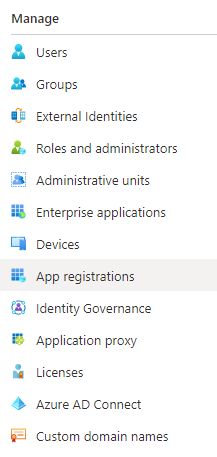


**Note**: If you are already logged into your organisations network, you will authenticate directly into the platform when you click on your Logiqc URL.

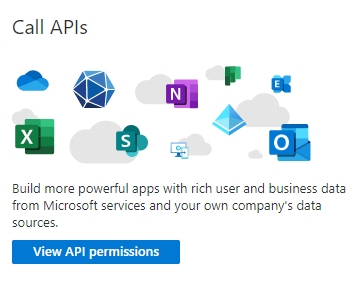
# Appendix

## Configuring permissions through App registrations.

1. From the AAD, select *App registrations*



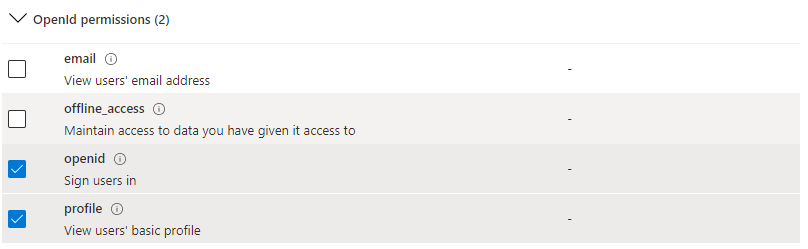
1. Select All applications
2. Select the Logiqc application.
3. Select View API permissions



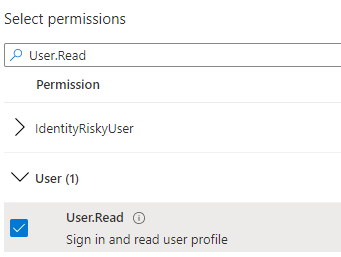
1. Select Add a permission.
2. Select Microsoft Graph.
3. Select Delegated permissions.



1. Select *openid* and profile under *OpenId permissions*

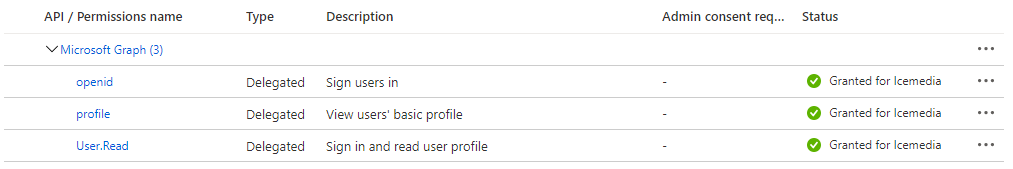


1. Select *User.Read* under User (Enter *User.Read* in the search bar)



1. Select *Add permissions*.
2. Select *Grant admin consent for <organisation name>*.
3. Select *Yes.*

You should see the following result.



A picture containing transport

Description automatically generated

PO Box 483, Paddington, Qld, Australia 4064  
AU +617 3216 0335 NZ 0800 002 280 E: info@logiqc.com.au W: logiqc.com.au