Identity management

SSO + user provisioning in Logiqc for Microsoft Entra ID

This manual describes how to configure the Logiqc platform as an enterprise application in Microsoft Entra ID and provision users.

**Contents**

[Audience & Scope 3](#_Toc184804483)

[Quick-start steps 3](#_Toc184804484)

[Configuration notes 4](#_Toc184804485)

[Prepare your Logiqc platform for SSO and User provisioning. 5](#_Toc184804486)

[Create Logiqc as an Enterprise Application 6](#_Toc184804487)

[Set up Single Sign On 8](#_Toc184804488)

[Set up authentication with the Logiqc platform 9](#_Toc184804489)

[Add users to the Logiqc Enterprise Application 14](#_Toc184804490)

[Set up automatic user provisioning with Logiqc. 14](#_Toc184804491)

[Provision users in Logiqc 19](#_Toc184804492)

[Activating new user accounts post SSO implementation. 24](#_Toc184804493)

[User login after SSO and User provisioning has been configured. 25](#_Toc184804494)

[Appendix 26](#_Toc184804495)

# 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 Microsoft Entra ID environment.

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.

**Entra ID**

1. Create Logiqc as a non-gallery application.
2. Configure SSO with Logiqc.
3. Authenticate to Logiqc.
4. Add users/groups 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 the Logiqc platform.
2. Understand how to activate Logiqc user accounts post SSO implementation in Logiqc.
3. Understand how to remove users from the Logiqc platform post SSO implementation.
4. 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 Entra ID 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 who require access to Logiqc 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 users are provisioned on the Logiqc platform, their accounts will initially be inactive. To activate a user account, please refer to the instructions outlined in this manual (**P24**). It is essential to note that inactive accounts do not utilise Logiqc licenses. A license is only allocated once a user account is activated.
* **Existing Logiqc user accounts** – After the provisioning of existing Logiqc user accounts, users can sign in with their Microsoft email addresses. This change eliminates the need to login with a separate Logiqc username and password.
* **Adding additional users once SSO has been implemented** – To add additional users to your platform after Single Sign-On (SSO) has been configured, your IT Administrator will need to register their Entra ID user account within the Logiqc Enterprise application. Following this process, the user's Logiqc account will initially be set to an inactive status on the Logiqc platform and will display as 'Awaiting activation'.
* **Removing users once SSO has been implemented** – Your IT Administrator will remove the users account from the Logiqc Enterprise application within Entra ID. This action will deactivate their Logiqc user account, thereby restricting access to the platform. Additionally, the Logiqc user license will be returned to the license pool for future use.
* **External user access post SSO implementation**. – For external users such as auditors or network administrators who don’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 platform 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 account.

* **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 email address in Entra ID.
  + 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 Microsoft email address, their account will not be provisioned and a second duplicate account will be added**. The provisioning process compares the email address in Entra ID against the email address in the users Logiqc account.

* **Provisioning NEW user accounts**:

## You do not need to manually create user accounts on the Logiqc platform. The responsibility of adding new users lies with your IT administrator, who will follow the user provisioning process outlined in this manual. Simply provide your IT admin with a list of individuals requiring access to the Logiqc platform.

## For IT Administrators 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 into your browser 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 Entra ID.
* You should only provision the user accounts provided. Do not provision other objects such as faxes, servers, or other objects. Accounts cannot be deleted from the Logiqc 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 (**P13**).

# Create Logiqc as an Enterprise Application

For the IT Manager or the person within your organisation who manages your Entra ID

1. Log into <https://entra.microsoft.com/>
2. Under **Applications**, open **Enterprise applications**

A screenshot of a computer

Description automatically generated

1. Select **New application**

A close-up of a computer screen

Description automatically generated

1. Select **Create your own application**  
     
   A screen shot of a computer

   Description automatically generated
2. Name the app, select the non-gallery option and click ‘Create’.  
     
   A screenshot of a application

   Description automatically generated

The name of your app

# Set up Single Sign On

1. Within the application, select ‘Set up single sign on’.

A white box with black text

Description automatically generated

1. Select Linked

A white rectangular box with black text

Description automatically generated

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)

A screenshot of a computer

Description automatically generated

Your Logiqc URL address

# Set up authentication with the Logiqc platform

1. Navigate back to **App Registrations.**

A screenshot of a computer

Description automatically generated

1. Under the **All applications** tab, click on your application.

A screenshot of a computer

Description automatically generated

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

A screenshot of a computer

Description automatically generated

1. Select **Add a platform**.

A close up of a message

Description automatically generated

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

A screenshot of a computer

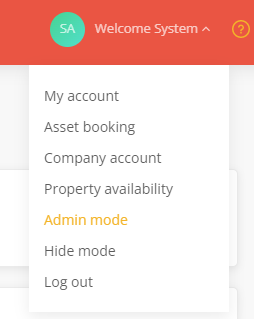
Description automatically generated

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.

A screenshot of a message

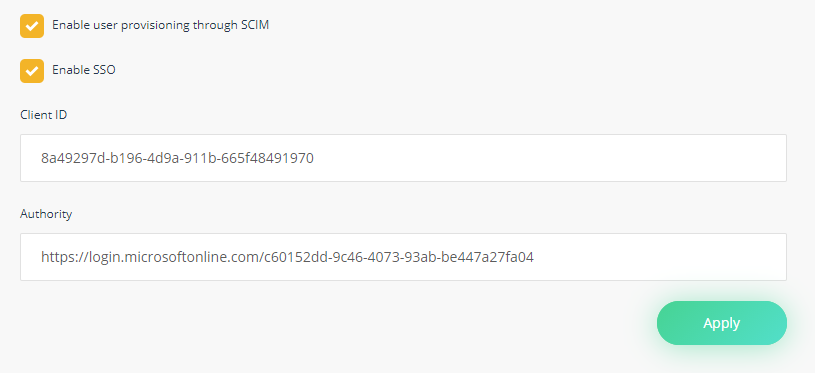
Description automatically generated

1. Log in to the Logiqc platform via your browser. (Your Logiqc administrator will provide you with the URL)
2. Under the User account menu (Top right) 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 details*.*



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.

A screenshot of a computer

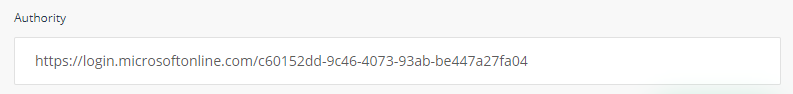
Description automatically generated

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

A screenshot of a computer

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: After enabling Single Sign-On (SSO) on the Logiqc platform, you will be required to log in exclusively with your Entra ID credentials. If you need to access the platform locally while user accounts are being set up, you can do so by appending "/login" to the Logiqc URL and logging in with your local Logiqc user account. For example, use the following format: https://YOUR\_URL.logiqc.com.au/login.** |

# Add users to the Logiqc Enterprise Application

You have the option to add users to your application as individuals, or via a group.

1. Open your application, and click **Assign users and groups**  
   A white background with black text

   Description automatically generated
2. Click **Add user/group**
3. Select your users and/or groups from your list and click **Assign**. Your users and groups are added.  
   A white background with black lines

   Description automatically generated

# Set up automatic user provisioning with Logiqc.

User provisioning allows user accounts and groups to be automatically added to the Logiqc platform from within the Logiqc Enterprise application.

1. From within your application, click **Get started** in **Provision User Accounts**.

A screenshot of a computer

Description automatically generated

1. Click **Connect your application** within the Create configuration section.

A screenshot of a computer

Description automatically generated

1. Enter the **Tenant URL**and **Secret token** (API Key) – Refer to the instructions below for generating the API key

A screenshot of a computer

Description automatically generated

The **Tenant URL** is the scim endpoint for your Logiqc platform e.g., <https://[YOUR_NAME].logiqc.com.au/scim>

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

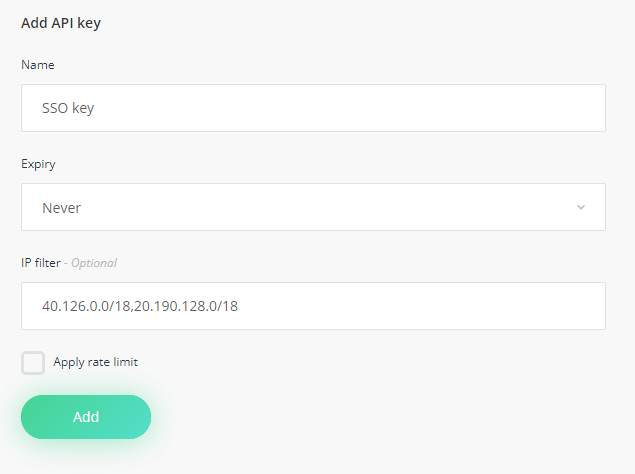
## Generating the secret token (API key) in your Logiqc

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.A screenshot of a phone

   Description automatically generated
2. Add the API key to the **Secret token** field in the **Admin Credentials** then click **Test Connection**.

A screenshot of a login box

Description automatically generated

1. Once the connection has been confirmed, click **Save**

# Provision users in Logiqc

## Configure the Mappings

1. Under Manage, select **Attribute mapping (preview).**

A screenshot of a computer menu

Description automatically generated

1. Click on **Provision Microsoft Entra ID Groups**

A screenshot of a computer

Description automatically generated

1. Set Provision Azure Active Directory Groups to Enabled – **No** and save the change.  
   A screenshot of a computer

   Description automatically generated
2. Leave **Provision Azure Active Directory Users** to Enabled - **Yes**

A screenshot of a computer

Description automatically generated

1. Click on **Provision Azure Active Directory Users**
2. Select **Show advanced options** and then click on **Review your schema here**

A close up of text

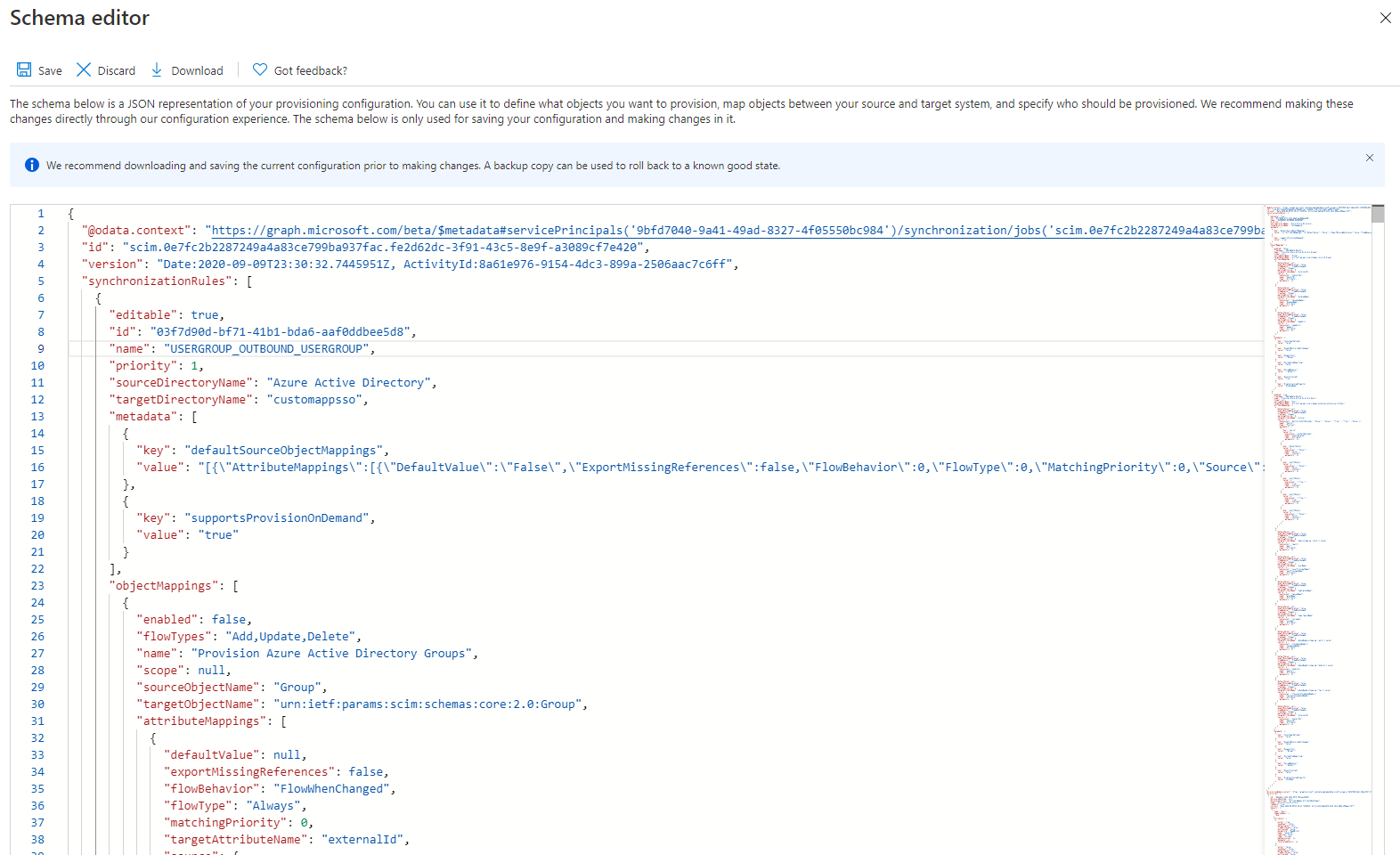
Description automatically generated

1. Remove the contents in the **Schema editor**.
2. 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. If you cannot open the contents, please contact [Logiqc Support](https://knowledgebase.logiqc.com.au/kb-tickets/new) requesting the schema.json file for SSO set up.

Click on this icon



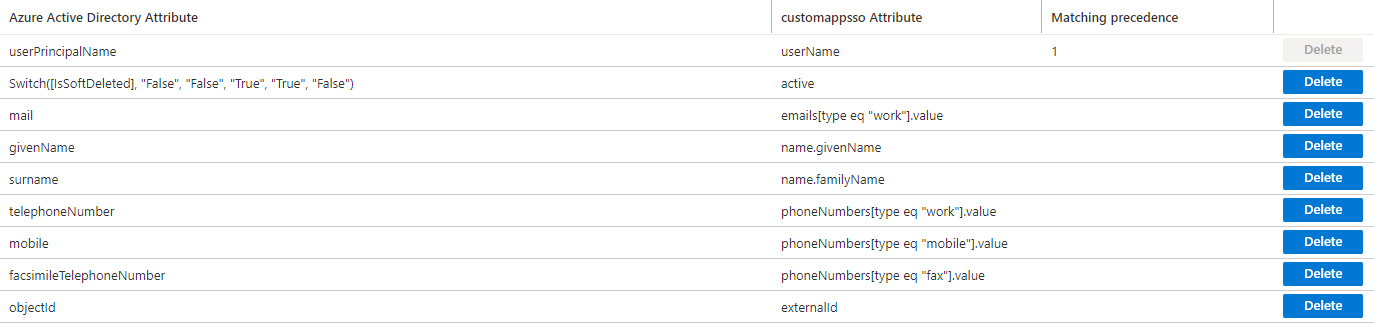
1. Paste the contents of schema.json into the **Schema Editor**.



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.

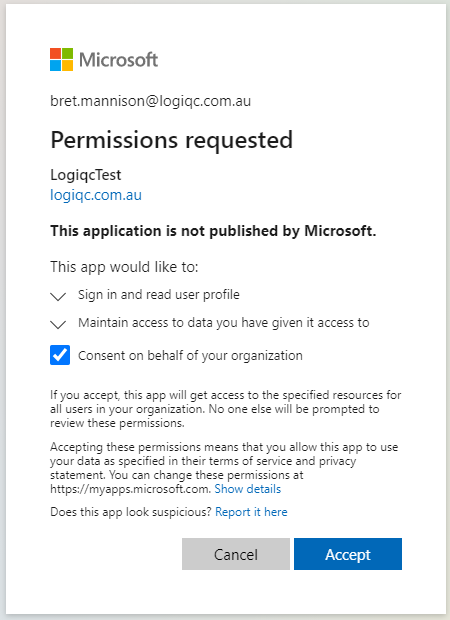


Existing users will be matched using the user’s external ID, username or email address. The external ID would be set if the user has been linked to SSO previously (or was previously provisioned).

1. Navigate back to **Provisioning**. **A screenshot of a computer program

   Description automatically generated**
2. Change Provisioning status to **ON** and **Save** the settings.A screenshot of a computer

   Description automatically generated
3. Go to your Logiqc platform and log out (if still logged in) and then log back in.
4. 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.**A screenshot of a computer

   Description automatically generated

The Logiqc application will need the following permissions:

A screenshot of a computer

Description automatically generated

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.

Once SSO is implemented, you won't need to manually create user accounts in the Logiqc platform. Your IT administrator will manage the addition of new users through the user provisioning process. Simply provide your IT admin with a list of individuals who need access to the Logiqc platform.

When Provisioned User accounts are created within the platform, they will initially be set to ‘inactive.’ To activate a user account, please follow the instructions outlined below.

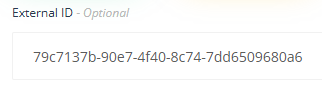
**Note**: Inactive user accounts do not consume Logiqc user licenses. A user licence is assigned once you activate a user account.

**To activate a provisioned user:** (Required Logiqc admin permissions - 'Create and edit users, roles, and teams'.)

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.

**Checking if an account has been successfully provisioned.**

Once an account has been provisioned, the email address, username fields cannot be edited. A provisioned user account will no longer have the ‘Change password’ option. They should have an external ID visible which can be found under the ‘Reminders and notifications’ component.



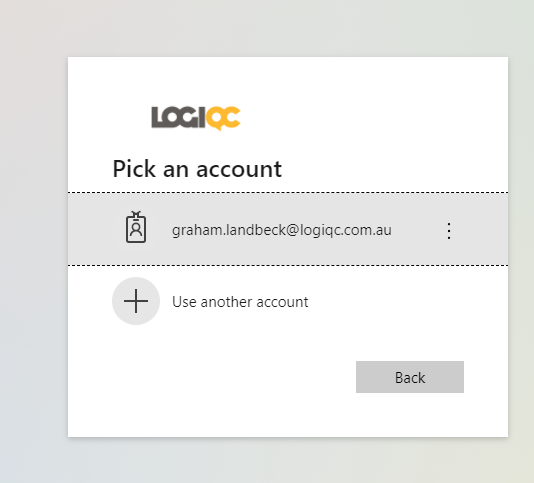
For existing Logiqc user accounts that have been provisioned as part of SSO implementation, the active user accounts do not need any further action as described above. Users accounts remain active with all the assigned account details.

**To remove a provisioned user:**

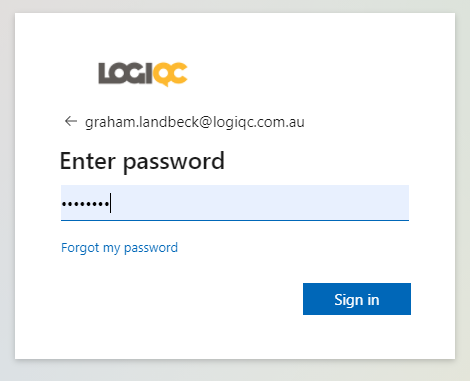
To remove a user, your IT administrator must delete the user from the Logiqc enterprise application within your organisation's Entra ID. This action will instantly deactivate the user account, thereby restricting access to the Logiqc platform. Additionally, the associated user license will be released back into the license pool, making it available for assignment to a new user. Remember to manage any tasks and responsibilities that were assigned to the departing user.

# 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 Entra ID account using their email address.



1. The password will be their Entra ID user account password.

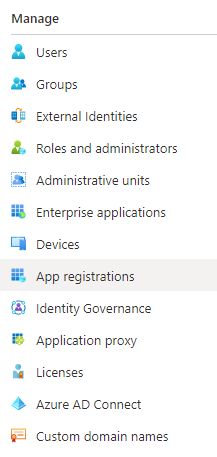


**Note**: If you are already logged into your organisations network, you will authenticate directly into the platform when you click on your Logiqc URL.

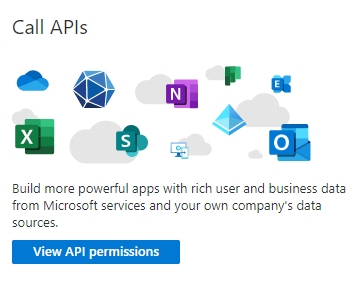
# Appendix

## Configuring permissions through App registrations.

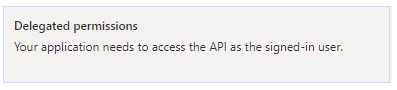
1. From the AAD, select *App registrations*



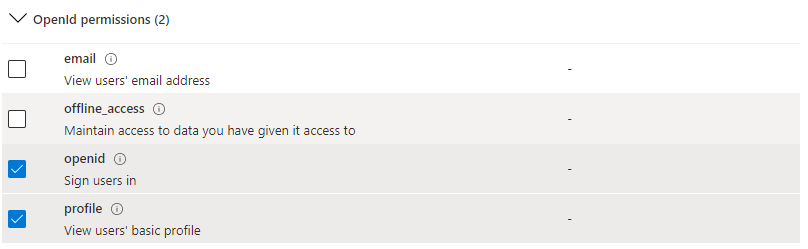
1. Select All applications
2. Select the Logiqc application.
3. Select View API permissions



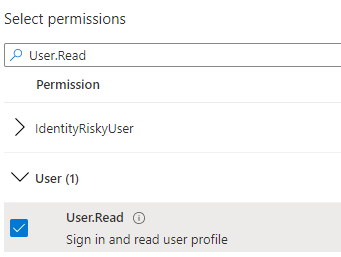
1. Select Add a permission.
2. Select Microsoft Graph.
3. Select Delegated permissions.



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

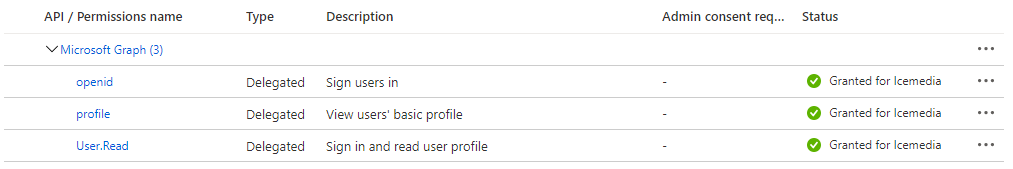


1. Select *User.Read* under User (Enter *User.Read* in the search bar)



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

You should see the following result.





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