VERSION 3.0

MARCH 6, 2024

ACTIVE DIRECTORY INTEGRATION

APP NUMBER: 010044

Powered by:

MYOB Greentree

TABLE OF CONTENTS

FEATURES

1. **Active Directory Integration.**

This App integrates Greentree with Windows Active Directory allowing secure Single Sign on using a user's Domain user.

Four new options are available on the User preferences screen under the Active Directory Tab. These options may only be configured by the *Super* user.

2. **Microsoft Entra ID Integration.**

This App also integrates Greentree with Microsoft Entra ID (formerly Azure AD) allowing secure Single Sign on using modern web authentication provided by Microsoft.

If this option is used Greentree will always authenticate the current Windows user using the security configured in Microsoft Entra ID, however the first two options below are used for access to Greentree.

This option requires the registration of a new enterprise application in MS Entra and entering identity information in the App control options. Instructions on setting up a new application are at the end of this document.

OPTIONS

1. **None**
    - Greentree username and password are used. No checking against Active Directory is done. If Microsoft Entra ID has successfully authenticated the user, this option will prevent single sign-on

2. **Use Windows Login (bypass GT password check)**
    - This option provides secure single sign-on. Greentree checks the currently logged on user is a valid user in the same Domain as the Greentree server **OR** Greentree uses Microsoft Entra ID to authenticate the current user. It then logs the user on to the matching Greentree user.
      If this fails, the normal Greentree username and password prompt is used for backup.

3. **Check Login on Active directory**
    - Greentree prompts the user to enter their Greentree username and password. Greentree checks that the provided user matches a valid Windows user.
    - This option is only considered secure if the Disable Server Side User Validation option (shown in the App Configuration section below) is not ticked. This ensures that the user is validated against the same Domain that the Greentree server is using.

4. **Check Login against current Active Directory User**
    - Greentree prompts the user to enter their Greentree username and password. Greentree checks that the provided user matches the current logged on Windows user.

- This option is only considered secure if the Disable Server Side User Validation option (shown in the App Configuration section below) is not ticked. This ensures that the user is validated against the same Domain that the Greentree server is using.

IMPORTANT NOTES

- We recommend that you test the configuration of the App thoroughly in a test system prior to deploying the App in your live Greentree system.
- Before installing and configuring the App, ensure that the Greentree username for each user is identical to his or her Windows Domain username, or identical to their account name (or one of the other identifier fields) in Microsoft Entra ID.
- Do not enable the App for any user that also needs to log in as the Super user as it will prevent them from being able to do so.
- The *Super* user Greentree account cannot be configured to use Active Directory Integration as a login but must be selected as a User in | System | Apps For Greentree | Apps Module Control | Active Directory Integration App| Edit Users
- Windows Domain accounts are maintained by the network administrator within Active Directory. The network administrator should be consulted before configuring this App for Greentree.
- Microsoft Entra ID configuration, including user accounts, is maintained by an administrator user to the Microsoft Azure platform your organisation. This administrator should be consulted for assistance in configuring this app and Microsoft Entra ID.
- This App provides Active Directory or Microsoft Entra ID integration for access to the core Greentree system. It does not provide Active Directory integration for external functionality such as FREE, ODBC, eModules, WebView and Greentree IQ, for which existing usernames and passwords are still required.

OTHER REQUIREMENTS

Greentree Modules: None.

Associated Apps: None.

OPTIONS

Greentree will behave according to which Option has been set for your user account under Other Greentree Configuration:

OPTION 1. None

- Click on the desktop icon to launch Greentree.
- If using Microsoft Entra ID integration, the standard web authentication process will be used, however once authenticated the normal Greentree login form will be shown.
- Enter your Greentree username and password.

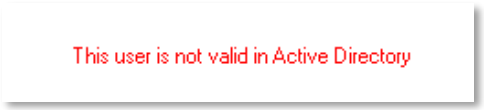
OPTION 2. Use Windows Login

- Click on the desktop icon to launch Greentree.
- If the user who is logged in to the computer is a valid Active Directory user Greentree will automatically log on as the Greentree user with a matching username.
- If using Microsoft Entra ID integration, the standard web authentication process will be used, and once authenticated Greentree will automatically log on as the matching Greentree user.
- If this fails the Greentree username and password prompt will appear.

OPTION 3. Check Login on Active directory

- Click on the desktop icon to launch Greentree.
- Enter your Greentree user name and password into the Greentree login screen and select the company you wish to log into.
- If your Greentree username matches an active Windows Network account ID, you will be logged in to Greentree.

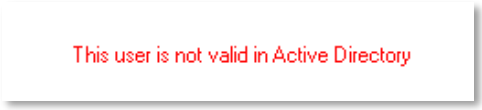
  Note: If there is no matching and active Windows Network account ID, you will receive this message:



OPTION 4. Check Login against current Active Directory User

- Click on the desktop icon to launch Greentree.
- Enter your Greentree user name and password into the Greentree login screen and select the company you wish to log into.
- If your Greentree username matches an active Windows Network account ID and if you are logged in to the network on that PC or terminal server session using that Windows account, you will be logged in to Greentree.

Note**:** If there is no matching and active Windows Network account ID, you will receive this message:

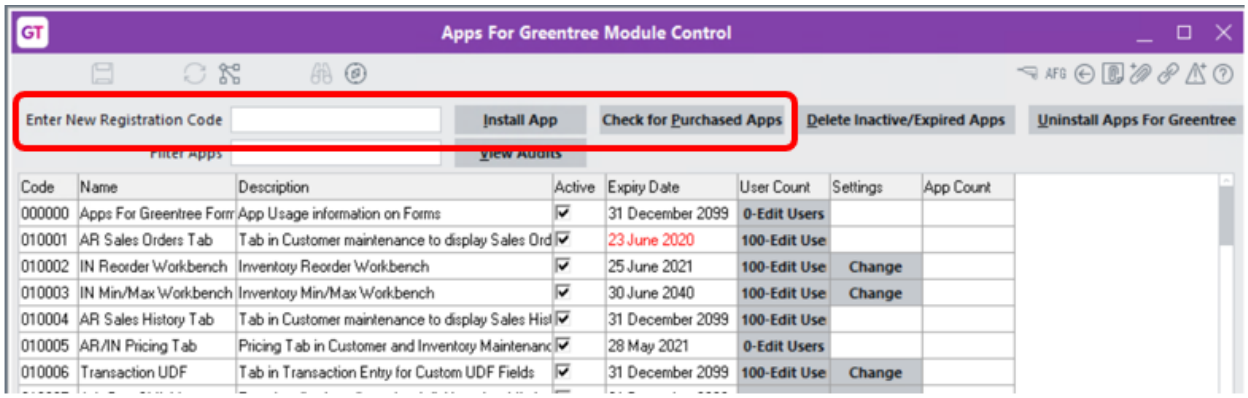


IMPLEMENTATION GUIDE

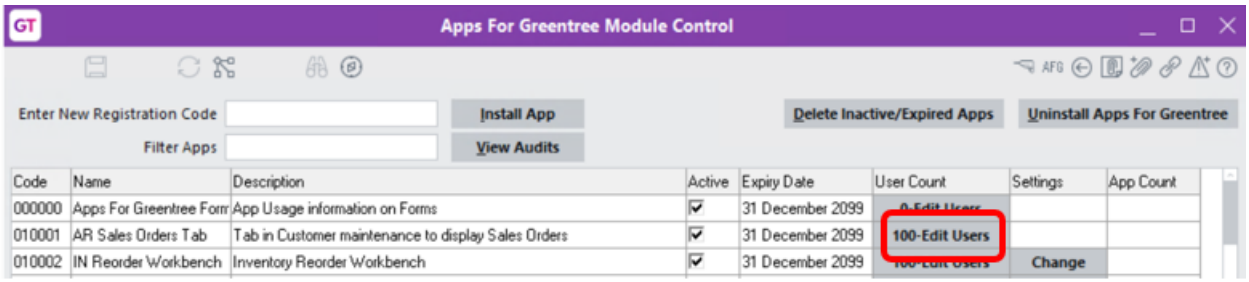
Please refer to the Important Notes section above before installing and configuring this App.

APP INSTALLATION

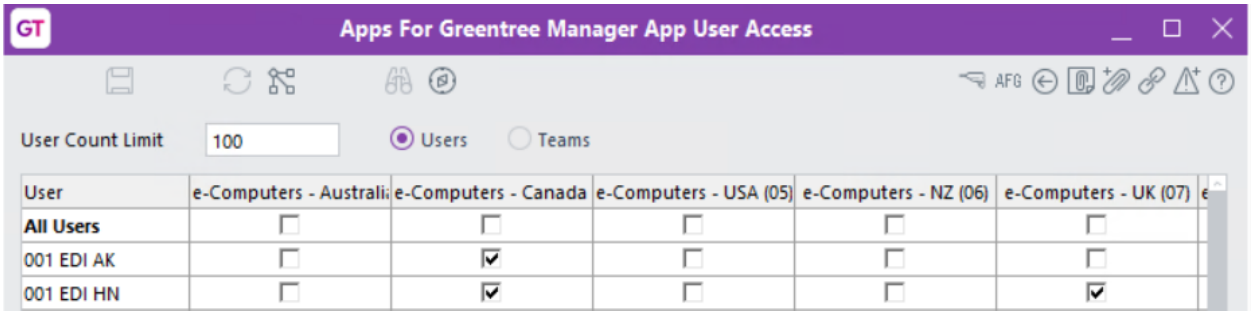
1. Log into Greentree as the Super user
2. Select the menu item | System | Apps For Greentree | Apps Module Control |
3. Either enter the New Registration Codes supplied and click Install App or click the Check for Purchased Apps button to display a list of apps recently purchased or renewed to install in bulk.



4. Select/Highlight the Active Directory Integration App.



5. Click on the Edit Users button and select the users who will be configured to use Active Directory Integration, for which companies.

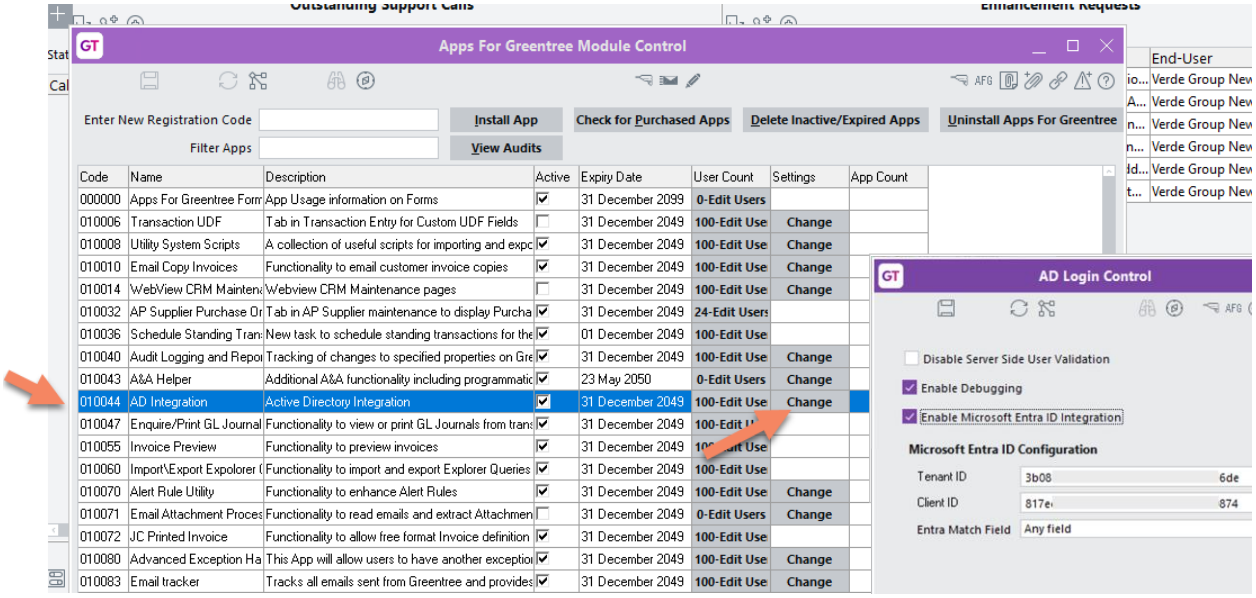


6. Once you have selected the users, Save the settings, and Close the window.

7. Save and Close the Module Control form.

APP CONFIGURATION

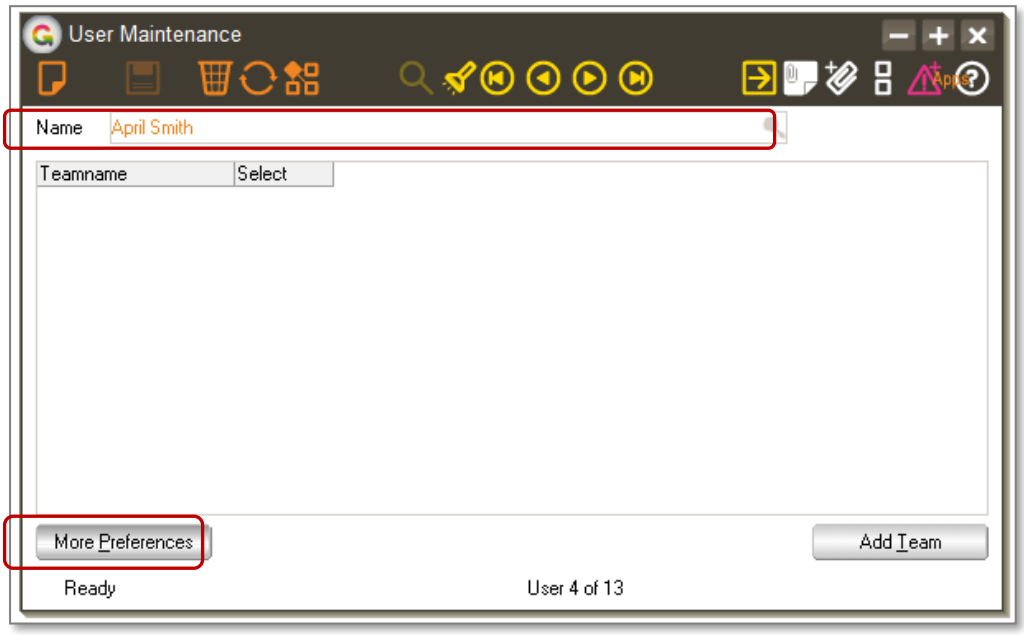
1. Select the menu item | System | Apps For Greentree | Apps Module Control |
2. Select/Highlight the Active Directory Integration App.
3. Click on the Change button.



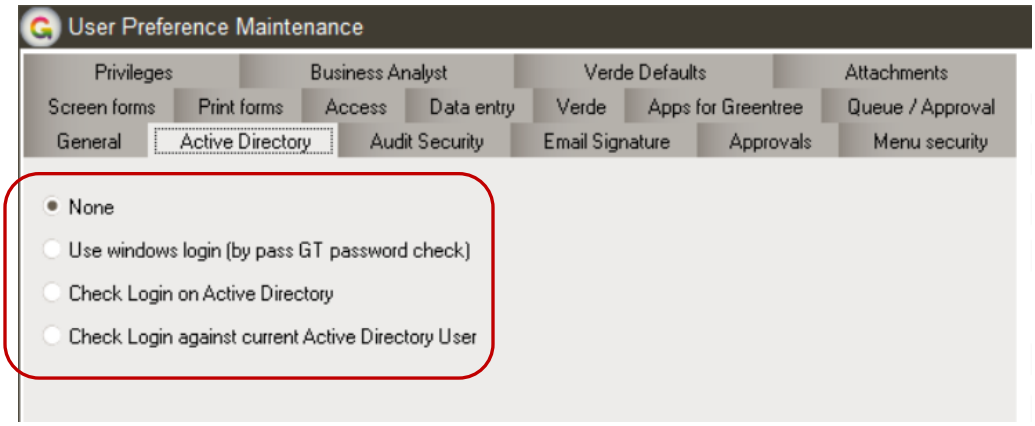
Disable Server Side User Validation	This option removes the security validation on the server and means the user is not validated against the same Domain that the Greentree server is using. Only use with caution.
Enable Debugging	Tick to enable debugging to track reasons for login failures.
Enable Microsoft Entra ID integration	Turns on authentication using security information configured in Microsoft Entra ID.
Tenant ID	The Tenant ID from Microsoft Entra ID – Organisation Overview.
Client ID	The Application ID from Microsoft Entra ID – App Registration.
Entra Match Field	Specify a particular field from Microsoft Entra ID that will be used to match the Greentree username (or email address).

OTHER GREENTREE CONFIGURATION

1. Select the menu item | System | System Setup | User Maintenance |
2. Select the User you want to change settings for and click on the More Preferences button



3. Click on the Active Directory tab
4. Click on the Active Directory option that will apply for the user. This setting is used for all companies that were configured for the user at step 5 of the App Installation section above.

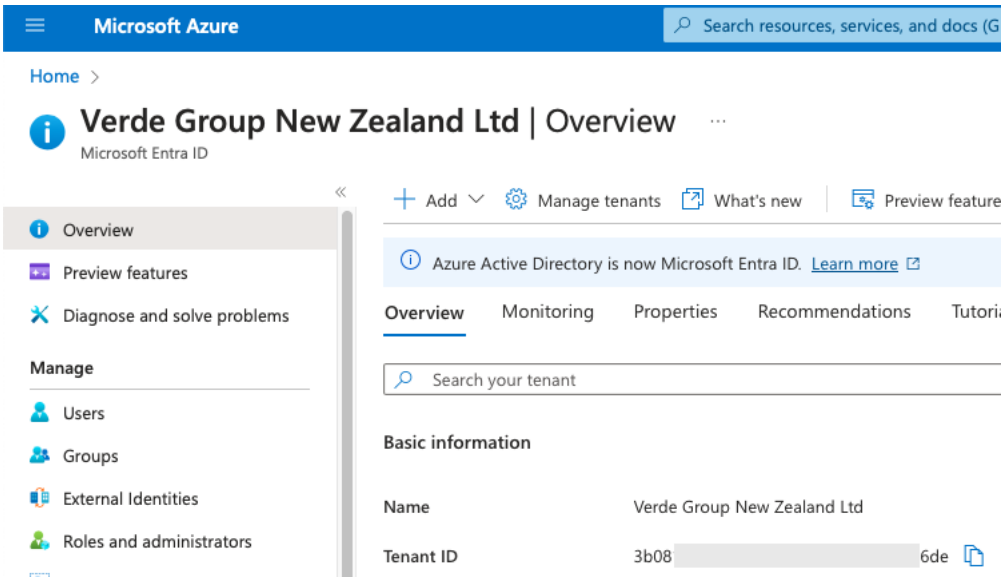


5. Save the settings, using the save (disk) icon in the header and Close the window.

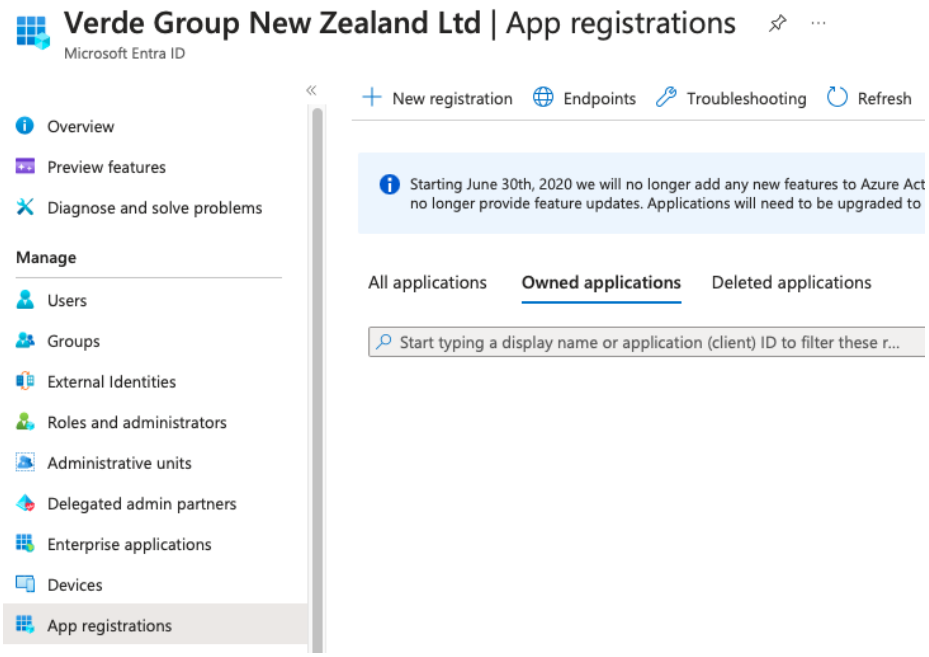
MICROSOFT ENTRA ID CONFIGURATION

Configuration of Entra ID through the Microsoft Azure portal should be performed by a user with administrator permissions. Log in to the Azure portal for the tenant you will be setting up.

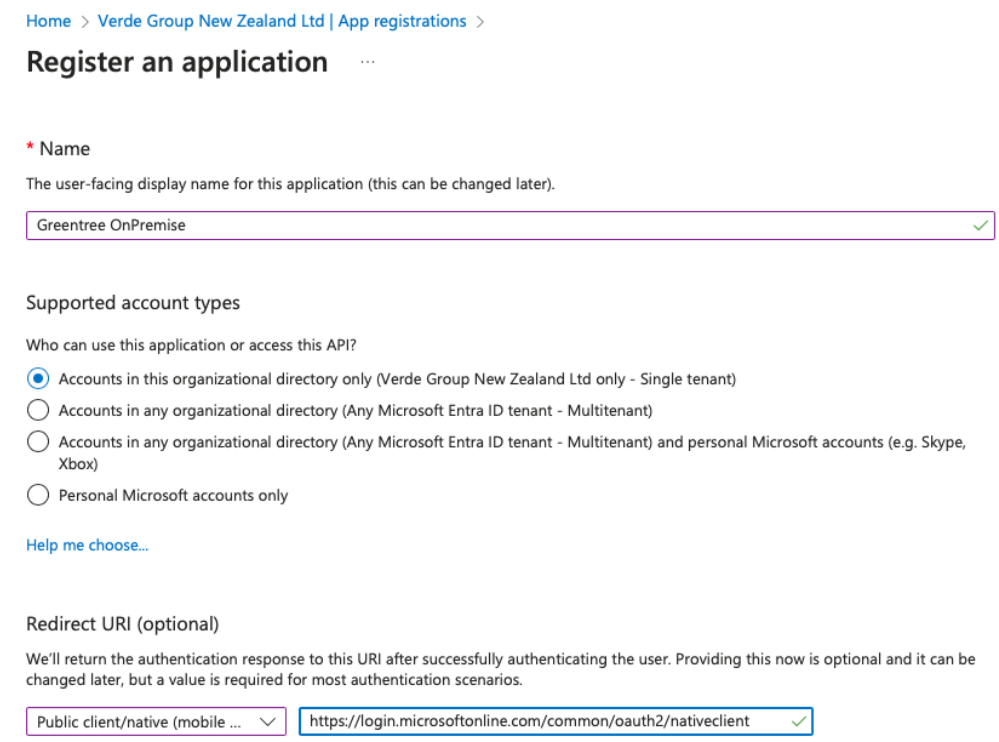
1. Select the menu item | ☰ | Microsoft Entra ID |
2. An overview of the organisation details is shown. Copy the Tenant ID that is shown on this page and paste in the App Configuration form in Greentree.



3. Select the menu item | ☰ | App registrations |

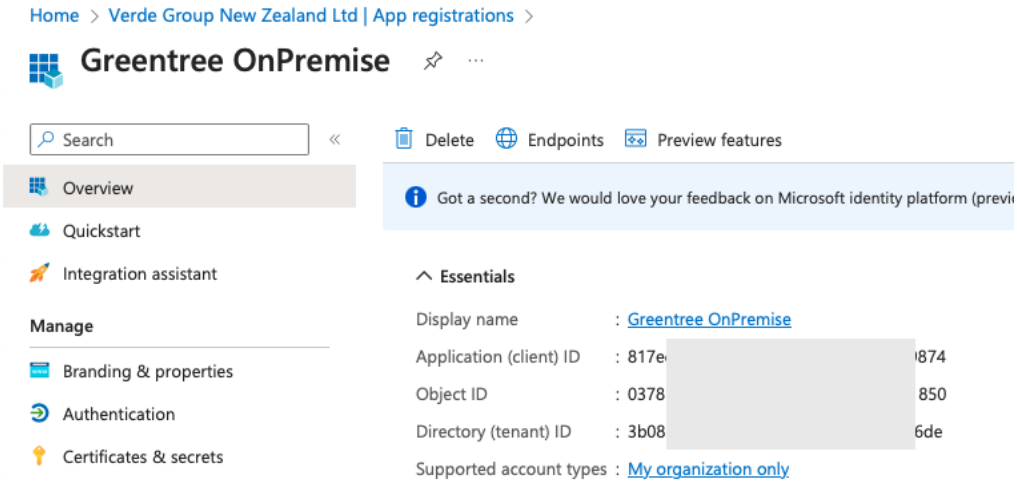


4. Click on the New registration button. Enter the application details. Note the name of the application is not important. Select the first option ("single tenant") and Enter https://login.microsoftonline.com/common/oauth2/nativeclient as the Redirect URI.

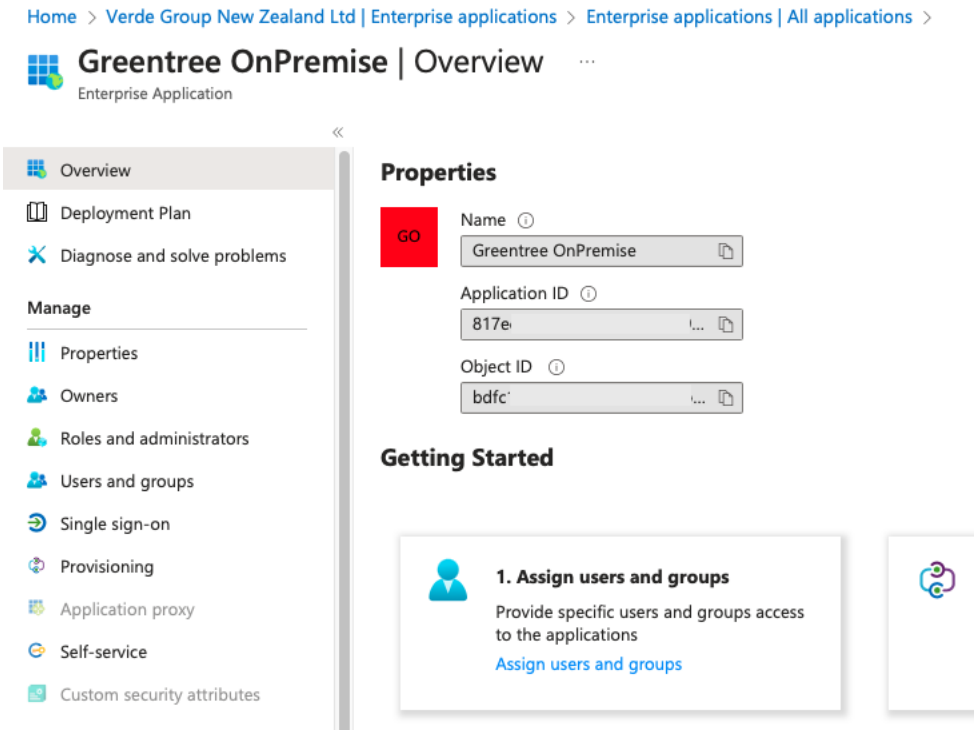


Click on the Register button to save the application.

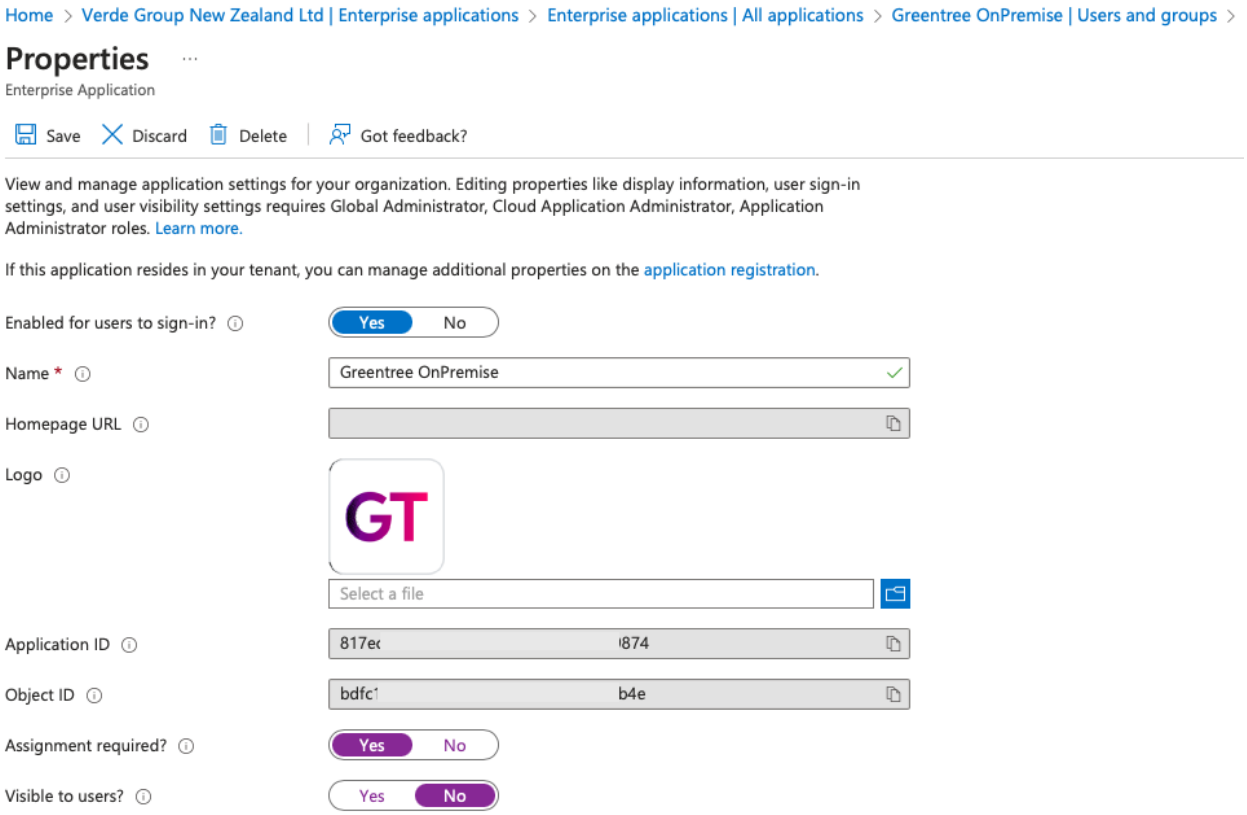
5. On the application details page Copy the Application (client) ID that is shown on this page and paste in the App Configuration form in Greentree.



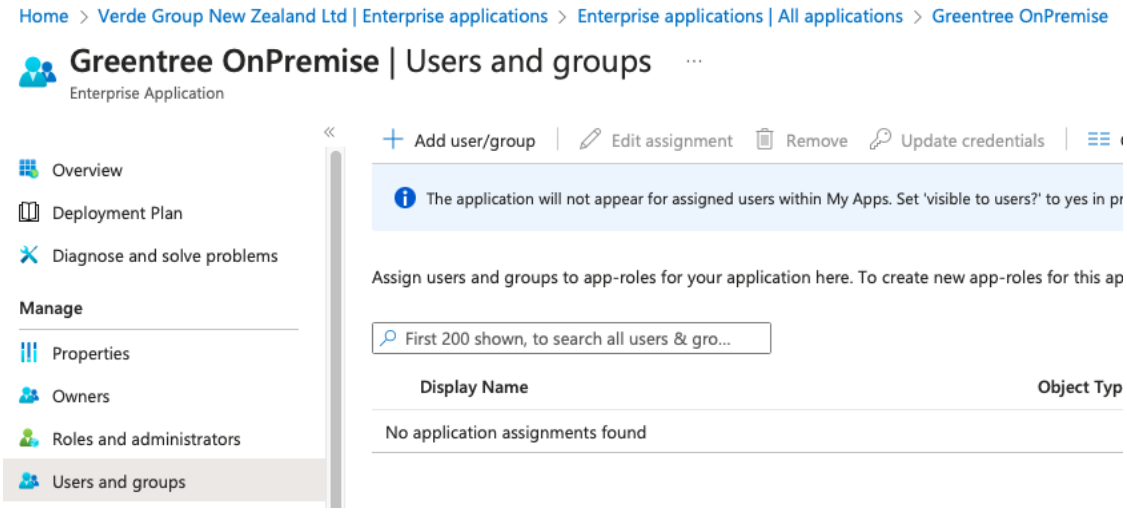
6. Select the menu item | Enterprise applications | From the list find the new application and select it to show the overview page.



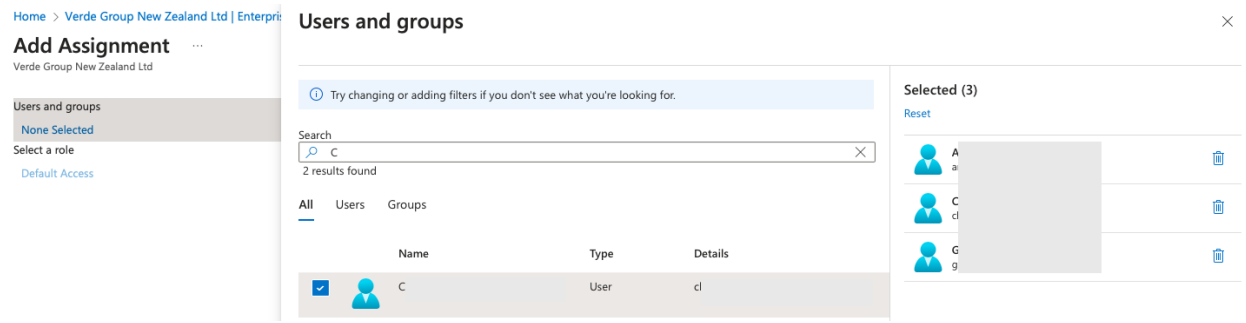
7. Select the menu item | Properties |
   Set the following properties:
   Enabled for users to sign-in? Yes
   Assignment required? Yes
   Visible to users? No



8. Assign users and/or groups to the application for access.
   Select the menu item | Users and groups |



9. Click on the Add user/group button. Select the users and/or groups to assign and then click on the Assign button.



10. Select the menu item | Permissions |

    On this screen click the Grant admin consent... button to enable authentication without requiring individual administrator approval for each user.