



GroupID
by imanami

Version 10



GroupID
Authenticate



GroupID
Automate



GroupID
Self-Service



GroupID
Synchronize



GroupID
Password Center



GroupID
Insights



GroupID
Mobile App



GroupID
Reports

Configure GroupID in Azure AD

Reference Guide

This publication applies to Imanami GroupID Version 10 and subsequent releases until otherwise indicated in new editions.

© **Copyright Imanami Corporation 2022.** Trademarks are the property of their respective owners.

Contents

Chapter 1 - Introduction.....	1	Chapter 3 - Identity Store Creation and Role	
Chapter 2 - Register GroupID in Azure.....	2	Assignment in GroupID	15
GroupID Application Registration and Permission		Create an Azure Identity Store	15
Assignment	2	GroupID Security Role Setting.....	18
Create a User in Azure AD.....	12	Limitations of Minimum Service Account	
		Permissions.....	19

Chapter 1 - Introduction

GroupID uses an identity store-based model. You can create an identity store for a supported identity provider and perform different functions on that identity provider through the identity store. These functions include group management tasks, such as creating groups, scheduling group updates, and expiring groups; user management tasks, such as creating users and mailboxes, managing users' profiles, and more.

GroupID supports the multiple identity providers for creating an identity store. Microsoft Azure is one of the identity providers that GroupID supports. The purpose of this guide is to provide information that will help configure GroupID in Microsoft Azure.

Chapter 2 - Register GroupID in Azure

To use Microsoft Azure Active Directory (Azure AD) identity provider, GroupID must first be registered in Azure portal. The registration grants GroupID access to a particular Azure Active Directory and its data, such as Azure AD groups and users.

GroupID requires:

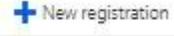
- An [application registered](#) for GroupID in Azure AD (with the Microsoft Graph API and Exchange API permissions).
- An Azure Directory Role for the [service account](#) for the Azure identity store.



See [Role and Permissions](#) section on [Administrator role permissions in Azure Active Directory](#) for reference.

GroupID Application Registration and Permission Assignment

This section discusses the GroupID application registration and permission assignment procedure.

1. Login to <https://portal.azure.com/> with a user that is part of the “Global Administrator” role or any role that has rights to register an app, such as the “Application administrator” role. This is required in order to give consent to certain permissions in the application.
2. In the Microsoft Azure portal, go to **Azure Active Directory > App registration** and click .

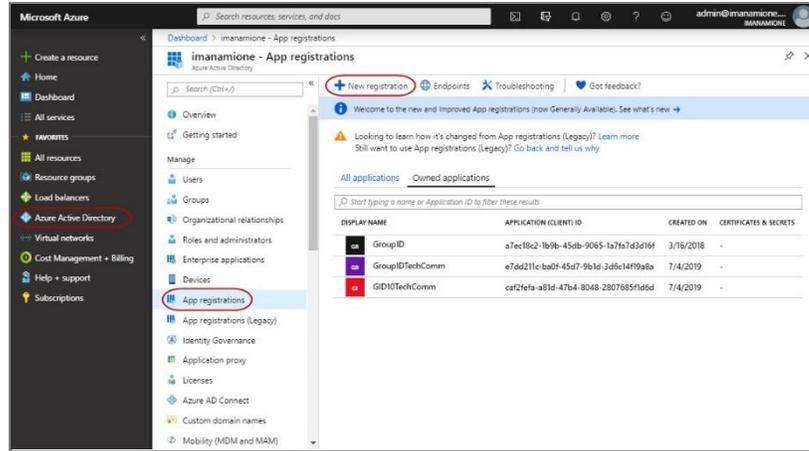


Figure 1: App Registration page

3. On the **Register an application** page, specify a name for the app. Select **Supported account types** as *Accounts in any organizational directory (Any Azure AD directory – Multitenant)*. Leave the Redirect URI as is and click **Register**.

Register an application

*** Name**
The user-facing display name for this application (this can be changed later).

Supported account types
Who can use this application or access this API?

Accounts in this organizational directory only (Imanami only - Single tenant)
 Accounts in any organizational directory (Any Azure AD directory - Multitenant)
 Accounts in any organizational directory (Any Azure AD directory - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox)
 Personal Microsoft accounts only

[Help me choose...](#)

Redirect URI (optional)
We'll return the authentication response to this URI after successfully authenticating the user. Providing this now is optional and it can be changed later, but a value is required for most authentication scenarios.

Select a platform

Register an app you're working on here. Integrate gallery apps and other apps from outside your organization by adding from [Enterprise applications](#).

By proceeding, you agree to the [Microsoft Platform Policies](#)

Register

Figure 2: Register an application page

4. The **Overview** page is displayed. Copy the *Application (client) ID* and keep it safe.

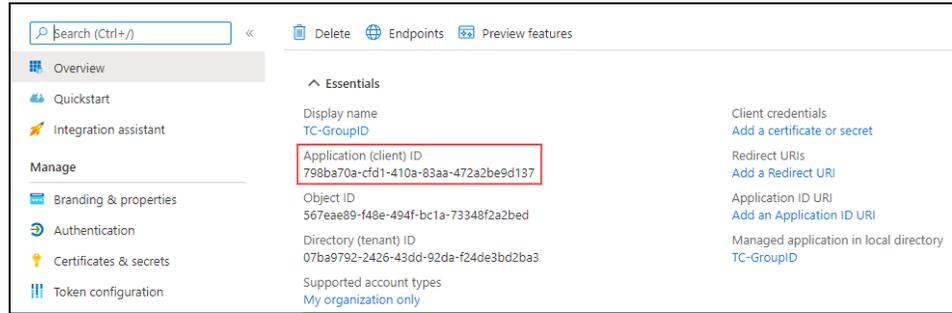


Figure 3: Overview page

5. Go to the **Authentication** node and set it as follows:

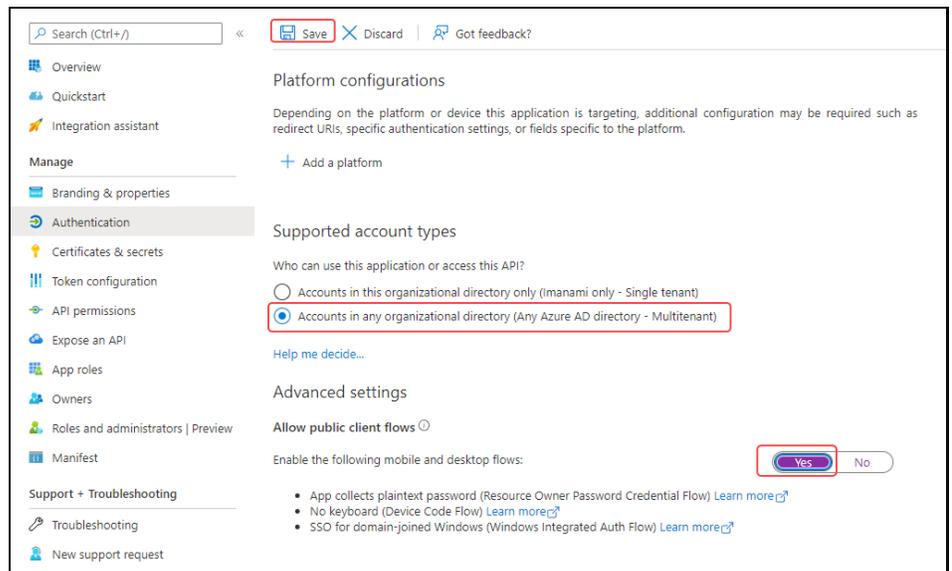


Figure 4: Authentication page

6. Click **Save**.

7. Go to the **API permissions** node and select **Add a permission**.

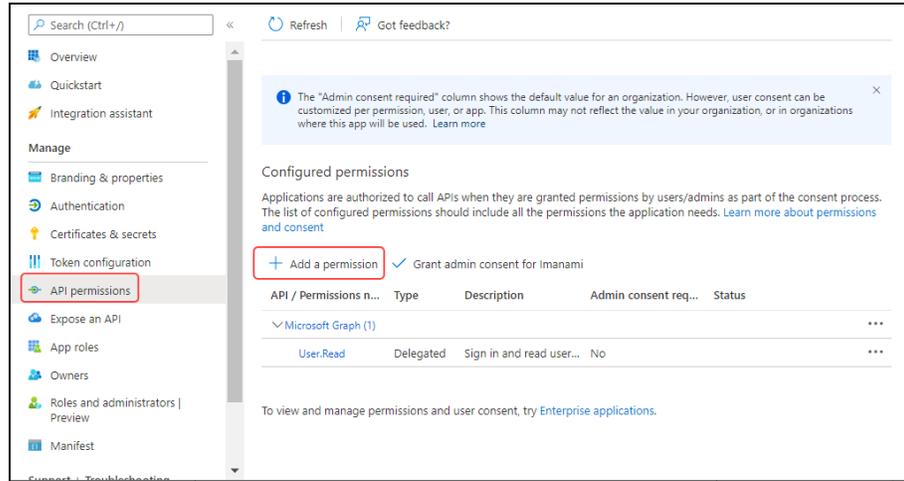
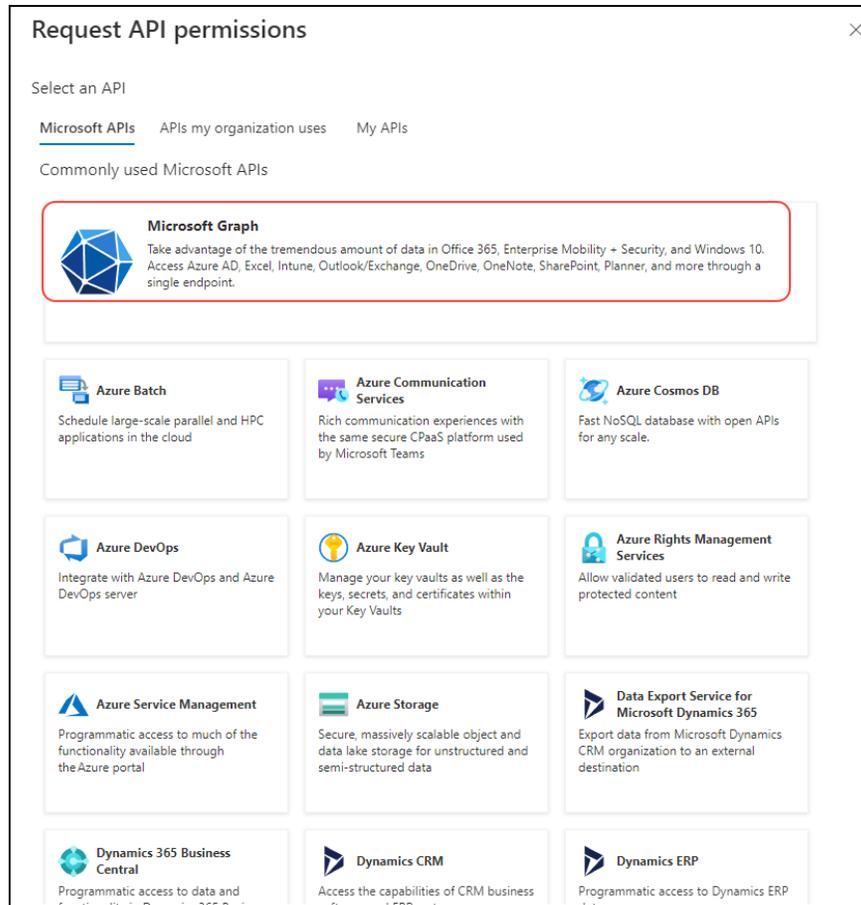


Figure 5: API Permissions page

8. The **Request API permissions** page opens. Click **Microsoft Graph API**.



9. Select the **Delegated permissions** tab.

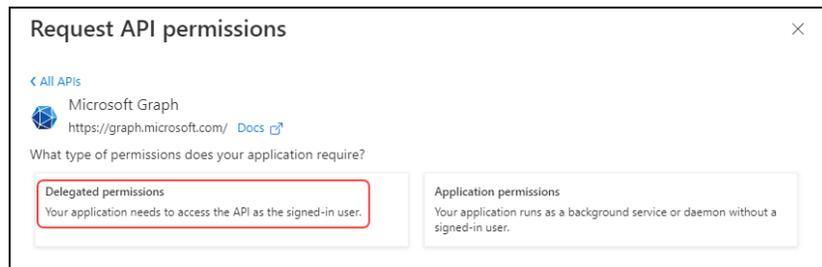


Figure 6: Request API permissions

10. Permissions get listed on the page. Set the following permissions for the Microsoft Graph API:

Permission	Admin consent required
<input checked="" type="checkbox"/> Directory (3)	
<input checked="" type="checkbox"/> Directory.AccessAsUser.All ⓘ Access directory as the signed in user	Yes
<input checked="" type="checkbox"/> Directory.Read.All ⓘ Read directory data	Yes
<input checked="" type="checkbox"/> Directory.ReadWrite.All ⓘ Read and write directory data	Yes
<input checked="" type="checkbox"/> EWS (1)	
<input checked="" type="checkbox"/> EWS.AccessAsUser.All ⓘ Access mailboxes as the signed-in user via Exchange Web Services	No
<input checked="" type="checkbox"/> Group (2)	
<input checked="" type="checkbox"/> Group.Read.All ⓘ Read all groups	Yes
<input checked="" type="checkbox"/> Group.ReadWrite.All ⓘ Read and write all groups	Yes
<input checked="" type="checkbox"/> IdentityProvider (2)	
<input checked="" type="checkbox"/> IdentityProvider.Read.All ⓘ Read identity providers	Yes
<input checked="" type="checkbox"/> IdentityProvider.ReadWrite.All ⓘ Read and write identity providers	Yes
<input checked="" type="checkbox"/> MailboxSettings (2)	
<input checked="" type="checkbox"/> MailboxSettings.Read ⓘ Read user mailbox settings	No
<input checked="" type="checkbox"/> MailboxSettings.ReadWrite ⓘ Read and write user mailbox settings	No

Mail (7)		
<input checked="" type="checkbox"/>	Mail.Read ⓘ Read user mail	No
<input checked="" type="checkbox"/>	Mail.Read.Shared ⓘ Read user and shared mail	No
<input checked="" type="checkbox"/>	Mail.ReadBasic ⓘ Read user basic mail	No
<input checked="" type="checkbox"/>	Mail.ReadWrite ⓘ Read and write access to user mail	No
<input checked="" type="checkbox"/>	Mail.ReadWrite.Shared ⓘ Read and write user and shared mail	No
<input checked="" type="checkbox"/>	Mail.Send ⓘ Send mail as a user	No
<input checked="" type="checkbox"/>	Mail.Send.Shared ⓘ Send mail on behalf of others	No
Member (1)		
<input checked="" type="checkbox"/>	Member.Read.Hidden ⓘ Read hidden memberships	Yes
User (8)		
<input checked="" type="checkbox"/>	User.Export.All ⓘ Export user's data	Yes
<input checked="" type="checkbox"/>	User.Invite.All ⓘ Invite guest users to the organization	Yes
<input checked="" type="checkbox"/>	User.ManageIdentities.All ⓘ Manage user identities	Yes
<input checked="" type="checkbox"/>	User.Read ⓘ Sign in and read user profile	No
<input checked="" type="checkbox"/>	User.Read.All ⓘ Read all users' full profiles	Yes
<input checked="" type="checkbox"/>	User.ReadBasic.All ⓘ Read all users' basic profiles	No
<input checked="" type="checkbox"/>	User.ReadWrite ⓘ Read and write access to user profile	No
<input checked="" type="checkbox"/>	User.ReadWrite.All ⓘ Read and write all users' full profiles	Yes

Figure 7: Microsoft Graph API permissions

Click the **Add permissions** button to add the selected permissions.

- Please note that some permissions require admin consent. Click **Grant admin consent for <username>** button.

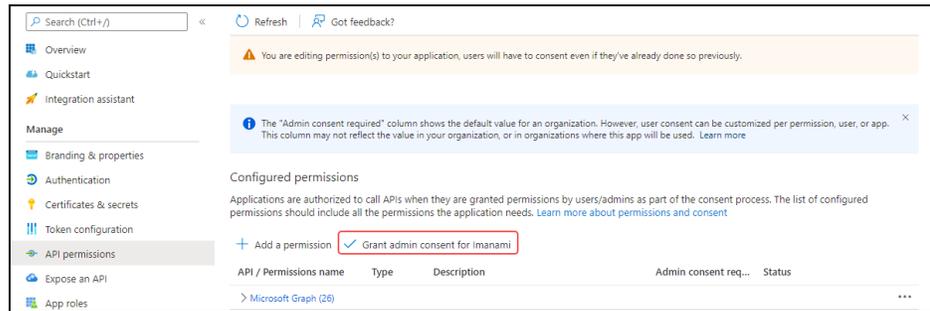
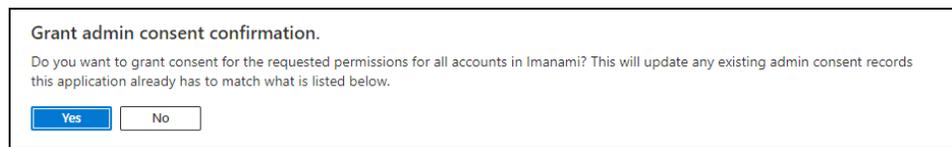


Figure 8: API Permissions page

The following message is displayed:



Click **Yes** to grant admin consent to all the listed permissions.

- Click **Add a permission** button (Figure 5). Follow the steps shown on the following snapshot:

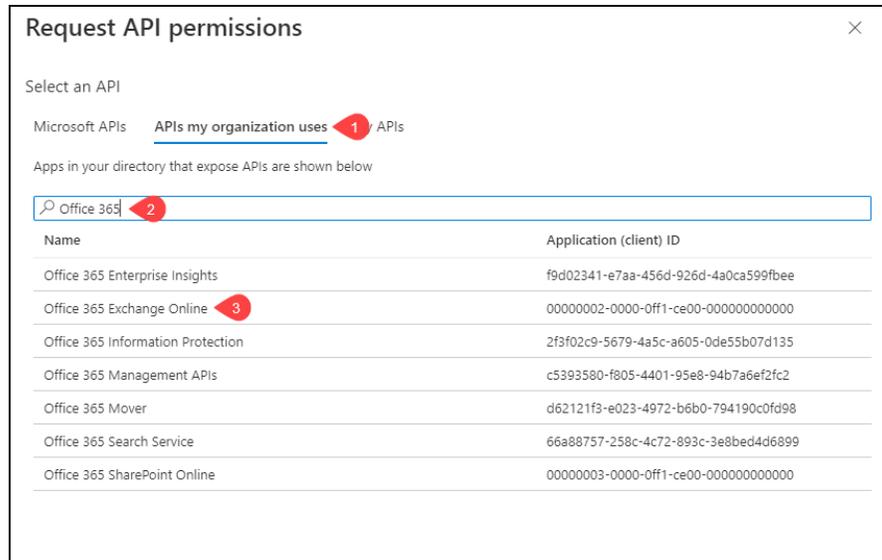


Figure 9: Request API permissions page

13. Click the **Delegated permissions** tab:

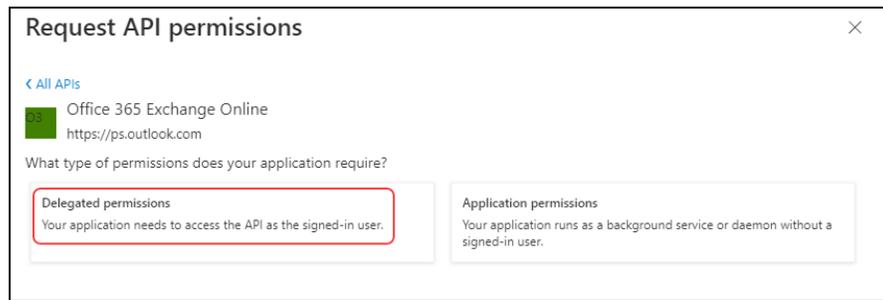


Figure 10: Delegated permissions option

And set the following permissions for the **Office 365 Exchange Online** API:

Permission	Admin consent required
<p>▼ Calendars (6)</p>	
<input checked="" type="checkbox"/> Calendars.Read ⓘ Read user calendars	No
<input checked="" type="checkbox"/> Calendars.Read.All ⓘ Read user and shared calendars	No
<input checked="" type="checkbox"/> Calendars.Read.Shared ⓘ Read user and shared calendars	No
<input checked="" type="checkbox"/> Calendars.ReadWrite ⓘ Read and write user calendars	No
<input checked="" type="checkbox"/> Calendars.ReadWrite.All ⓘ Read and write user and shared calendars	No
<input checked="" type="checkbox"/> Calendars.ReadWrite.Shared ⓘ Read and write user and shared calendars	No
<p>▼ Contacts (6)</p>	
<input checked="" type="checkbox"/> Contacts.Read ⓘ Read user contacts	No
<input checked="" type="checkbox"/> Contacts.Read.All ⓘ Read user and shared contacts	No
<input checked="" type="checkbox"/> Contacts.Read.Shared ⓘ Read user and shared contacts	No
<input checked="" type="checkbox"/> Contacts.ReadWrite ⓘ Read and write user contacts	No
<input checked="" type="checkbox"/> Contacts.ReadWrite.All ⓘ Read and write user and shared contacts	No
<input checked="" type="checkbox"/> Contacts.ReadWrite.Shared ⓘ Read and write user and shared contacts	No
<p>▼ EAS (1)</p>	
<input checked="" type="checkbox"/> EAS.AccessAsUser.All ⓘ Access mailboxes via Exchange ActiveSync	No
<p>▼ EWS (1)</p>	
<input checked="" type="checkbox"/> EWS.AccessAsUser.All ⓘ Access mailboxes as the signed-in user via Exchange Web Services	No
<p>▼ Exchange (1)</p>	
<input checked="" type="checkbox"/> Exchange.Manage ⓘ Manage Exchange configuration	No

<p>Group (2)</p>		
<input checked="" type="checkbox"/>	<p>Group.Read.All ⓘ Read all groups (preview)</p>	No
<input checked="" type="checkbox"/>	<p>Group.ReadWrite.All ⓘ Read and write all groups (preview)</p>	No
<p>MailboxSettings (2)</p>		
<input checked="" type="checkbox"/>	<p>MailboxSettings.Read ⓘ Read user mailbox settings</p>	No
<input checked="" type="checkbox"/>	<p>MailboxSettings.ReadWrite ⓘ Read and write user mailbox settings</p>	No
<p>Mail (10)</p>		
<input checked="" type="checkbox"/>	<p>Mail.Read ⓘ Read user mail</p>	No
<input checked="" type="checkbox"/>	<p>Mail.Read.All ⓘ Read user and shared mail</p>	No
<input checked="" type="checkbox"/>	<p>Mail.Read.Shared ⓘ Read user and shared mail</p>	No
<input checked="" type="checkbox"/>	<p>Mail.ReadBasic ⓘ Read user basic mail</p>	No
<input checked="" type="checkbox"/>	<p>Mail.ReadWrite ⓘ Read and write user mail</p>	No
<input checked="" type="checkbox"/>	<p>Mail.ReadWrite.All ⓘ Read and write user and shared mail</p>	No
<input checked="" type="checkbox"/>	<p>Mail.ReadWrite.Shared ⓘ Read and write user and shared mail</p>	No
<input checked="" type="checkbox"/>	<p>Mail.Send ⓘ Send mail as a user</p>	No
<input checked="" type="checkbox"/>	<p>Mail.Send.All ⓘ Send mail on behalf of others</p>	No
<input checked="" type="checkbox"/>	<p>Mail.Send.Shared ⓘ Send mail on behalf of others</p>	No
<p>User (5)</p>		
<input checked="" type="checkbox"/>	<p>User.Read ⓘ Read user profiles</p>	No
<input checked="" type="checkbox"/>	<p>User.Read.All ⓘ Read all users' full profiles</p>	Yes
<input checked="" type="checkbox"/>	<p>User.ReadBasic.All ⓘ Read all users' basic profiles</p>	No
<input checked="" type="checkbox"/>	<p>User.ReadBasic.All ⓘ Read all users' basic profiles</p>	No
<input checked="" type="checkbox"/>	<p>User.ReadWrite ⓘ Read and write user profiles</p>	No

Figure 11: Office 365 Exchange Online API Permissions

Click the [Add permissions](#) button to add the selected permissions.

Some permissions require admin consent. Click **Grant admin consent for <username>** button.

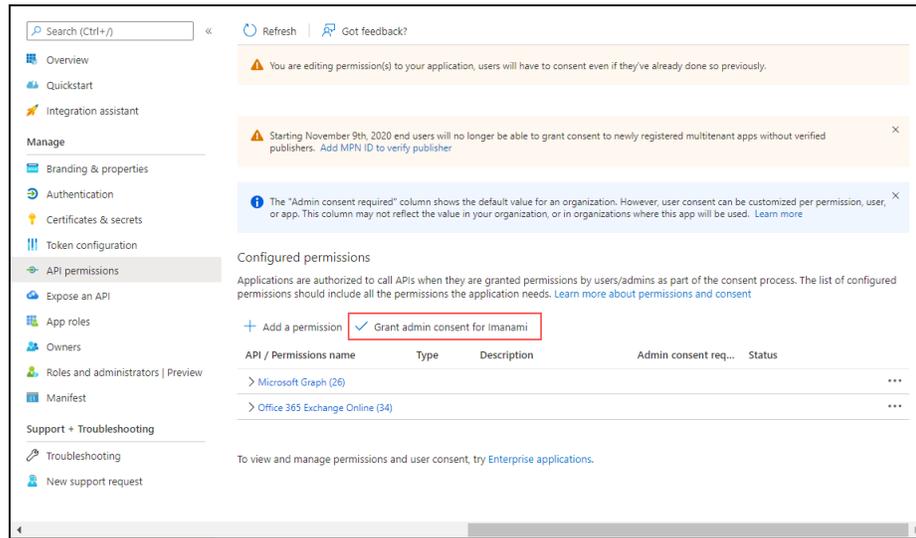
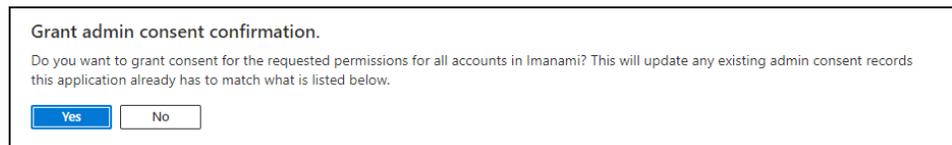


Figure 12: API Permissions page with Grant admin consent button

The following message is displayed:



Click **Yes** to grant admin consent to all the listed permissions for the Microsoft 365 Exchange Online API.

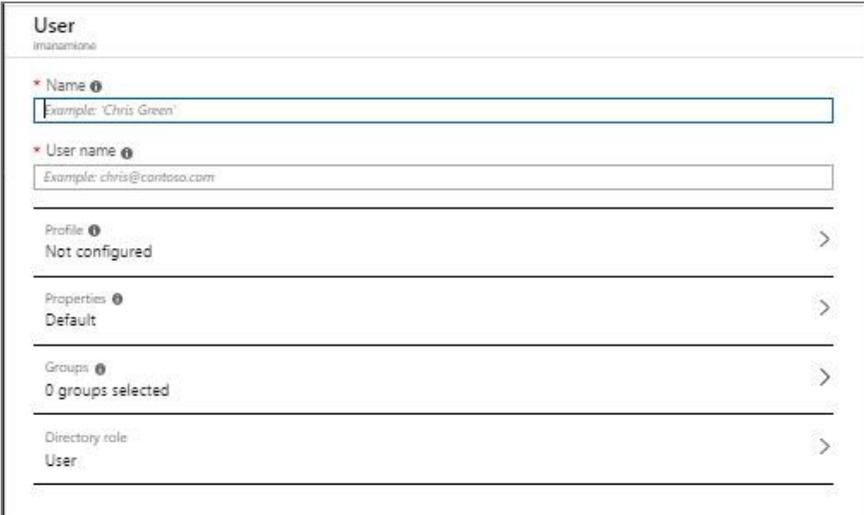
This completes the registration process of GroupID in Azure AD.

Create a User in Azure AD

Once your application has been registered with Azure AD, create a user in Azure AD that will be set as a service account while creating an identity store for Azure in GroupID.

To create a user in Azure AD:

1. In the Microsoft Azure portal, go to **Azure Active Directory > Users** and click



The screenshot shows the 'New user' page in the Azure portal. At the top, there is a blue plus icon followed by the text 'New user'. Below this is a form titled 'User' with the email address 'imran@imnami.com' displayed. The form has several sections:

- Name:** A text input field with a red asterisk and a help icon. The placeholder text is 'Example: Chris Green'.
- User name:** A text input field with a red asterisk and a help icon. The placeholder text is 'Example: chris@contoso.com'.
- Profile:** A section with the text 'Not configured' and a right-pointing chevron.
- Properties:** A section with the text 'Default' and a right-pointing chevron.
- Groups:** A section with the text '0 groups selected' and a right-pointing chevron.
- Directory role:** A section with the text 'User' and a right-pointing chevron.

Figure 13: New user page

2. On the **User** page:
 - Provide the first and last name of the new user in the **Name** box.
 - Provide the user name of the new user along with the domain name in the **User name** box.
 - Click the **Profile** box and provide more information about the user in the displayed pane.
 - Click the **Groups** box if you want to add the user to one or more existing groups.
 - Click the **Directory role** to add the user to an Azure AD administrator role. You can assign the user to be a [Global administrator](#) or [limited administrator](#) in Azure AD.

- **For Global administrator** (*recommended directory role assignment*)

Select the **Global administrator** option in the **Directory role** pane:

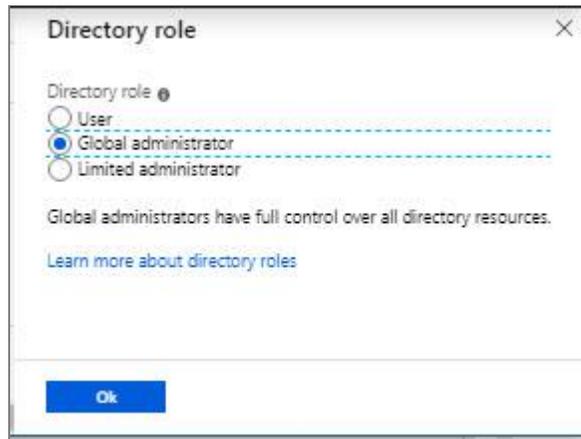


Figure 14: Directory Role pane

- **For Limited Administrator** (*Minimum Directory Role Assignment*)

Select the **Limited administrator** option in the **Directory role** pane (Figure 14):

Select the following two roles from the displayed list of roles:



These Azure AD administrator roles have the following rights

Exchange administrator can manage all aspects of the Exchange product

User administrator (User Account Administrator) can manage all aspects of users and groups, including resetting passwords for limited administrators.

For example, this role does not allow deleting a global administrator. User Account Administrators can change passwords for users, Helpdesk administrators, and other User Account Administrators only.

3. Click **OK**.



By default, the GroupID Administrator security role in an Azure identity store binds to Global Administrator. If minimum role assignment for the service account is used, the default Admin Security role criteria should also be changed to the User Account Administrators group.

4. When you provide information in the **Name** and **Username** boxes, the **Password** box, with an autogenerated password, is displayed. Copy that password. You'll need to give this password to the user for the initial sign-in process.



Azure forces new users to change their password at next logon by signing-in to Azure portal (<https://portal.azure.com>).

5. Select **Create**.

The user is created and added to your Azure AD tenant.

You can now [create an identity](#) store for Azure AD in GroupID.



Make sure you copy the application ID which is generated by Azure AD when the application is registered (Figure 3). This application ID will be required while creating an identity store for Azure AD.

Chapter 3 - Identity Store Creation and Role Assignment in GroupID

Once you have registered GroupID and created a user with required directory role in Azure, you can now create an Azure identity store in GroupID. This chapter walks you through the steps to create an Azure identity store and assign a role to the Azure user in GroupID.

Create an Azure Identity Store

1. In GroupID Management Console, click the **Identity Stores** node.
2. Click the **New Identity Store** option in the **Actions** pane. The **Create New Identity Store** wizard opens to the **Welcome** page.

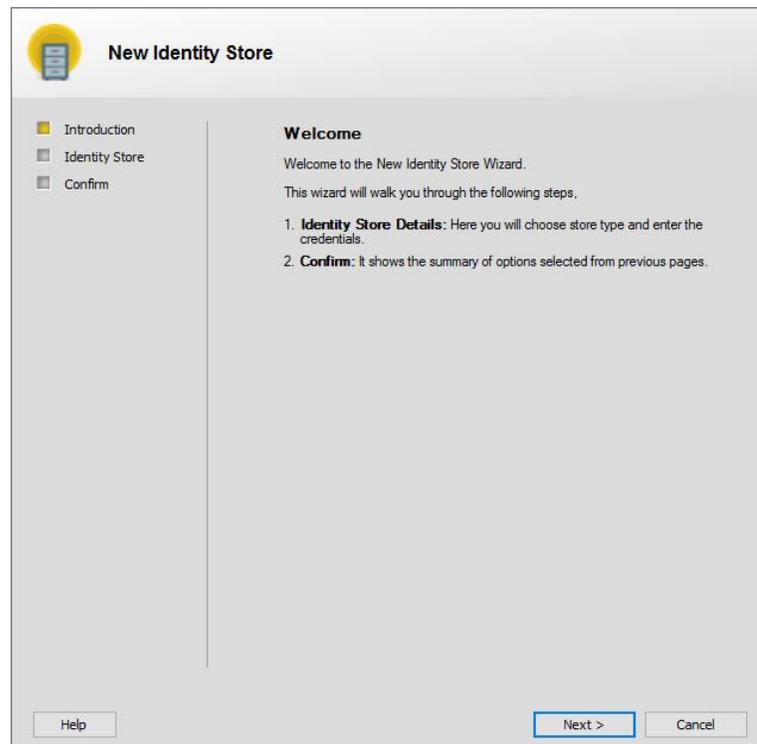


Figure 15: New Identity Store wizard – Welcome page

3. Read the welcome message and click **Next**.

Figure 16: New Identity Store wizard – Identity Store page

4. On the **Identity Store Details** page, provide the following information:
 - a. Select *Windows Azure* identity store type from the **Identity Store Type** list.
 - b. In the **Name** box, type a name for the identity store.
 - c. In the **Domain name** box, enter name of the Azure domain.
 - d. In the **Service Account** box, type the name of the service account for connecting to the Azure identity provider.

The service account must have sufficient privileges in Azure AD so that group and identity management operations can be performed using GroupID.



If you intend to use a service account user with [Global Administrator](#) directory role, then no change is required in the default GroupID security roles settings of Azure identity store. And if you intend to use a service account user with [Limited Administrator](#) directory role (i.e. User Administrator + Exchange Administrator), then the GroupID Administrator security role criteria group must be changed to [User Account Administrator](#).

- e. In the **Service Account Password** box, type the service account password.
- f. In the **Registered Application ID on Azure Active Directory** box, provide the application ID assigned to the application you registered on the Azure portal (Figure 3).
- g. Click **Next**.

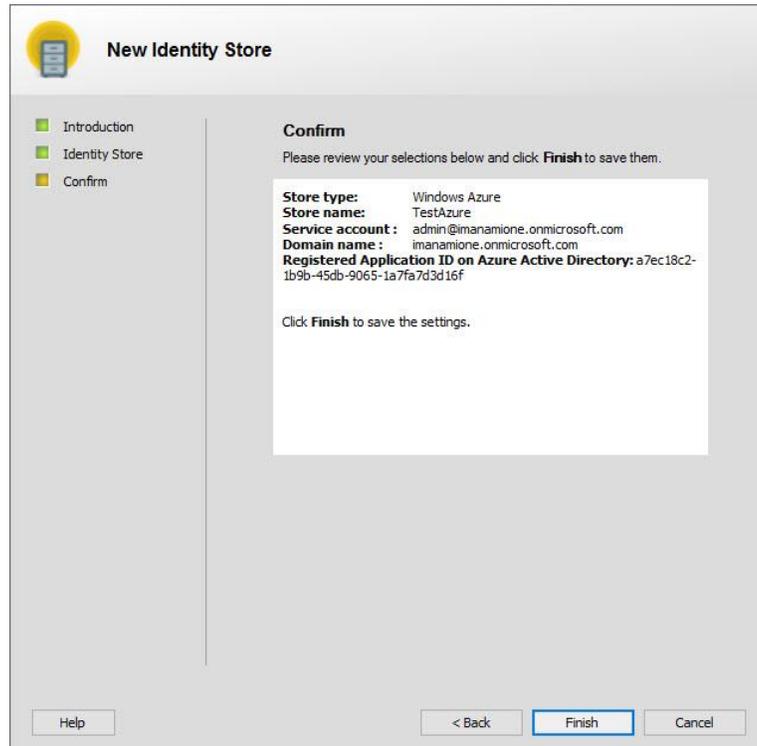


Figure 17: New Identity Store wizard – Confirm page

- 5. On the **Confirm** page, review your entered information and click **Finish** to complete the wizard.

To modify the entered information, click the **Back** button.

The new Azure identity store is now available on the **Identity Stores** tab against the **Identity Stores** node in GroupID Management Console.

This identity store is enabled by default; however, you can disable or delete it when it is not required any more.



After creating Azure identity store, wait for 10 – 15 minutes for the Azure AD domain to replicate to Elasticsearch and then start using Azure identity store in GroupID.

GroupID Security Role Setting

If you want to use a service account user with Limited Administrator role for Azure identity store, you have to assign it **User Account Administrator** role in GroupID.

1. In GroupID Management Console, click the **Identity Stores** node.
2. On the **Identity Stores** tab, double-click the Azure identity store to open its properties.
3. Click the **Security Roles** tab, select the Administrator role and click **Edit**.

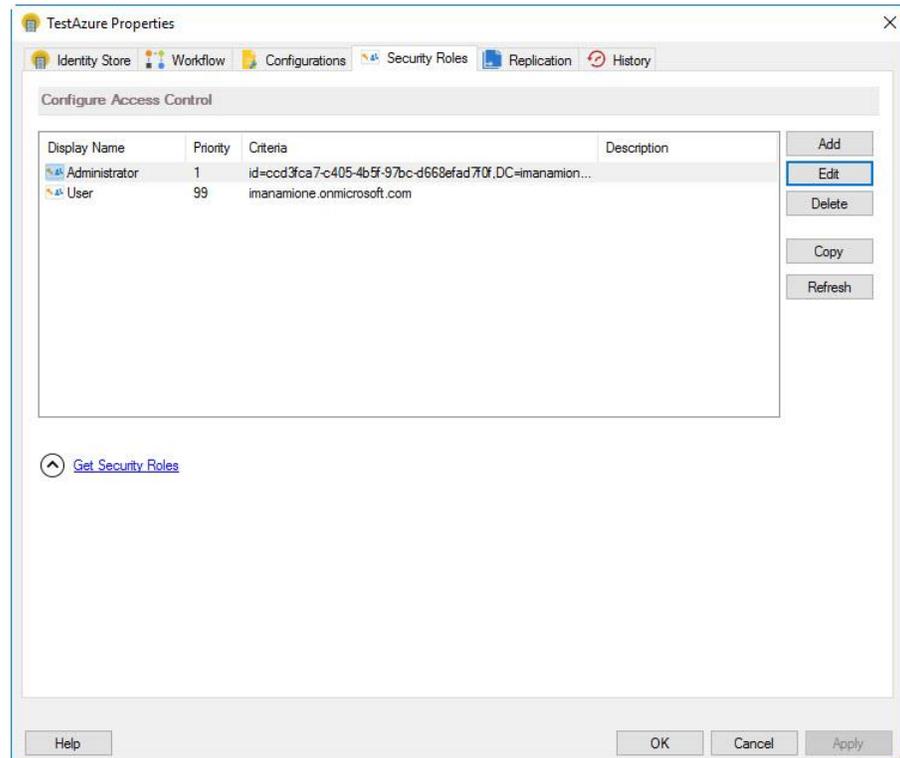


Figure 18: Identity Store Properties – Security Role tab

4. Click the **Criteria** tab and change the group to *User Account Administrator* by searching and selecting it on the **Find** dialog box.

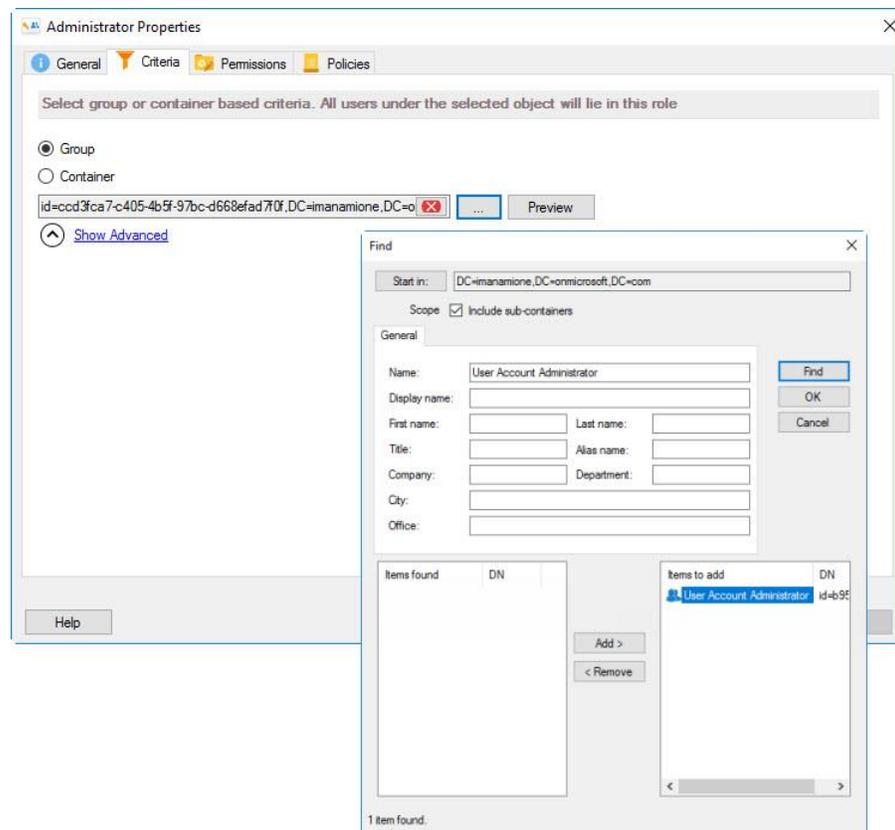


Figure 19: Identity Store Properties – Criteria tab

Click **OK** to close the **Find** dialog box.

Click **OK** to close Administrator properties and then Identity Store properties windows.

Limitations of Minimum Service Account Permissions

If you are using a service account with [minimum directory role assignments](#), the following limitations apply:

- Only the *User* role can be assigned to newly created *users* and *mailboxes* objects from GroupID. The same applies to existing *users* and *mailboxes*, as Directory Roles cannot be changed, using a service account with minimum directory role assignments.
- The password reset functionality would be limited to objects falling in the *User* role, *User Administrator* role, and *Helpdesk* role.



GroupID
by imanami

Imanami Corporation

2301 Armstrong Street
Livermore, CA 94551
United States

<https://www.imanami.com/>

Support: (925) 371-3000, Opt. 3
support@imanami.com

Sales: (925) 371-3000, Opt. 1
sales@imanami.com

Toll-Free: (800) 684-8515
Phone: (925) 371-3000
Fax: (925) 371-3001