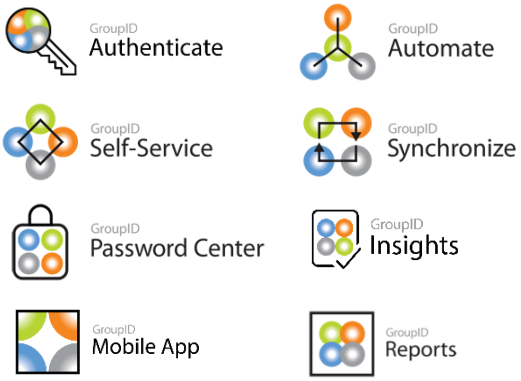
GroupID

by imanami | NOW PART OF netwrix

Version 10



Configure GroupID in Azure AD

Reference Guide

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

Contents

Chapter 1 - Introduction..... 1

Chapter 2 - Register GroupID in Azure..... 2

GroupID Application Registration and Permission Assignment..... 2

Create a User in Azure AD..... 13

Chapter 3 - Identity Store Creation and Role Assignment in GroupID 16

Create an Azure Identity Store..... 16

GroupID Security Role Setting 19

Limitations of Minimum Service Account Permissions 20

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 

.

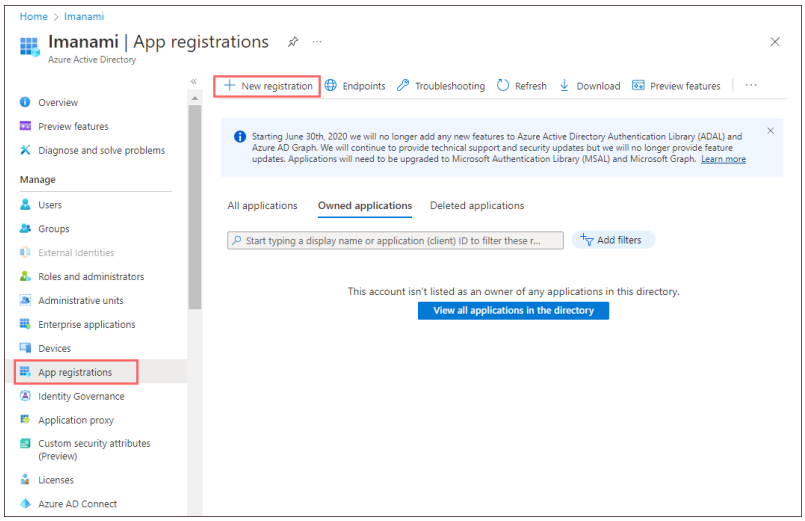


Figure 1: App Registration page

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**.

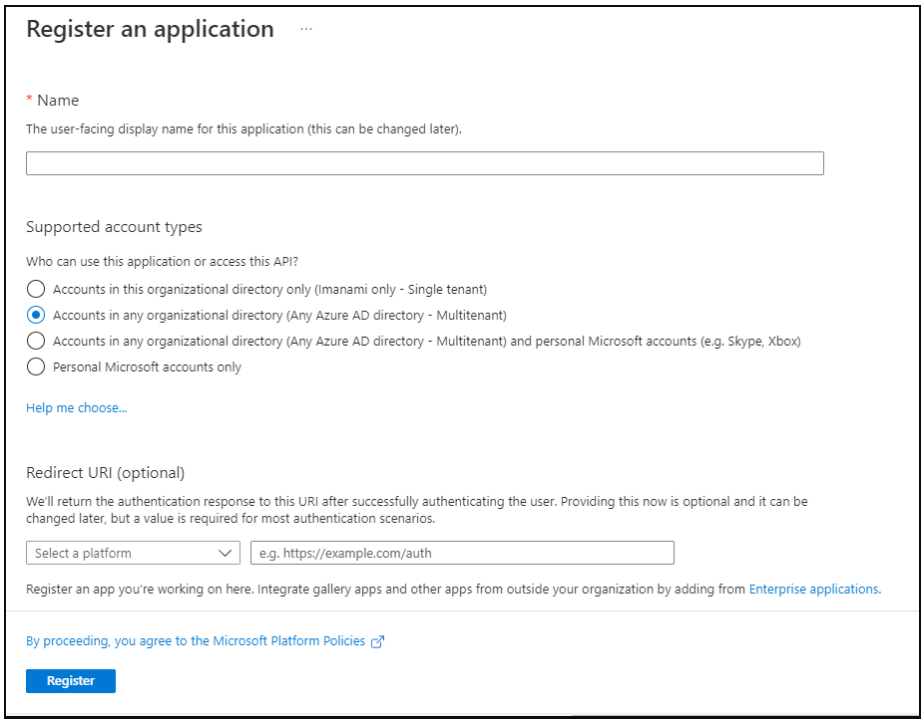


Figure 2: Register an application page

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:

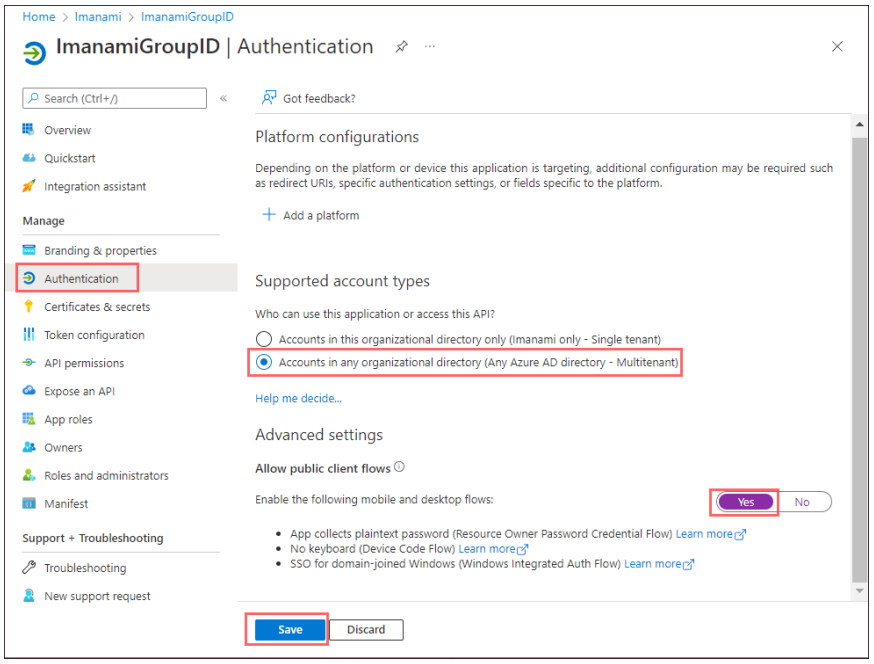


Figure 4: Authentication page

6. Click 

.

7. Click **Roles and administrators** node.

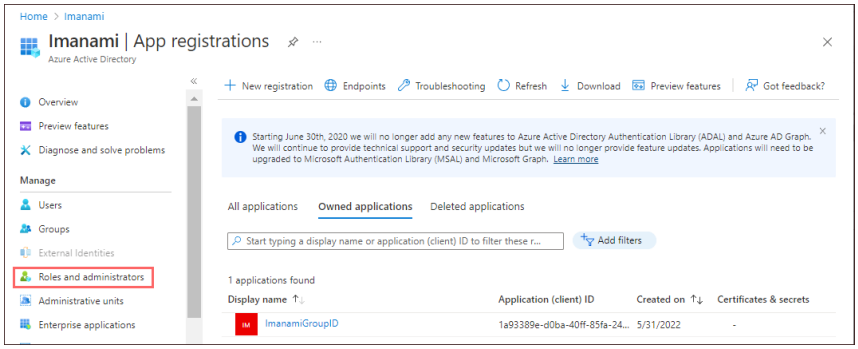


Figure.5: Roles and administrators node

8. On the **All roles** page, add your registered application to Global administrator role. Type global to filter out the Global administrator role. Click **Global administrator**.

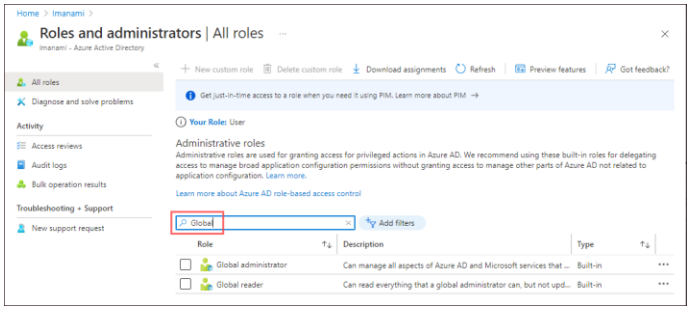


Figure.6: All roles page

Click **Add assignments.** On the Add assignment page, search your application and select it. Click the **Add** button. The application will be listed on the **Assignments** page.

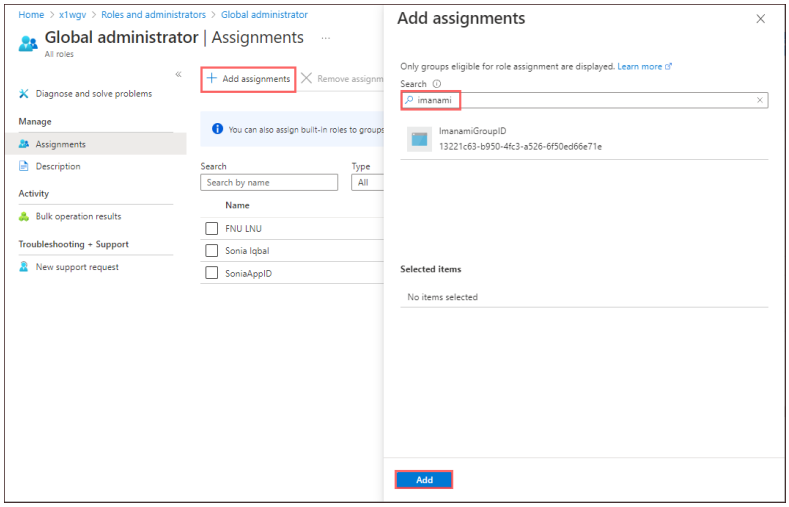


Figure 7: Assignments and Add assignments pages

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

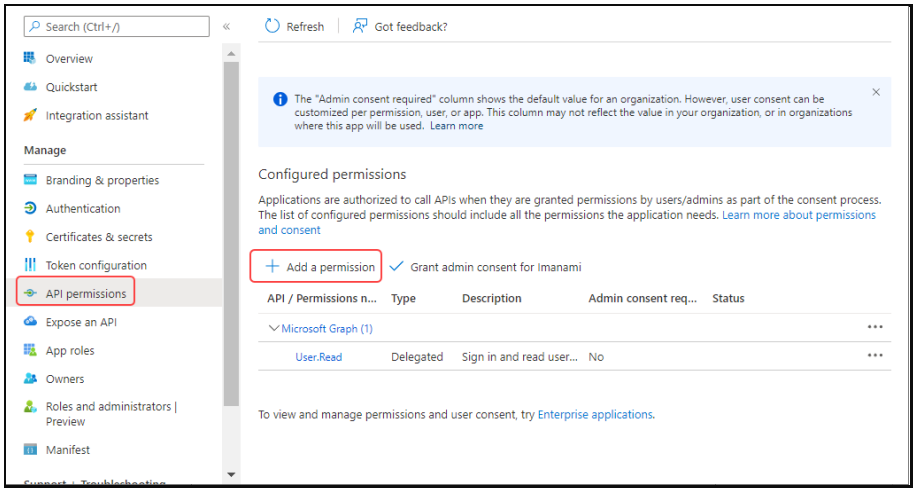


Figure 8: API Permissions page

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

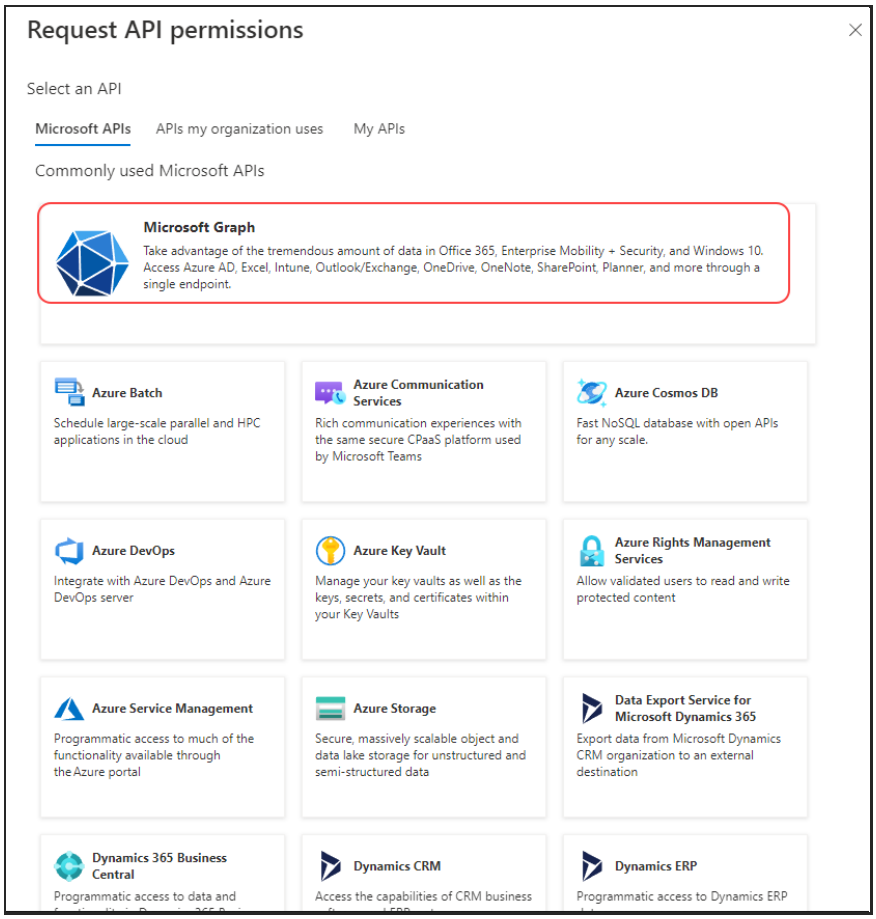


Figure 9: Request API permissions page

11. Select the **Delegated permissions** tab.

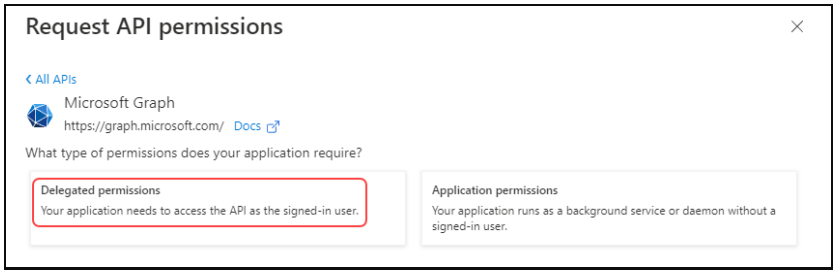


Figure 10: Request API permissions page

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

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

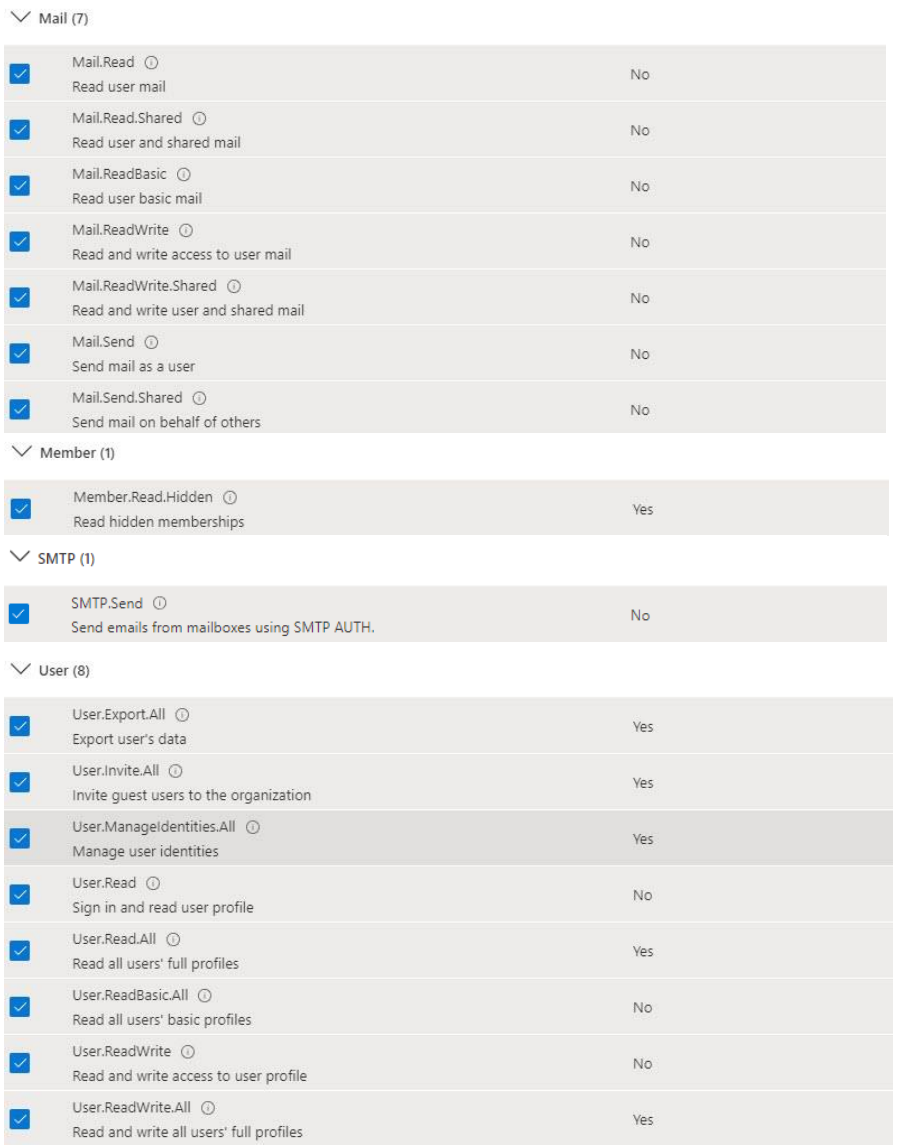


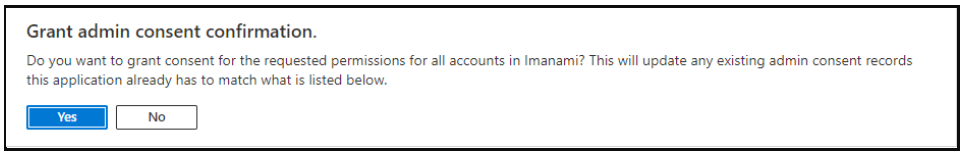
Figure 11: Microsoft Graph API permissions

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

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

Figure 12: API Permissions page

The following message is displayed:



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

14. Click **Add a permission** button (Figure 8). Follow the steps shown on the following snapshot:

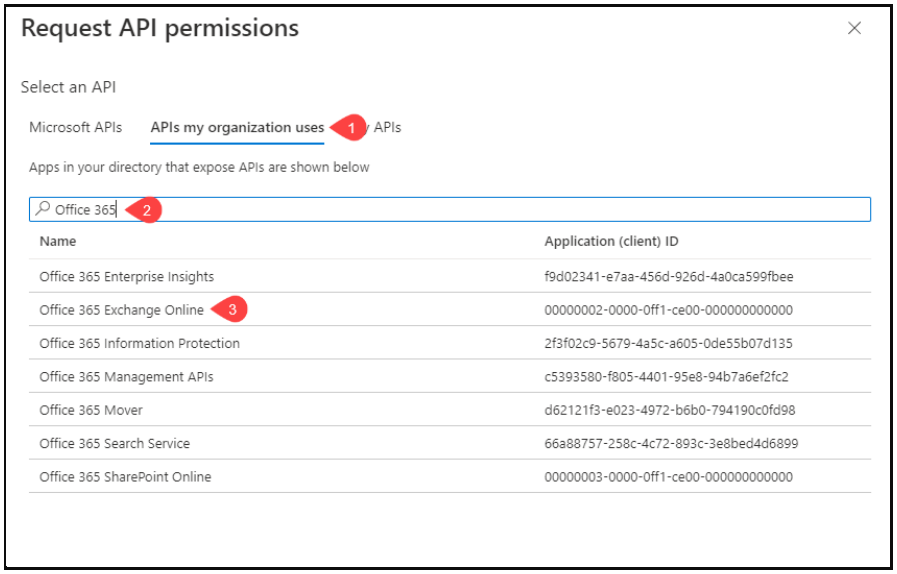


Figure 13: Request API permissions page

15. Click the Application permissions tab:

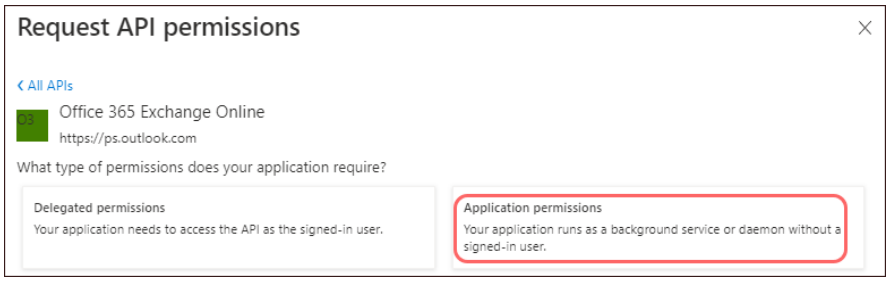


Figure 14: Application permissions option

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

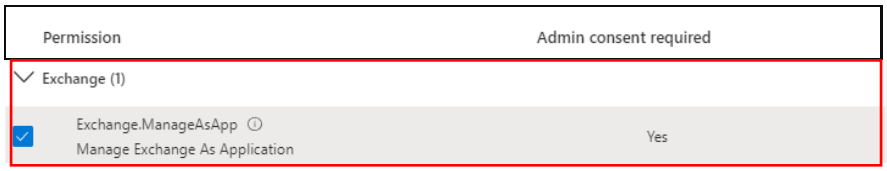


Figure 15: Office 365 Exchange Online API permissions

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

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

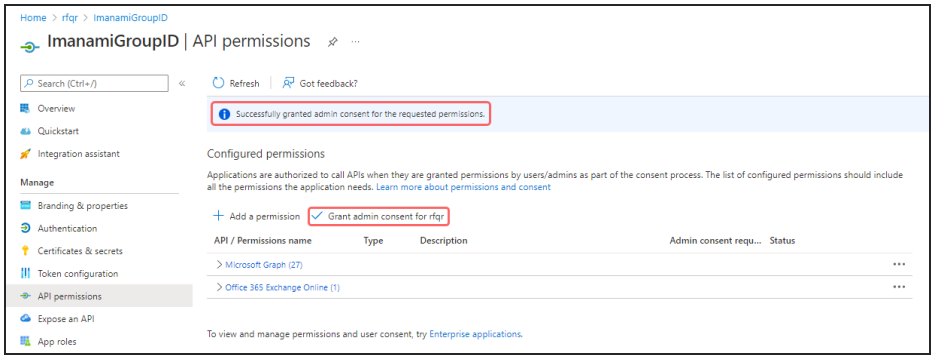
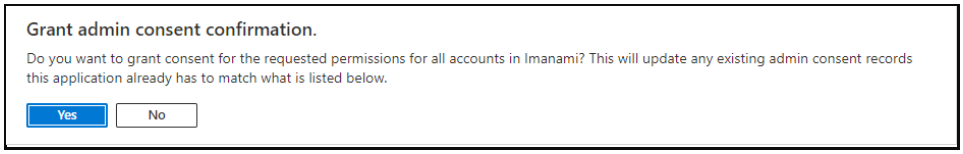


Figure 16: API Permissions page with Grant admin consent button

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.

Provide certificate for Modern Authentication

While configuring GroupID application in Azure AD you must provide a certificate. You can generate this certificate using GroupID PowerShell or any other third-party application.

To generate a certificate using GroupID PowerShell:

1. Login to GroupID server and run GroupID PowerShell as an administrator.
2. Run the following command:

```
$mycert = New-SelfSignedCertificate -DnsName
"contoso.org" -CertStoreLocation
"cert:\LocalMachine\My" -NotAfter (Get-
Date).AddYears(1) -KeySpec KeyExchange

$mycert | Export-Certificate -FilePath c:\mycert.cer
```

Figure 17: GroupID PowerShell command for certificate generation

The generated certificate will be saved at the root level of Drive C:.

In Azure portal, while configuring the GroupID application, upload this certificate using the **Certificate & secrets** node.

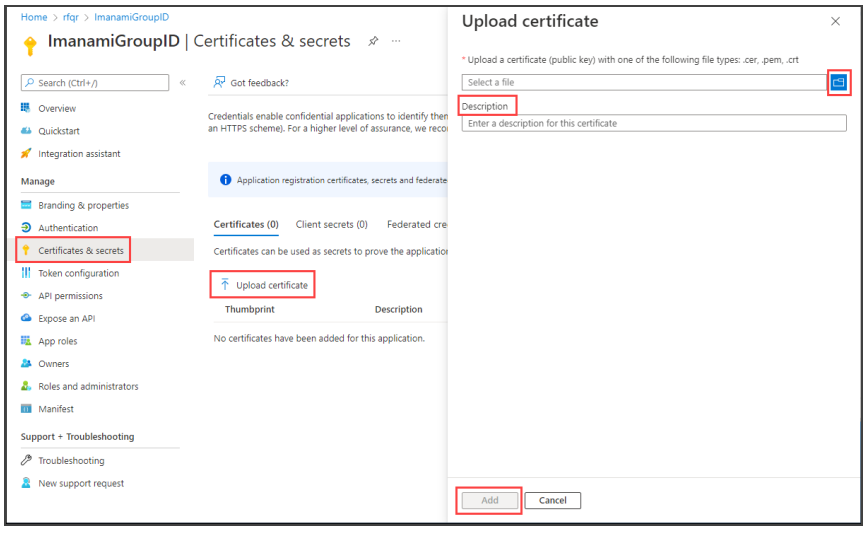


Figure 18: Certificates & secrets window

On the **Upload certificate** page:

1. Click browse to select the generated certificate, *mycert.cer*, from Drive C.
2. Provide a brief description for the certificate in the **Description** box.
3. Click **Add**.

3. After uploading the certificate successfully, Certificate **Thumbprint** is displayed. Copy it and keep it safe.

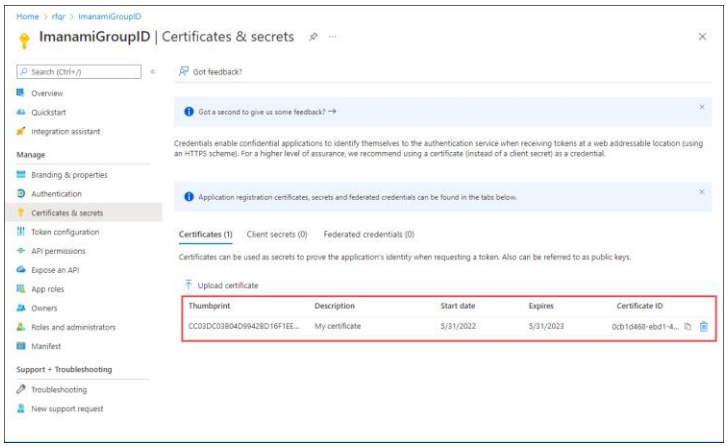


Figure 19: Certificates & secret window with certificate Thumbprint

The certificate **Thumbprint** will be used:

- While creating an Azure identity store (on the **Identity Store Details** page of new identity store creation wizard).
- On the Messaging System page in identity store properties when Exchange Online/Office 365 is set as a messaging provider.
- In Synchronize, in a Synchronize job, when you select AD as destination, and Office 365 as a messaging provider on the Sync Object page, you must provide the certificate Thumbprint.

Verify Modern Authentication

You can test Modern Authentication from GroupID Powershell in your tenant. First, verify that Exchange Online module is installed on your GroupID server using the:

```
Get-InstallModule -name exchangeonlinemanagement
```

Connect to Exchange Online via command shown in screenshot below and fetch some data

For that you need Certificate Thumbprint and Application ID of the registered app

```
Connect-ExchangeOnline -certificateThumbprint Thumbprint -
AppId App ID -organization organization name
```

To disconnect the Exchange Online session, use the following cmdlet:

```
Disconnect-ExchangeOnline
```

After this verification process, you can use the certificate Thumbprint in GroupID.

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 

.

Figure 20: 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:

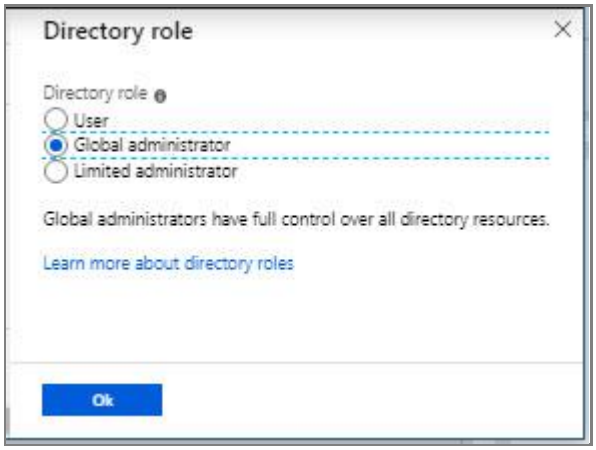
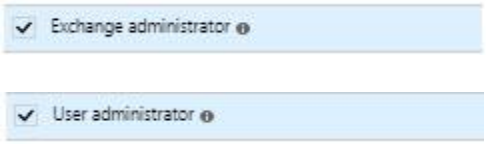


Figure 21: Directory Role pane

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

    Select the **Limited administrator** option in the **Directory role** pane (Figure 21):

    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 registerd 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.

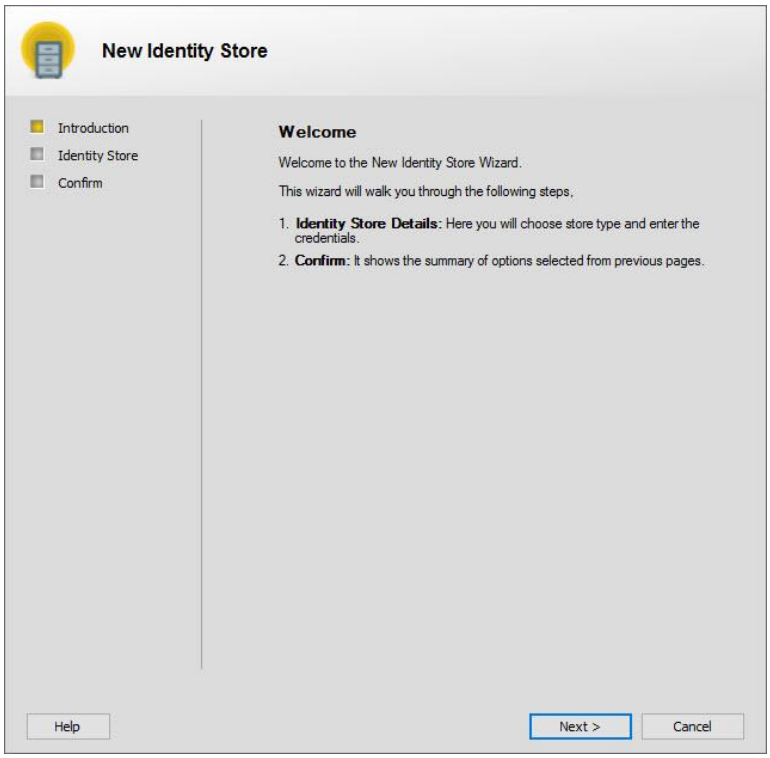


Figure 22: New Identity Store wizard – Welcome page

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

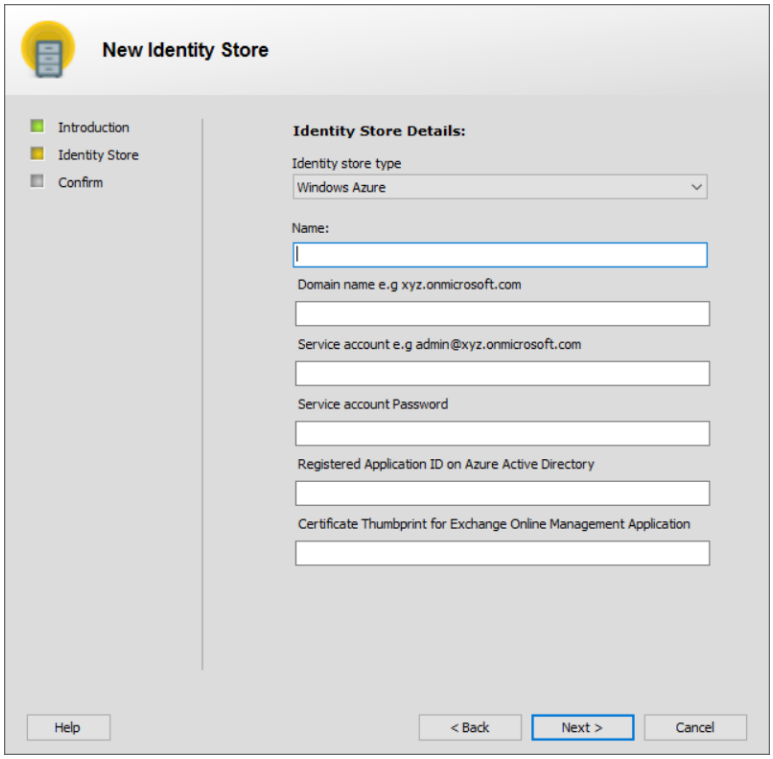


Figure 23: New Identity Store wizard – Identity Store page

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. In the **Certificate Thumbprint for Exchange Online Management Application** box, provide the value of Certificate Thumbprint assigned to the certificate you uploaded on the Azure portal (Figure 19).

h. Click **Next**.

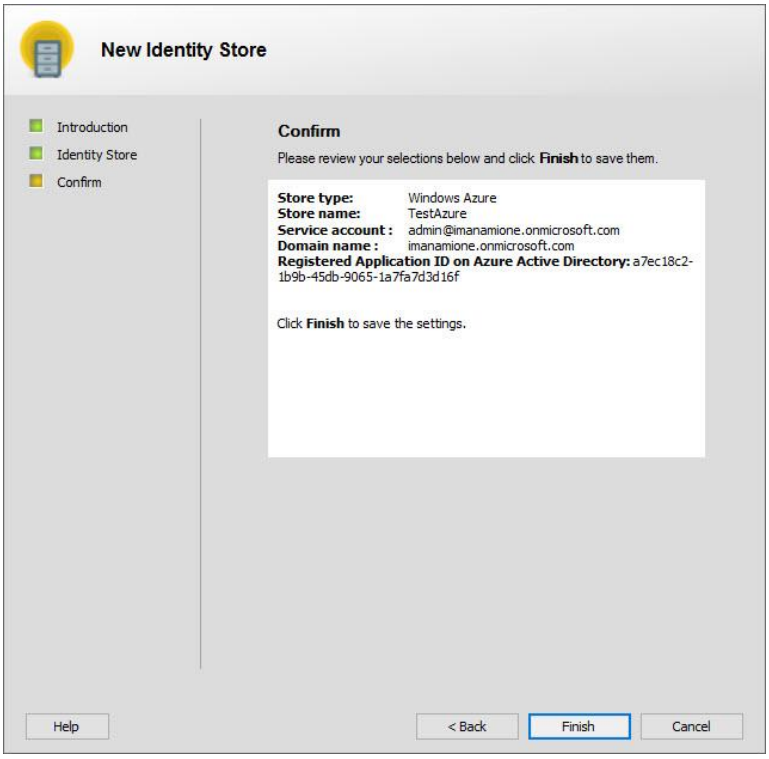


Figure 24: New Identity Store wizard – Confirm page

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**.

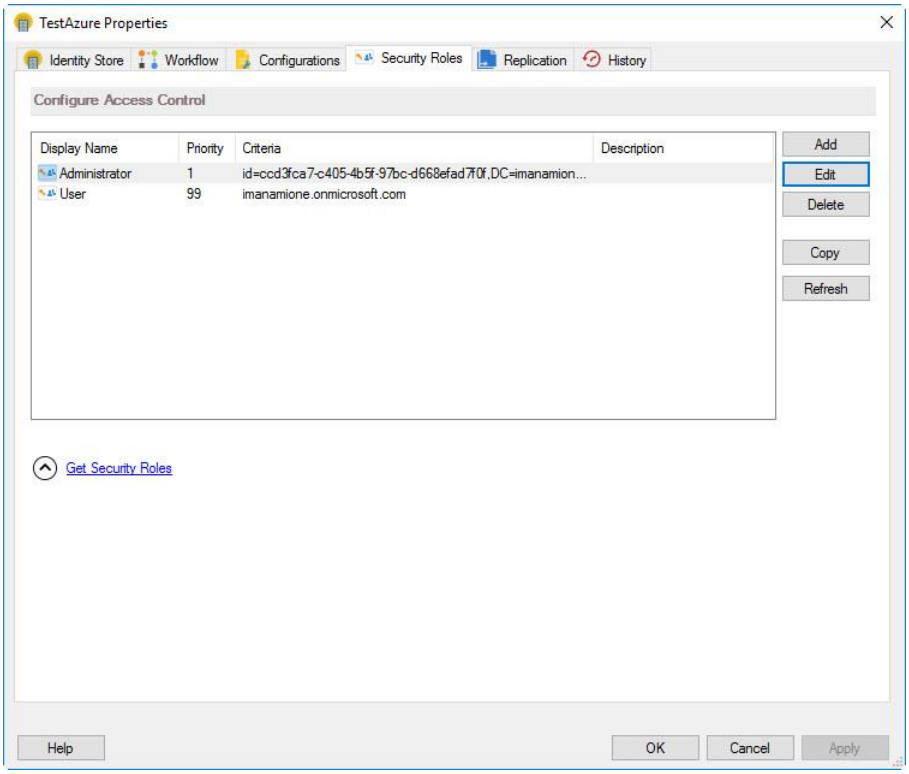


Figure 25: Identity Store Properties – Security Role tab

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

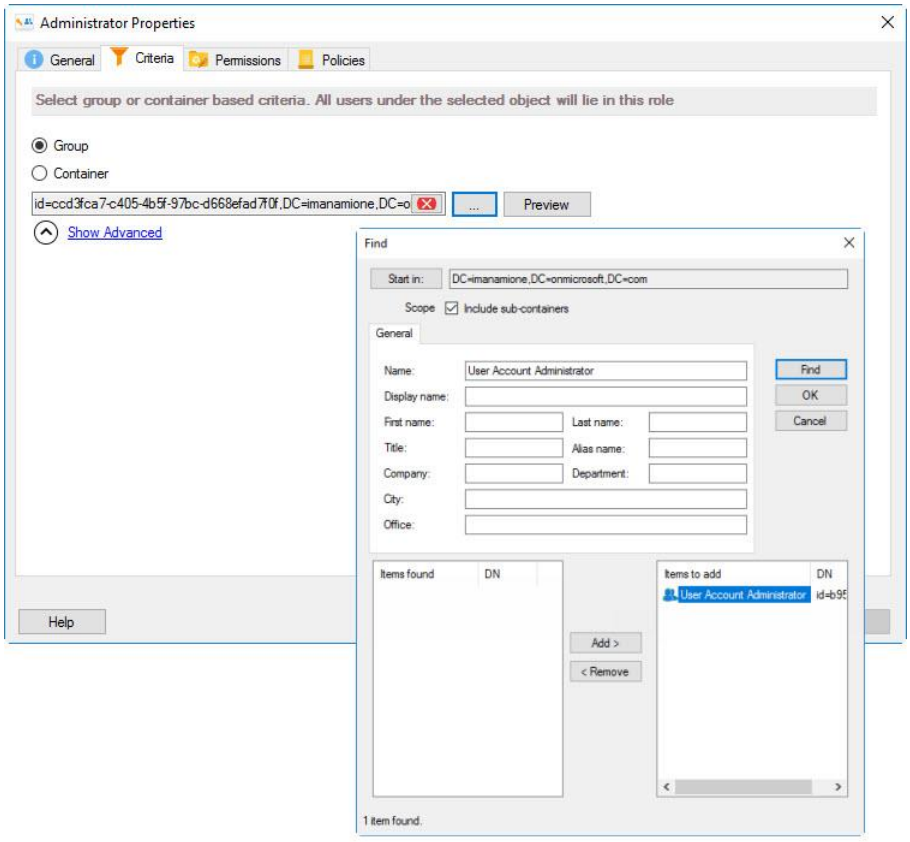


Figure 26: Identity Store Properties – Criteria tab

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 functionlity would be limited to objects falling in the *User* role, *User Administrator* role, and *Helpdesk* role.

Imanami | Now part of Netwrix

6160 Warren Parkway, Suite 100,
Frisco, TX 75034,
United States.
https://www.imanami.com/

Support: (925) 371-3000, Opt. 2
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