



A MITEL
PRODUCT
GUIDE

MiVoice Connect Integration with Microsoft Office 365 using modern Authentication

Application Registration with Azure AD for MS Office 365

Document Version 1.0

September 2022

Notices

The information contained in this document is believed to be accurate in all respects but is not warranted by **Mitel Networks™ Corporation (MITEL®)**. The information is subject to change without notice and should not be construed in any way as a commitment by Mitel or any of its affiliates or subsidiaries. Mitel and its affiliates and subsidiaries assume no responsibility for any errors or omissions in this document. Revisions of this document or new editions of it may be issued to incorporate such changes. No part of this document can be reproduced or transmitted in any form or by any means - electronic or mechanical - for any purpose without written permission from Mitel Networks Corporation.

Trademarks

The trademarks, service marks, logos and graphics (collectively "Trademarks") appearing on Mitel's Internet sites or in its publications are registered and unregistered trademarks of Mitel Networks Corporation (MNC) or its subsidiaries (collectively "Mitel") or others. Use of the Trademarks is prohibited without the express consent from Mitel. Please contact our legal department at legal@mitel.com for additional information. For a list of the worldwide Mitel Networks Corporation registered trademarks, please refer to the website: <http://www.mitel.com/trademarks>.

®,™ Trademark of Mitel Networks Corporation

© Copyright 2022, Mitel Networks Corporation

All rights reserved

Contents

1 Introduction.....	1
2 AZURE AD APPLICATION REGISTRATION.....	2

Microsoft is disabling the basic authentication method for MiVoice Connect starting October 2022 and thereafter will use only modern authentication methods. MiVoice Connect will use Oauth2 for integrating with Microsoft Office 365 services starting from Release 19.3 SP1. With Oauth2, there will be a separate Identity Platform (IdP) to authenticate the users of Microsoft services. The IdP used for Microsoft Office 365 integration will be Azure AD. To have Complete Modern Authentication Flow working in deployment, it requires Azure AD to trust Microsoft Office 365 service and also Azure to know Application which is using the Microsoft services. Application Registration with Azure AD addresses both these tasks and is explained in [Azure AD application registration](#) of this document.

As part of the Application Registration, Application ID, Redirect Uri, and Tenant ID will be generated by Azure AD. These field values must be noted.

 **Note:**

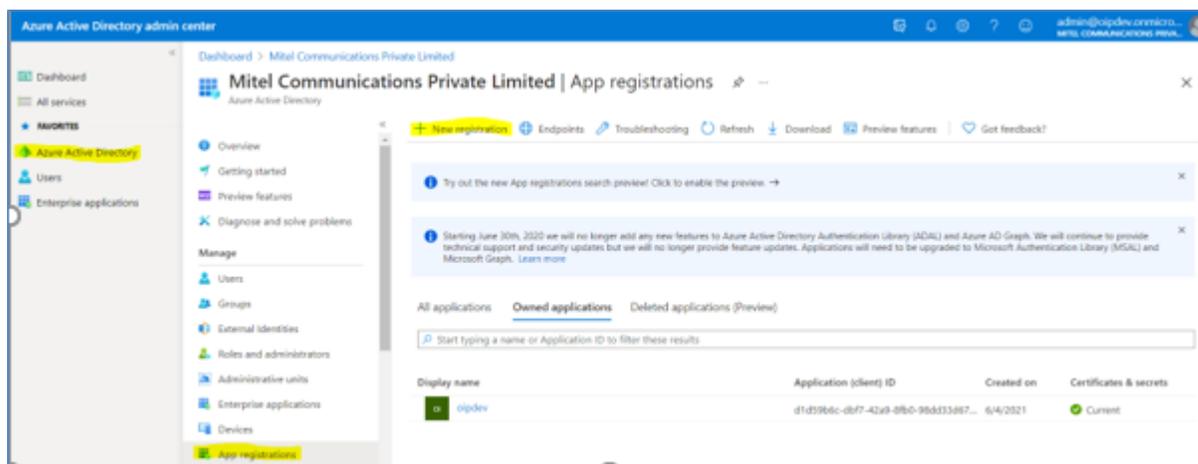
MiVoice Connect requires registering the application as public client in "*console application mode*". The steps explained in this document are only for registering the MiVC application in console application mode. It is assumed that the MiVoice Connect Administrator has Azure AD admin access to execute the steps explained in this document.

AZURE AD APPLICATION REGISTRATION

2

Following is the procedure for registering the MiVoice Connect Application with Azure AD.

1. Open a browser and navigate to the [Azure Active Directory admin center](#) and log in as an admin. In the page that opens, click **New Registration**.
2. Select **Azure Active Directory** in the left navigation pane, click **Manage > App registrations**.
3. Select **New registration**.



4. On the **Register an application** page, set the values as follows:

- a. Specify a **Name** for your app.
- b. In the **Supported account types** field, select **Accounts in this organizational directory only (Mitel Networks Corporation only - Single tenant)**.
- c. Under **Redirect URI (optional)**, do the following:
 - i. In the **Select a platform** field, select **Public client/native (mobile & desktop)** from the drop-down list.
 - ii. Enter the IP address or the FQDN of Server/ClientOAuth in the text box.

The screenshot shows the Azure AD portal interface for the 'ConnectClient1' application. The left-hand navigation pane is visible, with 'Authentication' selected. The main content area displays the 'Authentication' settings. The 'Redirect URIs' section is expanded, showing a list of URIs with checkboxes and delete icons. The 'Supported account types' section is also visible below.

Redirect URIs

The URIs we will accept as destinations when returning authentication responses (tokens) after successfully authenticating users. The redirect URI you send in the request to the login server should match one listed here. Also referred to as reply URLs. [Learn more about Redirect URIs and their restrictions](#)

- <https://login.microsoftonline.com/common/oauth2/nativeclient>
- [https://login.live.com/oauth20_desktop.srf \(LiveSDK\)](https://login.live.com/oauth20_desktop.srf)
- [msal4478d65c-ffd6-463f-8d37-63ab9ecb80f2://auth \(MSAL only\)](msal4478d65c-ffd6-463f-8d37-63ab9ecb80f2://auth)
- <https://10.211.126.218/clientoauth/>
- <https://raybaumhq.mivcblr.com/ClientOAuth>
- <https://10.211.44.167/ClientOAuth>
- <https://10.211.126.200/ClientOAuth/>

[Add URI](#)

Supported account types

Who can use this application or access this API?

Note:

The Microsoft Azure portal supports only **https** while using redirect URLs. The use of **http** is not permitted.

5. Click Register.

Azure Active Directory admin center

Dashboard > oauthnpm >

Register an application

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

npm

Supported account types

Who can use this application or access this API?

Accounts in this organizational directory only (oauthnpm 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.

Public client/native (mobile ...) https://login.microsoftonline.com/common/oauth2/nativeclient

By proceeding, you agree to the Microsoft Platform Policies

Register

6. From the next page, copy the values of the **Application (client) ID** and **Directory (tenant) ID** and save them, you will need them for Office365 OAuth authentication.

Home >

oipdev

Search

Delete Endpoints Preview features

Overview

Quickstart

Integration assistant

Manage

Branding & properties

Authentication

Certificates & secrets

Token configuration

API permissions

Expose an API

App roles

Owners

Roles and administrators

Essentials

Display name
oipdev

Application (client) ID
d65b4815-f19a-4f13-bc21-1bba8f75df61

Object ID
dd42879e-7c0d-44a2-bc68-9209a9678ca4

Directory (tenant) ID
9613561e-06f7-495c-8315-e6a2670c04cc

Supported account types
My organization only

Client credentials
0 certificate, 1 secret

Redirect URIs
0 web, 0 spa, 1 public client

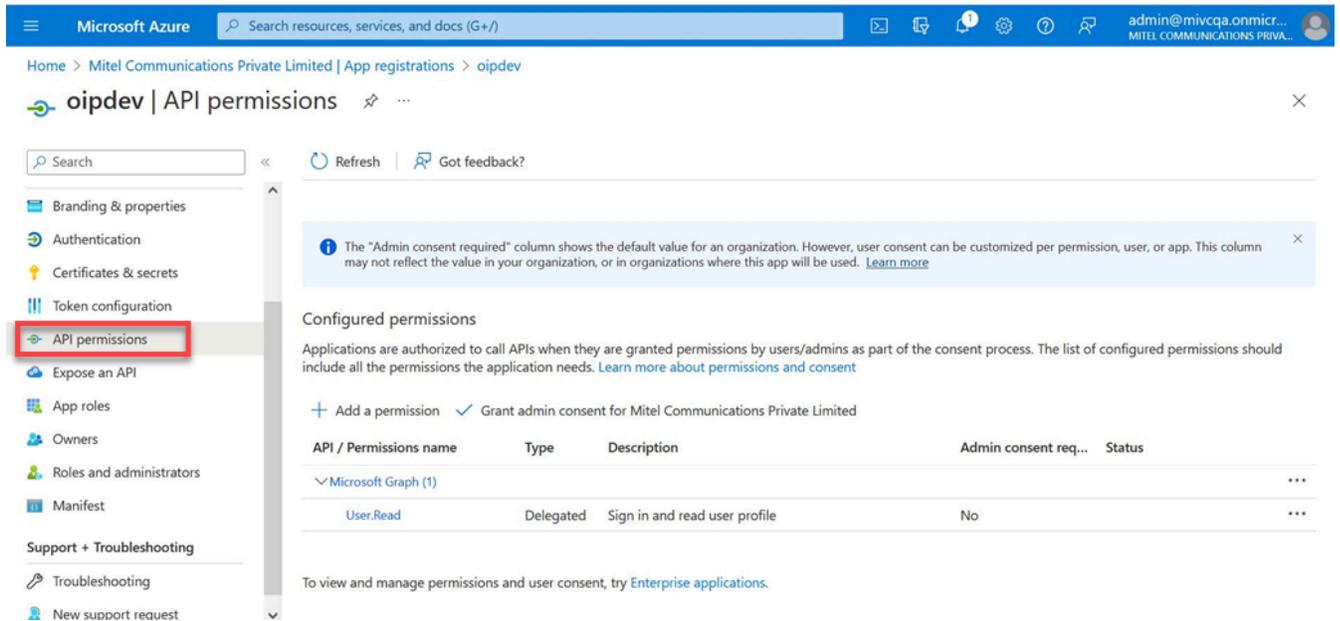
Application ID URI
Add an Application ID URI

Managed application in local directory
oipdev

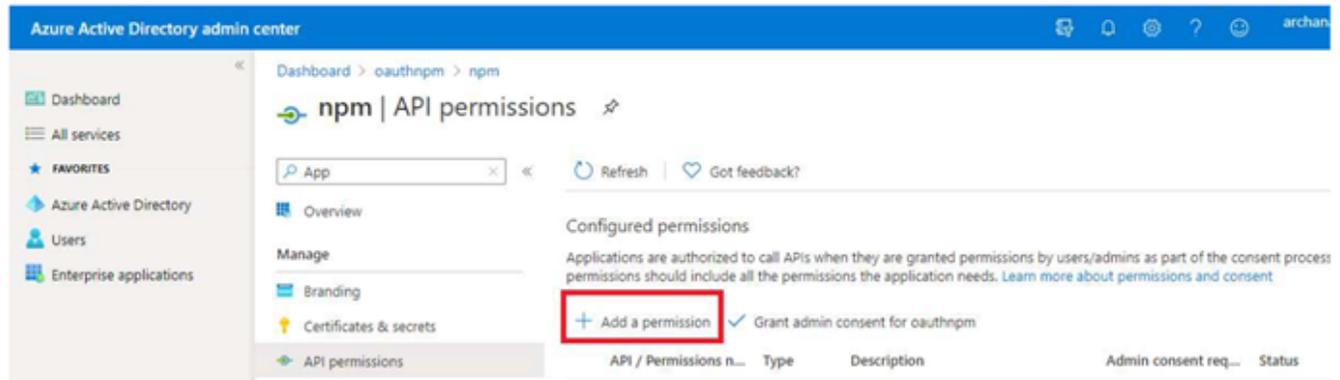
Starting June 30th, 2020 we will no longer add any new features to Azure Active Directory Authentication Library (ADAL) and Azure AD Graph. We will continue to provide technical support and security updates but we will no longer provide feature updates. Applications will need to be upgraded to Microsoft Authentication Library (MSAL) and Microsoft Graph. [Learn more](#)

Get Started Documentation

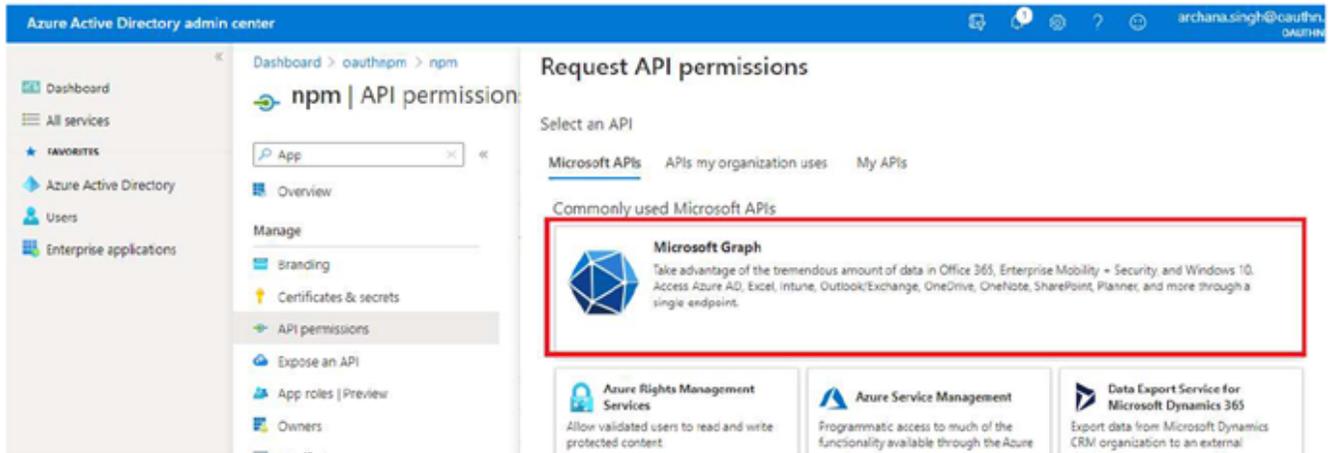
7. Go to Azure portal and click **API permissions**.



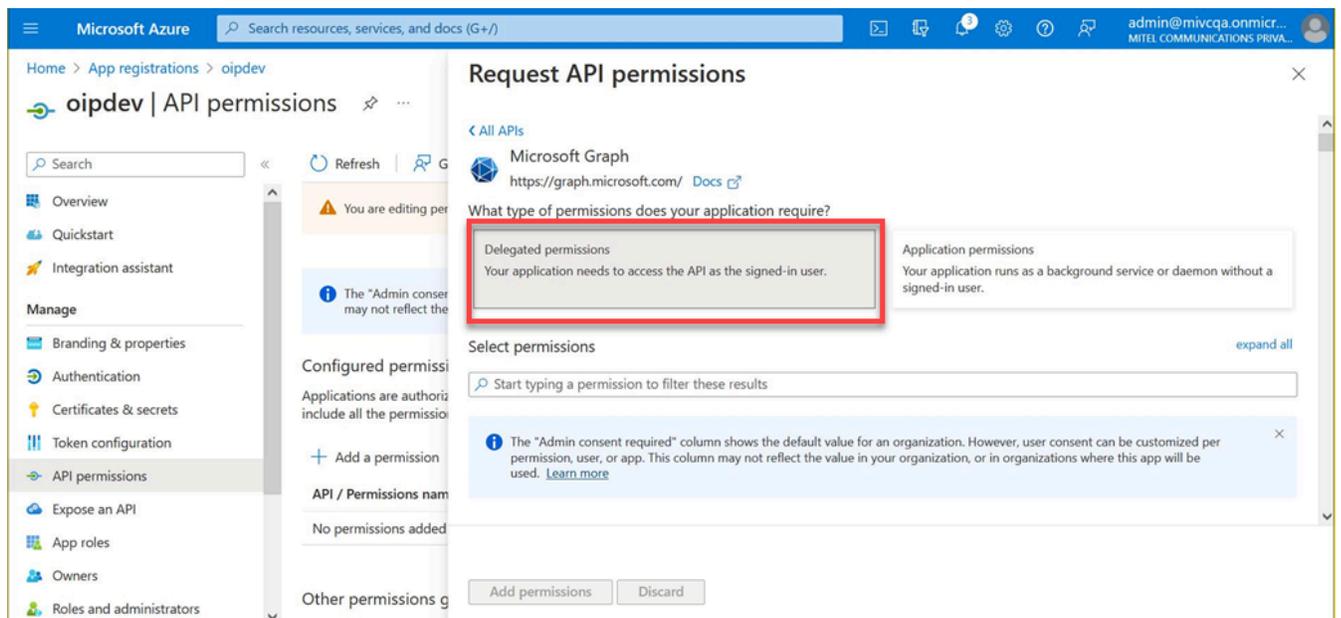
8. Click **Add a permission**. The **Request API permissions** page opens.



9. In the Request API permissions page, select **Microsoft Graph**.



10. Click **Delegated permissions**.



11. Under **Permission**, do the following:

a. Under **Calendars**, select the following options:

- **Calendars.Read**
- **Calendars.Read.Shared**
- **Calendars.ReadWrite**
- **Calendars.ReadWrite.Shared**

Request API permissions

Select permissions expand all

calendar

Permission	Admin consent required
<input checked="" type="checkbox"/> Calendars.Read ⓘ Read user calendars	No
<input checked="" type="checkbox"/> Calendars.Read.Shared ⓘ Read user and shared calendars	No
<input checked="" type="checkbox"/> Calendars.ReadWrite ⓘ Have full access to user calendars	No
<input checked="" type="checkbox"/> Calendars.ReadWrite.Shared ⓘ Read and write user and shared calendars	No

Add permissions **Discard**

b. Under **Contacts**, select the following options:

- **Contacts.Read**
- **Contacts.Read.Shared**
- **Contacts.ReadWrite**
- **Contacts.ReadWrite.Shared**

c. Under **OrgContact**, select the **OrgContact.Read.All** option.

Request API permissions



Permission	Admin consent required
✓ Contacts (4)	
<input checked="" type="checkbox"/> Contacts.Read ⓘ Read user contacts	No
<input checked="" type="checkbox"/> Contacts.Read.Shared ⓘ Read user and shared contacts	No
<input checked="" type="checkbox"/> Contacts.ReadWrite ⓘ Have full access to user contacts	No
<input checked="" type="checkbox"/> Contacts.ReadWrite.Shared ⓘ Read and write user and shared contacts	No
✓ OrgContact (1)	
<input checked="" type="checkbox"/> OrgContact.Read.All ⓘ Read organizational contacts	Yes

[Add permissions](#)[Discard](#)

d. Under **People**, select the following options:

- **People.Read**
- **People.Read.All**

Request API permissions ✕

What type of permissions does your application require?

Delegated permissions

Your application needs to access the API as the signed-in user.

Application permissions

Your application runs as a background service or daemon without a signed-in user.

Select permissions expand all

	Permission	Admin consent required
∨	People (2)	
<input checked="" type="checkbox"/>	People.Read ⓘ Read users' relevant people lists	No
<input checked="" type="checkbox"/>	People.Read.All ⓘ Read all users' relevant people lists	Yes

Add permissions
Discard

e. Under **EWS**, select the **EWS.AccessAsUser.All** option.

Request API permissions

Microsoft Graph
<https://graph.microsoft.com/> Docs

What type of permissions does your application require?

Delegated permissions

Your application needs to access the API as the signed-in user.

Application permissions

Your application runs as a background service or daemon without a signed-in user.

Select permissions expand all

Permission	Admin consent required
<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

Add permissions

Discard

12. Click **Add permissions** The **Configured permissions** page opens.

13. Click **Grant admin consent for oauthnrm**.

App

[Refresh](#) | [Got feedback?](#)

Overview

Manage

- Branding
- Certificates & secrets
- API permissions
- Expose an API
- App roles | Preview
- Owners
- Manifest

Configured permissions

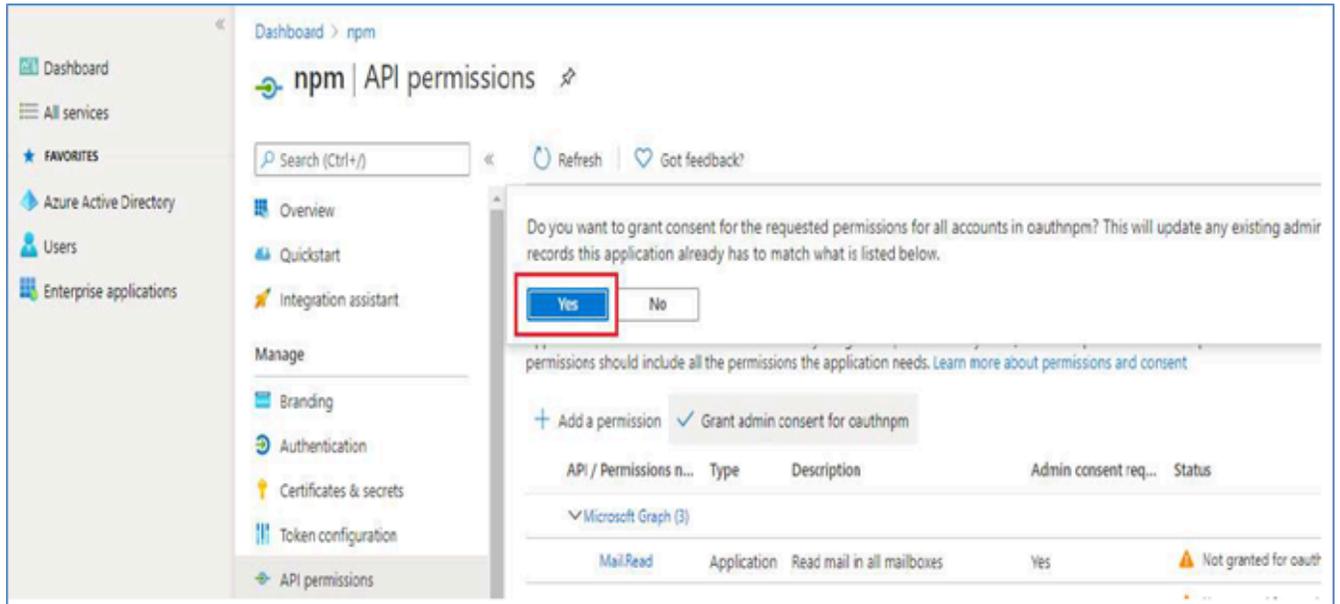
Applications are authorized to call APIs when they are granted permissions by users, permissions should include all the permissions the application needs. [Learn more at](#)

+ Add a permission

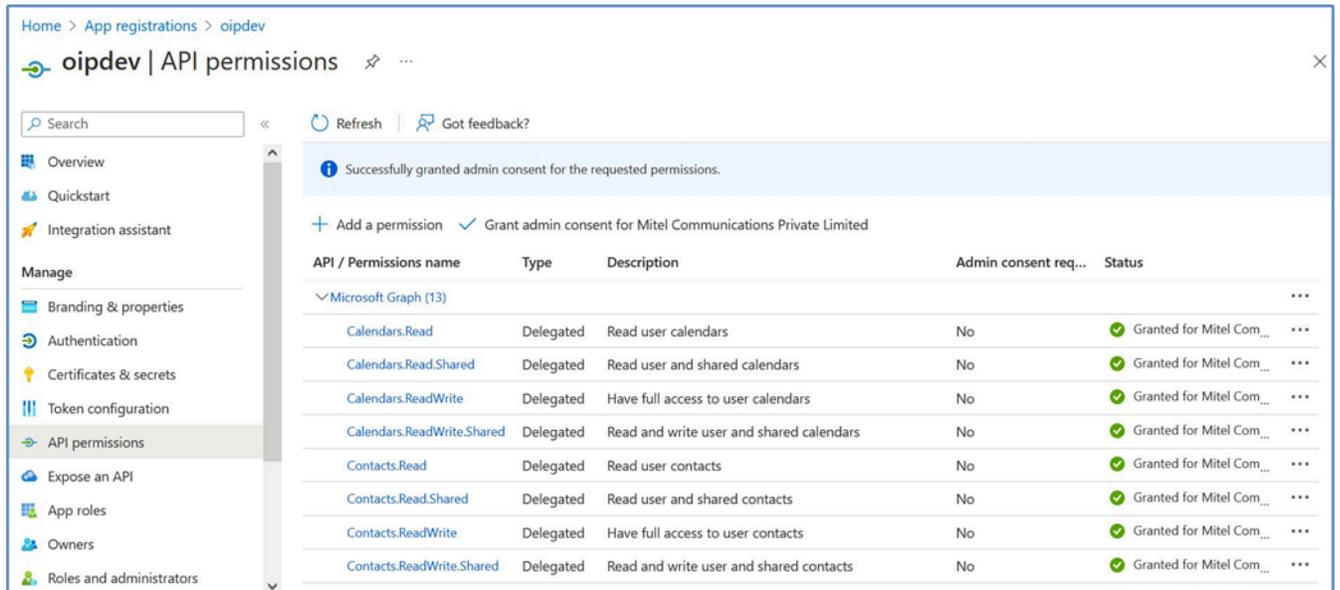
Grant admin consent for oauthnrm

API / Permissions n...	Type	Description
Microsoft Graph (3)		
Mail.Read	Application	Read mail in all mailboxes
Mail.ReadWrite	Application	Read and write mail in all mailboxes
Mail.Send	Application	Send mail as any user

14. Click **Yes** to complete the application registration for Office 365.



15. The following page appears after permission is granted for the selected configurations.



16. The values of the following fields will be required to be filled in the **Additional Parameters** page to configure D2 in MiVoice Connect:

- **Tenant-ID** (generated in Step-6)
- **Application-ID** (generated in Step-6)
- **Redirect-URI** (use the same Redirect URI that is used during the application configuration)

The screenshot displays the 'Additional Parameters' configuration page in the Mitel Connect Director interface. The left sidebar shows the navigation menu with 'Additional Parameters' selected. The main content area contains the following fields and settings:

- Max size: 20 MB (10-500)
- Service Appliance (Collaboration):
 - Exchange server:
 - Service appliance exchange server: outlook.office365.com
 - AppID: (highlighted with a red box)
 - Redirect URI: (highlighted with a red box)
 - Tenant ID: (highlighted with a red box)
- Log file storage:
 - Max days: 1 (1-30)
 - Max size: 20 MB (10-60000)
- Conferencing:
 - Global conferencing URL:
- Instant messaging:
 - Domain name: 10.211.48.31 (yourcompany.com)
 - Session timeout: 600 minutes (10-600)
 - Enable offline messaging
 - Enable TLS for IM
 - Client history retention period: 549 days (3-549)
- Client compatibility and upgrade:
 - Require secure client access (https)
 - Suppress client upgrade notifications
 - Minimum allowed client version: 214.100.3143.0 Example: 214.100.3143.0
 - Current version for the build: 214.100.3143.0 Example: 214.100.3143.0

This completes the registration of Azure AD with Microsoft Office 365.

